



Guía del usuario

# AWS IAM Identity Center



# AWS IAM Identity Center: Guía del usuario

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con ningún producto o servicio que no sea de Amazon, de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

# Table of Contents

|                                                                                                                                     |    |
|-------------------------------------------------------------------------------------------------------------------------------------|----|
| ¿Qué es IAM Identity Center? .....                                                                                                  | 1  |
| ¿Por qué utilizar el IAM Identity Center? .....                                                                                     | 1  |
| Cambio de nombre de IAM Identity Center .....                                                                                       | 3  |
| Los espacios de nombres antiguos siguen siendo los mismos .....                                                                     | 3  |
| Introducción .....                                                                                                                  | 4  |
| Requisitos previos y consideraciones sobre el IAM Identity Center .....                                                             | 5  |
| Elegir una Región de AWS .....                                                                                                      | 7  |
| Uso del IAM Identity Center únicamente para aplicaciones .....                                                                      | 13 |
| Funciones de IAM creadas por el Centro de Identidad de IAM .....                                                                    | 13 |
| Centro de identidad de IAM y AWS Organizations .....                                                                                | 14 |
| Instancias de IAM Identity Center .....                                                                                             | 15 |
| Cuenta de AWS Tipos de que pueden habilitar IAM Identity Center .....                                                               | 16 |
| Instancias de organización de IAM Identity Center .....                                                                             | 18 |
| Instancias de cuenta de IAM Identity Center .....                                                                                   | 19 |
| Eliminación de la instancia de IAM Identity Center .....                                                                            | 24 |
| Activar IAM Identity Center .....                                                                                                   | 27 |
| Para habilitar una instancia de IAM Identity Center .....                                                                           | 28 |
| Confirmación de orígenes de identidad .....                                                                                         | 30 |
| Actualice los firewalls y las puertas de enlace .....                                                                               | 32 |
| Consideraciones a la hora de permitir la inclusión de dominios y puntos de conexión de URL .....                                    | 33 |
| Tutoriales sobre orígenes de identidad .....                                                                                        | 35 |
| Active Directory .....                                                                                                              | 36 |
| CyberArk .....                                                                                                                      | 38 |
| Requisitos previos .....                                                                                                            | 39 |
| Consideraciones de SCIM .....                                                                                                       | 40 |
| Paso 1: habilite el aprovisionamiento en IAM Identity Center .....                                                                  | 40 |
| Paso 2: Configurar el aprovisionamiento en CyberArk .....                                                                           | 41 |
| (Opcional) Paso 3: configurar los atributos de usuario en CyberArk para el control de acceso (ABAC) en el IAM Identity Center ..... | 42 |
| (Opcional) Paso de atributos para el control de acceso .....                                                                        | 43 |
| Google Workspace .....                                                                                                              | 44 |
| Consideraciones .....                                                                                                               | 45 |
| Paso 1Google Workspace: Configurar la aplicación SAML .....                                                                         | 45 |

|                                                                                                                                                                                       |    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Paso 2: IAM Identity Center y Google Workspace: cambio del origen de identidad de IAM Identity Center y configuración de Google Workspace como proveedor de identidades de SAML ..... | 46 |
| Paso 3: Google Workspace: habilitación de las aplicaciones .....                                                                                                                      | 48 |
| Paso 4: IAM Identity Center: configuración del aprovisionamiento automático de IAM Identity Center .....                                                                              | 48 |
| Paso 5: Google Workspace: configuración del aprovisionamiento automático .....                                                                                                        | 49 |
| Paso de atributos para el control de acceso: opcional .....                                                                                                                           | 51 |
| Asigne acceso a Cuentas de AWS .....                                                                                                                                                  | 51 |
| Pasos a seguir a continuación .....                                                                                                                                                   | 54 |
| Solución de problemas .....                                                                                                                                                           | 54 |
| JumpCloud .....                                                                                                                                                                       | 55 |
| Requisitos previos .....                                                                                                                                                              | 56 |
| Consideraciones de SCIM .....                                                                                                                                                         | 56 |
| Paso 1: habilite el aprovisionamiento en IAM Identity Center .....                                                                                                                    | 57 |
| Paso 2: Configurar el aprovisionamiento en JumpCloud .....                                                                                                                            | 58 |
| (Opcional) Paso 3: configurar los atributos de usuario en JumpCloud para el control de acceso en IAM Identity Center .....                                                            | 59 |
| (Opcional) Paso de atributos para el control de acceso .....                                                                                                                          | 60 |
| Microsoft Entra ID .....                                                                                                                                                              | 60 |
| Requisitos previos .....                                                                                                                                                              | 61 |
| Consideraciones .....                                                                                                                                                                 | 61 |
| Paso 1: preparación de su inquilino de Microsoft .....                                                                                                                                | 63 |
| Paso 2: Prepara tu AWS cuenta .....                                                                                                                                                   | 65 |
| Paso 3: configuración y prueba de la conexión SAML .....                                                                                                                              | 68 |
| Paso 4: configuración y comprobación de la sincronización de SCIM .....                                                                                                               | 72 |
| Paso 5: Configurar ABAC: opcional .....                                                                                                                                               | 76 |
| Asigne acceso a Cuentas de AWS .....                                                                                                                                                  | 77 |
| Solución de problemas .....                                                                                                                                                           | 79 |
| Okta .....                                                                                                                                                                            | 82 |
| Consideraciones .....                                                                                                                                                                 | 83 |
| Paso 1: Okta: obtención de los metadatos de SAML de su cuenta de Okta .....                                                                                                           | 84 |
| Paso 2: IAM Identity Center: configuración de Okta como origen de identidad para IAM Identity Center .....                                                                            | 84 |
| Paso 3: IAM Identity Center and Okta: aprovisionar usuarios de Okta .....                                                                                                             | 86 |
| Paso 4: Okta: sincronización de los usuarios desde Okta con IAM Identity Center .....                                                                                                 | 87 |

|                                                                                                                              |     |
|------------------------------------------------------------------------------------------------------------------------------|-----|
| Paso de atributos para el control de acceso: opcional .....                                                                  | 89  |
| Asigne el acceso a Cuentas de AWS .....                                                                                      | 89  |
| Pasos a seguir a continuación .....                                                                                          | 92  |
| Solución de problemas .....                                                                                                  | 92  |
| OneLogin .....                                                                                                               | 94  |
| Requisitos previos .....                                                                                                     | 95  |
| Paso 1: habilite el aprovisionamiento en IAM Identity Center .....                                                           | 95  |
| Paso 2: Configurar el aprovisionamiento en OneLogin .....                                                                    | 96  |
| (Opcional) Paso 3: configurar los atributos de usuario en OneLogin para el control de<br>acceso en IAM Identity Center ..... | 98  |
| (Opcional) Paso de atributos para el control de acceso .....                                                                 | 99  |
| Solución de problemas .....                                                                                                  | 99  |
| Ping Identity .....                                                                                                          | 100 |
| PingFederate .....                                                                                                           | 100 |
| PingOne .....                                                                                                                | 108 |
| Directorio de Identity Center .....                                                                                          | 115 |
| Tutoriales de vídeo .....                                                                                                    | 121 |
| Autenticación mediante el IAM Identity Center .....                                                                          | 122 |
| Sesiones de autenticación .....                                                                                              | 122 |
| Revoca el acceso a los usuarios eliminados .....                                                                             | 127 |
| Conecte a los usuarios del personal .....                                                                                    | 129 |
| Usuarios, grupos y aprovisionamiento .....                                                                                   | 129 |
| Exclusividad del nombre de usuario y de la dirección de correo electrónico .....                                             | 129 |
| Grupos .....                                                                                                                 | 130 |
| Aprovisionamiento de usuarios y grupos .....                                                                                 | 130 |
| Desaprovisionamiento de usuarios y grupos .....                                                                              | 130 |
| Administración de su fuente de identidad .....                                                                               | 131 |
| Consideraciones para cambiar la fuente de identidad .....                                                                    | 132 |
| Cambiar su fuente de identidad .....                                                                                         | 136 |
| Administre el inicio de sesión y el uso de atributos para todos los tipos de fuentes de<br>identidad .....                   | 138 |
| Administración de identidades en IAM Identity Center .....                                                                   | 145 |
| Conexión un directorio Microsoft AD .....                                                                                    | 160 |
| Administrar un proveedor de identidades externo .....                                                                        | 181 |
| Uso del portal de AWS acceso .....                                                                                           | 197 |
| Activar el portal de AWS acceso .....                                                                                        | 198 |

|                                                                                                    |     |
|----------------------------------------------------------------------------------------------------|-----|
| Cómo iniciar sesión en el portal de AWS acceso de .....                                            | 198 |
| Restablecimiento de la contraseña .....                                                            | 202 |
| AWS CLI y acceso al AWS SDK .....                                                                  | 203 |
| Crear enlaces de acceso directo .....                                                              | 209 |
| Registro de un dispositivo para MFA .....                                                          | 211 |
| Personalización de la URL del portal de AWS acceso .....                                           | 213 |
| Autenticación multifactor .....                                                                    | 214 |
| Tipos de MFA disponibles .....                                                                     | 215 |
| Configuración de MFA .....                                                                         | 218 |
| Registrar un dispositivo MFA .....                                                                 | 225 |
| Cambiar el nombre y eliminar dispositivos MFA .....                                                | 227 |
| Acceso de aplicaciones .....                                                                       | 229 |
| AWS aplicaciones gestionadas .....                                                                 | 230 |
| Control del acceso a las aplicaciones .....                                                        | 230 |
| Compartición de información de identidad .....                                                     | 231 |
| Restringir el uso de aplicaciones gestionadas AWS .....                                            | 232 |
| Aplicaciones que puede utilizar con IAM Identity Center .....                                      | 233 |
| Configuración del Centro de Identidad de IAM para probar las aplicaciones gestionadas<br>AWS ..... | 237 |
| Visualización y modificación de los detalles de la aplicación .....                                | 244 |
| Deshabilitar una aplicación AWS gestionada .....                                                   | 245 |
| Habilitar sesiones de consola con identidad mejorada .....                                         | 245 |
| Aplicaciones administradas por el cliente .....                                                    | 249 |
| Aplicaciones SAML 2.0 y 2.0 OAuth .....                                                            | 250 |
| Configuración de aplicaciones de SAML 2.0 .....                                                    | 255 |
| Propagación de identidades de confianza .....                                                      | 259 |
| Ventajas de una propagación de identidad fiable .....                                              | 259 |
| Habilitar la propagación de identidades de forma fiable .....                                      | 259 |
| Cómo funciona la propagación de identidades confiable .....                                        | 260 |
| Requisitos y consideraciones previos .....                                                         | 261 |
| Casos de uso .....                                                                                 | 263 |
| Aplicaciones administradas por el cliente .....                                                    | 294 |
| Rotación de certificados .....                                                                     | 316 |
| Consideraciones antes de rotar un certificado .....                                                | 316 |
| Rotación de un certificado de IAM Identity Center .....                                            | 317 |
| Indicadores de estado de caducidad de certificados .....                                           | 319 |

|                                                                                                              |     |
|--------------------------------------------------------------------------------------------------------------|-----|
| Entender las propiedades de la aplicación .....                                                              | 320 |
| URL de inicio de la aplicación .....                                                                         | 320 |
| Estado de retransmisión .....                                                                                | 321 |
| Duración de la sesión .....                                                                                  | 322 |
| Asigne el acceso de los usuarios a las aplicaciones .....                                                    | 322 |
| Eliminar el acceso de los usuarios a aplicaciones .....                                                      | 323 |
| Asignación de atributos .....                                                                                | 324 |
| Cuenta de AWS acceso .....                                                                                   | 325 |
| Cuenta de AWS tipos .....                                                                                    | 325 |
| Asignación Cuenta de AWS de acceso .....                                                                     | 328 |
| La experiencia del usuario final .....                                                                       | 328 |
| Aplicación y limitación del acceso .....                                                                     | 329 |
| Delegación y aplicación del acceso .....                                                                     | 329 |
| Límite de acceso al almacén de identidades desde las cuentas de los miembros .....                           | 330 |
| Administración delegada .....                                                                                | 331 |
| Prácticas recomendadas .....                                                                                 | 331 |
| Requisitos previos .....                                                                                     | 332 |
| Registro de una cuenta miembro .....                                                                         | 332 |
| Anulación del registro de una cuenta miembro .....                                                           | 334 |
| Consulte las cuentas de administrador delegado .....                                                         | 335 |
| Acceso elevado temporal .....                                                                                | 335 |
| Socios AWS de seguridad validados para un acceso elevado temporal .....                                      | 336 |
| Se evaluaron las capacidades de acceso elevado temporal para su validación por parte de los socios AWS ..... | 337 |
| Acceso mediante inicio de sesión único a Cuentas de AWS .....                                                | 338 |
| Asigne el acceso de usuario o grupo a Cuentas de AWS .....                                                   | 339 |
| Eliminación del acceso de usuarios y grupos a una Cuenta de AWS .....                                        | 342 |
| Revocar una sesión de conjunto de permisos activa .....                                                      | 342 |
| Delegue quién puede asignar el acceso de inicio de sesión único .....                                        | 344 |
| Conjuntos de permisos .....                                                                                  | 346 |
| Creación de un conjunto de permisos que aplique los permisos de privilegio mínimo .....                      | 347 |
| Permisos predefinidos .....                                                                                  | 349 |
| Permisos personalizados .....                                                                                | 350 |
| Creación, administración y eliminación de conjuntos de permisos .....                                        | 353 |
| Configure las propiedades del conjunto de permisos .....                                                     | 367 |
| Referencias de conjuntos de permisos .....                                                                   | 374 |

|                                                                                  |     |
|----------------------------------------------------------------------------------|-----|
| Recomendaciones para evitar interrupciones en el acceso .....                    | 376 |
| Ejemplo de políticas de confianza personalizadas .....                           | 377 |
| Control de acceso basado en atributos .....                                      | 378 |
| Ventajas .....                                                                   | 379 |
| Lista de comprobación: configurar ABAC mediante el IAM Identity Center AWS ..... | 380 |
| Atributos para controlar el acceso .....                                         | 382 |
| Reparar el proveedor de identidad de IAM .....                                   | 390 |
| Roles vinculados a servicios .....                                               | 390 |
| Diseño de resiliencia y comportamiento regional .....                            | 392 |
| Diseñado para la disponibilidad .....                                            | 393 |
| Configure el acceso de emergencia al AWS Management Console .....                | 393 |
| Resumen de la configuración del acceso de emergencia .....                       | 394 |
| Cómo diseñar sus roles de operaciones críticas .....                             | 395 |
| Cómo planificar su modelo de acceso .....                                        | 396 |
| Cómo diseñar una asignación de roles, cuentas y grupos de emergencia .....       | 397 |
| Cómo crear la configuración de acceso de emergencia .....                        | 398 |
| Tareas de preparación de emergencias .....                                       | 399 |
| Proceso de conmutación por error de emergencia .....                             | 399 |
| Volver a las operaciones normales .....                                          | 400 |
| Configuración única de una aplicación de federación de IAM directa en Okta ..... | 400 |
| Seguridad .....                                                                  | 404 |
| Administración de identidades y accesos para IAM Identity Center .....           | 405 |
| Autenticación .....                                                              | 405 |
| Control de acceso .....                                                          | 405 |
| Información general sobre la administración del acceso .....                     | 406 |
| Políticas basadas en identidades (políticas de IAM) .....                        | 410 |
| AWS políticas gestionadas .....                                                  | 418 |
| Cómo utilizar roles vinculados a servicios .....                                 | 440 |
| Consola de IAM Identity Center y autorización de la API .....                    | 448 |
| Acciones de la API después de noviembre de 2023 .....                            | 449 |
| Acciones de la API después de octubre de 2020 .....                              | 450 |
| AWS STS claves de condición para el Centro de Identidad de IAM .....             | 452 |
| UserId .....                                                                     | 453 |
| IdentityStoreArn .....                                                           | 453 |
| ApplicationArn .....                                                             | 454 |
| CredentialId .....                                                               | 454 |



|                                                                                                                                               |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------|-----|
| InstanceArn .....                                                                                                                             | 454 |
| Registro y supervisión .....                                                                                                                  | 455 |
| Registrar las llamadas a la API de IAM Identity Center con AWS CloudTrail .....                                                               | 455 |
| Registro del IAM Identity Center SCIM con AWS CloudTrail .....                                                                                | 496 |
| Amazon EventBridge .....                                                                                                                      | 503 |
| Registrar errores de sincronización de AD configurables .....                                                                                 | 503 |
| Validación de conformidad .....                                                                                                               | 506 |
| Estándares de conformidad admitidos .....                                                                                                     | 507 |
| Resiliencia .....                                                                                                                             | 509 |
| Seguridad de la infraestructura .....                                                                                                         | 510 |
| Etiquetado de recursos .....                                                                                                                  | 511 |
| Restricciones de las etiquetas .....                                                                                                          | 512 |
| Administre las etiquetas con la consola .....                                                                                                 | 512 |
| AWS CLI ejemplos .....                                                                                                                        | 513 |
| Asignación de etiquetas .....                                                                                                                 | 513 |
| Visualización de etiquetas .....                                                                                                              | 514 |
| Eliminación de etiquetas .....                                                                                                                | 514 |
| Cómo aplicar etiquetas al crear un conjunto de permisos .....                                                                                 | 515 |
| acciones de API .....                                                                                                                         | 515 |
| Integración de AWS CLI con IAM Identity Center .....                                                                                          | 516 |
| Cómo integrar AWS CLI con IAM Identity Center .....                                                                                           | 516 |
| Consideraciones sobre acceso privado .....                                                                                                    | 517 |
| Cuotas .....                                                                                                                                  | 518 |
| Cuotas de aplicaciones .....                                                                                                                  | 518 |
| Cuenta de AWS cuotas .....                                                                                                                    | 519 |
| Cuotas de Active Directory .....                                                                                                              | 520 |
| Cuotas de almacén de identidades de IAM Identity Center .....                                                                                 | 520 |
| Límites de solicitudes de IAM Identity Center .....                                                                                           | 521 |
| Cuotas adicionales .....                                                                                                                      | 521 |
| Solución de problemas .....                                                                                                                   | 523 |
| Problemas al crear una instancia de cuenta de IAM Identity Center .....                                                                       | 523 |
| Recibe un error al intentar ver la lista de aplicaciones en la nube que están preconfiguradas<br>para funcionar con IAM Identity Center ..... | 523 |
| Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM<br>Identity Center .....                                | 525 |

|                                                                                                                                                |        |
|------------------------------------------------------------------------------------------------------------------------------------------------|--------|
| Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo .....                                      | 525    |
| Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo .....                               | 527    |
| Los usuarios no pueden iniciar sesión cuando su nombre de usuario está en formato UPN .....                                                    | 528    |
| Al modificar un rol de IAM, aparece el error: “No se puede realizar la operación en el rol protegido”. .....                                   | 529    |
| Los usuarios del directorio no pueden restablecer su contraseña .....                                                                          | 529    |
| En un conjunto de permisos se hace referencia a mi usuario, pero no puede acceder a las cuentas o aplicaciones asignadas .....                 | 530    |
| No puedo configurar correctamente mi aplicación del catálogo de aplicaciones .....                                                             | 530    |
| Error: “Se ha producido un error inesperado” cuando un usuario intenta iniciar sesión con un proveedor de identidad externo .....              | 531    |
| Error: “No se pudieron habilitar los atributos del control de acceso” .....                                                                    | 532    |
| El mensaje “El navegador no es compatible” aparece cuando intento registrar un dispositivo para MFA .....                                      | 532    |
| El grupo “Usuarios de dominio” de Active Directory no se sincroniza correctamente con IAM Identity Center .....                                | 532    |
| Error de credenciales de MFA no válidas .....                                                                                                  | 533    |
| El mensaje “Se ha producido un error inesperado” aparece cuando intento registrarme o iniciar sesión con una aplicación de autenticación ..... | 533    |
| Aparece el mensaje de error “No es usted, somos nosotros” cuando intento iniciar sesión en el IAM Identity Center .....                        | 533    |
| Mis usuarios no reciben correos electrónicos de IAM Identity Center .....                                                                      | 534    |
| Error: no puedes delete/modify/remove/assign acceder a los conjuntos de permisos aprovisionados en la cuenta de administración .....           | 534    |
| Error: no se encontró el token de sesión o no es válido .....                                                                                  | 534    |
| Historial de documentos .....                                                                                                                  | 536    |
| AWS Glosario .....                                                                                                                             | 546    |
| .....                                                                                                                                          | dxlvii |

# ¿Qué es IAM Identity Center?

AWS IAM Identity Center es la AWS solución para conectar a los usuarios de su fuerza laboral con aplicaciones AWS gestionadas, como Amazon Q Developer y Amazon QuickSight, y otros AWS recursos. Puede conectar su proveedor de identidad actual y sincronizar los usuarios y grupos de su directorio, o bien crear y gestionar sus usuarios directamente en el IAM Identity Center. A continuación, puede utilizar el IAM Identity Center para una de las siguientes opciones o para ambas:

- Acceso de los usuarios a las aplicaciones
- Acceso de los usuarios a Cuentas de AWS

## ¿Ya utilizas IAM para acceder a? Cuentas de AWS

No necesita realizar ningún cambio en sus Cuenta de AWS flujos de trabajo actuales para utilizar el IAM Identity Center y acceder a las aplicaciones AWS gestionadas. Si utiliza la [federación con IAM](#) o usuarios de IAM para el Cuenta de AWS acceso, sus usuarios pueden seguir Cuentas de AWS accediendo de la misma manera que siempre lo han hecho y usted puede seguir utilizando sus flujos de trabajo actuales para gestionar ese acceso.

## ¿Por qué utilizar el IAM Identity Center?

IAM Identity Center optimiza y simplifica el acceso de los usuarios del personal a las aplicaciones Cuentas de AWS, o a ambas, mediante las siguientes funciones clave.

### Integración con aplicaciones gestionadas AWS

[AWS aplicaciones administradas](#) como Amazon Q Developer e Amazon Redshift integradas con IAM Identity Center. El IAM Identity Center proporciona a las aplicaciones AWS gestionadas una visión común de los usuarios y los grupos.

### Propagación de identidad de confianza en aplicaciones

Gracias a la propagación de identidades fiable, las aplicaciones AWS gestionadas, como Amazon, QuickSight pueden compartir de forma segura la identidad de un usuario con otras aplicaciones AWS gestionadas, por ejemplo, Amazon Redshift y autorizar el acceso a AWS los recursos en función de la identidad del usuario. Puede auditar más fácilmente la actividad de los usuarios porque CloudTrail los eventos se registran en función del usuario y de las acciones

que este haya iniciado. De ese modo, resulta más sencillo entender quién ha accedido a qué. Para obtener información sobre los casos de uso compatibles, incluida end-to-end la guía de configuración, consulte [Casos de uso de propagación de identidades de confianza](#).

## Un lugar para asignar permisos a varias Cuentas de AWS

Con los permisos de varias cuentas, el IAM Identity Center ofrece un único lugar para asignar permisos a grupos de usuarios de varias Cuentas de AWS. Puede crear permisos basados en funciones laborales habituales o definir permisos personalizados que se adapten a sus necesidades de seguridad. A continuación, puede asignar esos permisos a los usuarios de la fuerza laboral para controlar su acceso a determinados recursos Cuentas de AWS.

Esta característica opcional solo está disponible para las [instancias de organización](#) de IAM Identity Center.

## Un punto de federación para simplificar el acceso de los usuarios a AWS

Al proporcionar un punto de federación, IAM Identity Center reduce el esfuerzo administrativo necesario para utilizar varias aplicaciones AWS gestionadas y Cuentas de AWS. Con IAM Identity Center, solo se federa una vez y solo se tiene que gestionar un certificado cuando se utiliza un proveedor de identidades de [SAML 2.0](#). El IAM Identity Center proporciona a las aplicaciones AWS gestionadas una visión común de los usuarios y grupos para casos prácticos de propagación de identidades fiables o cuando los usuarios comparten el acceso a los AWS recursos con otras personas.

Para obtener información acerca de cómo configurar los proveedores de identidad de uso habitual para que funcionen con el IAM Identity Center, consulte [Tutoriales de fuentes de identidad de IAM Identity Center](#). Si no tiene un proveedor de identidad existente, puede [crear y gestionar usuarios directamente en el IAM Identity Center](#).

## Dos modos de implementación

IAM Identity Center admite dos tipos de instancias: las instancias de organización y las instancias de cuenta. La práctica recomendada es usar una instancia de organización. Es la única instancia que permite gestionar el acceso a las aplicaciones Cuentas de AWS y se recomienda para todo uso de producción de las mismas. Se implementa una instancia de organización en la cuenta AWS Organizations de administración y proporciona un punto único desde el que administrar el acceso de los usuarios AWS.

Las instancias de cuenta están vinculadas al lugar Cuenta de AWS en el que están habilitadas. Utilice las instancias de cuenta del IAM Identity Center únicamente para admitir despliegues

aislados de determinadas aplicaciones AWS gestionadas. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

Portal web de fácil acceso para sus usuarios

El portal de AWS acceso es un portal web fácil de usar que proporciona a sus usuarios un acceso sin problemas a todas las aplicaciones asignadas Cuentas de AWS, o a ambas.

## Cambio de nombre de IAM Identity Center

El 26 de julio de 2022, AWS Single Sign-On pasó a llamarse. AWS IAM Identity Center

### Los espacios de nombres antiguos siguen siendo los mismos

Los espacios de nombres de sso y identitystore API, junto con los siguientes espacios de nombres relacionados, permanecen sin cambios por motivos de compatibilidad con versiones anteriores.

- Comandos de la CLI
  - [aws configure sso](#)
  - [identitystore](#)
  - [sso](#)
  - [sso-admin](#)
  - [sso-oidc](#)
- [Políticas administradas](#) que contienen prefijos de AWSSSO y AWSIdentitySync
- [Puntos de conexión de servicio](#) que contienen sso e identitystore
- Recursos de [AWS CloudFormation](#) contienen prefijos de AWS::SSO
- [Rol vinculado al servicio](#) que contiene AWSServiceRoleForSSO
- Consola URLs que contiene y sso singlessignon
- Documentación URLs que contiene singlessignon

# Getting started with IAM Identity Center

A continuación se describe cómo comenzar a utilizar IAM Identity Center.

## 1. Activar IAM Identity Center

Al [activar el Centro de Identidad de IAM](#), puede elegir entre dos tipos de instancias del Centro de Identidad de IAM. Estos tipos son: [instancias de organización](#) (recomendadas) e instancias de [cuentas](#). Para obtener más información sobre las distintas funciones de estos tipos de instancias, consulte las [instancias de organización y cuenta de IAM Identity Center](#).

### Note

Una vez activado el Centro de Identidad de IAM, puede iniciar sesión y abrir la [consola del Centro de Identidad de IAM](#) mediante una de las siguientes acciones:

- Instancia de la organización: inicie sesión para AWS usar credenciales con permisos administrativos en la cuenta de administración.
- Instancia de cuenta: inicie sesión con AWS credenciales con permisos administrativos en la ubicación en la Cuenta de AWS que el Centro de Identidad de IAM esté activado.

## 2. Conecte su fuente de identidad a IAM Identity Center

En la consola de IAM Identity Center, confirme la fuente de identidades que desee utilizar. Consulte lo siguiente para ver las fuentes de identidad:

- Proveedor de identidad externo: si ya tiene un proveedor de identidad para administrar los usuarios de su fuerza laboral, puede conectarlo al Centro de identidades de IAM. Para obtener más información sobre cómo configurar los proveedores de identidad de uso habitual para que funcionen con IAM Identity Center, consulte [Tutoriales de fuentes de identidad de IAM Identity Center](#).
- Active Directory: si utiliza Active Directory para gestionar los usuarios de su plantilla, puede conectarlo al IAM Identity Center. Para obtener más información, consulte [Uso de Active Directory como origen de identidad](#).
- Centro de identidad de IAM: también puede [crear y administrar usuarios y grupos directamente en el Centro de identidad de IAM](#).

## 3. Configure el acceso de los usuarios a Cuentas de AWS (solo en la instancia de la organización)

Si utiliza una instancia de organización del Centro de identidades de IAM, puede [asignar el acceso de un usuario o grupo a Cuentas de AWS](#), utilizando [conjuntos de permisos](#) para conceder a sus usuarios el acceso a los recursos Cuentas de AWS y a los recursos.

#### 4. Configure el acceso de los usuarios a las aplicaciones

Con IAM Identity Center, puede conceder a los usuarios acceso a dos tipos de aplicaciones:

##### a. [AWS aplicaciones gestionadas](#)

- Puede utilizar IAM Identity Center con aplicaciones AWS gestionadas como Amazon Q Business y Amazon Redshift. AWS CLI Para obtener más información, consulte [AWS aplicaciones gestionadas](#) y [Integración de AWS CLI con IAM Identity Center](#).

##### b. [Aplicaciones administradas por el cliente](#)

- Puede integrar cualquiera de los siguientes tipos de aplicaciones administradas por el cliente con el IAM Identity Center:
  - [Aplicaciones incluidas en el catálogo del IAM Identity Center](#)
  - [Sus aplicaciones personalizadas](#)
- Tras configurar la aplicación, puede [asignar a sus usuarios el acceso a la aplicación](#).

#### 5. Proporcione a sus usuarios las instrucciones de inicio de sesión para el portal de AWS acceso

El portal de AWS acceso es un portal web que proporciona a los usuarios acceso estable a todas sus aplicaciones asignadas Cuentas de AWS, a o ambas. Los nuevos usuarios de IAM Identity Center deben activar sus credenciales de usuario antes de poder iniciar sesión en el portal de AWS acceso.

Para obtener información sobre cómo iniciar sesión en el portal de AWS acceso, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario. Para obtener más información sobre el proceso de inicio de sesión en el portal de AWS acceso, consulte [Iniciar sesión en el portal de AWS acceso](#).

## Requisitos previos y consideraciones sobre el IAM Identity Center

Puede utilizar IAM Identity Center para acceder únicamente a las aplicaciones AWS gestionadas, Cuentas de AWS únicamente o a ambas. Si utiliza la federación de IAM para gestionar el acceso Cuentas de AWS, puede seguir haciéndolo mientras utiliza el IAM Identity Center para acceder a las aplicaciones.

Antes de habilitar el Centro de identidades de IAM, tenga en cuenta lo siguiente:

- AWS Región

Puede habilitar el Centro de Identidad de IAM en una sola región [compatible](#) para cada instancia del Centro de Identidad de IAM. Si desea utilizar el Centro de identidades de IAM para acceder a AWS las cuentas mediante un único inicio de sesión, todos los usuarios de su organización deben poder acceder a la región. Si piensa utilizar el Centro de identidad de IAM para acceder a las aplicaciones, tenga en cuenta que algunas aplicaciones AWS gestionadas, como Amazon SageMaker AI, solo pueden funcionar en las regiones que admiten. Asegúrese de activar el Centro de Identidad de IAM en una región compatible con las aplicaciones AWS gestionadas que desee utilizar con él. Además, muchas aplicaciones AWS gestionadas solo pueden funcionar en la misma región en la que habilitó el Centro de identidad de IAM. Por estos motivos, asegúrese de elegir la región adecuada al activar el Centro de identidades de IAM. Para obtener más información, consulte [Consideraciones a la hora de elegir una Región de AWS](#).

- Solo acceso a las aplicaciones

Puede usar el Centro de identidad de IAM solo para el acceso de los usuarios a aplicaciones como Amazon Q Developer, utilizando su proveedor de identidad actual. Para obtener más información, consulte [Uso del IAM Identity Center únicamente para el acceso de los usuarios a las aplicaciones](#).

 Note

El propietario de la aplicación gestiona de forma independiente el acceso a los recursos de la aplicación.

- Cuota de funciones de IAM

El Centro de Identidad de IAM crea funciones de IAM para conceder a los usuarios permisos para acceder a los recursos de la cuenta. Para obtener más información, consulte [Funciones de IAM creadas por el Centro de Identidad de IAM](#).

- El Centro de Identidad de IAM y AWS Organizations

AWS Organizations se recomienda, pero no es obligatorio, para su uso con el Centro de identidades de IAM. Si no ha creado una organización, no tiene que hacerlo. Si ya ha configurado el Centro de Identidad de IAM AWS Organizations y lo va a añadir a su organización, asegúrese de que todas las AWS Organizations funciones estén habilitadas. Para obtener más información, consulte [Centro de identidad de IAM y AWS Organizations](#).



## Consideraciones a la hora de elegir una Región de AWS

Puede activar el Centro de Identidad de IAM de una sola vez, con el soporte Región de AWS que prefiera y que esté disponible para los usuarios de todo el mundo. Esta disponibilidad global le facilita la configuración del acceso de los usuarios a múltiples Cuentas de AWS aplicaciones. A continuación se presentan las principales consideraciones a la hora de elegir un Región de AWS.

- Ubicación geográfica de sus usuarios: si selecciona una región que esté geográficamente más cercana a la mayoría de sus usuarios finales, estos tendrán una latencia de acceso más baja al portal de AWS acceso y a las aplicaciones AWS gestionadas, como Amazon SageMaker AI.
- Disponibilidad de las aplicaciones AWS administradas: las aplicaciones administradas solo pueden funcionar en el Regiones de AWS lugar en el que están disponibles. Habilite el Centro de Identidad de IAM en una región compatible con las aplicaciones AWS administradas que desee utilizar con él. Muchas aplicaciones administradas de AWS también pueden funcionar solo en la misma región en la que habilitó el IAM Identity Center.
- Soberanía digital: las normas de soberanía digital o las políticas de la empresa pueden exigir el uso de una determinada Región de AWS. Consulte con el departamento legal de su empresa.
- Fuente de identidad: si utiliza [AWS Managed Microsoft AD](#) su directorio autogestionado de [Active Directory \(AD\)](#) como fuente de identidad, su región de origen debe coincidir con la región Región de AWS en la que habilitó el IAM Identity Center.
- Regiones de suscripción (regiones que están deshabilitadas de forma predeterminada): una región de suscripción es una Región de AWS que está deshabilitada de forma predeterminada. Debe activar la región registrada para utilizarla. Para obtener más información, consulte [Administrar el centro de identidad de IAM en una](#) región con suscripción voluntaria.
- Correos electrónicos entre regiones con Amazon Simple Email Service: en algunas regiones, el Centro de Identidad de IAM puede llamar a [Amazon Simple Email Service \(Amazon SES\)](#) de una región diferente para enviar correos electrónicos. En estas llamadas entre regiones, el IAM Identity Center envía determinados atributos de usuario a la otra región. Para obtener más información, consulte [Correos electrónicos entre regiones con Amazon SES](#).

### Temas

- [Operaciones y almacenamiento de datos por región del Centro de Identidad de IAM](#)
- [Conmutación Regiones de AWS](#)
- [Deshabilitar una Región de AWS donde el Centro de Identidad de IAM esté activado](#)

## Operaciones y almacenamiento de datos por región del Centro de Identidad de IAM

Descubra cómo el IAM Identity Center gestiona el almacenamiento de datos y las operaciones en todas partes. Regiones de AWS

Comprenda cómo el Centro de Identidad de IAM almacena los datos

Al habilitar el IAM Identity Center, todos los datos que configure en él se almacenarán en la región en la que los configuró. Estos datos incluyen configuraciones de directorios, conjuntos de permisos, instancias de aplicaciones y asignaciones de usuarios a las Cuenta de AWS aplicaciones. Si utiliza el almacén de identidades de IAM Identity Center, todos los usuarios y grupos que cree en IAM Identity Center también se almacenan en la misma región.

Correos electrónicos entre regiones con Amazon SES

IAM Identity Center utiliza [Amazon Simple Email Service \(Amazon SES\)](#) para enviar correos electrónicos a los usuarios finales cuando estos intentan iniciar sesión con una contraseña de un solo uso (OTP) como segundo factor de autenticación. Estos correos electrónicos también se envían para determinados eventos de administración de identidades y credenciales, como cuando se invita al usuario a configurar una contraseña inicial, verificar una dirección de correo electrónico y restablecer la contraseña. Amazon SES está disponible en un subconjunto de los Regiones de AWS que admite IAM Identity Center.

IAM Identity Center llama a los puntos de conexión locales de Amazon SES cuando Amazon SES está disponible localmente en una Región de AWS. Cuando Amazon SES no está disponible localmente, IAM Identity Center llama a los puntos de conexión de Amazon SES que se encuentren en una Región de AWS diferente, como se indica en la siguiente tabla.

| Código de región de IAM Identity Center | Nombre de región de IAM Identity Center | Código de región de Amazon SES | Nombre de región de Amazon SES |
|-----------------------------------------|-----------------------------------------|--------------------------------|--------------------------------|
| ap-east-1                               | Asia-Pacífico (Hong Kong)               | ap-northeast-2                 | Asia-Pacífico (Seúl)           |
| ap-south-2                              | Asia-Pacífico (Hyderabad)               | ap-south-1                     | Asia-Pacífico (Bombay)         |
| ap-southeast-4                          | Asia-Pacífico (Melbourne)               | ap-southeast-2                 | Asia-Pacífico (Sídney)         |

| Código de región de IAM Identity Center | Nombre de región de IAM Identity Center | Código de región de Amazon SES | Nombre de región de Amazon SES      |
|-----------------------------------------|-----------------------------------------|--------------------------------|-------------------------------------|
| ap-southeast-5                          | Asia-Pacífico (Malasia)                 | ap-southeast-1                 | Asia-Pacífico (Singapur)            |
| ca-west-1                               | Oeste de Canadá (Calgary)               | ca-central-1                   | Canadá (centro)                     |
| eu-south-2                              | Europa (España)                         | eu-west-3                      | Europa (París)                      |
| eu-central-2                            | Europa (Zúrich)                         | eu-central-1                   | Europa (Fráncfort)                  |
| me-central-1                            | Medio Oriente (EAU)                     | eu-central-1                   | Europa (Fráncfort)                  |
| us-gov-east-1                           | AWS GovCloud (Este de EE. UU.)          | us-gov-west-1                  | AWS GovCloud (Estados Unidos-Oeste) |

En estas llamadas entre regiones, IAM Identity Center puede enviar los siguientes atributos de usuario:

- Dirección de correo electrónico
- Nombre
- Apellido
- Cuenta en AWS Organizations
- AWS URL del portal de acceso
- Nombre de usuario
- ID de directorio
- ID de usuario

Administrar IAM Identity Center en una región de activación opcional (región que está deshabilitada de forma predeterminada)

La mayoría de Regiones de AWS están habilitadas para funcionar en todos los AWS servicios de forma predeterminada, pero debe habilitar las siguientes [regiones de suscripción](#) si quiere utilizar el Centro de identidad de IAM:

- Africa (Cape Town)
- Asia-Pacífico (Hong Kong)
- Asia-Pacífico (Hyderabad)
- Asia-Pacífico (Yakarta)
- Asia-Pacífico (Melbourne)
- Asia-Pacífico (Malasia)
- Oeste de Canadá (Calgary)
- Europa (Milán)
- Europa (España)
- Europa (Zúrich)
- Israel (Tel Aviv)
- Medio Oriente (Baréin)
- Medio Oriente (EAU)

Si despliega el Centro de Identidad de IAM en una región en la que haya optado por participar, deberá habilitar esta región en todas las cuentas para las que desee gestionar el acceso al Centro de Identidad de IAM. Todas las cuentas necesitan esta configuración, independientemente de si va a crear recursos en esa región o no. Puede habilitar una región para las cuentas corrientes de su organización y debe repetir esta acción cuando añada cuentas nuevas. Para obtener instrucciones, consulte [Habilitar o deshabilitar una región de su organización](#) en la Guía del AWS Organizations usuario. Para evitar repetir estos pasos adicionales, puede optar por implementar su centro de identidad de IAM en una [región habilitada de forma predeterminada](#).

 Note

Su cuenta de AWS miembro debe estar habilitada en la misma región que la región en la que se encuentra su instancia del Centro de Identidad de IAM para que pueda acceder a la cuenta de AWS miembro desde el AWS portal de acceso.

Los metadatos se almacenan en las regiones en las que se ha habilitado

Al habilitar el Centro de Identidad de IAM para una cuenta de administración en una suscripción voluntaria Región de AWS, los siguientes metadatos del Centro de Identidad de IAM para cualquier cuenta de miembro se almacenan en la región.

- ID de cuenta
- Nombre de cuenta
- Correo electrónico de la cuenta
- Nombres de recursos de Amazon (ARNs) de las funciones de IAM que el Centro de Identidad de IAM crea en la cuenta del miembro

Regiones de AWS que están habilitados de forma predeterminada

Las siguientes regiones están habilitadas de forma predeterminada y puede habilitar el Centro de identidad de IAM en estas regiones.

- Este de EE. UU. (Ohio)
- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Oregón)
- Oeste de EE. UU. (Norte de California)
- Europa (París)
- América del Sur (São Paulo)
- Asia-Pacífico (Bombay)
- Europa (Estocolmo)
- Asia-Pacífico (Seúl)
- Asia-Pacífico (Tokio)

- Europa (Irlanda)
- Europa (Fráncfort)
- Europa (Londres)
- Asia-Pacífico (Singapur)
- Asia-Pacífico (Sídney)
- Canadá (centro)
- Asia-Pacífico (Osaka)

## Conmutación Regiones de AWS

Le recomendamos que instale IAM Identity Center en una región que desee mantener disponible para los usuarios, no en una región que pueda tener que deshabilitar. Para obtener más información, consulte [Consideraciones a la hora de elegir una Región de AWS](#).

Para cambiar de región del centro de identidad de IAM, solo tiene que [eliminar la instancia actual del centro de identidad de IAM](#) y crear una instancia en otra región. Si ya ha activado una aplicación AWS gestionada con su instancia actual del IAM Identity Center, desactive la aplicación antes de eliminar el IAM Identity Center. Para obtener instrucciones sobre cómo deshabilitar las aplicaciones AWS administradas, consulte. [Deshabilitar una aplicación AWS gestionada](#)

### Consideraciones de configuración en la nueva región

Debe volver a crear los usuarios, los grupos, los conjuntos de permisos, las aplicaciones y las asignaciones en la nueva instancia de IAM Identity Center. Puede utilizar la asignación de cuentas y aplicaciones del IAM Identity Center [APIs](#) para obtener una instantánea de la configuración y, a continuación, utilizarla para volver a crear la configuración en una nueva región. Al cambiar a otra región, también se cambia la URL del [portal de AWS acceso](#), lo que proporciona a los usuarios un acceso de inicio de sesión único a sus Cuentas de AWS aplicaciones. Es posible que también tengas que volver a crear alguna configuración del IAM Identity Center a través de la consola de administración de tu nueva instancia.

### Deshabilitar una Región de AWS donde el Centro de Identidad de IAM esté activado

Si desactiva una Región de AWS en el que esté instalado el Centro de Identidad de IAM, el Centro de Identidad de IAM también estará deshabilitado. Una vez inhabilitado el Centro de identidad de IAM en una región, los usuarios de esa región no tendrán acceso mediante un inicio de sesión único a ninguna de las aplicaciones. Cuentas de AWS

Para volver a activar el Centro de Identidad de IAM de forma [opcional Regiones de AWS](#), debe volver a activar la región. Como el Centro de Identidad de IAM debe volver a procesar todos los eventos pausados, volver a habilitar el Centro de Identidad de IAM puede llevar algún tiempo.

 Note

El Centro de Identidad de IAM solo puede gestionar el acceso a aquellos Cuentas de AWS que estén habilitados para su uso en un. Región de AWS Para gestionar el acceso a todas las cuentas de su organización, active el Centro de identidad de IAM en la cuenta de gestión de forma Región de AWS que se active automáticamente para su uso con el Centro de identidades de IAM.

Para obtener más información sobre la activación y la desactivación Regiones de AWS, consulte [Gestión Regiones de AWS en la AWS referencia general](#).

## Uso del IAM Identity Center únicamente para el acceso de los usuarios a las aplicaciones

Puede utilizar el Centro de identidad de IAM para que los usuarios accedan a aplicaciones como Amazon Q Developer o a ambas. Cuentas de AWS Puede conectar su proveedor de identidad actual y sincronizar los usuarios y grupos de su directorio, o bien [crear y gestionar usuarios directamente en el IAM Identity Center](#). Para obtener información sobre cómo conectar su proveedor de identidad actual al IAM Identity Center, consulte el [Tutoriales de fuentes de identidad de IAM Identity Center](#).

### ¿Ya utilizas IAM para acceder a? Cuentas de AWS

No necesita realizar ningún cambio en sus Cuenta de AWS flujos de trabajo actuales para utilizar el IAM Identity Center y acceder a las aplicaciones AWS gestionadas. Si utiliza la [federación con IAM](#) o usuarios de IAM para el Cuenta de AWS acceso, sus usuarios pueden seguir Cuentas de AWS accediendo de la misma manera que siempre lo han hecho y usted puede seguir utilizando sus flujos de trabajo actuales para gestionar ese acceso.

## Funciones de IAM creadas por el Centro de Identidad de IAM

Al asignar un usuario a una AWS cuenta, el Centro de Identidad de IAM crea funciones de IAM para conceder a los usuarios permisos de acceso a los recursos.

Cuando asigna un conjunto de permisos, el IAM Identity Center crea los roles de IAM controlados por el IAM Identity Center correspondientes en cada cuenta y adjunta a esos roles las políticas especificadas en el conjunto de permisos. El Centro de Identidad de IAM administra la función y permite que los usuarios autorizados que haya definido la asuman mediante el portal de acceso o. AWS CLI A medida que modifica el conjunto de permisos, IAM Identity Center garantiza que las políticas y los roles de IAM correspondientes se actualicen en consecuencia.

 Note

Los conjuntos de permisos no se utilizan para conceder permisos a las aplicaciones.

Si ya has configurado las funciones de IAM en tu cuenta Cuenta de AWS, te recomendamos que compruebes si tu cuenta se acerca a la cuota de funciones de IAM. La cuota predeterminada de roles de IAM por cuenta es de 1000 roles. Para obtener más información, consulte [Cuotas de objetos de IAM](#).

Si se acerca a la cuota, considere solicitar un aumento de la cuota. De lo contrario, es posible que tenga problemas con IAM Identity Center al aprovisionar conjuntos de permisos a cuentas que hayan superado la cuota de roles de IAM. Para obtener información sobre cómo solicitar un aumento de cuota, consulte [Solicitar un aumento de cuota](#) en la Guía del usuario de Service Quotas.

 Note

Si está revisando las funciones de IAM en una cuenta que ya utiliza el Centro de identidad de IAM, es posible que observe que los nombres de las funciones comienzan por “AWSReservedSSO\_”. Estas son las funciones que el servicio del Centro de Identidad de IAM ha creado en la cuenta y provienen de la asignación de un conjunto de permisos a la cuenta.

## Centro de identidad de IAM y AWS Organizations

AWS Organizations se recomienda, pero no es obligatorio, para su uso con el Centro de identidades de IAM. Si no ha creado una organización, no tiene que hacerlo. Al activar el Centro de Identidad de IAM, elegirá si desea habilitar el servicio con. AWS Organizations Al configurar una organización, la cuenta Cuenta de AWS que la configura se convierte en la cuenta de administración de la organización. El usuario raíz de la Cuenta de AWS es ahora el propietario de la cuenta de



administración de la organización. Todas las Cuentas de AWS adicionales que invite a su organización son cuentas de miembro. La cuenta de administración crea los recursos, las unidades organizativas y las políticas de la organización que administran las cuentas de miembro. La cuenta de administración delega los permisos a las cuentas de miembro.

 Note

Le recomendamos que habilite el Centro de Identidad de IAM con AWS Organizations, lo que crea una instancia de organización del Centro de Identidad de IAM. Nuestra práctica recomendada es una instancia de organización, ya que es compatible con todas las características de IAM Identity Center y proporciona capacidades de administración centralizada. Para obtener más información, consulte [Instancias de organización de IAM Identity Center](#).

Si ya ha configurado el Centro de Identidad de IAM AWS Organizations y lo va a añadir a su organización, asegúrese de que todas las AWS Organizations funciones estén habilitadas. Al crear una organización, las características se habilitan de manera predeterminada. Para obtener más información, consulte [Habilitar todas las características en la organización](#) en la Guía del usuario de AWS Organizations .

Para habilitar una instancia de organización del Centro de identidades de IAM, debe iniciar sesión en su cuenta de AWS Organizations administración como usuario con credenciales administrativas o como usuario raíz (no se recomienda a menos que no existan otros usuarios administrativos). AWS Management Console Para obtener más información, consulte [Creación y administración de una AWS organización](#) en la Guía del AWS Organizations usuario.

Si ha iniciado sesión con las credenciales administrativas de una cuenta de AWS Organizations miembro, puede habilitar una instancia de cuenta del IAM Identity Center. Las instancias de cuentas tienen capacidades limitadas y están vinculadas a una sola AWS cuenta.

## Instancias de organización y cuenta de IAM Identity Center

Una instancia es una implementación única de IAM Identity Center. Hay dos tipos de instancias disponibles para IAM Identity Center: las instancias de organización y las instancias de cuenta.

- Instancia de organización (recomendada)

Una instancia del centro de identidad de IAM que se habilita en la cuenta AWS Organizations de administración. Las instancias de organización admiten todas las características de IAM Identity Center. Le recomendamos que implemente una instancia de organización en lugar de instancias de cuenta para minimizar la cantidad de puntos de administración.

- Instancia de cuenta

Una instancia de IAM Identity Center vinculada a una única Cuenta de AWS y visible únicamente dentro de la AWS región Cuenta de AWS y en la que está habilitada. Utilice una instancia de cuenta para situaciones más sencillas con una sola cuenta. Puede habilitar una instancia de cuenta a partir de cualquiera de las siguientes opciones:

- Y Cuenta de AWS eso no lo gestiona AWS Organizations
- Una cuenta de miembro en AWS Organizations

## Cuenta de AWS Tipos de que pueden habilitar IAM Identity Center

Para habilitar IAM Identity Center, inicie sesión en la AWS Management Console con una de las siguientes credenciales, en función del tipo de instancia que desee crear:

- Su cuenta AWS Organizations de administración (recomendada): necesaria para crear una [instancia organizativa](#) del IAM Identity Center. Utilice una instancia de organización para los permisos de varias cuentas y las asignaciones de aplicaciones en toda la organización.
- Su cuenta de AWS Organizations miembro de: utilícela para crear una [instancia de cuenta](#) de IAM Identity Center para permitir las asignaciones de aplicaciones dentro de esa cuenta de miembro. En una organización pueden existir una o más cuentas con una instancia de nivel de miembro.
- Una instancia independiente Cuenta de AWS: se utiliza para crear una instancia de [organización o una instancia de cuenta](#) del IAM Identity Center. Cuenta de AWS no administra la independiente. AWS Organizations Puede asociar únicamente una instancia de IAM Identity Center a una independiente Cuenta de AWS y utilizarla para las asignaciones de aplicaciones dentro de esa independiente. Cuenta de AWS

Utilice la siguiente tabla para comparar las capacidades que ofrece el tipo de instancia:

| Funcionalidad                                                                                                    | Instancia en la cuenta AWS Organizations de administración de (método recomendado)     | Instancia en una cuenta de miembro                                                     | Instancia en una independiente Cuenta de AWS                                             |
|------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| Administración de usuarios                                                                                       |  Sí   |  Sí   |  Sí   |
| AWS Portal de acceso por para el acceso mediante inicio de sesión único a sus aplicaciones AWS administradas por |  Sí   |  Sí   |  Sí   |
| OAuth Aplicaciones administradas por el cliente de 2.0 (OIDC)                                                    |  Sí  |  Sí  |  Sí  |
| Permisos para varias cuentas                                                                                     |  Sí |  No |  No |
| AWS Portal de acceso por para el acceso mediante inicio de sesión único a sus Cuentas de AWS                     |  Sí |  No |  No |
| Aplicaciones de SAML 2.0 administradas por el cliente                                                            |  Sí |  No |  No |

| Funcionalidad                                            | Instancia en la cuenta AWS Organizations de administración de (método recomendado) | Instancia en una cuenta de miembro                                                  | Instancia en una independiente Cuenta de AWS                                             |
|----------------------------------------------------------|------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|
| El administrador delegado puede administrar la instancia |   | S  | N  No |

Para obtener más información acerca de las aplicaciones AWS administradas por y IAM Identity Center, consulte [AWS aplicaciones gestionadas que puede utilizar con el Centro de identidades de IAM](#).

## Temas

- [Instancias de organización de IAM Identity Center](#)
- [Instancias de cuenta de IAM Identity Center](#)
- [Eliminación de la instancia de IAM Identity Center](#)

## Instancias de organización de IAM Identity Center

Al habilitar IAM Identity Center junto con AWS Organizations, se crea una instancia de organización de IAM Identity Center. La instancia de organización debe estar habilitada en su cuenta de administración y puede administrar de forma centralizada el acceso de los usuarios y grupos con una sola instancia de organización. Solo puede tener una instancia de organización para cada cuenta de administración de AWS Organizations.

Si habilitó IAM Identity Center antes del 15 de noviembre de 2023, tiene una instancia de organización de IAM Identity Center.

Para habilitar una instancia de organización del IAM Identity Center, consulte [Para habilitar una instancia de IAM Identity Center](#).

## Cuándo usar una instancia de organización

Las instancias de organización son el método principal para activar IAM Identity Center y, por lo general, se recomienda usar una instancia de organización. Las instancias de organización ofrecen los siguientes beneficios:

- Compatibilidad con todas las características de IAM Identity Center: incluye la administración de permisos para varias Cuentas de AWS de su organización y la asignación del acceso a las aplicaciones administradas por el cliente.
- Reducción de la cantidad de puntos de administración: una instancia de organización tiene un único punto de administración, que es la cuenta de administración. Le recomendamos que habilite una instancia de organización en lugar de una instancia de cuenta para reducir la cantidad de puntos de administración.
- Control central de la creación de instancias de cuenta: puede controlar si las cuentas de los miembros de su organización pueden crear instancias de cuenta, siempre y cuando no haya implementado una instancia de IAM Identity Center en su organización en una región de activación opcional (una Región de AWS que está deshabilitada de forma predeterminada).

Para obtener instrucciones sobre cómo habilitar una instancia de organización del IAM Identity Center, consulte [Para habilitar una instancia de IAM Identity Center](#).

## Instancias de cuenta de IAM Identity Center

Con una instancia de cuenta de IAM Identity Center, puede implementar aplicaciones administradas por compatibles y aplicaciones AWS administradas por el cliente basadas en OIDC. Las instancias de cuenta permiten implementar aplicaciones de forma aislada en una sola al usar las características del Cuenta de AWS portal de acceso y de las identidades de la plantilla de IAM Identity Center.

Las instancias de cuenta están vinculadas a una única Cuenta de AWS y se utilizan únicamente para administrar el acceso de usuarios y grupos a las aplicaciones compatibles de la misma cuenta y Región de AWS. Tiene un límite de una instancia de cuenta por Cuenta de AWS. Puedes crear una instancia de cuenta a partir de una de las siguientes opciones: una cuenta de miembro AWS Organizations o una cuenta independiente Cuenta de AWS que no esté gestionada por AWS Organizations.

Para obtener instrucciones sobre cómo habilitar una instancia de cuenta del IAM Identity Center, consulte [Para habilitar una instancia de IAM Identity Center](#) y seleccione la pestaña Cuenta.

## Cuándo usar una instancia de cuenta

En la mayoría de los casos, se recomienda usar una [instancia de organización](#). Utilice las instancias de cuenta solo si se da una de las siguientes situaciones:

- Desea ejecutar una prueba temporal de una aplicación AWS administrada por compatible para determinar si la aplicación se adapta a las necesidades de su empresa.
- No tiene previsto adoptar IAM Identity Center en toda su organización, pero quiere admitir una o varias aplicaciones AWS administradas por administradas por.
- Tiene una instancia de organización de IAM Identity Center, pero desea implementar una aplicación administrada por AWS compatible en un conjunto aislado de usuarios que son distintos de los usuarios de la instancia de organización.
- No controla la AWS organización en la que opera. Por ejemplo, un tercero controla la AWS organización que administra su Cuentas de AWS.

### Important

Si piensa utilizar IAM Identity Center para admitir aplicaciones en varias cuentas, utilice una instancia de organización. Las instancias de cuentas no admiten este caso de uso.

## AWS Aplicaciones administradas por que admiten las instancias de cuenta

Consulte [AWS aplicaciones gestionadas que puede utilizar con el Centro de identidades de IAM](#) para obtener información sobre qué aplicaciones AWS administradas de admiten instancias de cuenta de IAM Identity Center. Compruebe la disponibilidad de la creación de instancias de cuenta con su aplicación AWS administrada por.

## Restricciones de disponibilidad de las cuentas de los miembros

Para implementar instancias de cuentas del IAM Identity Center en las cuentas de AWS Organizations los miembros, debe cumplirse una de las siguientes condiciones:

- No hay ninguna instancia de organización del IAM Identity Center en su organización de .
- Hay una instancia de organización del IAM Identity Center en su organización de y el administrador de la instancia permite la creación de instancias de cuentas del IAM Identity Center (para las instancias de la organización creadas después del 15 de noviembre de 2023).

- Hay una instancia de organización del IAM Identity Center en su organización de y el administrador de la instancia ha habilitado manualmente la creación de instancias de cuentas por parte de las cuentas de los miembros de la organización (en el caso de las instancias de la organización creadas antes del 15 de noviembre de 2023). Para obtener instrucciones, consulte [Permita la creación de instancias de cuenta en las cuentas de los miembros](#).

Cuando se cumpla una de las condiciones anteriores, todas las siguientes condiciones deben ser verdaderas:

- El administrador no ha creado ninguna [política de control de servicio](#) que impida a las cuentas de los miembros crear instancias de cuenta.
- Independientemente de la, no tiene una instancia de IAM Identity Center en esta misma cuenta. Región de AWS
- Trabaja en una en la Región de AWS que IAM Identity Center está disponible. Para obtener información acerca de las regiones, consulte [Operaciones y almacenamiento de datos por región del Centro de Identidad de IAM](#).

## Consideraciones sobre las instancias de cuenta

Una instancia de cuenta está diseñada para casos de uso especializados y ofrece un subconjunto de características disponibles para una instancia de organización. Tenga en cuenta lo siguiente antes de crear una instancia de cuenta:

- Las instancias de cuenta no admiten conjuntos de permisos y, por lo tanto, no admiten el acceso a Cuentas de AWS.
- No puede convertir ni fusionar una instancia de cuenta en una instancia de organización.
- Solo determinadas [aplicaciones administradas por AWS](#) admiten las instancias de cuenta.
- Utilice instancias de cuenta para usuarios aislados que utilizarán las aplicaciones en una sola cuenta y durante la vida útil de las aplicaciones utilizadas.
- Las aplicaciones que están asociadas a una instancia de cuenta deben permanecer asociadas a la instancia de cuenta hasta que elimine la aplicación y sus recursos.
- Una instancia de cuenta debe permanecer en la Cuenta de AWS en la que se creó.

## Permita la creación de instancias de cuenta en las cuentas de los miembros

Si habilitó IAM Identity Center antes del 15 de noviembre de 2023, tiene una [instancia de organización](#) del IAM Identity Center en la que las cuentas de los miembros pueden crear instancias de cuentas deshabilitada de forma predeterminada. Puede elegir si las cuentas de miembros pueden crear instancias de cuenta mediante la habilitación de la característica de instancias de cuenta en la consola del IAM Identity Center.

Para habilitar la creación de instancias de cuentas por parte de las cuentas de miembros de su organización

### Important

La habilitación de las instancias de cuenta de IAM Identity Center para las cuentas de los miembros es una operación de una sola vez. Esto significa que esta operación no se puede revertir. Una vez habilitada, puede limitar la creación de instancias de cuenta mediante la creación de una política de control de servicio (SCP). Para ver las instrucciones, consulte [Control de la creación de instancias de cuenta con políticas de control de servicio](#).

1. Abra la [consola de IAM Identity Center](#).
2. Seleccione Configuración y, a continuación, seleccione la pestaña Administración.
3. En la sección Instancias de cuenta de IAM Identity Center, seleccione Habilitar instancias de cuenta de IAM Identity Center.
4. En el cuadro de diálogo Habilitar instancias de cuenta de IAM Identity Center, confirme que desea permitir que las cuentas de miembros de su organización creen instancias de cuenta; para ello, seleccione Habilitar.

## Uso de políticas de control de servicio para controlar la creación de instancias de cuenta

La capacidad de las cuentas de los miembros para crear instancias de cuentas depende de cuándo se haya activado IAM Identity Center:

- Antes de noviembre de 2023: debe [permitir la creación de instancias de cuentas en las cuentas de los miembros](#), lo cual es una acción que no se puede anular.



- Después del 15 de noviembre de 2023, las cuentas de los miembros pueden crear instancias de cuentas de forma predeterminada.

En cualquier caso, puede usar las políticas de control de servicio (SCPs) para:

- Impida que todas las cuentas de los miembros creen instancias de cuentas.
- Permita que solo cuentas de miembros específicas creen instancias de cuentas.

### Impida las instancias de cuenta

Utilice el procedimiento siguiente para generar una SCP que impida a las cuentas de los miembros crear instancias de cuenta de IAM Identity Center.

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de control, en la sección Administración central, seleccione el botón Impedir instancias de cuentas.
3. En el cuadro de diálogo Asociar una SCP para impedir la creación de nuevas instancias de cuenta, se le ofrecerá una SCP. Cópiela y pulse el botón Ir al panel de control de SCP. Se le dirigirá a la [AWS Organizations consola](#) de para crear la SCP o asociarla como una instrucción a una SCP existente. SCPs son una característica de. AWS Organizations Para obtener instrucciones sobre cómo conectar una SCP, consulte [Asociar y desasociar políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .

### Limite las instancias de cuentas

En lugar de impedir la creación de todas las instancias de cuentas, esta política deniega cualquier intento de crear una instancia de cuenta del Centro de Identidad de IAM a todas, Cuentas de AWS excepto a las que se indican explícitamente en el "**<ALLOWED-ACCOUNT-ID>**" marcador de posición.

Example : Política de denegación que limita la creación de instancias de cuentas

```
{  
  
  "Version": "2012-10-17",  
  "Statement" : [  
    {  
      "Sid": "DenyMemberAccountInstances",
```

```
    "Effect": "Deny",
    "Action": "sso:CreateInstance",
    "Resource": "*",
    "Condition": {
      "StringNotEquals": {
        "aws:PrincipalAccount": [ "<ALLOWED-ACCOUNT-ID>" ]
      }
    }
  ]
}
```

- Sustituya [ "<ALLOWED-ACCOUNT-ID>" ] por los Cuentas de AWS ID reales que desee permitir para crear una instancia de cuenta del IAM Identity Center.
- Puede enumerar varias cuentas permitidas IDs en el formato de matriz: [ "111122223333", "444455556666" ].
- Adjunte esta política al SCP de su organización para aplicar un control centralizado sobre la creación de instancias de cuentas de IAM Identity Center.

Para obtener instrucciones sobre cómo conectar una SCP, consulte [Asociar y desasociar políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .

## Eliminación de la instancia de IAM Identity Center

Cuando se elimina una instancia de IAM Identity Center, se eliminan todos los datos de esa instancia y no se pueden recuperar. En la siguiente tabla se describen los datos que se eliminan en función del tipo de directorio que está configurado en IAM Identity Center.

| ¿Qué datos se eliminan?                                                                      | Directorio conectado : AWS Managed Microsoft AD, Conector de AD Connector o proveedor de identidad externo | Almacén de identidades de IAM Identity Center                                          |  |
|----------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|--|
| Todos los conjuntos que ha configurado para Cuentas de AWS                                   |  S                        |  Sí   |  |
| Todas las aplicaciones que ha configurado en IAM Identity Center                             |  S                        |  Sí   |  |
| Todas las asignaciones de usuarios que ha configurado para sus aplicaciones Cuentas de AWS y |  S                       |  Sí  |  |
| Todos los usuarios y grupos del directorio o almacén                                         | N/D                                                                                                        |  Sí |  |

Utilice el siguiente procedimiento para eliminar su instancia de IAM Identity Center.

#### Cómo eliminar su instancia de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página Configuración, seleccione la pestaña Administración.
4. En la sección Eliminar la configuración de IAM Identity Center, seleccione Eliminar.

5. En el cuadro de diálogo Eliminar la configuración de IAM Identity Center, marque todas las casillas de verificación para confirmar que entiende que los datos se van a eliminar. Escriba su instancia de IAM Identity Center en el cuadro de texto y, a continuación, seleccione Confirmar.

# Activar IAM Identity Center

Cuando habilite IAM Identity Center, elegirá un tipo de AWS IAM Identity Center instancia para habilitarla. Una instancia de un servicio es una implementación única de un servicio en su AWS entorno. Hay dos tipos de instancias disponibles para IAM Identity Center: las instancias de organización y las instancias de cuenta. Los tipos de instancias que puede habilitar dependen del tipo de cuenta en la que haya iniciado sesión.

La siguiente lista identifica el tipo de instancias del IAM Identity Center que puede habilitar para cada tipo de: Cuenta de AWS

- Su cuenta AWS Organizations de administración (recomendada): necesaria para crear una [instancia organizativa](#) del IAM Identity Center. Utilice una instancia de organización para los permisos de varias cuentas y las asignaciones de aplicaciones en toda la organización.
- Su cuenta de AWS Organizations miembro de: utilícela para crear una [instancia de cuenta](#) de IAM Identity Center para permitir las asignaciones de aplicaciones dentro de esa cuenta de miembro. En una organización pueden existir una o más cuentas con una instancia de nivel de miembro.
- Una instancia independiente Cuenta de AWS: se utiliza para crear una instancia de [organización o una instancia de cuenta](#) del IAM Identity Center. Cuenta de AWS no administra la independiente. AWS Organizations Solo puede asociar una instancia de IAM Identity Center a una independiente Cuenta de AWS y utilizarla para las asignaciones de aplicaciones dentro de esa independiente. Cuenta de AWS

## Important

La cuenta de administración de la organización puede controlar si [las cuentas de los miembros de la organización pueden crear instancias de cuentas del IAM Identity Center](#) mediante una política de control de servicios.

Para comparar las distintas capacidades que proporcionan los distintos tipos de instancias, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

Antes de activar el Centro de identidades de IAM, le recomendamos que revise el [Requisitos previos y consideraciones sobre el IAM Identity Center](#).

# Para habilitar una instancia de IAM Identity Center

Seleccione la pestaña correspondiente al tipo de instancia del IAM Identity Center que desee habilitar, ya sea una instancia de organización o de cuenta:

## Organization (recommended)

1. Realice una de las siguientes acciones para iniciar sesión en la AWS Management Console.
  - Primera vez que AWS utiliza (usuario raíz): inicie sesión como propietario de cuenta; para ello, elija Usuario raíz de la e ingrese la dirección de Cuenta de AWS correo electrónico de. En la siguiente página, escriba su contraseña.
  - Ya utiliza una independiente Cuenta de AWS (credenciales de IAM): inicie sesión AWS con sus credenciales de IAM con permisos administrativos.
  - Ya utiliza AWS Organizations (credenciales de IAM): inicie sesión con las credenciales de cuenta de administración.
2. Abra la [consola de IAM Identity Center](#).
3. En Activar el IAM Identity Center, seleccione Activar.
4. En la AWS Organizations página Habilitar el centro de identidad de IAM con, revise la información y, a continuación, seleccione Habilitar para completar el proceso.

### Note

AWS Organizations solo puede habilitar el Centro de identidad de IAM en una sola AWS región. Tras activar el Centro de Identidad de IAM, si necesita cambiar la región en la que está activado el Centro de Identidad de IAM, debe [eliminar](#) la instancia actual y crear una instancia en la otra región.

Después de habilitar la instancia de su organización, se recomienda realizar los siguientes pasos para terminar de configurar el entorno:

- Asegúrese de que utiliza la fuente de identidad que eligió. Si ya tiene un origen de identidad, puede seguir utilizándolo. Para obtener más información, consulte [Confirme sus orígenes de identidad del IAM Identity Center](#).
- Registro de una cuenta miembro como administrador delegado. Para obtener más información, consulte [Administración delegada](#).

- El IAM Identity Center le proporciona un portal de acceso a los AWS recursos. Si filtra el acceso a AWS dominios de o puntos de conexión de URL específicos mediante una solución de filtrado de contenido web, como cortafuegos de nueva generación (NGFW) o puertas de enlace web seguras (SWG), consulte. [Actualice los firewalls y las puertas de enlace para permitir el acceso a Portal de acceso a AWS](#)

## Account

1. Realice una de las siguientes acciones para iniciar sesión en la AWS Management Console.
  - Primera vez que AWS utiliza (usuario raíz): inicie sesión como propietario de cuenta; para ello, elija Usuario raíz de la e ingrese la dirección de Cuenta de AWS correo electrónico de. En la siguiente página, escriba su contraseña.
  - Ya utiliza AWS (credenciales de IAM): inicie sesión con sus credenciales de IAM con permisos administrativos.
  - Ya utiliza AWS Organizations (credenciales de IAM): inicie sesión con las credenciales administrativas de su cuenta de miembro.
2. Abra la [consola de IAM Identity Center](#).
3. Si es la primera vez que utiliza una cuenta independiente AWS o la tiene Cuenta de AWS, en Activar el centro de identidad de IAM, seleccione Activar.

Aparecerá la página Habilitar el centro de identidad de IAM con. AWS Organizations Recomendamos esta opción, aunque no es obligatoria.

Seleccione el enlace para habilitar una instancia de cuenta de IAM Identity Center.

4. Si es administrador de una cuenta de AWS Organizations miembro, en Habilitar una instancia de cuenta del IAM Identity Center, seleccione Habilitar una instancia de cuenta.
5. En la página Habilitar una instancia de cuenta del Centro de Identidad de IAM, revise la información y, si lo desea, añada las etiquetas que desee asociar a esta instancia de cuenta. A continuación, seleccione Activar para completar el proceso.

### Note

Si su AWS cuenta es miembro de una organización, es posible que haya restricciones a la hora de habilitar una instancia de cuenta del IAM Identity Center.

- Si su organización activó el Centro de identidades de IAM antes del 15 de noviembre de 2023, la posibilidad de que las cuentas de los miembros creen instancias de cuentas está deshabilitada de forma predeterminada y debe habilitarla la cuenta de administración de la organización.
- Si su organización activó el Centro de identidad de IAM después del 15 de noviembre de 2023, la posibilidad de que las cuentas de los miembros creen instancias de cuentas está habilitada de forma predeterminada. Sin embargo, las políticas de control de servicio se pueden utilizar para impedir la creación de instancias de cuenta de IAM Identity Center dentro de una organización.

Para obtener más información, consulte [the section called “Permitir la creación de instancias de cuentas en las cuentas de los miembros”](#) y [the section called “SCPs para la creación de instancias de cuenta”](#).

## Confirme sus orígenes de identidad del IAM Identity Center

Su origen de identidad en IAM Identity Center define dónde se administran sus usuarios y grupos. Después de habilitar IAM Identity Center, asegúrese de que utiliza el origen de identidad que eligió. Si ya tiene un origen de identidad, puede seguir utilizándolo.

Si ya administra usuarios y grupos en Active Directory o un IdP externo, le recomendamos que considere la posibilidad de conectar esta fuente de identidad al habilitar el Centro de identidades de IAM y elegir su fuente de identidad. Esto debe hacerse antes de crear usuarios y grupos en el directorio predeterminado de Identity Center y de realizar cualquier asignación.

Si ya administra usuarios y grupos en una fuente de identidad en IAM Identity Center, cambiar a una fuente de identidad diferente podría eliminar todas las asignaciones de usuarios y grupos que configuró en IAM Identity Center. Si esto ocurre, todos los usuarios, incluido el usuario administrativo del Centro de identidades de IAM, perderán el acceso de inicio de sesión único a sus aplicaciones. Cuentas de AWS Para obtener más información, consulte [Consideraciones para cambiar la fuente de identidad](#).

To confirm your identity source

1. Abra la [consola de IAM Identity Center](#)



2. En la página del panel, debajo de la sección Pasos de configuración recomendados, seleccione Confirme su origen de identidad. Para acceder a esta página, también puede seleccionar Configuración y la pestaña Origen de identidad.
3. No tiene que realizar ninguna acción si desea conservar el origen de identidad asignado. Si prefiere cambiarlo, seleccione Acciones y, a continuación, seleccione Cambiar el origen de identidad.

Puede elegir una de las siguientes opciones como origen de identidad:

#### Directorio de Identity Center

Cuando se habilita IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como origen de identidad predeterminado. Si aún no utiliza otro proveedor de identidad externo, puede empezar a crear sus usuarios y grupos y asignar su nivel de acceso a sus aplicaciones y a las suyas. Cuentas de AWS Para ver un tutorial sobre el uso de este origen de identidad, consulte [Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center](#).

#### Active Directory

Si ya está gestionando los usuarios y grupos de su AWS Managed Microsoft AD directorio mediante AWS Directory Service o de su directorio autogestionado en Active Directory (AD), le recomendamos que conecte ese directorio cuando active el Centro de identidades de IAM. No cree ningún usuario ni grupo en el directorio predeterminado de Identity Center. IAM Identity Center utiliza la conexión proporcionada por AWS Directory Service para sincronizar la información de usuarios, grupos y miembros del directorio de origen de Active Directory con el almacén de identidades de IAM Identity Center. Para obtener más información, consulte [Conexión un directorio Microsoft AD](#).

#### Note

El Centro de Identidad de IAM no SAMBA4 admite Simple AD como fuente de identidad.

#### Proveedor de identidades externo

Para proveedores de identidad externos (IdPs), como Okta o Microsoft Entra ID, puede utilizar el Centro de identidades de IAM para autenticar identidades IdPs mediante el estándar

Security Assertion Markup Language (SAML) 2.0. El protocolo SAML no proporciona ninguna forma de consultar al IdP para obtener información sobre los usuarios y los grupos. Debe hacer que IAM Identity Center conozca a esos usuarios y grupos aprovisionándolos en IAM Identity Center. Puede realizar el aprovisionamiento automático (sincronización) de la información de usuarios y grupos desde su IdP a IAM Identity Center mediante el protocolo del sistema de administración de identidades entre dominios (SCIM) v2.0 si su IdP admite SCIM. De lo contrario, puede aprovisionar manualmente los usuarios y grupos; para ello, ingrese manualmente los nombres de usuario, la dirección de correo electrónico y los grupos en IAM Identity Center.

Para obtener instrucciones detalladas sobre cómo configurar su fuente de identidad, consulte [Tutoriales de fuentes de identidad de IAM Identity Center](#).

 Note

Si tiene previsto utilizar un proveedor de identidades externo, tenga en cuenta que el IdP externo, no IAM Identity Center, administra la configuración de la autenticación multifactor (MFA). Los proveedores de identidad externos no admiten la MFA en el IAM Identity Center. Para obtener más información, consulte [Solicitar MFA a los usuarios](#).

## Actualice los firewalls y las puertas de enlace para permitir el acceso a Portal de acceso a AWS

El portal de AWS acceso proporciona a los usuarios un acceso de inicio de sesión único a todas sus aplicaciones en la nube Cuentas de AWS y a las más utilizadas, como Office 365, Concur, Salesforce y muchas más. Para lanzar varias aplicaciones rápidamente, basta con elegir el icono Cuenta de AWS o la aplicación en el portal.

 Note

AWS las aplicaciones gestionadas se integran con el Centro de Identidad de IAM y lo utilizan para los servicios de autenticación y directorio, pero es posible que no utilicen el portal de AWS acceso para acceder a las aplicaciones.

Si filtra el acceso a AWS dominios o puntos de enlace de URL específicos mediante una solución de filtrado de contenido web, como firewalls de última generación (NGFW) o Secure Web Gateways (SWG), debe permitir incluir en la lista los dominios y puntos de enlace de URL asociados al portal de acceso. AWS

La siguiente lista proporciona los dominios y puntos de enlace URL que debe añadir a las listas de permitidos de su solución de filtrado de contenido web.

- *[Directory ID or alias].awsapps.com*
- \*.aws.dev
- \*.awsstatic.com
- \*.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- \*.sso.amazonaws.com
- \*.sso.*[Region]*.amazonaws.com
- \*.sso-portal.*[Region]*.amazonaws.com
- *[Region]*.prod.pr.panorama.console.api.aws/panoramamaroute
- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- \*.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

## Consideraciones a la hora de permitir la inclusión de dominios y puntos de conexión de URL

Además de los requisitos de la lista de permitidos para el portal de AWS acceso, es posible que los demás servicios y aplicaciones que utilice exijan la inclusión de dominios en la lista de dominios permitidos.

- Para acceder a Cuentas de AWS la consola del AWS Management Console IAM Identity Center y a ella desde su portal de AWS acceso, debe permitir incluir dominios adicionales en la lista. Consulte [Solución de problemas](#) en la Guía de introducción para AWS Management Console obtener una lista de AWS Management Console dominios.

- Para acceder a las aplicaciones AWS gestionadas desde su portal de AWS acceso, debe permitir incluir sus dominios respectivos en una lista. Consulte la documentación de servicio correspondiente para obtener orientación.
- Si utiliza un software externo, como externo IdPs (por ejemplo, Okta y Microsoft Entra ID), tendrás que incluir sus dominios en tus listas de dominios permitidos.

# Tutoriales de fuentes de identidad de IAM Identity Center

Puede conectar su fuente de identidad existente en su cuenta AWS Organizations de administración de a [una instancia de organización del IAM Identity Center](#). Si no tiene un proveedor de identidad existente, puede crear y gestionar los usuarios directamente en el directorio predeterminado del IAM Identity Center. Puede tener un origen de identidad por organización.

En los tutoriales de esta sección, se describe cómo configurar una instancia de organización del IAM Identity Center con una fuente de identidad de uso común, cómo crear un usuario administrativo y si utiliza el IAM Identity Center para gestionar el acceso a Cuentas de AWS, crear y configurar conjuntos de permisos. Si utiliza el IAM Identity Center únicamente para acceder a las aplicaciones, no necesita utilizar conjuntos de permisos.

Estos tutoriales no describen cómo configurar instancias de cuenta del IAM Identity Center. Puede usar instancias de cuentas para asignar usuarios y grupos a las aplicaciones, pero no puede usar este tipo de instancia para administrar el acceso de los usuarios a Cuentas de AWS. Para obtener más información, consulte [Instancias de cuenta de IAM Identity Center](#).

## Note

Antes de iniciar cualquiera de estos tutoriales, habilite el IAM Identity Center. Para obtener más información, consulte [Activar IAM Identity Center](#).

## Temas

- [Uso de Active Directory como origen de identidad](#)
- [Setting up SCIM provisioning between CyberArk and IAM Identity Center](#)
- [Configuración de SAML y SCIM con Google Workspace e IAM Identity Center](#)
- [Uso del centro de identidad de IAM para conectarse con su JumpCloud Plataforma de directorios](#)
- [Configure SAML y SCIM con Microsoft Entra ID y el Centro de identidad de IAM](#)
- [Configuración de SAML y SCIM con Okta e IAM Identity Center](#)
- [Configuración del aprovisionamiento de SCIM entre OneLogin y el Centro de Identidad de IAM](#)
- [Utilización Ping Identity productos con IAM Identity Center](#)
- [Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center](#)
- [Tutoriales de vídeo](#)

# Uso de Active Directory como origen de identidad

Si administra los usuarios en su directorio de mediante AWS Directory Service o en su AWS Managed Microsoft AD directorio autoadministrado de Active Directory (AD), puede cambiar el origen de identidad de IAM Identity Center para que funcione con esos usuarios. Le recomendamos que considere la posibilidad de conectar este origen de identidad al habilitar IAM Identity Center y elegir el origen de identidad. Hacerlo antes de crear usuarios y grupos en el directorio predeterminado del Identity Center lo ayudará a evitar la configuración adicional que se requiere si cambia el origen de identidad más adelante.

Para utilizar Active Directory como origen de identidad, la configuración debe cumplir los siguientes requisitos previos:

- Si está usando AWS Managed Microsoft AD, debe habilitar Centro de identidades de IAM en la misma Región de AWS donde su AWS Managed Microsoft AD directorio de está configurado. Centro de identidades de IAM almacena los datos de asignación en la misma región que el directorio. Para administrar Centro de identidades de IAM, es posible que deba cambiarse a la región en la que está configurado Centro de identidades de IAM. Además, tenga en cuenta que el portal de AWS acceso de utiliza la misma URL de acceso que su directorio.
- Utilice un Active Directory que resida en la cuenta de administración:

Debe tener un conector de AD existente o AWS Managed Microsoft AD directorio de configurado en AWS Directory Service, y debe residir dentro de su cuenta AWS Organizations de administración de. Solo puede conectar un directorio de conector de AD o un directorio en AWS Managed Microsoft AD a la vez. Si necesita admitir varios dominios o bosques, utilice AWS Managed Microsoft AD. Para obtener más información, consulte:

- [Conectar un directorio en AWS Managed Microsoft AD al Centro de identidades de IAM](#)
- [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#)
- Utilice una instancia de Active Directory que resida en la cuenta de administrador delegado:

Si planea habilitar un administrador delegado de IAM Identity Center y usar Active Directory como origen de identidad de IAM Identity Center, puede usar un conector de AD existente o AWS Managed Microsoft AD directorio de configurado en el directorio de que reside en AWS la cuenta de administrador delegado.

Si decide cambiar la fuente de identidad de IAM Identity Center de cualquier otra fuente a Active Directory, o cambiarla de Active Directory a cualquier otra fuente, el directorio debe residir en

(ser propiedad de) la cuenta de miembro administrador delegado de IAM Identity Center, si existe alguna; de lo contrario, debe estar en la cuenta de administración.

En este tutorial se explica la configuración básica para usar Active Directory como origen de identidad de IAM Identity Center.

## Paso 1: conexión de Active Directory y especificación de un usuario

Si ya utiliza Active Directory, los siguientes temas lo ayudarán a prepararse para conectar su directorio a Centro de identidades de IAM.

### Note

Si planea conectar un AWS Managed Microsoft AD directorio de o un directorio autogestionado en Active Directory y no está utilizando RADIUS MFA AWS Directory Service con, active la MFA en IAM Identity Center.

### AWS Managed Microsoft AD

1. Revise la guía en [Conexión un directorio Microsoft AD](#).
2. Siga los pasos de [Conectar un directorio en AWS Managed Microsoft AD al Centro de identidades de IAM](#).
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM. Para obtener más información, consulte [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

### Directorio autogestionado en Active Directory

1. Revise la guía en [Conexión un directorio Microsoft AD](#).
2. Siga los pasos de [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#).
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM. Para obtener más información, consulte [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

## Paso 2: sincronización de un usuario administrativo en IAM Identity Center

Tras conectar el directorio al Centro de identidades de IAM, puede especificar el usuario al que quiere conceder permisos administrativos y, a continuación, sincronizar ese usuario del directorio con el Centro de identidades de IAM.

1. Abra la [Consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de Administrar sincronización, elija la pestaña Usuarios y, continuación, seleccione Añadir usuarios y grupos.
5. En la pestaña Usuarios, en Usuario, ingrese el nombre de usuario exacto y seleccione Agregar.
6. En Usuarios y grupos añadidos, haga lo siguiente:
  - a. Confirme que se ha especificado el usuario a quien desea conceder permisos administrativos.
  - b. Seleccione la casilla de verificación situada a la izquierda del nombre de usuario.
  - c. Elija Enviar
7. En la página Administrar sincronización, el usuario que especificó aparece en la lista de Ámbito de usuarios sincronizados.
8. En el panel de navegación, seleccione Usuarios.
9. En la página Usuarios, es posible que el usuario que especificó tarde algún tiempo en aparecer en la lista. Seleccione el icono de actualización para actualizar la lista de usuarios.

En este momento, el usuario no tiene acceso a la cuenta de administración. Para configurar el acceso administrativo a esta cuenta, debe crear un conjunto de permisos administrativos y asignar el usuario a ese conjunto de permisos. Para obtener más información, consulte [Crea un conjunto de permisos](#).

## Setting up SCIM provisioning between CyberArk and IAM Identity Center

El IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios desde CyberArk Directory Platform al Centro de identidades de IAM. Este



aprovisionamiento utiliza el protocolo sistema de administración de identidades entre dominios (SCIM) v2.0. Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

Esta conexión se configura en CyberArk utilizando el punto de conexión SCIM y el token de acceso del IAM Identity Center. Al configurar la sincronización de SCIM, se crea un mapeo de los atributos de usuario en CyberArk a los atributos nombrados en el Centro de identidades de IAM. Esto hace que los atributos esperados coincidan entre el Centro de Identidad de IAM y CyberArk.

Esta guía se basa en CyberArk a partir de agosto de 2021. Los pasos para las versiones más recientes pueden variar. Esta guía contiene algunas notas sobre la configuración de la autenticación de usuarios mediante SAML.

#### Note

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#). A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

## Temas

- [Requisitos previos](#)
- [Consideraciones de SCIM](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: Configurar el aprovisionamiento en CyberArk](#)
- [\(Opcional\) Paso 3: configurar los atributos de usuario en CyberArk para el control de acceso \(ABAC\) en el IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)

## Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- CyberArk suscripción o prueba gratuita. Para suscribirse a una prueba gratuita, visite [CyberArk](#).
- Una cuenta habilitada para IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).

- Una conexión SAML desde tu CyberArk cuenta al Centro de Identidad de IAM, tal y como se describe en [CyberArk documentación para el Centro de Identidad de IAM](#).
- Asocie el conector de IAM Identity Center a los roles, usuarios y organizaciones a los que desee permitir el acceso a las Cuentas de AWS.

## Consideraciones de SCIM

Las siguientes son consideraciones a tener en cuenta a la hora de utilizar CyberArk federación para IAM Identity Center:

- Solo los roles asignados en la sección de aprovisionamiento de aplicaciones se sincronizarán con IAM Identity Center.
- El script de aprovisionamiento solo se admite en su estado predeterminado; una vez modificado, el aprovisionamiento de SCIM podría fallar.
  - Solo se puede sincronizar un atributo de número de teléfono y el valor predeterminado es “teléfono del trabajo”.
- Si el mapeo de roles es CyberArk La aplicación IAM Identity Center ha cambiado, se espera el siguiente comportamiento:
  - Si se cambian los nombres de los roles, no habrá cambios en los nombres de los grupos en IAM Identity Center.
  - Si se cambian los nombres de los grupos, se crearán nuevos grupos en IAM Identity Center y los grupos antiguos permanecerán sin miembros.
- El comportamiento de sincronización y desaprovisionamiento de los usuarios se puede configurar desde el CyberArk Aplicación IAM Identity Center, asegúrese de configurar el comportamiento correcto para su organización. Estas son las opciones:
  - Sobrescriba (o no) a los usuarios del directorio de Identity Center con el mismo nombre principal.
  - Elimine el aprovisionamiento de usuarios del Centro de Identidad de IAM cuando el usuario se retire del CyberArk rol.
  - Cancele el aprovisionamiento de usuarios: deshabilite o elimine.

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

## Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie el punto final y el token de acceso de SCIM. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

### Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione Cerrar.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes mediante el CyberArk Aplicación IAM Identity Center. Estos pasos se explican en el procedimiento siguiente.

## Paso 2: Configurar el aprovisionamiento en CyberArk

Utilice el siguiente procedimiento en el CyberArk Aplicación IAM Identity Center para permitir el aprovisionamiento con IAM Identity Center. En este procedimiento se presupone que ya ha añadido el CyberArk La aplicación IAM Identity Center a su CyberArk consola de administración en Aplicaciones web. Si aún no lo ha hecho, consulte los [Requisitos previos](#) y complete este procedimiento para configurar el aprovisionamiento de SCIM.

## Para configurar el aprovisionamiento en CyberArk

1. Abra el icono CyberArk Aplicación del Centro de Identidad de IAM que agregó como parte de la configuración de SAML para CyberArk (Aplicaciones > Aplicación web). Consulte [Requisitos previos](#).
2. Elija la aplicación IAM Identity Center y vaya a la sección Aprovisionamiento.
3. Marque la casilla Habilitar el aprovisionamiento para esta aplicación y elija Live Mode.
4. En el procedimiento anterior, copió el valor del punto de conexión del SCIM de IAM Identity Center. Pegue ese valor en el campo URL del servicio SCIM, en el CyberArk La aplicación IAM Identity Center estableció el tipo de autorización como encabezado de autorización.
5. Configure el tipo de encabezado como token al portador.
6. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Bearer Token del CyberArk Aplicación IAM Identity Center.
7. Haga clic en Verificar para probar y aplicar la configuración.
8. En las opciones de sincronización, elija el comportamiento correcto para el que desea realizar el aprovisionamiento saliente CyberArk para que funcione. Puede optar por sobrescribir (o no) a los usuarios actuales de IAM Identity Center con un nombre principal y un comportamiento de desaprovisionamiento similares.
9. En Role Mapping, configure el mapeo desde CyberArk roles, en el campo Nombre, al grupo del Centro de Identidad de IAM, en el Grupo de destino.
10. Cuando haya terminado, haga clic en Guardar, en la parte inferior.
11. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Usuarios sincronizados de CyberArk aparecerá en la página de usuarios. Estos usuarios ya pueden asignarse a cuentas y conectarse dentro de IAM Identity Center.

## (Opcional) Paso 3: configurar los atributos de usuario en CyberArk para el control de acceso (ABAC) en el IAM Identity Center

Se trata de un procedimiento opcional para CyberArk si decide configurar los atributos del IAM Identity Center para gestionar el acceso a sus AWS recursos. Los atributos que defina en CyberArk se transmiten en una aserción de SAML al Centro de Identidad de IAM. A continuación, debe crear un conjunto de permisos en el Centro de Identidad de IAM para gestionar el acceso en función de los atributos de los que ha pasado CyberArk.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

Para configurar los atributos de usuario en CyberArk para el control de acceso en el IAM Identity Center

1. Abra el icono CyberArk Aplicación del Centro de Identidad de IAM que instaló como parte de la configuración de SAML para CyberArk (Aplicaciones > Aplicaciones web).
2. Vaya a la opción Respuesta SAML.
3. En Atributos, añada los atributos relevantes a la tabla siguiendo la siguiente lógica:
  - a. El nombre del atributo es el nombre del atributo original de CyberArk.
  - b. El Valor del atributo es el nombre del atributo que se envía en la aserción SAML a IAM Identity Center.
4. Seleccione Save.

## (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo Name configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

# Configuración de SAML y SCIM con Google Workspace e IAM Identity Center

Si su organización Google Workspace lo utiliza, puede integrar a sus usuarios Google Workspace en el IAM Identity Center para darles acceso a los AWS recursos de. Puede lograr esta integración al cambiar la fuente de identidad del IAM Identity Center de la fuente de identidad predeterminada del IAM Identity Center a Google Workspace.

La información de los usuarios de Google Workspace se sincroniza con IAM Identity Center mediante el [protocolo del sistema de administración de identidades entre dominios \(SCIM\) 2.0](#). Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

Esta conexión se configura en Google Workspace mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador de IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en Google Workspace con los atributos nombrados en IAM Identity Center. Esta asignación vincula los atributos de usuario esperados entre IAM Identity Center y Google Workspace. Para ello, debe configurarse Google Workspace como proveedor de identidades y conectarse con su IAM Identity Center.

## Objetivo

Los pasos de este tutorial lo ayudarán a establecer la conexión SAML entre Google Workspace y AWS. Más adelante, sincronizará a los usuarios de Google Workspace mediante SCIM. Para comprobar que todo está configurado correctamente, tras completar los pasos de configuración, iniciará sesión como Google Workspace usuario y verificará el acceso a AWS los recursos de. Tenga en cuenta que este tutorial se basa en un entorno de prueba con un directorio de Google Workspace pequeño. No se incluyen en este tutorial las estructuras de directorios, como los grupos y las unidades organizativas. Tras completar este tutorial, sus usuarios podrán acceder al portal de AWS acceso con sus Google Workspace credenciales.

### Note

Para suscribirse a una versión de prueba gratuita de Google Workspace, vaya a [Google Workspace](#) en el sitio web de Google's.

Si aún no ha habilitado IAM Identity Center, consulte [Activar IAM Identity Center](#).

## Consideraciones

- Antes de configurar el aprovisionamiento de SCIM entre Google Workspace e IAM Identity Center, le recomendamos revisar primero [Consideraciones para utilizar el aprovisionamiento automático](#).
- La sincronización automática de SCIM desde Google Workspace actualmente está limitada al aprovisionamiento de usuarios. Por el momento, no se admite el aprovisionamiento automático de grupos. Los grupos se pueden crear manualmente con el comando [create-group](#) de AWS CLI Identity Store o la API AWS Identity and Access Management (IAM). [CreateGroup](#) Como alternativa, puede utilizar [ssosync](#) para sincronizar los usuarios de Google Workspace y los grupos en el IAM Identity Center.
- Todos los usuarios de Google Workspace deben tener un valor especificado para Nombre, Apellidos, Nombre de usuario y Nombre de visualización.
- Cada usuario de Google Workspace tiene un único valor por atributo de datos, como la dirección de correo electrónico o el número de teléfono. Los usuarios que tengan varios valores no se sincronizarán. Si hay usuarios que tienen varios valores en sus atributos, elimine los atributos duplicados antes de intentar aprovisionar el usuario en IAM Identity Center. Por ejemplo, solo se puede sincronizar un atributo de número de teléfono. Como el atributo de número de teléfono predeterminado es “teléfono del trabajo”, utilice el atributo “teléfono del trabajo” para almacenar el número de teléfono del usuario, incluso si el número de teléfono del usuario es un teléfono fijo o móvil.
- Los atributos siguen sincronizados si el usuario está deshabilitado en IAM Identity Center, pero sigue activo en Google Workspace.
- Si existe un usuario en el directorio de Identity Center con el mismo nombre de usuario y correo electrónico, el usuario se sobrescribirá y sincronizará mediante SCIM desde Google Workspace.
- Hay algunas consideraciones adicionales a la hora de cambiar la fuente de identidad. Para obtener más información, consulte [the section called “Cómo cambiar de IAM Identity Center a un IdP externo”](#).

## Paso 1 Google Workspace: Configurar la aplicación SAML

1. Inicie sesión en la consola de administración de Google con una cuenta con privilegios de superadministrador.
2. En el panel de navegación izquierdo de la consola de administración de Google, elija Apps y seleccione Apps web y móviles.
3. En la lista desplegable Agregar aplicación, seleccione Buscar aplicaciones.

4. En el cuadro de búsqueda, ingrese Amazon Web Services y, a continuación, seleccione la aplicación Amazon Web Services (SAML) de la lista.
5. En la página Detalles del proveedor de identidad de Google: Amazon Web Services, puede realizar una de las siguientes acciones:
  - a. Descargar los metadatos del IdP.
  - b. Copie la URL del SSO, la URL del ID de la entidad y la información del certificado.

Necesitará el archivo XML o la información de la URL en el paso 2.

6. Antes de continuar con el siguiente paso en la consola de administración de Google, deje esta página abierta y vaya a la consola del IAM Identity Center.

## Paso 2: IAM Identity Center y Google Workspace: cambio del origen de identidad de IAM Identity Center y configuración de Google Workspace como proveedor de identidades de SAML

1. Inicie sesión en la [consola de IAM Identity Center](#) con un rol con permisos administrativos.
2. Elija Configuración en el panel de navegación izquierdo.
3. En la página Configuración, seleccione Acciones y, a continuación, seleccione Cambiar el origen de identidad.
  - Si no ha habilitado el IAM Identity Center,, consulte [Activar IAM Identity Center](#) para obtener más información. Tras activar y acceder al IAM Identity Center por primera vez, accederá al panel, donde podrá seleccionar la fuente de identidad.
4. En la página Elegir el origen de identidad, seleccione Proveedor de identidades externo y, a continuación, seleccione Siguiente.
5. Se abre la página Configurar un proveedor de identidad externo. Para completar esta página y la página de Google Workspace del paso 1, deberá completar lo siguiente:
  - En la sección metadatos del proveedor de identidad de la consola de IAM Identity Center, deberá realizar una de las siguientes acciones:
    - i. Cargue los metadatos de SAML Google como metadatos de SAML del IdP en la consola del IAM Identity Center.



- ii. Copie y pegue la URL del SSO de Google en el campo URL de inicio de sesión del IdP, la URL del emisor de Google en el campo URL del emisor del IdP y cargue el certificado de Google como certificado de IdP.
6. Tras introducir los metadatos de Google en la sección de metadatos del proveedor de identidades de la consola del IAM Identity Center, copie la URL del IAM Identity Assertion Consumer Service (ACS) y la URL del emisor del IAM Identity Center. En el siguiente paso, debe proporcionarlos URLs en la consola de Google administración.
7. Deje la página de la consola de IAM Identity Center y vuelva a la consola de administración de Google. Debería estar en la página de Amazon Web Services: detalles del proveedor de servicios. Seleccione Continuar.
8. En la página Service provider details, ingrese los valores de ACS URL y Entity ID. Ha copiado estos valores en el paso anterior y se encuentran en la consola de IAM Identity Center.
  - Pegue la URL del IAM Identity Center Assertion Consumer Service (ACS) en el campo URL de ACS.
  - Pegue la URL del emisor del IAM Identity Center en el campo ID de entidad.
9. En la página Detalles del proveedor del servicio, rellene los campos que aparecen debajo de ID de nombre de la siguiente manera:
  - En Name ID format, seleccione EMAIL.
  - En Name ID, seleccione Basic Information > Primary email.
10. Elija Continuar.
11. En la página Attribute Mapping, en Attributes, seleccione ADD MAPPING y, a continuación, configure estos campos en GoogleGoogle Directory attribute:
  - Para el atributo de la aplicación **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**, seleccione el campo Información básica, correo electrónico principal entre los atributos de Google Directory.
  - Para el atributo de la aplicación `https://aws.amazon.com/SAML/Attributes/Role`, seleccione cualquier atributo de Google Directory. Un atributo del directorio de Google podría ser Departamento.
12. Seleccione Finish.
13. Vuelva a la consola de IAM Identity Center y seleccione Siguiente. En la página Revisar y confirmar, revise la información y, a continuación, ingrese ACEPTAR en el espacio correspondiente. Elija Cambiar fuente de identidad.

Ya está listo para habilitar la aplicación de Amazon Web Services en Google Workspace para poder aprovisionar a los usuarios en IAM Identity Center.

## Paso 3: Google Workspace: habilitación de las aplicaciones

1. Vuelve a la Consola de Google administración y a tu AWS IAM Identity Center aplicación, que encontrarás en Aplicaciones y Aplicaciones web y móviles.
2. En el panel User access, junto a User access, seleccione la flecha hacia abajo para expandir User access para mostrar el panel Service status.
3. En el panel Service status, seleccione ON for everyone y, a continuación, seleccione SAVE.

### Note

Para ayudar a mantener el principio de privilegios mínimos, le recomendamos que, después de completar este tutorial, cambie Service status a OFF for everyone. Solo los usuarios que necesiten acceder a AWS deben tener el servicio habilitado. Puede usar grupos o unidades organizativas de Google Workspace para dar acceso a los usuarios a un subconjunto concreto de usuarios.

## Paso 4: IAM Identity Center: configuración del aprovisionamiento automático de IAM Identity Center

1. Vuelva a la consola de IAM Identity Center.
2. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
3. En el cuadro de diálogo de aprovisionamiento automático entrante, copie todos los valores de las opciones siguientes. En el paso 5 de este tutorial, introducirá estos valores para configurar el aprovisionamiento automático en Google Workspace.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

 Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar.

#### 4. Seleccione Cerrar.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, en el siguiente paso configurará el aprovisionamiento automático en Google Workspace.

## Paso 5: Google Workspace: configuración del aprovisionamiento automático

1. Vuelva a la consola de administración de Google y a su aplicación de AWS IAM Identity Center, que se encuentran en Apps y Apps web y móviles. En la sección Aprovisionamiento automático, elija Configurar aprovisionamiento automático.
2. En el procedimiento anterior, copió el valor del token de acceso en la consola de IAM Identity Center. Pegue ese valor en el campo Token de acceso y seleccione Continuar. Además, en el procedimiento anterior, copió el valor del punto de conexión de SCIM en la consola del IAM Identity Center. Pegue ese valor en el campo URL del punto de conexión y elija Continuar.
3. Compruebe que todos los atributos obligatorios de IAM Identity Center (los marcados con un asterisco) estén asignados a los atributos de Google Cloud Directory. Si no es así, haga clic en la flecha hacia abajo y asigne el atributo correspondiente. Elija Continuar.
4. En la sección Provisioning scope, puede seleccionar un grupo con su directorio de Google Workspace para proporcionar acceso a la aplicación de Amazon Web Services. Omita este paso y seleccione Continue.
5. En la sección Deprovisioning, puede elegir cómo responder a los diferentes eventos que impiden el acceso de un usuario. Para cada situación, puede especificar el tiempo que debe transcurrir antes de que comience el desaprovisionamiento:
  - en menos de 24 horas
  - después de un día
  - después de siete días
  - después de 30 días

Cada situación tiene una configuración de tiempo para cuándo suspender el acceso a una cuenta y cuándo eliminarla.

 Tip

Configure siempre más tiempo antes de eliminar la cuenta de un usuario que para suspenderla.

6. Seleccione Finalizar. Volverá a la página de la aplicación de Amazon Web Services.
7. En la sección Autoaprovisionamiento, active el conmutador para cambiarlo de Inactivo a Activo.

 Note

El control deslizante de activación está deshabilitado si IAM Identity Center no está activado para los usuarios. Seleccione Acceso de usuario y active la aplicación para activar el control deslizante.

8. En el cuadro de diálogo de confirmación, elija Activar.
9. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. En la página Users se muestran los usuarios de su directorio de Google Workspace que creó SCIM. Si los usuarios aún no aparecen en la lista, es posible que el aprovisionamiento aún esté en proceso. El aprovisionamiento puede tardar hasta 24 horas, aunque en la mayoría de los casos se completa en cuestión de minutos. Asegúrese de actualizar la ventana del navegador cada pocos minutos.

Seleccione un usuario y consulte sus detalles. La información debe coincidir con la información del directorio de Google Workspace.

 ¡Enhorabuena!

Ha configurado correctamente una conexión SAML entre Google Workspace y AWS y ha comprobado que el aprovisionamiento automático funciona. Ahora puede asignar a estos usuarios cuentas y aplicaciones en IAM Identity Center. Para este tutorial, en el siguiente paso designaremos a uno de los usuarios como administrador de IAM Identity Center mediante la concesión de permisos administrativos en la cuenta de administración.

## Paso de atributos para el control de acceso: opcional

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Asigne acceso a Cuentas de AWS

Los siguientes pasos solo son necesarios para conceder acceso Cuentas de AWS únicamente a. Estos pasos no son necesarios para conceder el acceso a AWS las aplicaciones de.

### Note

Para completar este paso, necesitará una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Paso 1: IAM Identity Center: conceder a los usuarios de Google Workspace acceso a las cuentas

1. Vuelva a la consola de IAM Identity Center. En el panel de navegación del IAM Identity Center, en **Permisos para varias cuentas**, seleccione **Cuentas de AWS**.

2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la raíz organizativa con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:
  - a. En Paso 1: selección de usuarios y grupos, elija el usuario que realizará la función del trabajo de administrador. A continuación, elija Siguiente.
  - b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.
    - i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:
      - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
      - En Política para un conjunto de permisos predefinido, elija AdministratorAccess.Elija Siguiente.
    - ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

La configuración predeterminada crea un conjunto de permisos *AdministratorAccess* con una duración de sesión establecida en una hora.
    - iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.
    - iv. En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.
    - v. En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de *AdministratorAccess* permisos que creó aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.
  - c. En Paso 3: revisión y envío, revise el usuario y el conjunto de permisos seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que la Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Se le devuelve a la Cuentas de AWS página de las. Un mensaje de notificación le informa de que se Cuenta de AWS ha reaprovisionado la y se ha aplicado el conjunto de permisos actualizado. Cuando el usuario inicie sesión, tendrá la opción de elegir el *AdministratorAccess* rol.

 Note

La sincronización automática de SCIM de Google Workspace solo permite el aprovisionamiento de usuarios. Por el momento, no se admite el aprovisionamiento automático de grupos. No puede crear grupos para los usuarios de Google Workspace mediante la AWS Management Console. Tras aprovisionar a los usuarios, puede crear grupos mediante el comando [create-group](#) de AWS CLI Identity Store o la API de IAM. [CreateGroup](#)

## Paso 2 Google Workspace: Confirme Google Workspace el acceso de los usuarios a los recursos AWS

1. Inicie sesión en Google con una cuenta de usuario de prueba. Para obtener información sobre cómo agregar usuarios a Google Workspace, consulte la [documentación de Google Workspace](#).
2. Seleccione el icono del lanzador de Google apps (símbolo).
3. Desplácese a la parte inferior de la lista de aplicaciones donde se encuentran las aplicaciones personalizadas de Google Workspace. Aparece la aplicación de Amazon Web Services.
4. Seleccione la aplicación Amazon Web Services. Ha iniciado sesión en el portal de AWS acceso y puede ver el Cuenta de AWS icono de. Amplíe el icono para ver la lista de a las Cuentas de AWS que puede acceder el usuario. En este tutorial, solo trabajó con una cuenta, por lo que al expandir el icono solo se muestra una cuenta.
5. Seleccione la cuenta para ver los conjuntos de permisos disponibles para el usuario. En este tutorial, creó el conjunto de AdministratorAccesspermisos.
6. Junto al conjunto de permisos hay enlaces para el tipo de acceso disponible para ese conjunto de permisos. Cuando creó el conjunto de permisos, especificó que se habilitó el acceso

mediante programación y con la Consola de administración, por lo que esas dos opciones están presentes. Seleccione Consola de administración para abrir la AWS Management Console.

7. El usuario ha iniciado sesión en la consola.

## Pasos a seguir a continuación

Ahora que ha configurado Google Workspace como proveedor de identidades y ha aprovisionado a usuarios en IAM Identity Center, puede hacer lo siguiente:

- Utilice el comando [create-group de AWS CLI](#) Identity Store o la API de IAM [CreateGroup](#) para crear grupos para sus usuarios.

Los grupos son útiles a la hora de asignar el acceso a las Cuentas de AWS y a las aplicaciones. En lugar de asignarlo a cada usuario de manera individual, concede permisos a un grupo. Más adelante, al agregar o eliminar usuarios de un grupo, el usuario obtiene o pierde de forma dinámica el acceso a las cuentas y aplicaciones que haya asignado al grupo.

- Para configurar los permisos en función de los cargos en el trabajo; consulte [Create a permission set](#).

Los conjuntos de permisos definen el nivel de acceso que tienen los usuarios y grupos en una Cuenta de AWS. Los conjuntos de permisos se almacenan en IAM Identity Center y se pueden aprovisionar a una o varias Cuentas de AWS. Puedes asignar más de un conjunto de permisos a un usuario.

### Note

Como administrador de IAM Identity Center, en ocasiones tendrá que sustituir los certificados de IdP antiguos por otros más nuevos. Por ejemplo, debe sustituir un certificado cuando se aproxime la fecha de vencimiento del certificado. El proceso de sustituir un certificado antiguo por uno más nuevo se denomina rotación de certificados. Asegúrese de revisar cómo [administrar los certificados de SAML](#) para Google Workspace.

## Solución de problemas

Para saber cómo solucionar problemas generales de SCIM y SAML con Google Workspace, consulte las secciones siguientes:



- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- Para solucionar problemas en Google Workspace, consulte la [documentación de Google Workspace](#).

Los recursos relacionados siguientes pueden ayudarle a solucionar problemas cuando trabaje con AWS:

- [AWS re:Post](#): busque recursos relacionados FAQs y enlaces a otros recursos para ayudarle a solucionar problemas.
- [AWS Support](#): obtenga soporte técnico

## Uso del centro de identidad de IAM para conectarse con su JumpCloud Plataforma de directorios

El IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de los usuarios desde JumpCloud Plataforma de directorio en el IAM Identity Center. Este aprovisionamiento utiliza el protocolo de [Lenguaje de marcado de seguridad \(SAML\) 2.0](#). Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

Esta conexión se configura en JumpCloud utilizando el punto de conexión SCIM y el token de acceso del IAM Identity Center. Al configurar la sincronización de SCIM, se crea un mapeo de los atributos de usuario en JumpCloud a los atributos nombrados en el Centro de identidades de IAM. Esto hace que los atributos esperados coincidan entre el Centro de Identidad de IAM y JumpCloud.

Esta guía se basa en JumpCloud a partir de junio de 2021. Los pasos para las versiones más recientes pueden variar. Esta guía contiene algunas notas sobre la configuración de la autenticación de usuarios mediante SAML.

En los siguientes pasos se explica cómo habilitar el aprovisionamiento automático de usuarios y grupos desde JumpCloud al IAM Identity Center mediante el protocolo SCIM.

 Note

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#). A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

## Temas

- [Requisitos previos](#)
- [Consideraciones de SCIM](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: Configurar el aprovisionamiento en JumpCloud](#)
- [\(Opcional\) Paso 3: configurar los atributos de usuario en JumpCloud para el control de acceso en IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)

## Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- JumpCloud suscripción o prueba gratuita. Para suscribirse a una versión de prueba gratuita, visite [JumpCloud](#).
- Una cuenta habilitada para IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).
- Una conexión SAML desde tu JumpCloud cuenta al Centro de Identidad de IAM, tal y como se describe en [JumpCloud documentación para el Centro de Identidad de IAM](#).
- Asocie el conector de IAM Identity Center a los grupos a los que desee permitir el acceso a las cuentas de AWS .

## Consideraciones de SCIM

Las siguientes son consideraciones a tener en cuenta a la hora de utilizar JumpCloud federación para el Centro de Identidad de IAM.

- Solo los grupos asociados al conector de inicio de sesión AWS único en JumpCloud se sincronizará con el SCIM.
- Solo se puede sincronizar un atributo de número de teléfono y el valor predeterminado es “teléfono del trabajo”.
- Usuarios en JumpCloud el directorio debe tener el nombre y los apellidos configurados para sincronizarse con el IAM Identity Center con SCIM.
- Los atributos siguen sincronizados si el usuario está deshabilitado en el Centro de Identidad de IAM, pero se siguen activando en JumpCloud.
- Si desea activar la sincronización con SCIM únicamente para la información del usuario, desmarque la opción “Habilitar la administración de grupos de usuarios y la pertenencia a grupos” en el conector.

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie el punto final y el token de acceso del SCIM. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

 Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

## 5. Seleccione Cerrar.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes mediante el JumpCloud Conector de IAM Identity Center. Estos pasos se explican en el procedimiento siguiente.

## Paso 2: Configurar el aprovisionamiento en JumpCloud

Utilice el siguiente procedimiento en JumpCloud El conector del IAM Identity Center permite el aprovisionamiento con el IAM Identity Center. En este procedimiento se presupone que ya ha añadido el JumpCloud El conector de IAM Identity Center a su JumpCloud portal de administración y grupos. Si aún no lo ha hecho, consulte los [Requisitos previos](#) y complete este procedimiento para configurar el aprovisionamiento de SCIM.

Para configurar el aprovisionamiento en JumpCloud

1. Abra el icono JumpCloud El conector del Centro de Identidad de IAM que instaló como parte de la configuración de SAML para JumpCloud (Autenticación de usuario > Centro de identidad de IAM). Consulte [Requisitos previos](#).
2. Seleccione el conector IAM Identity Center y, a continuación, elija la tercera pestaña Gestión de identidades.
3. Marque la casilla Habilitar la administración de grupos de usuarios y la pertenencia a grupos en esta aplicación si desea que los grupos se sincronicen con SCIM.
4. Haga clic en Configurar.
5. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL base del JumpCloud Conector de IAM Identity Center.
6. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Token Key del JumpCloud Conector de IAM Identity Center.

7. Haga clic en Activar para aplicar la configuración.
8. Asegúrese de tener activado un indicador verde junto a Inicio de sesión único activado.
9. Vaya a la cuarta pestaña Grupos de usuarios y marque los grupos que desee aprovisionar con SCIM.
10. Cuando haya terminado, haga clic en Guardar, en la parte inferior.
11. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Usuarios sincronizados de JumpCloud aparecen en la página de usuarios. Estos usuarios ya pueden asignarse a cuentas en IAM Identity Center.

## (Opcional) Paso 3: configurar los atributos de usuario en JumpCloud para el control de acceso en IAM Identity Center

Se trata de un procedimiento opcional para JumpCloud si decide configurar los atributos del Centro de Identidad de IAM para gestionar el acceso a sus AWS recursos. Los atributos que defina en JumpCloud se transmiten en una aserción de SAML al Centro de Identidad de IAM. A continuación, debe crear un conjunto de permisos en el Centro de Identidad de IAM para gestionar el acceso en función de los atributos de los que ha pasado JumpCloud.

Antes de iniciar este procedimiento, habilite primero la característica [Atributos para el control de acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

Para configurar los atributos de usuario en JumpCloud para el control de acceso en el IAM Identity Center

1. Abra el icono JumpCloud El conector de IAM Identity Center que instaló como parte de la configuración de SAML para JumpCloud (Autenticación de usuario > Centro de identidad de IAM).
2. Elija el conector de IAM Identity Center. A continuación, elija la segunda pestaña para IAM Identity Center.
3. En la parte inferior de esta pestaña está la asignación de atributos de usuario. Elija Añadir nuevo atributo y, a continuación siga estos pasos para cada atributo que vaya a añadir para su uso en IAM Identity Center para el control de acceso.

- a. En el campo Nombre del atributo proporcionado por el servicio, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName..`  
Reemplace **AttributeName** con el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:Email`.
  - b. En la JumpCloud Campo Nombre de atributo, elija los atributos de usuario de su JumpCloud directorio. Por ejemplo, Correo electrónico (trabajo).
4. Seleccione Guardar.

## (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Configure SAML y SCIM con Microsoft Entra ID y el Centro de identidad de IAM

AWS IAM Identity Center admite la integración con el [lenguaje de marcado para aserciones de seguridad \(SAML\) 2.0](#), así como el [aprovisionamiento automático](#) (sincronización) de la información

de usuarios y grupos desde Microsoft Entra ID (anteriormente conocido como Azure Active Directory o Azure AD) al IAM Identity Center mediante el protocolo [System for Cross-Domain Identity Management \(SCIM\) 2.0](#). Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

## Objetivo

En este tutorial, configurará un laboratorio de pruebas y configurará una conexión SAML y el aprovisionamiento de SCIM entre Microsoft Entra ID e IAM Identity Center. Durante los pasos iniciales de preparación, creará un usuario de prueba (Nikki Wolf) en ambos Microsoft Entra ID y el Centro de identidad de IAM, que utilizarás para probar la conexión SAML en ambas direcciones. Más adelante, como parte de los pasos del SCIM, crearás un usuario de prueba diferente (Richard Roe) para comprobar los nuevos atributos en Microsoft Entra ID se están sincronizando con el Centro de Identidad de IAM según lo previsto.

## Requisitos previos

Antes de empezar con este tutorial, primero tendrá que definir lo siguiente:

- A Microsoft Entra ID inquilino. Para obtener más información, consulte [Inicio rápido: configurar un inquilino](#) en Microsoft .
- Una cuenta AWS IAM Identity Center habilitada. Para más información, consulte [Activar IAM Identity Center](#) en la Guía del usuario de AWS IAM Identity Center .

## Consideraciones

Las siguientes son consideraciones importantes sobre Microsoft Entra ID esto puede afectar a la forma en que planea implementar el [aprovisionamiento automático](#) con IAM Identity Center en su entorno de producción mediante el protocolo SCIM v2.

### Aprovisionamiento automático

Antes de comenzar a implementar SCIM, le recomendamos revisar primero las [Consideraciones para utilizar el aprovisionamiento automático](#).

### Atributos para controlar el acceso

Los atributos para el control de acceso se utilizan en las políticas de permisos que determinan quién de su fuente de identidad puede acceder a sus recursos. AWS Si se elimina un atributo de un usuario en Microsoft Entra ID, ese atributo no se eliminará del usuario correspondiente en el Centro

de identidades de IAM. Se trata de una limitación conocida en Microsoft Entra ID. Si un atributo se cambia a un valor diferente (no vacío) en un usuario, ese cambio se sincronizará con el Centro de identidades de IAM.

### Agrupación anidada

La Microsoft Entra ID el servicio de aprovisionamiento de usuarios no puede leer ni aprovisionar usuarios en grupos anidados. Solo se pueden leer y aprovisionar los usuarios que sean miembros inmediatos de un grupo asignado explícitamente. Microsoft Entra ID no desglosa de forma recursiva las pertenencias a grupos de usuarios o grupos asignados indirectamente (usuarios o grupos que son miembros de un grupo asignado directamente). Para obtener más información, consulte el ámbito basado en las [tareas](#) en la Microsoft . Como alternativa, puede utilizar la sincronización AD [configurable de IAM Identity Center](#) para realizar la integración Active Directory grupos con el Centro de identidades de IAM.

### Grupos dinámicos

La Microsoft Entra ID el servicio de aprovisionamiento de usuarios puede leer y aprovisionar usuarios en grupos [dinámicos](#). Consulte a continuación un ejemplo que muestra la estructura de usuarios y grupos al utilizar grupos dinámicos y cómo se muestran en IAM Identity Center. Estos usuarios y grupos se aprovisionaron desde Microsoft Entra ID al IAM Identity Center a través de SCIM

Por ejemplo, si Microsoft Entra ID la estructura de los grupos dinámicos es la siguiente:

1. Grupo A con los miembros ua1, ua2
2. Grupo B con miembros ub1
3. Grupo C con miembros uc1
4. Grupo K con una regla para incluir a los miembros de los grupos A, B, C
5. Grupo K con una regla para incluir a los miembros de los grupos A, B, C

Después de aprovisionar la información de usuarios y grupos desde Microsoft Entra ID al IAM Identity Center a través de SCIM, la estructura será la siguiente:

1. Grupo A con los miembros ua1, ua2
2. Grupo B con miembros ub1
3. Grupo C con miembros uc1
4. Grupo K con miembros ua1, ua2, ub1, uc1
5. Grupo L con miembros ub1, uc1



Cuando configure el aprovisionamiento automático mediante grupos dinámicos, tenga en cuenta las siguientes consideraciones.

- Un grupo dinámico puede incluir un grupo anidado. Sin embargo, Microsoft Entra ID el servicio de aprovisionamiento no aplanar el grupo anidado. Por ejemplo, si tiene la siguiente Microsoft Entra ID estructura para grupos dinámicos:
  - El grupo A es un elemento principal del grupo B.
  - El grupo A tiene a ua1 como miembro.
  - El grupo B tiene a ub1 como miembro.

El grupo dinámico que incluye al grupo A solo incluirá a los miembros directos del grupo A (es decir, ua1). No incluirá de forma recursiva a los miembros del grupo B.

- Los grupos dinámicos no pueden contener otros grupos dinámicos. Para obtener más información, consulte [las limitaciones de la vista previa](#) en la Microsoft .

## Paso 1: preparación de su inquilino de Microsoft

En este paso, explicará cómo instalar y configurar su aplicación AWS IAM Identity Center empresarial y cómo asignar el acceso a una aplicación recién creada Microsoft Entra ID usuario de prueba.

### Step 1.1 >

Paso 1.1: Configurar la aplicación AWS IAM Identity Center empresarial en Microsoft Entra ID

En este procedimiento, se instala la aplicación AWS IAM Identity Center empresarial en Microsoft Entra ID. Necesitará esta aplicación más adelante para configurar su conexión SAML con AWS.

1. Inicie sesión en el [Centro de administración de Microsoft Entra](#) como mínimo como administrador de aplicaciones en la nube.
2. Vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione New application.
3. En la página Browse Microsoft Entra Gallery, ingrese **AWS IAM Identity Center** en el cuadro de búsqueda.
4. Seleccione AWS IAM Identity Center de los resultados.
5. Seleccione Crear.

## Step 1.2 >

### Paso 1.2: Crea un usuario de prueba en Microsoft Entra ID

Nikki Wolf es el nombre de tu Microsoft Entra ID usuario de prueba que creará en este procedimiento.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Users > All users.
2. Seleccione New user y, a continuación, seleccione Create new user en la parte superior de la pantalla.
3. En User principal name, ingrese **NikkiWolf** y, a continuación, seleccione el dominio y la extensión que desee. Por ejemplo, NikkiWolf@*example.org*.
4. En Display name, ingrese **NikkiWolf**.
5. En Password, ingrese una contraseña segura o seleccione el icono del ojo para mostrar la contraseña que se generó automáticamente y copie o anote el valor que aparece.
6. Seleccione Properties y, en Name, ingrese **Nikki**. En Last name, ingrese **Wolf**.
7. Elija Review + create y, a continuación, seleccione Create.

## Step 1.3

### Paso 1.3: Pon a prueba la experiencia de Nikki antes de asignar sus permisos a AWS IAM Identity Center

En este procedimiento, verificará que Nikki puede iniciar sesión correctamente en el [portal Mi cuenta](#) de Microsoft.

1. En el mismo navegador, abra una pestaña nueva, vaya a la página de inicio de sesión del [portal Mi cuenta](#) e ingrese la dirección de correo electrónico completa de Nikki. Por ejemplo, NikkiWolf@*example.org*
2. Cuando se le pida, ingrese la contraseña de Nikki y, a continuación, seleccione Sign in. Si se trata de una contraseña generada automáticamente, se le solicitará que la cambie.
3. En la página Action Required, seleccione Ask later para omitir la solicitud de métodos de seguridad adicionales.
4. En la página Mi cuenta, en el menú de navegación izquierdo, seleccione Mis aplicaciones. Tenga en cuenta que, además de los complementos, no se muestra ninguna aplicación en

este momento. Agregará una aplicación de AWS IAM Identity Center que aparecerá aquí en un paso posterior.

## Step 1.4

### Paso 1.4: Asigne permisos a Nikki en Microsoft Entra ID

Ahora que ha comprobado que Nikki puede acceder correctamente al portal Mi cuenta, utilice este procedimiento para asignar su usuario a la aplicación de AWS IAM Identity Center.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center en la lista.
2. A la izquierda, seleccione Users and groups.
3. Elija Agregar usuario o grupo. Puede ignorar el mensaje que indica que los grupos no están disponibles para su asignación. En este tutorial no se utilizan grupos para las asignaciones.
4. En la página Add Assignment, en Users, seleccione None Selected.
5. Seleccione y NikkiWolf, a continuación, elija Seleccionar.
6. En la página Añadir tarea, elija Asignar. NikkiWolf ahora aparece en la lista de usuarios que están asignados a la AWS IAM Identity Center aplicación.

## Paso 2: Prepara tu AWS cuenta

En este paso, explicará cómo usarla IAM Identity Center para configurar los permisos de acceso (mediante un conjunto de permisos), cree manualmente el usuario correspondiente de Nikki Wolf y asígnele los permisos necesarios para administrar los AWS recursos.

### Step 2.1 >

#### Paso 2.1: Crea un conjunto de RegionalAdmin permisos en IAM Identity Center

Este conjunto de permisos se utilizará para conceder a Nikki los permisos de AWS cuenta necesarios para gestionar las regiones desde la página de la cuenta del AWS Management Console. De forma predeterminada, todos los demás permisos para ver o administrar cualquier otra información de la cuenta de Nikki están denegados.

1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.

3. Elija Crear conjunto de permisos.
4. En la página Seleccionar el tipo de conjunto de permisos, seleccione Conjunto de permisos personalizado y seleccione Siguiente.
5. Seleccione Política insertada para ampliarla y, a continuación, siga estos pasos para crear una política para el conjunto de permisos:
  - a. Seleccione Agregar nueva instrucción para crear una instrucción de política.
  - b. En Editar instrucción, seleccione Cuenta de la lista y, a continuación, seleccione las siguientes casillas de verificación.

- **ListRegions**

- **GetRegionOptStatus**

- **DisableRegion**

- **EnableRegion**

- c. Junto a Agregar un recurso, elija Agregar.
- d. En la página Agregar recurso, en Tipo de recurso, seleccione Todos los recursos y, a continuación, seleccione Agregar recurso. Compruebe que la política sea similar a la siguiente:

```
{
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "account:ListRegions",
        "account:DisableRegion",
        "account:EnableRegion",
        "account:GetRegionOptStatus"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

6. Elija Siguiente.

7. En la página Especificar los detalles del conjunto de permisos, en Nombre de conjunto de permisos, escriba **RegionalAdmin** y, a continuación, seleccione Siguiente.
8. En la página Review and create (Revisar y crear), elija Create (Crear). Debería RegionalAdmin aparecer en la lista de conjuntos de permisos.

## Step 2.2 >

### Paso 2.2: Cree el NikkiWolf usuario correspondiente en IAM Identity Center

Dado que el protocolo SAML no proporciona un mecanismo para consultar el IdP (Microsoft Entra ID) y cree usuarios automáticamente aquí, en el Centro de Identidad de IAM, utilice el siguiente procedimiento para crear manualmente un usuario en el Centro de Identidad de IAM que refleje los atributos principales del usuario de Nikki Wolf en Microsoft Entra ID.

1. Abra la [consola de IAM Identity Center](#).
2. Seleccione Usuarios, Agregar usuario y, a continuación, proporcione la siguiente información:
  - a. Tanto para el nombre de usuario como para la dirección de correo electrónico: introduce la misma **NikkiWolf@yourcompanydomain.extension** que utilizaste al crear tu Microsoft Entra ID usuario. Por ejemplo, NikkiWolf@example.org.
  - b. Confirmar dirección de correo electrónico: vuelva a ingresar la dirección de correo electrónico del paso anterior
  - c. Nombre: ingrese **Nikki**.
  - d. Apellidos: ingrese **Wolf**.
  - e. Nombre de visualización: ingrese **Nikki Wolf**.
3. Seleccione Siguiente dos veces, y a continuación, seleccione Agregar usuario.
4. Seleccione Close (Cerrar).

## Step 2.3

### Paso 2.3: Asigne a Nikki el conjunto de RegionalAdmin permisos en IAM Identity Center

Aquí encontrará el lugar Cuenta de AWS en el que Nikki administrará las regiones y, a continuación, asignará los permisos necesarios para que pueda acceder correctamente al portal de AWS acceso.

1. Abra la [consola de IAM Identity Center](#)

2. En Permisos para varias cuentas, elija Cuentas de AWS.
3. Seleccione la casilla de verificación situada junto al nombre de la cuenta (por ejemplo *Sandbox*) a la que quiere conceder a Nikki el acceso para gestionar las regiones y, a continuación, seleccione Asignar usuarios y grupos.
4. En la página Asignar usuarios y grupos, seleccione la pestaña Usuarios, busque y marque la casilla situada junto a Nikki y, a continuación, seleccione Siguiente.

5.  
Example

<caption>On the Seleccione conjuntos de permisos page, choose the RegionalAdmin permission set created in Step 2.1, and then choose Next.</caption>

6. En la página Revisar y enviar, revise sus selecciones y, a continuación, elija Enviar.

## Paso 3: configuración y prueba de la conexión SAML

En este paso, configura la conexión SAML mediante la aplicación AWS IAM Identity Center empresarial en Microsoft Entra ID junto con la configuración del IdP externo en el Centro de identidad de IAM.

### Step 3.1 >

Paso 3.1: recopilación de los metadatos del proveedor de servicios necesarios de IAM Identity Center

En este paso, iniciará el asistente para cambiar la fuente de identidad desde la consola del IAM Identity Center y recuperará el archivo de metadatos y la URL de inicio de sesión AWS específica que deberá introducir al configurar la conexión con Microsoft Entra ID en el siguiente paso.

1. En la [consola de IAM Identity Center](#), elija Configuración.
2. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, Cambiar fuente de identidad.
3. En la página Elegir el origen de identidad, seleccione Proveedor de identidades externo y, a continuación, seleccione Siguiente.
4. En la página Configurar un proveedor de identidad externo, en Metadatos del proveedor de servicios, seleccione Descargar el archivo de metadatos para descargarlo el archivo XML.
5. En la misma sección, busque el valor de URL de inicio de sesión del portal de acceso de AWS y cópielo. Deberá ingresar este valor en el siguiente paso cuando se le pida.

6. Deje esta página abierta y continúe con el paso siguiente (**Step 3.2**) para configurar la aplicación AWS IAM Identity Center empresarial en Microsoft Entra ID. Más adelante, volverás a esta página para completar el proceso.

### Step 3.2 >

#### Paso 3.2: Configure la aplicación AWS IAM Identity Center empresarial en Microsoft Entra ID

Este procedimiento establece la mitad de la conexión SAML en Microsoft mediante los valores del archivo de metadatos y la URL de inicio de sesión que obtuvo en el último paso.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. En el panel de la izquierda, elija 2. Configure el inicio de sesión único.
3. En la página Configurar el inicio de sesión único con SAML, seleccione SAML. Luego, seleccione Subir archivo de metadatos, seleccione el icono de la carpeta, seleccione el archivo de metadatos del proveedor de servicios que descargó en el paso anterior y, a continuación, seleccione Agregar.
4. En la página de configuración básica de SAML, compruebe que los valores del identificador y de la URL de respuesta apuntan ahora a los puntos finales AWS que empiezan por. `https://<REGION>.signin.aws.amazon.com/platform/saml/`
5. En Sign on URL (Optional), pegue el valor de URL de inicio de sesión del portal de acceso de AWS que copió en el paso anterior (**Step 3.1**), seleccione Save y, a continuación, seleccione X para cerrar la ventana.
6. Si se te pide que pruebes el inicio de sesión único con AWS IAM Identity Center, selecciona No, lo probaré más tarde. Realizará esta verificación en un paso posterior.
7. En la página Set up Single Sign-On with SAML, en la sección SAML Certificates, junto a Federation Metadata XML, seleccione Download para guardar el archivo de metadatos en el sistema. Deberá cargar este archivo en el siguiente paso cuando se le pida.

### Step 3.3 >

#### Paso 3.3: Configura el Microsoft Entra ID IdP externo en AWS IAM Identity Center

Aquí volverá al asistente Cambiar el origen de identidad de la consola de IAM Identity Center para completar la segunda mitad de la conexión SAML en AWS.

1. Vuelva a la sesión del navegador que dejó abierta en **Step 3.1** en la consola de IAM Identity Center.
2. En la página Configurar un proveedor de identidad externo, en la sección Metadatos del proveedor de identidad, en Metadatos SAML del IdP, pulse el botón Elegir archivo y seleccione el archivo de metadatos del proveedor de identidad que descargó desde Microsoft Entra ID en el paso anterior y, a continuación, selecciona Abrir.
3. Elija Siguiente.
4. Cuando haya leído el aviso legal y tenga todo listo para continuar, ingrese **ACCEPT**.
5. Seleccione Cambiar el origen de identidad para aplicar los cambios.

### Step 3.4 >

#### Paso 3.4: comprobación de que Nikki se redirige al portal de acceso de AWS

En este procedimiento, probará la conexión SAML; para ello, iniciará sesión en el portal Mi cuenta de Microsoft con las credenciales de Nikki. Una vez autenticado, seleccionará la AWS IAM Identity Center aplicación que redirigirá a Nikki al portal de AWS acceso.

1. Vaya a la página de inicio de sesión del [portal Mi cuenta](#) e ingrese la dirección de correo electrónico completa de Nikki. Por ejemplo, **NikkiWolf** @ *example.org*
2. Cuando se le pida, ingrese la contraseña de Nikki y, a continuación, seleccione Sign in.
3. En la página Mi cuenta, en el menú de navegación izquierdo, seleccione Mis aplicaciones.
4. En la página My Apps, seleccione la aplicación denominada AWS IAM Identity Center. Esto debería solicitarle una autenticación adicional.
5. En la página de inicio de sesión de Microsoft, elige tus NikkiWolf credenciales. Si se te solicita la autenticación por segunda vez, vuelve a elegir tus NikkiWolf credenciales. Esto debería redirigirlo automáticamente al portal de AWS acceso.

#### Tip

Si no se le redirige correctamente, compruebe que el valor de URL de inicio de sesión del portal de acceso de AWS que ha ingresado en **Step 3.2** coincide con el valor que ha copiado en **Step 3.1**.

6. Compruebe que su Cuentas de AWS pantalla.



 Tip

Si la página está vacía y no se Cuentas de AWS muestra, confirme que Nikki se ha asignado correctamente al conjunto de RegionalAdminpermisos (consulte **Step 2.3**).

## Step 3.5

## Paso 3.5: comprobación del nivel de acceso de Nikki para administrar su Cuenta de AWS

En este paso, comprobará el nivel de acceso de Nikki para administrar la configuración regional de su Cuenta de AWS. Nikki solo debe tener los privilegios de administrador suficientes para administrar las regiones desde la página Cuentas.

1. En el portal de AWS acceso, seleccione la pestaña Cuentas para ver la lista de cuentas. Aparecen los nombres de las cuentas IDs, las cuentas y las direcciones de correo electrónico asociadas a las cuentas en las que haya definido conjuntos de permisos.
2. Elija el nombre de la cuenta (por ejemplo *Sandbox*) en la que aplicó el conjunto de permisos (consulte **Step 2.3**). Esto ampliará la lista de conjuntos de permisos entre los que Nikki puede elegir para administrar su cuenta.
3. Luego, RegionalAdmin elija la consola de administración para asumir la función que definió en el conjunto de RegionalAdminpermisos. Esto le redirige a la página de inicio de la AWS Management Console .
4. En la esquina superior derecha de la consola, seleccione el nombre de cuenta y, a continuación, seleccione Cuenta. El enlace le dirigirá a la página Cuenta. Observe que en todas las demás secciones de esta página aparece un mensaje en el que se indica que no tiene los permisos necesarios para ver ni modificar esos ajustes.
5. En la página Cuenta, desplácese hacia abajo hasta la sección Regiones de AWS . Seleccione la casilla de verificación de cualquier región disponible en la tabla. Tenga en cuenta que Nikki tiene los permisos necesarios para habilitar o deshabilitar la lista de regiones de su cuenta, tal y como estaba previsto.

 ¡Bien hecho!

Los pasos del 1 al 3 lo ayudaron a implementar y probar correctamente la conexión SAML. Ahora, para completar el tutorial, le recomendamos que continúe con el paso 4 para implementar el aprovisionamiento automático.

## Paso 4: configuración y comprobación de la sincronización de SCIM

En este paso, configurará el [aprovisionamiento automático](#) (sincronización) de la información del usuario desde Microsoft Entra ID al IAM Identity Center mediante el protocolo SCIM v2.0. Esta conexión se configura en Microsoft Entra ID utilizando su terminal SCIM para el IAM Identity Center y un token portador creado automáticamente por el IAM Identity Center.

Al configurar la sincronización de SCIM, se crea un mapeo de los atributos de usuario en Microsoft Entra ID a los atributos nombrados en el Centro de identidades de IAM. Esto hace que los atributos esperados coincidan entre el Centro de Identidad de IAM y Microsoft Entra ID.

Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de los usuarios que residen principalmente en Microsoft Entra ID al IAM Identity Center mediante la aplicación IAM Identity Center en Microsoft Entra ID.

### Step 4.1 >

#### Paso 4.1: Cree un segundo usuario de prueba en Microsoft Entra ID

Para realizar las pruebas, creará un nuevo usuario (Richard Roe) en Microsoft Entra ID. Más adelante, después de configurar la sincronización con SCIM, comprobará que este usuario y todos los atributos relevantes se han sincronizado correctamente con el IAM Identity Center.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Users > All users.
2. Seleccione New user y, a continuación, seleccione Create new user en la parte superior de la pantalla.
3. En User principal name, ingrese **RichRoe** y, a continuación, seleccione el dominio y la extensión que desee. Por ejemplo, @. RichRoe~~example~~.org
4. En Display name, ingrese **RichRoe**.

5. En Password, ingrese una contraseña segura o seleccione el icono del ojo para mostrar la contraseña que se generó automáticamente y copie o anote el valor que aparece.
6. Seleccione Properties y, a continuación, facilite los siguientes valores:
  - First name: ingrese **Richard**.
  - Last name: ingrese **Roe**.
  - Job title: ingrese **Marketing Lead**.
  - Department: ingrese **Sales**.
  - Employee ID: ingrese **12345**.
7. Elija Review + create y, a continuación, seleccione Create.

## Step 4.2 >

### Paso 4.2: habilitación del aprovisionamiento automático en IAM Identity Center

En este procedimiento, utilizará la consola del IAM Identity Center para habilitar el aprovisionamiento automático de los usuarios y grupos procedentes de Microsoft Entra ID al Centro de identidades de IAM.

1. Abra la [consola de IAM Identity Center](#) y seleccione Configuración en el panel izquierdo de navegación.
2. En la página Configuración, en la pestaña Origen de identidad, observe que Método de aprovisionamiento está establecido en Manual.
3. Busque el cuadro de información Aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie todos los valores de las opciones siguientes. Deberá pegarlos en el siguiente paso cuando configure el aprovisionamiento en Microsoft Entra ID.
  - a. Punto final SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

 Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar.

5. Seleccione Cerrar.
6. En la pestaña Origen de identidad, observe que Método de aprovisionamiento ahora está establecido en SCIM.

## Step 4.3 &gt;

## Paso 4.3: Configurar el aprovisionamiento automático en Microsoft Entra ID

Ahora que ha establecido su usuario de RichRoe prueba y ha activado el SCIM en el IAM Identity Center, puede continuar con la configuración de los ajustes de sincronización del SCIM en Microsoft Entra ID.

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. Seleccione Provisioning y, en Manage, vuelva a seleccionar Provisioning.
3. En Provisioning Mode, seleccione Automatic.
4. En Admin Credentials, en Tenant URL, pegue el valor de la URL de Punto de conexión de SCIM que copió anteriormente en **Step 4.2**. En Secret Token, pegue el valor de Access token.
5. Elija Test Connection. Debería ver un mensaje que indica que las credenciales probadas se autorizaron correctamente para habilitar el aprovisionamiento.
6. Seleccione Save.
7. En Manage, seleccione Users and groups y, a continuación, seleccione Add user/group.
8. En la página Add Assignment, en Users, seleccione None Selected.
9. Seleccione y, a continuación RichRoe, elija Seleccionar.
10. En la página Agregar asignación, elija Asignar.
11. Seleccione Overview y, a continuación, seleccione Start provisioning.

## Step 4.4

### Paso 4.4: comprobación de que se ha producido la sincronización

En esta sección, verificará que el usuario de Richard se aprovisionó correctamente y que todos los atributos se muestran en IAM Identity Center.

1. En la [consola de IAM Identity Center](#), seleccione Usuarios.
2. En la página de usuarios, debería aparecer su RichRoeusuario. Observe que, en la columna Creado por, el valor está establecido en SCIM.
3. Seleccione RichRoe, en Perfil, comprobar que los siguientes atributos se hayan copiado de Microsoft Entra ID.
  - Nombre: **Richard**.
  - Apellido: **Roe**.
  - Departamento: **Sales**.
  - Título: **Marketing Lead**.
  - Número de empleado: **12345**.

Ahora que el usuario de Richard se ha creado en IAM Identity Center, puede asignarlo a cualquier conjunto de permisos para controlar el nivel de acceso que tiene a sus recursos de AWS . Por ejemplo, puede asignar RichRoeal conjunto de **RegionalAdmin** permisos que utilizó anteriormente para conceder a Nikki los permisos para administrar regiones (consulte **Step 2.3**) y, a continuación, probar su nivel de acceso utilizando **Step 3.5**.

#### ¡Enhorabuena!

Has configurado correctamente una conexión SAML entre Microsoft AWS y has comprobado que el aprovisionamiento automático funciona para mantener todo sincronizado. Ahora puede aplicar lo aprendido para configurar su entorno de producción de forma más fluida.

## Paso 5: Configurar ABAC: opcional

Ahora que se ha configurado SAML y SCIM, puede optar por configurar el control de acceso basado en atributos (ABAC). El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos basados en atributos.

With Microsoft Entra ID, puede utilizar cualquiera de los dos métodos siguientes para configurar ABAC para su uso con el IAM Identity Center.

### Configure user attributes in Microsoft Entra ID for access control in IAM Identity Center

Configure los atributos de usuario en Microsoft Entra ID para el control de acceso en el IAM Identity Center

En el siguiente procedimiento, determinará qué atributos hay Microsoft Entra ID el IAM Identity Center debe utilizarlos para gestionar el acceso a sus AWS recursos. Una vez definido, Microsoft Entra ID envía estos atributos al centro de identidad de IAM mediante aserciones de SAML. A continuación, tendrá que ir al Centro de Identidad de IAM para gestionar el acceso [Crea un conjunto de permisos](#), en función de los atributos de los que ha pasado Microsoft Entra ID.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. Elija Single sign-on (Inicio de sesión único).
3. En la sección Attributes & Claims, elija Edit.
4. En la página Attributes & Claims, haga lo siguiente:
  - a. Elija Añadir nueva reclamación.
  - b. En Nombre, escriba `AccessControl:AttributeName`. Sustituya `AttributeName` por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `AccessControl:Department`.
  - c. En Namespace (Espacio de nombres), escriba `https://aws.amazon.com/SAML/Attributes`.
  - d. En Source (Origen), elija Attribute (Atributo).

- e. En el caso del atributo Fuente, utilice la lista desplegable para elegir el Microsoft Entra ID atributos de usuario. Por ejemplo, `user.department`.
5. Repita el paso anterior para cada atributo que necesite enviar a IAM Identity Center en la aserción SAML.
6. Seleccione Save.

## Configure ABAC using IAM Identity Center

### Configuración de ABAC con IAM Identity Center

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un conjunto de `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `Department=billing`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/
AccessControl:Department">
<saml:AttributeValue>billing
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Asigne acceso a Cuentas de AWS

Los siguientes pasos solo son necesarios para conceder acceso Cuentas de AWS únicamente a. Estos pasos no son necesarios para conceder el acceso a AWS las solicitudes.

 Note

Para completar este paso, necesitará una instancia organizativa de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Paso 1: Centro de identidad de IAM: subvención Microsoft Entra ID acceso de los usuarios a las cuentas

1. Vuelva a la consola de IAM Identity Center. En el panel de navegación del IAM Identity Center, en Permisos para varias cuentas, seleccione Cuentas de AWS.
2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la raíz organizativa con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:
  - a. En Paso 1: selección de usuarios y grupos, elija el usuario que realizará la función del trabajo de administrador. A continuación, elija Siguiente.
  - b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.
    - i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:
      - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
      - En Política para un conjunto de permisos predefinido, elija AdministratorAccess.

Elija Siguiente.

- ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

La configuración predeterminada crea un conjunto de permisos denominado **AdministratorAccess** con una duración de sesión establecida en una hora.

- iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página



Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.

- iv. En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.
- v. En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de **AdministratorAccess** permisos que creó aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.
- c. En Paso 3: revisión y envío, revise el usuario y el conjunto de permisos seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Volverá a la Cuentas de AWS página. Un mensaje de notificación le informa de que se Cuenta de AWS ha vuelto a aprovisionar y se ha aplicado el conjunto de permisos actualizado. Cuando el usuario inicie sesión, tendrá la opción de elegir el **AdministratorAccess** rol.

## Paso 2: Microsoft Entra ID: Confirma Microsoft Entra ID el acceso de los usuarios a AWS los recursos

1. Regrese a la Microsoft Entra IDconsola y navegue hasta la aplicación de inicio de sesión basada en SAML de IAM Identity Center.
  2. Seleccione Usuarios y grupos y seleccione Añadir usuarios o grupos. Añadirá el usuario que creó en este tutorial en el paso 4 a Microsoft Entra ID "Hello, World!". Al añadir el usuario, le permitirá iniciar sesión en él. AWS Busca el usuario que creaste en el paso 4. Si hubiera seguido este paso, sería **RichardRoe**.
- Para ver una demostración, consulte [Federar su instancia de IAM Identity Center existente con Microsoft Entra ID](#)

## Solución de problemas

Para solucionar problemas generales de SCIM y SAML con Microsoft Entra ID, consulte las siguientes secciones:

- [Problemas de sincronización con Microsoft Entra ID y el Centro de identidad de IAM](#)
- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- [Recursos adicionales](#)

## Problemas de sincronización con Microsoft Entra ID y el Centro de identidad de IAM

Si tiene problemas con Microsoft Entra ID los usuarios no se sincronizan con el Centro de Identidad de IAM, puede deberse a un problema de sintaxis que el Centro de Identidad de IAM ha detectado cuando se añade un nuevo usuario al Centro de Identidad de IAM. Puede confirmarlo consultando la Microsoft Entra ID registros de auditoría de eventos fallidos, como un 'Export'. El motivo del estado de este evento indicará:

```
{"schema":["urn:ietf:params:scim:api:messages:2.0:Error"],"detail":"Request is unparsable, syntactically incorrect, or violates schema.","status":"400"}
```

También puede comprobar AWS CloudTrail el evento fallido. Para ello, busque en la consola del historial de eventos o CloudTrail utilice el siguiente filtro:

```
"eventName":"CreateUser"
```

El error del CloudTrail evento indicará lo siguiente:

```
"errorCode": "ValidationException",  
  "errorMessage": "Currently list attributes only allow single item"
```

En última instancia, esta excepción significa que uno de los valores transferidos desde Microsoft Entra ID contenía más valores de los previstos. La solución consiste en revisar los atributos del usuario en Microsoft Entra ID, asegurándose de que ninguno contenga valores duplicados. Un ejemplo habitual de valores duplicados es la presencia de varios valores en los números de contacto, como el número de móvil, del trabajo y el fax. Aunque son valores independientes, todos se transfieren al IAM Identity Center con el atributo principal phoneNumbers.

Para obtener sugerencias generales acerca de la solución de problemas de SCIM, consulte [Resolución de problemas](#).

## Microsoft Entra ID Sincronización de cuentas de invitado

Si desea sincronizar su Microsoft Entra ID los usuarios invitados al Centro de identidad de IAM, consulten el siguiente procedimiento.

Microsoft Entra ID el correo electrónico de los usuarios invitados es diferente a Microsoft Entra ID usuarios. Esta diferencia provoca problemas al intentar sincronizar Microsoft Entra ID usuarios invitados con el centro de identidad de IAM. Por ejemplo, consulte la siguiente dirección de correo electrónico para un usuario invitado:

`exampleuser_domain.com#EXT@domain.onmicrosoft.com.`

El Centro de Identidad de IAM espera que la dirección de correo electrónico de un usuario no contenga ese formato. *EXT@domain*

1. En la consola del [Centro de administración de Microsoft Entra](#), vaya a Identity > Applications > Enterprise applications y, a continuación, seleccione AWS IAM Identity Center.
2. Diríjase a la pestaña Inicio de sesión único en el panel izquierdo.
3. Seleccione Editar, que aparece junto a Atributos y notificaciones del usuario.
4. Seleccione un Identificador de usuario único (ID de nombre) después de las Notificaciones obligatorias.
5. Creará dos condiciones de reclamación para su Microsoft Entra ID usuarios y usuarios invitados:
  - a. En Microsoft Entra ID usuarios, cree un tipo de usuario para los miembros con el atributo de origen establecido en `user.userprincipalname`.
  - b. En Microsoft Entra ID usuarios invitados, creen un tipo de usuario para invitados externos con el atributo de origen establecido en `user.mail`.
  - c. Seleccione Guardar y vuelva a intentar iniciar sesión como Microsoft Entra ID usuario invitado.

## Recursos adicionales

- Para obtener sugerencias generales acerca de la solución de problemas de SCIM, consulte [Resolución de problemas de IAM Identity Center](#).

- En Microsoft Entra ID solución de problemas, consulte [Microsoft documentación](#).
- Para obtener más información sobre la federación entre varias Cuentas de AWS, consulte [Asegurar Cuentas de AWS con Azure Active Directory Federation](#).

Los siguientes recursos pueden ayudarle a solucionar problemas a medida que trabaja con AWS:

- [AWS re:Post](#)- Busca otros recursos FAQs y enlaces a ellos para ayudarte a solucionar problemas.
- [AWS Support](#): obtenga soporte técnico

## Configuración de SAML y SCIM con Okta e IAM Identity Center

Puede aprovisionar o sincronizar la información de usuarios y grupos desde Okta a IAM Identity Center de forma automática mediante el protocolo del [sistema de administración de identidades entre dominios \(SCIM\) 2.0](#). Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

Esta conexión se configura en Okta, mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario en Okta con los atributos nombrados en IAM Identity Center. Esta asignación vincula los atributos de usuario esperados entre IAM Identity Center y su cuenta de Okta.

Okta admite las siguientes características de aprovisionamiento cuando se conecta al IAM Identity Center a través de SCIM:

- Crear usuarios: los usuarios asignados a la aplicación IAM Identity Center Okta se aprovisionan en IAM Identity Center.
- Actualizar los atributos de usuario: los cambios en los atributos de los usuarios que están asignados a la aplicación IAM Identity Center Okta se actualizan en IAM Identity Center.
- Desactivar usuarios: los usuarios que no están asignados en la aplicación IAM Identity Center Okta están deshabilitados en IAM Identity Center.
- Transferencia de grupos: los grupos (y sus miembros) de Okta se sincronizan con IAM Identity Center.

 Note

Para minimizar la sobrecarga administrativa tanto en Okta como en IAM Identity Center, le recomendamos que asigne y transfiera grupos en lugar de usuarios individuales.

## Objetivo

En este tutorial, seguirá las indicaciones para configurar una conexión SAML con IAM Identity Center en Okta. Más adelante, sincronizará los usuarios desde Okta mediante SCIM. En este escenario, administrará todos los usuarios y grupos en Okta. Los usuarios inician sesión a través del portal de Okta. Para comprobar que todo está configurado correctamente, tras completar los pasos de configuración, iniciará sesión como Okta usuario y verificará el acceso a AWS los recursos de.

 Note

Puede registrarse para obtener una cuenta de Okta ([prueba gratuita](#)) que tenga instalada la [aplicación IAM Identity Center](#) de Okta. En el caso de los productos de pago de Okta, es posible que deba confirmar que su licencia de Okta admite la administración del ciclo de vida o capacidades similares que permitan el aprovisionamiento saliente. Estas características pueden ser necesarias para configurar SCIM desde Okta a IAM Identity Center. Si aún no ha habilitado IAM Identity Center, consulte [Activar IAM Identity Center](#).

## Consideraciones

- Antes de configurar el aprovisionamiento de SCIM entre Okta e IAM Identity Center, le recomendamos revisar primero [Consideraciones para utilizar el aprovisionamiento automático](#).
- Todos los usuarios de Okta deben tener un valor especificado para Nombre, Apellidos, Nombre de usuario y Nombre de visualización.
- Cada usuario de Okta tiene un único valor por atributo de datos, como la dirección de correo electrónico o el número de teléfono. Los usuarios que tengan varios valores no se sincronizarán. Si hay usuarios que tienen varios valores en sus atributos, elimine los atributos duplicados antes de intentar aprovisionar el usuario en IAM Identity Center. Por ejemplo, solo se puede sincronizar un atributo de número de teléfono. Como el atributo de número de teléfono predeterminado es

“teléfono del trabajo”, utilice el atributo “teléfono del trabajo” para almacenar el número de teléfono del usuario, incluso si el número de teléfono del usuario es un teléfono fijo o móvil.

- Cuando se utiliza Okta con IAM Identity Center, este se configura generalmente como una aplicación en Okta. Esto le permite configurar varias instancias de IAM Identity Center como múltiples aplicaciones, lo que permite el acceso a varias organizaciones de AWS , dentro de una sola instancia de Okta.
- Los derechos y los atributos de rol no son compatibles y no se pueden sincronizar con IAM Identity Center.
- Actualmente, no es posible usar el mismo grupo de Okta para la transferencia de tareas y grupos. Para mantener una pertenencia uniforme a los grupos entre Okta e IAM Identity Center, cree un grupo independiente y configúrelo para enviar grupos a IAM Identity Center.

## Paso 1: Okta: obtención de los metadatos de SAML de su cuenta de Okta

1. Inicie sesión en el Okta admin dashboard, expanda Applications y, a continuación, seleccione Applications.
2. En la página Applications, elija Browse App Catalog (Examinar catálogo de aplicaciones).
3. En el cuadro de búsqueda AWS IAM Identity Center, escriba y seleccione la aplicación para agregar la aplicación IAM Identity Center.
4. Seleccione la pestaña Sign On.
5. En SAML Signing Certificates, seleccione Actions y, a continuación, View IdP Metadata. Se abre una nueva pestaña del navegador en la que se muestra el árbol de documentos de un archivo XML. Seleccione todo el XML de `<md:EntityDescriptor>` a `</md:EntityDescriptor>` y cópielo en un archivo de texto.
6. Guarde el archivo de texto como `metadata.xml`.

Deje el Okta admin dashboard abierto; seguirá usando esta consola en los pasos posteriores.

## Paso 2: IAM Identity Center: configuración de Okta como origen de identidad para IAM Identity Center

1. Abra la [consola de IAM Identity Center](#) como usuario con privilegios administrativos.
2. Elija Configuración en el panel de navegación izquierdo.

3. En la página Configuración, seleccione Acciones y, a continuación, seleccione Cambiar el origen de identidad.
4. En Elegir la fuente de identidad, seleccione Proveedor de identidades externo y, a continuación, Siguiente.
5. En Configurar un proveedor de identidad externo, haga lo siguiente:
  - a. En Metadatos del proveedor de servicios, seleccione Descargar archivo de metadatos para descargar el archivo de metadatos de IAM Identity Center y guardarlo en el sistema. Proporcionará el archivo de metadatos de SAML de IAM Identity Center a Okta más adelante en este tutorial.

Copie los siguientes elementos en un archivo de texto para acceder a ellos fácilmente:

- URL del Servicio de consumidor de aserciones (ACS) de IAM Identity Center
- URL del emisor de IAM Identity Center

Necesitará estos valores más adelante en este tutorial.

- b. En Metadatos del proveedor de identidad, en Metadatos SAML del IdP, seleccione Elegir archivo y, a continuación, seleccione el archivo metadata.xml que creó en el paso anterior.
  - c. Elija Siguiente.
6. Cuando haya leído el aviso legal, introduzca ACCEPT para continuar.
7. Elija Cambiar fuente de identidad.

Deje la AWS consola de abierta; seguirá usándola en el próximo paso.

8. Vuelva a la pestaña Iniciar sesión de la AWS IAM Identity Center aplicación Okta admin dashboard y, a continuación, seleccione Editar.
9. En Advanced Sign-on Settings, ingrese lo siguiente:
  - En el campo ACS URL, ingrese el valor que ha copiado de URL del Servicio de consumidor de aserciones (ACS) de IAM Identity Center.
  - En Issuer URL, ingrese el valor que ha copiado de URL del emisor de IAM Identity Center.
  - En Application username format, seleccione una de las opciones del menú.

Asegúrese de que el valor que elija sea único para cada usuario. Para este tutorial, seleccione Okta username.

## 10. Seleccione Save.

Ya tiene todo listo para aprovisionar a usuarios desde Okta a IAM Identity Center. Deje el Okta admin dashboard abierto y vuelva a la consola de IAM Identity Center para continuar con el siguiente paso.

## Paso 3: IAM Identity Center and Okta: aprovisionar usuarios de Okta

1. En la consola de IAM Identity Center, en la página Configuración, busque el cuadro de información Aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión de SCIM y el token de acceso.
2. En el cuadro de diálogo Aprovisionamiento automático entrante, copie cada uno de los valores de las siguientes opciones:
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

### Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en Okta más adelante en este tutorial.

3. Seleccione Cerrar.
4. Vuelva al Okta admin dashboard y acceda a la aplicación IAM Identity Center.
5. En la página de la aplicación IAM Identity Center, seleccione la pestaña Aprovisionamiento y, a continuación, en el menú de navegación de la izquierda, en Configuración, seleccione Integración.
6. Seleccione Edit y, a continuación, active la casilla de verificación situada junto a Enable API integration para habilitar el aprovisionamiento automático.
7. Configure Okta con los valores de aprovisionamiento de SCIM de AWS IAM Identity Center que copió anteriormente en este paso:
  - a. En el campo Base URL, ingrese el valor de Punto de conexión de SCIM.



- b. En el campo API Token, ingrese el valor de Token de acceso.
8. Elija Verificar credenciales de API para comprobar que las credenciales introducidas son válidas.  
  
Aparecerá el mensaje AWS IAM Identity Center was verified successfully!.
9. Seleccione Save. Pasará a la sección de Configuración, con Integración seleccionada.
10. En Configuración, seleccione A la aplicación y, a continuación, active la casilla Habilitar para cada una de las características de Aprovisionar a la aplicación que desee habilitar. Para este tutorial, seleccione todas las opciones.
11. Seleccione Save.

Ya tiene todo listo para sincronizar los usuarios desde Okta con IAM Identity Center.

## Paso 4: Okta: sincronización de los usuarios desde Okta con IAM Identity Center

De forma predeterminada, no hay ningún usuario o grupo asignado a su aplicación IAM Identity Center de Okta. Los grupos de aprovisionamiento aprovisionan a los usuarios que sean miembros del grupo. Complete los siguientes pasos para sincronizar grupos y usuarios con AWS IAM Identity Center.

1. En la página de la aplicación IAM Identity Center de Okta, seleccione la pestaña Tareas. Puede asignar personas y grupos a la aplicación IAM Identity Center.
  - a. Para asignar personas:
    - En la página Assignments, seleccione Assign y, a continuación, seleccione Assign to people.
    - Seleccione los usuarios de Okta que desee que tengan acceso a la aplicación IAM Identity Center. Seleccione Asignar, luego Guardar y volver y, a continuación, seleccione Terminado.

Esto inicia el proceso de aprovisionamiento de los usuarios en IAM Identity Center.

- b. Para asignar grupos:
    - En la página Assignments, seleccione Assign y, a continuación, seleccione Assign to groups.

- Seleccione los grupos de Okta que desee que tengan acceso a la aplicación IAM Identity Center. Seleccione Asignar, luego Guardar y volver y, a continuación, seleccione Terminado.

Esto inicia el proceso de aprovisionamiento del usuario o los usuarios en IAM Identity Center.

 Note

Es posible que deba especificar más atributos para el grupo si no están presentes en todos los registros de usuario. Los atributos especificados para el grupo anularán cualquier valor de atributo individual.

2. Seleccione la pestaña Transferir grupos. Elija el grupo de Okta que desee sincronizar con IAM Identity Center. Seleccione Save.

El estado del grupo cambia a Active después de que el grupo y sus miembros se hayan transferido a IAM Identity Center.

3. Vuelva a la pestaña Assignments.
4. Para agregar usuarios individuales de Okta a IAM Identity Center, realice los siguientes pasos:
  - a. En la página de tareas, seleccione Asignar y, a continuación, seleccione Asignar a personas.
  - b. Seleccione los usuarios de Okta que desee que tengan acceso a la aplicación IAM Identity Center. Seleccione Asignar, luego Guardar y volver y, a continuación, seleccione Terminado.

Esto inicia el proceso de aprovisionamiento de los usuarios individuales en IAM Identity Center.

 Note

También puede asignar usuarios y grupos a la AWS IAM Identity Center aplicación desde la página Applications del Okta admin dashboard. Para ello, seleccione el icono Settings, seleccione Assign to Users o Assign to Groups y, a continuación, especifique el usuario o el grupo.

5. Vuelva a la consola de IAM Identity Center. En el menú de navegación de la izquierda, seleccione Users. Debería ver la lista de usuarios rellena por sus usuarios de Okta.

#### ¡Enhorabuena!

Ha configurado correctamente una conexión SAML entre Okta y AWS y ha comprobado que el aprovisionamiento automático funciona. Ahora puede asignar a estos usuarios cuentas y aplicaciones en IAM Identity Center. Para este tutorial, en el siguiente paso designaremos a uno de los usuarios como administrador de IAM Identity Center mediante la concesión de permisos administrativos en la cuenta de administración.

## Paso de atributos para el control de acceso: opcional

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Asigne el acceso a Cuentas de AWS

Los siguientes pasos solo son necesarios para conceder acceso Cuentas de AWS únicamente a. Estos pasos no son necesarios para conceder el acceso a AWS las aplicaciones de.

 Note

Para completar este paso, necesitará una instancia de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Paso 1: IAM Identity Center: conceder a los usuarios de Okta acceso a las cuentas

1. En el panel de navegación del IAM Identity Center, en Permisos para varias cuentas, seleccione Cuentas de AWS.
2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la raíz organizativa con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:
  - a. En Paso 1: selección de usuarios y grupos, elija el usuario que realizará la función del trabajo de administrador. A continuación, elija Siguiente.
  - b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.
    - i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:
      - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
      - En Política para un conjunto de permisos predefinido, elija AdministratorAccess.Elija Siguiente.
    - ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

La configuración predeterminada crea un conjunto de permisos denominado **AdministratorAccess** con una duración de sesión establecida en una hora.
    - iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.

En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.

En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de *AdministratorAccess* permisos que creó aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.

- c. En Paso 3: revisión y envío, revise el usuario y el conjunto de permisos seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que la Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Regresará a la Cuentas de AWS página de las. Un mensaje de notificación le informa de que se Cuenta de AWS ha reaprovisionado la y se ha aplicado el conjunto de permisos actualizado. Cuando el usuario inicie sesión, tendrá la opción de elegir el *AdministratorAccess* rol.

## Paso 2: Okta: confirmación del acceso de los usuarios de Okta a los recursos de AWS

1. Inicie sesión con una cuenta de prueba a Okta dashboard.
2. En Mis aplicaciones, seleccione el icono de AWS IAM Identity Center.
3. Debería ver el Cuenta de AWS icono. Amplíe el icono para ver la lista de a las Cuentas de AWS que puede acceder el usuario. En este tutorial, solo trabajó con una cuenta, por lo que al expandir el icono solo se muestra una cuenta.
4. Seleccione la cuenta para ver los conjuntos de permisos disponibles para el usuario. En este tutorial, creó el conjunto de AdministratorAccesspermisos.
5. Junto al conjunto de permisos hay enlaces para el tipo de acceso disponible para ese conjunto de permisos. Cuando creó el conjunto de permisos, especificó el acceso mediante la AWS Management Console y con el acceso de programación. Seleccione Consola de administración para abrir la AWS Management Console.
6. El usuario ha iniciado sesión en la AWS Management Console.

## Pasos a seguir a continuación

Ahora que ha configurado Okta como proveedor de identidades y ha aprovisionado a usuarios en IAM Identity Center, puede hacer lo siguiente:

- Conceda acceso a Cuentas de AWS, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).
- Para conceder acceso a las aplicaciones en la nube, consulte [Asignar el acceso de los usuarios a las aplicaciones en la consola de IAM Identity Center](#).
- Para configurar los permisos en función de los cargos en el trabajo; consulte [Crear un conjunto de permisos](#).

## Solución de problemas

Para saber cómo solucionar problemas generales de SCIM y SAML con Okta, consulte las secciones siguientes:

- [Reaprovisionamiento de usuarios y grupos eliminados de IAM Identity Center](#)
- [Error de aprovisionamiento automático en Okta](#)
- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- [Recursos adicionales](#)

## Reaprovisionamiento de usuarios y grupos eliminados de IAM Identity Center

- Puede recibir el siguiente mensaje de error en la consola de Okta si intenta cambiar un usuario o un grupo en Okta que alguna vez se sincronizó y luego se eliminó del IAM Identity Center:
  - No se AWS IAM Identity Center pudo enviar automáticamente el perfil de un usuario *Jane Doe* a la aplicación: se produjo un error al intentar actualizar el perfil de *jane\_doe@example.com*: No se devolvió ningún usuario para el usuario *xxxxx-xxxxxx-xxxxx-xxxxxxx*

- Falta el grupo vinculado en AWS IAM Identity Center. Cambia el grupo vinculado para volver a aumentar las membresías del grupo.
- También puede recibir el siguiente mensaje de error en los registros del sistema de Okta para los usuarios o grupos del IAM Identity Center sincronizados o eliminados:
  - Error de Okta: Eventfailed application.provision.user.push\_profile: No se devolvió ningún usuario para el usuario `xxxxxx-xxxxxx-xxxxxx-xxxxxx`
  - Error de Okta: application.provision.group\_push.mapping.update.or.delete.failed.with.error: Falta el grupo vinculado en. AWS IAM Identity Center Cambia el grupo vinculado para volver a aumentar las membresías del grupo.

#### Warning

Si ha sincronizado Okta e IAM Identity Center mediante SCIM, debe eliminar los usuarios y los grupos de Okta en lugar del IAM Identity Center.

### Resolución de problemas de usuarios eliminados de IAM Identity Center

Para solucionar este problema con los usuarios eliminados del IAM Identity Center, los usuarios deben eliminarse de Okta. Si fuera necesario, también habría que volver a crear estos usuarios en Okta. Cuando se vuelva a crear el usuario en Okta, también se volverá a aprovisionar en el IAM Identity Center a través de SCIM. Para obtener más información sobre eliminar un usuario, consulte la [documentación de Okta](#).

#### Note

Si necesita eliminar el acceso de un usuario de Okta al IAM Identity Center, primero debe eliminarlo de su Group Push y, después, de su grupo de tareas en Okta. De este modo, se garantiza que el usuario deje de pertenecer a su grupo asociado en el IAM Identity Center. Para obtener más información sobre la resolución de problemas de Group Push, consulte la [documentación de Okta](#).

### Resolución de problemas de grupos eliminados de IAM Identity Center

Para solucionar este problema con los IAM Identity Center eliminados, el grupo debe eliminarse de Okta. Si fuera necesario, estos grupos también deberían volver a crearse en Okta mediante Group

Push. Cuando se vuelva a crear el usuario en Okta, también se volverá a aprovisionar en el IAM Identity Center a través de SCIM. Para obtener más información sobre la eliminación de un grupo, consulte la [documentación de Okta](#).

## Error de aprovisionamiento automático en Okta

Si recibe un error en Okta:

AWS IAM Identity Center Falló el aprovisionamiento automático del usuario Jane Doe a la aplicación: no se encontró el usuario coincidente

Consulte la [documentación de la Okta](#) para obtener más información.

## Recursos adicionales

- Para obtener sugerencias generales acerca de la solución de problemas de SCIM, consulte [Resolución de problemas de IAM Identity Center](#).

Los recursos relacionados siguientes pueden ayudarle a solucionar problemas cuando trabaje con AWS:

- [AWS re:Post](#): busque FAQs recursos relacionados para ayudarle a solucionar problemas.
- [AWS Support](#): obtenga soporte técnico

## Configuración del aprovisionamiento de SCIM entre OneLogin y el Centro de Identidad de IAM

El IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de usuarios y grupos desde OneLogin al IAM Identity Center mediante el protocolo System for Cross-Domain Identity Management (SCIM) v2.0. Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

Esta conexión se configura en OneLogin, utilizando su terminal SCIM para el IAM Identity Center y un token portador creado automáticamente por el IAM Identity Center. Al configurar la sincronización de SCIM, se crea un mapeo de los atributos de usuario en OneLogin a los atributos nombrados en el Centro de identidades de IAM. Esto hace que los atributos esperados coincidan entre el Centro de Identidad de IAM y OneLogin.



Los siguientes pasos explican cómo habilitar el aprovisionamiento automático de usuarios y grupos desde OneLogin al IAM Identity Center mediante el protocolo SCIM.

 Note

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#).

## Temas

- [Requisitos previos](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: Configurar el aprovisionamiento en OneLogin](#)
- [\(Opcional\) Paso 3: configurar los atributos de usuario en OneLogin para el control de acceso en IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)
- [Solución de problemas](#)

## Requisitos previos

Antes de comenzar, necesitará lo siguiente:

- A OneLogin account. Si no tiene una cuenta existente, puede obtener una cuenta de prueba gratuita o una cuenta de desarrollador en el [OneLogin sitio web](#).
- Una cuenta habilitada para IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).
- Una conexión SAML desde tu OneLogin cuenta en el Centro de Identidad de IAM. Para obtener más información, consulte [Habilitar el inicio de sesión único entre OneLogin y AWS](#) en el blog de AWS Partner Network.

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

## Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie el punto final y el token de acceso de SCIM. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

### Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione Cerrar.

Ha configurado el aprovisionamiento en la consola de IAM Identity Center. Ahora tiene que realizar las tareas restantes con el OneLogin consola de administración tal y como se describe en el siguiente procedimiento.

## Paso 2: Configurar el aprovisionamiento en OneLogin

Utilice el siguiente procedimiento en OneLogin consola de administración para permitir la integración entre el IAM Identity Center y la aplicación IAM Identity Center. Este procedimiento supone que ya ha configurado la aplicación AWS Single Sign-On en OneLogin para la autenticación SAML. Si aún no ha creado esta conexión SAML, hágalo antes de continuar y, a continuación, vuelva aquí para completar el proceso de aprovisionamiento del SCIM. Para obtener más información sobre cómo

configurar SAML con OneLogin, consulte [Habilitar el inicio de sesión único entre OneLogin y AWS](#) en el blog de AWS Partner Network.

Para configurar el aprovisionamiento en OneLogin

1. Inicie sesión en OneLogin, a continuación, vaya a Aplicaciones > Aplicaciones.
2. En la página Aplicaciones, busque la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center. Elija la y, a continuación, elija Configuración en el panel de navegación.
3. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL base de SCIM en OneLogin. Además, en el procedimiento anterior, copió el valor del token de acceso en el Centro de identidades de IAM. Pegue ese valor en el campo SCIM Bearer Token de OneLogin.
4. Junto a Conexión API, haga clic en Habilitar y, a continuación, en Guardar para completar la configuración.
5. En el panel de navegación, seleccione Provisioning (Aprovisionamiento).
6. Seleccione las casillas de verificación Habilitar el aprovisionamiento, Crear usuario, Eliminar usuario y Actualizar usuario y, a continuación, seleccione Guardar.
7. En el panel de navegación, seleccione Usuarios.
8. Haga clic en Más acciones y seleccione Sincronizar inicios de sesión. Deberías recibir el mensaje Sincronizar usuarios con single sign-On de AWS .
9. Vuelva a hacer clic en Más acciones y, a continuación, seleccione Volver a aplicar las asignaciones de derechos. Debería recibir el mensaje Se están reaplicando las asignaciones.
10. En este punto, debería comenzar el proceso de aprovisionamiento. Para confirmarlo, vaya a Actividad > Eventos y supervise el progreso. Los eventos de aprovisionamiento correctos, así como los errores, deberían aparecer en la secuencia de eventos.
11. Para comprobar que todos sus usuarios y grupos se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Sus usuarios sincronizados de OneLogin aparecen en la página de usuarios. También puede ver sus grupos sincronizados en la página Grupos.
12. Para sincronizar automáticamente los cambios de los usuarios con IAM Identity Center, vaya a la página de Aprovisionamiento, busque la sección Requerir la aprobación del administrador antes de realizar esta acción, anule la selección de Crear usuario, Eliminar usuario o Actualizar usuario y haga clic en Guardar.

## (Opcional) Paso 3: configurar los atributos de usuario en OneLogin para el control de acceso en IAM Identity Center

Se trata de un procedimiento opcional para OneLogin si decide configurar los atributos que utilizará en el Centro de identidades de IAM para gestionar el acceso a sus AWS recursos. Los atributos que defina en OneLogin se transmiten en una aserción de SAML al Centro de Identidad de IAM. A continuación, creará un conjunto de permisos en el Centro de Identidad de IAM para gestionar el acceso en función de los atributos desde los que haya pasado OneLogin.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

Para configurar los atributos de usuario en OneLogin para el control de acceso en el IAM Identity Center

1. Inicie sesión en OneLogin, a continuación, vaya a Aplicaciones > Aplicaciones.
2. En la página Aplicaciones, busque la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center. Elija y, a continuación, seleccione Parámetros en el panel de navegación.
3. En la sección Parámetros obligatorios, haga lo siguiente para cada atributo que desee utilizar en IAM Identity Center:
  - a. Elija +.
  - b. En Nombre del campo, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName` y sustituya **AttributeName** por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.
  - c. En Banderas, marque la casilla situada junto a Incluir en la afirmación de SAML y seleccione Guardar.
  - d. En el campo Valor, utilice la lista desplegable para elegir OneLogin atributos de usuario. Por ejemplo, Departamento.
4. Seleccione Guardar.

## (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Solución de problemas

Lo siguiente puede ayudarle a solucionar algunos problemas comunes que pueden surgir al configurar el aprovisionamiento automático con OneLogin.

Los grupos no se aprovisionan en IAM Identity Center

De forma predeterminada, los grupos no se pueden aprovisionar desde OneLogin al Centro de identidades de IAM. Asegúrese de haber activado el aprovisionamiento de grupos para su aplicación del Centro de Identidad de IAM en OneLogin. Para ello, inicia sesión en OneLogin consola de administración y asegúrese de que la opción `Incluir` en el aprovisionamiento de usuarios esté seleccionada en las propiedades de la aplicación IAM Identity Center (aplicación IAM Identity Center > Parámetros > Grupos). Para obtener más información sobre cómo crear grupos en OneLogin, incluyendo cómo sincronizarlos OneLogin roles como grupos en SCIM, consulte la [OneLogin sitio web](#).

No se sincroniza nada desde OneLogin al Centro de identidad de IAM, a pesar de que todos los ajustes sean correctos

Además de la nota anterior sobre la aprobación del administrador, tendrá que volver a aplicar las asignaciones de derechos para que se apliquen muchos cambios de configuración. Esto se encuentra en Aplicaciones > Aplicaciones > Aplicación IAM Identity Center > Más acciones. Puede ver los detalles y los registros de la mayoría de las acciones en OneLogin, incluidos los eventos de sincronización, en Actividad > Eventos.

He eliminado o desactivado un grupo en OneLogin, pero sigue apareciendo en el Centro de identidades de IAM

OneLogin actualmente no admite la operación SCIM DELETE para grupos, lo que significa que el grupo sigue existiendo en el Centro de Identidad de IAM. Por lo tanto, deberá eliminar el grupo directamente de IAM Identity Center para asegurarse de que se eliminen todos los permisos correspondientes en IAM Identity Center para ese grupo.

He eliminado un grupo del Centro de Identidad de IAM sin eliminarlo primero de OneLogin y ahora tengo problemas con la sincronización de usuarios y grupos

Para solucionar esta situación, primero asegúrese de no tener reglas o configuraciones de aprovisionamiento de grupos redundantes en OneLogin. Por ejemplo, un grupo asignado directamente a una aplicación junto con una regla que publica en el mismo grupo. A continuación, elimine los grupos no deseados de IAM Identity Center. Por último, en OneLogin, Actualice los derechos (aplicación IAM Identity Center > Aprovisionamiento > Derechos) y, a continuación, vuelva a aplicar las asignaciones de derechos (aplicación IAM Identity Center > Más acciones). Para evitar este problema en el futuro, primero realice el cambio para dejar de aprovisionar el grupo en OneLogin, a continuación, elimine el grupo del Centro de identidades de IAM.

## Utilización Ping Identity productos con IAM Identity Center

Los siguientes ejemplos de Ping Identity los productos se han probado con el IAM Identity Center.

### Temas

- [PingFederate](#)
- [PingOne](#)

## PingFederate

El Centro de Identidad de IAM admite el aprovisionamiento automático (sincronización) de la información de usuarios y grupos desde PingFederate producto de Ping Identity (en adelante»Ping»)

al Centro de identidad de IAM. Este aprovisionamiento utiliza el protocolo sistema de administración de identidades entre dominios (SCIM) v2.0. Para obtener más información, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

Esta conexión se configura en PingFederate utilizando el punto de conexión SCIM y el token de acceso del IAM Identity Center. Al configurar la sincronización de SCIM, se crea un mapeo de los atributos de usuario en PingFederate a los atributos nombrados en el Centro de identidades de IAM. Esto hace que los atributos esperados coincidan entre el Centro de Identidad de IAM y PingFederate.

Esta guía se basa en PingFederate versión 10.2. Los pasos para las versiones más recientes pueden variar. Contacto Ping para obtener más información sobre cómo configurar el aprovisionamiento en el Centro de Identidad de IAM para otras versiones de PingFederate.

En los siguientes pasos se explica cómo habilitar el aprovisionamiento automático de usuarios y grupos desde PingFederate al IAM Identity Center mediante el protocolo SCIM.

#### Note

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#). A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

## Temas

- [Requisitos previos](#)
- [Consideraciones](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: Configurar el aprovisionamiento en PingFederate](#)
- [\(Opcional\) Paso 3: configurar los atributos de usuario en PingFedVelocidad para el control de acceso en el IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)
- [Solución de problemas](#)

## Requisitos previos

Necesitará lo siguiente antes de empezar:

- Un en funcionamiento PingFederate servidor. Si no tiene un existente PingFederate servidor, es posible que puedas obtener una prueba gratuita o una cuenta de desarrollador en el sitio web de [Ping Identity](#). La versión de prueba incluye licencias y descargas de software y la documentación asociada.
- Una copia del PingFederate El software IAM Identity Center Connector está instalado en su PingFederate servidor. Para obtener más información sobre cómo obtener este software, consulte [IAM Identity Center Connector](#) en el Ping Identity sitio web.
- Una cuenta habilitada para IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).
- Una conexión SAML desde tu PingFederate instancia al centro de identidad de IAM. Para obtener instrucciones sobre cómo configurar esta conexión, consulte la PingFederate . En resumen, la ruta recomendada es utilizar el conector del IAM Identity Center para configurar el «SSO del navegador» en PingFederate, utilizando las funciones de «descarga» e «importación» de metadatos en ambos extremos para intercambiar metadatos de SAML entre PingFederate y el Centro de identidad de IAM.

## Consideraciones

Las siguientes son consideraciones importantes sobre PingFederate eso puede afectar a la forma en que se implementa el aprovisionamiento con IAM Identity Center.

- Si se elimina un atributo (como un número de teléfono) de un usuario del almacén de datos configurado en PingFederate, ese atributo no se eliminará del usuario correspondiente en el Centro de identidades de IAM. Se trata de una limitación conocida en PingFederate's implementación del aprovisionador. Si un atributo se cambia a un valor diferente (no vacío) en un usuario, ese cambio se sincroniza con IAM Identity Center.

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.



3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione **Habilitar**. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie el punto final y el token de acceso del SCIM. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione **Mostrar token** para copiar el valor.

 **Warning**

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione **Cerrar**.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes mediante el PingFederate consola administrativa., Los pasos se describen en el siguiente procedimiento.

## Paso 2: Configurar el aprovisionamiento en PingFederate

Utilice el siguiente procedimiento en el PingFederate consola administrativa para permitir la integración entre el IAM Identity Center y el IAM Identity Center Connector. En este procedimiento, se presupone que ya ha instalado el software del conector de IAM Identity Center. Si aún no lo ha hecho, consulte los [Requisitos previos](#) y complete este procedimiento para configurar el aprovisionamiento de SCIM.

 **Important**

Si las recetas PingFederate el servidor no se ha configurado previamente para el aprovisionamiento de SCIM saliente, por lo que es posible que deba realizar un cambio en el

archivo de configuración para habilitar el aprovisionamiento. Para obtener más información, consulte Ping . En resumen, debe modificar la configuración en el `pf.provisioner.mode` `pingfederate-<version>/pingfederate/bin/run.properties` a un valor distinto al OFF (que es el predeterminado) y reiniciar el servidor si se está ejecutando actualmente. Por ejemplo, puede optar por utilizarla STANDALONE si actualmente no tiene una configuración de alta disponibilidad con PingFederate.

Para configurar el aprovisionamiento en PingFederate

1. Inicie sesión en el PingFederate consola administrativa.
2. Seleccione Aplicaciones en la parte superior de la página y, a continuación, haga clic en SP Connections.
3. Localice la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center y haga clic en el nombre de la conexión.
4. Seleccione el tipo de conexión en los encabezados de navegación oscuros situados en la parte superior de la página. Debería ver que el SSO del navegador ya estaba seleccionado en su configuración anterior de SAML. Si no es así, primero debe completar esos pasos antes de continuar.
5. Seleccione la casilla de verificación Aprovisionamiento saliente, elija IAM Identity Center Cloud Connector como tipo y haga clic en Guardar. Si el IAM Identity Center Cloud Connector no aparece como opción, asegúrese de haber instalado el IAM Identity Center Cloud Connector y de haber reiniciado su PingFederate servidor.
6. Haga clic en Siguiente varias veces hasta llegar a la página Aprovisionamiento saliente y, a continuación, haga clic en el botón Configurar aprovisionamiento.
7. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL de SCIM en el PingFederate console. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo Token de acceso del PingFederate console. Haga clic en Guardar.
8. En la página Configuración del canal (Configurar canal), haga clic en Crear.
9. Introduzca un nombre del canal para este nuevo canal de aprovisionamiento (por ejemplo **AWSIAMIdentityCenterchannel**) y haga clic en Siguiente.
10. En la página Origen, elija el almacén de datos activo que desee utilizar para la conexión al IAM Identity Center y haga clic en Siguiente.

 Note

Si aún no ha configurado un origen de datos, deberá hacerlo ahora. Consulte la Ping para obtener información sobre cómo elegir y configurar una fuente de datos en PingFederate.

11. En la página Configuración de origen, confirme que todos los valores son correctos para la instalación y, a continuación, haga clic en Siguiente.
12. En la página Ubicación de origen, introduzca la configuración adecuada para su origen de datos y, a continuación, haga clic en Siguiente. Por ejemplo, si utiliza Active Directory como directorio LDAP:
  - a. Introduzca el DN base de su bosque de AD (por ejemplo, **DC=myforest,DC=mydomain,DC=com**).
  - b. En Usuarios > DN de grupo, especifique un único grupo que contenga todos los usuarios que desee aprovisionar al IAM Identity Center. Si no existe ese grupo único, créelo en AD, vuelva a esta configuración y, a continuación, introduzca el DN correspondiente.
  - c. Especifique si desea buscar subgrupos (Búsqueda anidada) y cualquier filtro LDAP necesario.
  - d. En Usuarios > DN de grupo, especifique un único grupo que contenga todos los usuarios que desee aprovisionar al IAM Identity Center. En muchos casos, puede ser el mismo DN que especificó en la sección Usuarios. Introduzca los valores búsqueda anidada y filtro según sea necesario.
13. En la página Asignación de atributos, asegúrese de lo siguiente y, a continuación, haga clic en Siguiente:
  - a. El campo userName debe asignarse a un atributo con formato de correo electrónico (user@domain.com). También debe coincidir con el valor que el usuario utilizará para iniciar sesión en Ping. Este valor, a su vez, se rellena en la notificación del nameId de SAML durante la autenticación federada y se utiliza para hacer coincidir con el usuario de IAM Identity Center. Por ejemplo, cuando utilice Active Directory, puede optar por especificar el UserPrincipalName como userName.
  - b. Los demás campos con un sufijo \* deben asignarse a atributos que no sean nulos para los usuarios.

14. En la página Activación y resumen, defina el estado del canal como Activo para que la sincronización comience inmediatamente después de guardar la configuración.
15. Confirme que todos los valores de configuración de la página son correctos y haga clic en Listo.
16. En la página Administrar canales, haga clic en Guardar.
17. En este punto, comienza el aprovisionamiento. Para confirmar la actividad, puede ver el archivo provisioner.log, que se encuentra de forma predeterminada en pingfederate-<version>/pingfederate/logdirectorio de su PingFederate servidor.
18. Para comprobar que los usuarios y los grupos se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Usuarios sincronizados de PingFederate aparecen en la página de usuarios. También puede ver sus grupos sincronizados en la página Grupos.

### (Opcional) Paso 3: configurar los atributos de usuario en PingFedVelocidad para el control de acceso en el IAM Identity Center

Este es un procedimiento opcional para PingFederate si decide configurar los atributos que utilizará en el Centro de identidades de IAM para gestionar el acceso a sus AWS recursos. Los atributos que defina en PingFederate se transmiten en una aserción de SAML al Centro de Identidad de IAM. A continuación, creará un conjunto de permisos en el Centro de Identidad de IAM para gestionar el acceso en función de los atributos desde los que haya pasado PingFederate.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

Para configurar los atributos de usuario en PingFederate para el control de acceso en el IAM Identity Center

1. Inicie sesión en el PingFederate consola administrativa.
2. Seleccione Aplicaciones en la parte superior de la página y, a continuación, haga clic en SP Connections.
3. Localice la aplicación que creó anteriormente para establecer su conexión SAML con IAM Identity Center y haga clic en el nombre de la conexión.
4. Seleccione el tipo de conexión en los encabezados de navegación oscuros situados en la parte superior de la página. A continuación, haga clic en Configurar el SSO del navegador.

5. En la página Configurar el SSO del navegador, seleccione Creación de aserciones y, a continuación, haga clic en Configurar creación de aserciones.
6. En la página Configurar la creación de aserciones, elija Contrato de atributos.
7. En la página Contrato de atributos, en la sección Ampliar el contrato, añada un nuevo atributo siguiendo estos pasos:
  - a. En el cuadro de texto, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`, sustituya **AttributeName** por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.
  - b. En Formato de nombre de atributo, elija `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`.
  - c. Elija Añadir, y a continuación, elija Siguiente.
8. En la página de asignación de fuentes de autenticación, elija la instancia de adaptador configurada con su aplicación.
9. En la página Cumplimiento del contrato de atributo, elija el origen (almacén de datos) y el valor (atributo del almacén de datos) para el contrato de atributo `https://aws.amazon.com/SAML/Attributes/AccessControl:Department`.

 Note

Si aún no ha configurado un origen de datos, deberá hacerlo ahora. Consulte la Ping para obtener información sobre cómo elegir y configurar una fuente de datos en PingFederate.

10. Haga clic en Siguiente varias veces hasta llegar a la página de activación y resumen y, a continuación, haga clic en Guardar.

## (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Solución de problemas

Para solucionar problemas generales de SCIM y SAML con PingFederate, consulte las siguientes secciones:

- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- Para obtener más información sobre las PingFederate, consulte [PingFederate documentación](#).

Los siguientes recursos pueden ayudarle a solucionar problemas mientras trabaja con AWS:

- [AWS re:Post](#)- Busca otros recursos FAQs y enlaces a ellos para ayudarte a solucionar problemas.
- [AWS Support](#): obtenga soporte técnico

## PingOne

El Centro de Identidad de IAM admite el aprovisionamiento automático (sincronización) de la información de los usuarios desde PingOne producto de Ping Identity (en adelante «Ping») al Centro de identidad de IAM. Este aprovisionamiento utiliza el protocolo sistema de administración de identidades entre dominios (SCIM) v2.0. Esta conexión se configura en PingOne utilizando el punto

de conexión SCIM y el token de acceso del IAM Identity Center. Al configurar la sincronización de SCIM, se crea un mapeo de los atributos de usuario en PingOne a los atributos nombrados en el Centro de identidades de IAM. Esto hace que los atributos esperados coincidan entre el Centro de Identidad de IAM y PingOne.

En los siguientes pasos, se explica cómo habilitar el aprovisionamiento automático de usuarios desde PingOne al IAM Identity Center mediante el protocolo SCIM.

#### Note

Antes de comenzar a implementar SCIM, le recomendamos que revise las [Consideraciones para utilizar el aprovisionamiento automático](#). A continuación, continúe con las consideraciones adicionales que se indican en la siguiente sección.

## Temas

- [Requisitos previos](#)
- [Consideraciones](#)
- [Paso 1: habilite el aprovisionamiento en IAM Identity Center](#)
- [Paso 2: Configurar el aprovisionamiento en PingOne](#)
- [\(Opcional\) Paso 3: configurar los atributos de usuario en PingOne para el control de acceso en IAM Identity Center](#)
- [\(Opcional\) Paso de atributos para el control de acceso](#)
- [Solución de problemas](#)

## Requisitos previos

Necesitará lo siguiente antes de empezar:

- A PingOne suscripción o prueba gratuita, con funciones de autenticación federada y aprovisionamiento. Para obtener más información sobre cómo obtener una prueba gratuita, consulte la [Ping Identity](#) sitio web.
- Una cuenta habilitada para IAM Identity Center ([gratuita](#)). Para más información, consulte [Activar IAM Identity Center](#).
- La PingOne La aplicación IAM Identity Center se agregó a su PingOne portal de administración. Puede obtener el PingOne La aplicación IAM Identity Center desde el PingOne Catálogo de

aplicaciones. Para obtener información general, consulte [Agregar una aplicación del catálogo](#) de aplicaciones en el Ping Identity sitio web.

- Una conexión SAML desde tu PingOne instancia al centro de identidad de IAM. Después del PingOne La aplicación IAM Identity Center se haya agregado a su PingOne portal de administración, debe usarlo para configurar una conexión SAML desde su PingOne instancia al Centro de identidades de IAM. Utilice las funciones de «descarga» e «importación» de metadatos en ambos extremos para intercambiar metadatos de SAML entre PingOne y el Centro de identidad de IAM. Para obtener instrucciones sobre cómo configurar esta conexión, consulte la PingOne .

## Consideraciones

Las siguientes son consideraciones importantes sobre PingOne eso puede afectar a la forma en que se implementa el aprovisionamiento con IAM Identity Center.

- PingOne no admite el aprovisionamiento de grupos a través de SCIM. Contacto Ping para obtener la información más reciente sobre el apoyo grupal en SCIM para PingOne.
- Los usuarios pueden seguir siendo aprovisionados desde PingOne después de deshabilitar el aprovisionamiento en el PingOne portal de administración. Si necesita finalizar el aprovisionamiento inmediatamente, elimine el token portador del SCIM correspondiente o desactívelo en [Aprovisionamiento de un proveedor de identidad externo al IAM Identity Center mediante SCIM](#), en IAM Identity Center.
- Si se elimina un atributo de un usuario del almacén de datos configurado en PingOne, ese atributo no se eliminará del usuario correspondiente en el Centro de identidades de IAM. Se trata de una limitación conocida en PingOne's implementación del aprovisionador. Si se modifica un atributo, el cambio se sincronizará con IAM Identity Center.
- Las siguientes son notas importantes sobre la configuración de SAML en PingOne:
  - IAM Identity Center solo es compatible con `emailaddress` como formato de NameId. Esto significa que debe elegir un atributo de usuario que sea único en su directorio en PingOne, no nulo y con el formato de correo electrónico/UPN (por ejemplo, `user@domain.com`) para la asignación de SAML\_SUBJECT en PingOne. El correo electrónico (trabajo) es un valor razonable para probar las configuraciones con el PingOne directorio integrado.
  - Usuarios en PingOne con una dirección de correo electrónico que contenga un carácter +, es posible que no puedan iniciar sesión en el Centro de Identidad de IAM debido a errores como 'SAML\_215' o 'Invalid input'. Para solucionar este problema, en PingOne, elija la opción Avanzada para el mapeo SAML\_SUBJECT en Attribute Mappings. A continuación,



defina el formato de ID de nombre para enviarlo a SP: to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress en el menú desplegable.

## Paso 1: habilite el aprovisionamiento en IAM Identity Center

En este primer paso, utilizará la consola de IAM Identity Center para habilitar el aprovisionamiento automático.

Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie el punto final y el token de acceso de SCIM. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.
  - a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/ /scim/v21111111111-2222-3333-4444-555555555555`
  - b. Token de acceso: seleccione Mostrar token para copiar el valor.

### Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione Cerrar.

Ahora que ha configurado el aprovisionamiento en la consola de IAM Identity Center, debe completar las tareas restantes mediante el PingOne Aplicación IAM Identity Center. Estos pasos se explican en el procedimiento siguiente.

## Paso 2: Configurar el aprovisionamiento en PingOne

Utilice el siguiente procedimiento en el PingOne Aplicación IAM Identity Center para permitir el aprovisionamiento con IAM Identity Center. En este procedimiento se presupone que ya ha añadido el PingOne La aplicación IAM Identity Center a su PingOne portal de administración. Si aún no lo ha hecho, consulte los [Requisitos previos](#) y complete este procedimiento para configurar el aprovisionamiento de SCIM.

Para configurar el aprovisionamiento en PingOne

1. Abra el icono PingOne Aplicación del Centro de Identidad de IAM que instaló como parte de la configuración de SAML para PingOne (Aplicaciones > Mis aplicaciones). Consulte [Requisitos previos](#).
2. Desplácese hasta el final de la página. En Aprovisionamiento de usuarios, elija el enlace completo para acceder a la configuración de aprovisionamiento de usuarios de su conexión.
3. En la página de instrucciones de aprovisionamiento, seleccione Continuar con el siguiente paso.
4. En el procedimiento anterior, copió el valor del punto de conexión de SCIM en IAM Identity Center. Pegue ese valor en el campo URL de SCIM del PingOne Aplicación IAM Identity Center. En el procedimiento anterior, copió el valor del token de acceso en IAM Identity Center. Pegue ese valor en el campo ACCESS\_TOKEN del PingOne Aplicación IAM Identity Center.
5. Para REMOVE\_ACTION, elija Desactivada o Eliminada (consulte el texto de descripción de la página para obtener más información).
6. En la página de asignación de atributos, elija un valor para usarlo en la afirmación SAML\_SUBJECT (NameId), siguiendo las instrucciones de [Consideraciones](#) que aparecen anteriormente en esta página. A continuación elija Continuar con el paso siguiente.
7. En la página PingOne Personalización de la aplicación: página del Centro de identidad de IAM, realice los cambios de personalización que desee (opcional) y haga clic en Continuar con el siguiente paso.
8. En la página Acceso grupal, seleccione los grupos que contienen los usuarios que desea habilitar para el aprovisionamiento y el inicio de sesión único en IAM Identity Center. Elija Continuar con el paso siguiente.
9. Desplácese hasta el final de la página y seleccione Finalizar para iniciar el aprovisionamiento.
10. Para comprobar que los usuarios se han sincronizado correctamente con IAM Identity Center, vuelva a la consola de IAM Identity Center y seleccione Usuarios. Usuarios sincronizados de PingOne aparecerá en la página de usuarios. Estos usuarios ahora pueden asignarse a cuentas en IAM Identity Center.

Recuerda que PingOne no admite el aprovisionamiento de grupos o la pertenencia a grupos a través de SCIM. Contacto Ping para obtener más información.

### (Opcional) Paso 3: configurar los atributos de usuario en PingOne para el control de acceso en IAM Identity Center

Se trata de un procedimiento opcional para PingOne si decide configurar los atributos del IAM Identity Center para gestionar el acceso a sus AWS recursos. Los atributos que defina en PingOne se pasa en una aserción de SAML al Centro de Identidad de IAM. A continuación, debe crear un conjunto de permisos en el Centro de Identidad de IAM para gestionar el acceso en función de los atributos de los que ha pasado PingOne.

Antes de comenzar con este procedimiento, debe habilitar la característica [Atributos para controlar el acceso](#). Para obtener más información acerca de cómo hacerlo, consulte [Habilitación y configuración de atributos para el control de acceso](#).

Para configurar los atributos de usuario en PingOne para el control de acceso en el IAM Identity Center

1. Abra el icono PingOne Aplicación del Centro de Identidad de IAM que instaló como parte de la configuración de SAML para PingOne (Aplicaciones > Mis aplicaciones).
2. Elija Editar y, a continuación, elija Continuar con el siguiente paso hasta llegar a la página Asignaciones de atributos.
3. En la página Asignaciones de atributos, elija Añadir nuevo atributo. A continuación, siga estos pasos para cada atributo que vaya a añadir para su uso en IAM Identity Center para el control de acceso.
  - a. En el campo Atributo de la aplicación, introduzca `https://aws.amazon.com/SAML/Attributes/AccessControl:AttributeName`. Sustituya `AttributeName` por el nombre del atributo que está esperando en IAM Identity Center. Por ejemplo, `https://aws.amazon.com/SAML/Attributes/AccessControl:Email`.
  - b. En el campo Atributo o Valor literal de Identity Bridge, elija los atributos de usuario de su PingOne directorio. Por ejemplo, Correo electrónico (trabajo).
4. Elija Siguiente y, a continuación, haga clic en Terminar.

## (Opcional) Paso de atributos para el control de acceso

Si lo desea, puede utilizar la característica [Atributos para controlar el acceso](#) de IAM Identity Center para transferir un elemento `Attribute` con el atributo `Name` configurado como `https://aws.amazon.com/SAML/Attributes/AccessControl:{TagKey}`. Este elemento le permite pasar atributos como etiquetas de sesión en la aserción SAML. Para obtener más información, consulte [Transferencia de etiquetas de sesión en AWS STS](#) en la Guía del usuario de IAM.

Para pasar atributos como etiquetas de sesión, incluya el elemento `AttributeValue` que especifica el valor de la etiqueta. Por ejemplo, utilice el siguiente atributo para pasar los pares clave-valor de etiquetas `CostCenter = blue`.

```
<saml:AttributeStatement>
<saml:Attribute Name="https://aws.amazon.com/SAML/Attributes/AccessControl:CostCenter">
<saml:AttributeValue>blue
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Si necesita añadir varios atributos, incluya un elemento `Attribute` independiente para cada etiqueta.

## Solución de problemas

Para solucionar problemas generales de SCIM y SAML con PingOne, consulte las siguientes secciones:

- [Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo](#)
- [Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center](#)
- [Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo](#)
- Para obtener más información sobre las PingOne, consulte [PingOne documentación](#).

Los siguientes recursos pueden ayudarle a solucionar problemas mientras trabaja con AWS:

- [AWS re:Post](#)- Busca otros recursos FAQs y enlaces a ellos para ayudarte a solucionar problemas.

- [AWS Support](#): obtenga soporte técnico

## Configuración del acceso de los usuarios con el directorio predeterminado de IAM Identity Center

Cuando se habilita IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como origen de identidad predeterminado, así que no tiene que seleccionar uno. Si su organización utiliza otro proveedor de identidades, como Microsoft Active Directory, Microsoft Entra ID o Okta, considere la posibilidad de integrar ese origen de identidad con IAM Identity Center en lugar de utilizar la configuración predeterminada.

### Objetivo

En este tutorial, utilizará el directorio predeterminado como fuente de identidad y una instancia de organización del IAM Identity Center para configurar y probar un usuario administrativo. Este usuario administrativo crea y administra usuarios y grupos y concede el AWS acceso con conjuntos de permisos. En los siguientes pasos, creará lo siguiente:

- Un usuario administrativo llamado *Nikki Wolf*
- Un grupo llamado *Admin team*
- Un conjunto de permisos denominado *AdminAccess*

Para comprobar que todo se ha creado correctamente, debe iniciar sesión y establecer la contraseña del usuario administrativo. Tras completar este tutorial, puede utilizar el usuario administrativo para añadir más usuarios al Centro de identidades de IAM, crear conjuntos de permisos adicionales y configurar el acceso organizativo a las aplicaciones. Como alternativa, si desea conceder a los usuarios el acceso a la aplicación, puede seguir el [paso 1](#) de este procedimiento y [configurar el acceso a la aplicación](#).

### Requisitos previos

Se necesitan los siguientes requisitos previos para completar este tutorial:

- [Activar IAM Identity Center](#) y tener una [instancia organizativa de IAM Identity Center](#).
  - Si tiene una [instancia de cuenta](#) de IAM Identity Center, puede crear usuarios y grupos, así como concederles acceso a las aplicaciones. Para obtener más información, consulte [Acceso a las aplicaciones](#).

- Inicie sesión en la consola del IAM Identity Center AWS Management Console y acceda a ella de la siguiente manera:
  - Nuevo para AWS (usuario root): inicie sesión como propietario de la cuenta seleccionando el usuario Cuenta de AWS root e introduciendo su dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
  - Si ya lo utilizas AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
  - [Para obtener más ayuda para iniciar sesión en AWS Management Console, consulte AWS Sign-In la Guía.](#)
- Puede configurar la autenticación multifactorial para los usuarios del IAM Identity Center. Para obtener más información, consulte [Configuración de MFA en el centro de identidad de IAM.](#)

## Paso 1: adición de un usuario

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación de IAM Identity Center, seleccione Usuarios y, a continuación, seleccione Agregar usuario.
3. En la página Especificar los detalles del usuario, rellene la siguiente información:

- Nombre de usuario: para este tutorial, introduzca. *nikkiw*

Al crear los usuarios, seleccione nombres de usuario que sean fáciles de recordar. Sus usuarios deben recordar el nombre de usuario para iniciar sesión en el portal de AWS acceso y no podrá cambiarlo más adelante.

- Contraseña: seleccione Enviar un correo electrónico a este usuario con las instrucciones de configuración de la contraseña (recomendado).

Esta opción envía al usuario un correo electrónico de Amazon Web Services, con el asunto Invitación para unirse a IAM Identity Center. El correo electrónico proviene de `no-reply@signin.aws` o `no-reply@login.awsapps.com`. Agregue estas direcciones de correo electrónico a su lista de remitentes aprobados.

- Dirección de correo electrónico: ingrese una dirección de correo electrónico del usuario en la que pueda recibir el correo electrónico. A continuación, vuelva a escribirla para confirmarla. Cada usuario debe tener una dirección de correo electrónico única.
- En Nombre, ingrese el nombre del usuario. En este tutorial, escriba *Nikki*.

- En Apellido, ingrese el apellido del usuario. En este tutorial, escriba *Wolf*.
  - Nombre de visualización: el valor predeterminado es el nombre y apellido del usuario. Si desea cambiar el nombre de visualización, puede ingresar otro nombre. El nombre de visualización está visible en el portal de inicio de sesión y en la lista de usuarios.
  - Complete la información opcional si lo desea. No se usa durante este tutorial y puede cambiarla más adelante.
4. Elija Siguiente. Aparece la página Agregar usuario a grupos. Vamos a crear un grupo al que asignarle permisos administrativos en lugar de dárselos directamente *Nikki*.

Seleccione Crear grupo.

Se abre una nueva pestaña del navegador para mostrar la página Crear grupo.

- a. En Detalles del grupo, en Nombre del grupo, ingrese un nombre para el grupo. Recomendamos un nombre de grupo que identifique el rol del grupo. En este tutorial, escriba *Admin team*.
  - b. Seleccione Crear grupo.
  - c. Cierre la pestaña Grupos del navegador para volver a la pestaña Agregar usuario del navegador.
5. En el área Grupos, seleccione el botón Actualizar. El *Admin team* grupo aparece en la lista.

Seleccione la casilla de verificación situada junto a *Admin team*, a continuación, elija Siguiente.

6. En la página Revisar y agregar usuario, confirme lo siguiente:
- La información principal aparece tal y como quería.
  - En Grupos se muestra el usuario agregado al grupo que ha creado

Si desea realizar cambios, seleccione Editar. Cuando todos los detalles sean correctos, seleccione Agregar usuario.

Un mensaje de notificación le informará de que se ha agregado el usuario.

A continuación, añadirá permisos administrativos para que el *Admin team* grupo *Nikki* tenga acceso a los recursos.

## Paso 2: adición de permisos administrativos

### Important

Siga estos pasos solo si ha activado una [instancia organizativa de IAM Identity Center](#).

1. En el panel de navegación del IAM Identity Center, en Permisos para varias cuentas, seleccione Cuentas de AWS.
2. En la página Cuentas de AWS, la opción Estructura organizativa muestra la organización con las cuentas situadas por debajo de ella en la jerarquía. Seleccione la casilla de verificación de su cuenta de administración y, a continuación, seleccione Asignar usuarios o grupos.
3. Aparecerá el flujo de trabajo Asignar usuarios y grupos. Consta de tres pasos:
  - a. Para el paso 1: Seleccione los usuarios y los grupos, elija el **Admin team** grupo que ha creado. A continuación, elija Siguiente.
  - b. En Paso 2: selección de conjuntos de permisos, elija Crear conjunto de permisos para abrir una nueva pestaña que le guiará por los tres subpasos necesarios para crear un conjunto de permisos.
    - i. En Paso 1: selección del tipo de conjunto de permisos, haga lo siguiente:
      - En Tipo de conjunto de permisos, seleccione Conjunto de permisos predefinido.
      - En Política para un conjunto de permisos predefinido, elija AdministratorAccess.Elija Siguiente.
    - ii. En Paso 2: especificación de los detalles del conjunto de permisos, mantenga la configuración predeterminada y seleccione Siguiente.

La configuración predeterminada crea un conjunto de permisos denominado **AdministratorAccess** con una duración de sesión establecida en una hora. Puede cambiar el nombre del conjunto de permisos al introducir un nombre nuevo en el campo Nombre del conjunto de permisos.
    - iii. En el paso 3: revisar y crear, compruebe que el tipo de conjunto de permisos utiliza la política AWS gestionada AdministratorAccess. Seleccione Crear. En la página Conjuntos de permisos, aparece una notificación que le informa de que se creó el conjunto de permisos. Ya puede cerrar esta pestaña en su navegador web.



En la pestaña Asignar usuarios y grupos del navegador, todavía está en Paso 2: selección de los conjuntos de permisos, donde empezó el flujo de trabajo de creación de conjuntos de permisos.

En el área Conjuntos de permisos, pulse el botón Actualizar. El conjunto de *AdministratorAccess* permisos que ha creado aparece en la lista. Seleccione la casilla de verificación del conjunto de permisos y, a continuación, seleccione Siguiente.

- c. En la página Paso 3: Revisar y enviar las tareas, confirme que el *Admin team* grupo y el conjunto de *AdministratorAccess* permisos están seleccionados y, a continuación, seleccione Enviar.

La página se actualiza con un mensaje en el que se indica que Cuenta de AWS se está configurando. Espere hasta que finalice el proceso.

Volverá a la Cuentas de AWS página. Un mensaje de notificación le informa de que se Cuenta de AWS ha vuelto a aprovisionar y se ha aplicado el conjunto de permisos actualizado.

 ¡Enhorabuena!

Ha configurado correctamente su primer usuario, grupo y conjunto de permisos.

En la siguiente parte de este tutorial, probará el *Nikki's* acceso iniciando sesión en el portal de AWS acceso con sus credenciales administrativas y configurando su contraseña. Cierre la sesión de la consola.

### Paso 3: Probar el acceso de los usuarios

Ahora que *Nikki Wolf* es un usuario de su organización, puede iniciar sesión y acceder a los recursos para los que tiene permiso de acuerdo con su conjunto de permisos. Para comprobar que el usuario está configurado correctamente, en el siguiente paso utilizarás *Nikki's* las credenciales para iniciar sesión y configurar su contraseña. Cuando agregaste el usuario *Nikki Wolf* en el paso 1, elegiste *Nikki* recibir un correo electrónico con las instrucciones para configurar la contraseña. Es hora de abrir el correo electrónico y hacer lo siguiente:

1. En el correo electrónico, seleccione el enlace Aceptar la invitación para aceptar la invitación.

 Note

El correo electrónico también incluye el nombre de *Nikki 's* usuario y la URL del portal de AWS acceso que utilizarán para iniciar sesión en la organización. Registre esta información para usarla más adelante.

Accederá a la página de registro de nuevos usuarios, donde podrá establecer la *Nikki 's* contraseña y [registrar su dispositivo MFA](#).

2. Tras configurar la *Nikki 's* contraseña, accederá a la página de inicio de sesión. Ingresa *nikkiw* y selecciona Siguiente, luego ingresa la *Nikki 's* contraseña y selecciona Iniciar sesión.
3. Se abre el portal de AWS acceso y muestra la organización y las aplicaciones a las que puede acceder.

Seleccione la organización para ampliarla en una lista y, a Cuentas de AWS continuación, seleccione la cuenta para ver las funciones que puede utilizar para acceder a los recursos de la cuenta.

Cada conjunto de permisos tiene dos métodos de administración que puede utilizar: rol o claves de acceso.

- Rol, por ejemplo *AdministratorAccess*: abre el AWS Console Home.
- Claves de acceso: proporcionan credenciales que puede usar con el AWS CLI o y el AWS SDK. Incluye la información para usar credenciales de corta duración que se actualizan automáticamente o claves de acceso de corta duración. Para obtener más información, consulte [Obtención de las credenciales de usuario de IAM Identity Center para la AWS CLI o AWS SDKs](#).

4. Elija el enlace del rol para iniciar sesión en AWS Console Home.

Has iniciado sesión y has accedido a la AWS Console Home página. Explore la consola y confirme que tiene el acceso que esperaba.

## Pasos a seguir a continuación

Ahora que ha creado un usuario administrativo en IAM Identity Center, puede hacer lo siguiente:

- [Asignar aplicaciones](#)
- [Agregar otros usuarios](#)
- [Asignar usuarios a las cuentas](#)
- [Configurar conjuntos de permisos adicionales](#)

 Note

Puede asignar varios conjuntos de permisos al mismo usuario. Para seguir la práctica recomendada de aplicar permisos con privilegios mínimos, después de crear un conjunto de permisos administrativos, cree un conjunto de permisos más restrictivo y asígnelo al mismo usuario. De esta forma, podrá acceder a la suya únicamente Cuenta de AWS con los permisos que necesite, en lugar de con permisos administrativos.

Una vez que los usuarios [acepten la invitación](#) para activar su cuenta e inicien sesión en el portal de AWS acceso, los únicos elementos que aparecen en el Cuentas de AWS portal son los roles y las aplicaciones a los que están asignados.

## Tutoriales de vídeo

Como recurso adicional, puede utilizar estos tutoriales en video para obtener más información sobre la configuración de proveedores de identidad externos:

- [Migración entre proveedores de identidad externos en AWS IAM Identity Center](#)
- [Federar su instancia existente con AWS IAM Identity CenterMicrosoft Entra ID](#)

# Autenticación mediante el IAM Identity Center

Un usuario inicia sesión en el portal de AWS acceso con su nombre de usuario. Cuando lo hace, IAM Identity Center redirige la solicitud al servicio de autenticación de IAM Identity Center en función del directorio asociado a la dirección de correo electrónico del usuario. Una vez autenticados, los usuarios tienen acceso de inicio de sesión único a cualquiera de las AWS cuentas y aplicaciones de terceros (software-as-a-serviceSaaS) que aparecen en el portal sin necesidad de solicitar más datos de inicio de sesión. Esto significa que los usuarios ya no necesitan realizar un seguimiento de las credenciales de varias cuentas para las distintas AWS aplicaciones asignadas que utilizan a diario.

## Sesiones de autenticación

El Centro de Identidad de IAM mantiene dos tipos de sesiones de autenticación: una para representar el inicio de sesión de los usuarios en el Centro de Identidad de IAM y otra para representar el acceso de los usuarios a las aplicaciones AWS gestionadas, como Amazon SageMaker AI Studio o Amazon Managed Grafana. Cada vez que un usuario inicia sesión en IAM Identity Center, se crea una sesión de inicio de sesión durante el tiempo configurado en IAM Identity Center, que puede ser de hasta 90 días. Para obtener más información, consulte [Configure la duración de la sesión del portal de acceso AWS y de las aplicaciones integradas del IAM Identity Center](#). Cada vez que el usuario accede a una aplicación, la sesión de inicio de sesión del Centro de Identidad de IAM se utiliza para crear una sesión de aplicación del Centro de Identidad de IAM para esa aplicación. Las sesiones de las aplicaciones de IAM Identity Center tienen una duración actualizable de 1 hora, es decir, las sesiones de aplicaciones de IAM Identity Center se actualizan automáticamente cada hora, siempre que la sesión de inicio de sesión en IAM Identity Center de la que se obtuvieron esas sesiones siga siendo válida. Si el usuario cierra sesión mediante el portal de AWS acceso, finaliza la sesión de inicio de sesión del usuario. La próxima vez que la aplicación actualice su sesión, la sesión de la aplicación finalizará.

Cuando el usuario utiliza el Centro de Identidad de IAM para acceder AWS Management Console o AWS CLI, la sesión de inicio de sesión del Centro de Identidad de IAM se utiliza para obtener una sesión de IAM, tal como se especifica en el conjunto de permisos correspondiente del Centro de Identidad de IAM (más específicamente, el Centro de Identidad de IAM asume una función de IAM, que administra el Centro de Identidad de IAM, en la cuenta de destino). Las sesiones de IAM persisten incondicionalmente durante el tiempo especificado para el conjunto de permisos.

**Note**

El Centro de identidad de IAM no admite el cierre de sesión único de SAML iniciado por un proveedor de identidad que actúe como fuente de identidad y no envía el cierre de sesión único de SAML a las aplicaciones de SAML que utilizan el Centro de identidades de IAM como proveedor de identidad.

Cuando un administrador del Centro de Identidad de IAM [elimina](#) o [deshabilita](#) a un usuario, el usuario pierde inmediatamente el acceso al portal de acceso y no puede volver a iniciar sesión para iniciar una nueva aplicación o sesión de rol de IAM. AWS El usuario perderá el acceso a las sesiones de la aplicación existentes en 30 minutos. Todas las sesiones de rol de IAM existentes continuarán en función de la duración de la sesión configurada en el conjunto de permisos del Centro de Identidad de IAM. La duración máxima de la sesión puede ser de 12 horas.

Cuando un administrador del Centro de Identidad de IAM [revoca la sesión de un usuario](#) o cuando un usuario cierra sesión, el usuario pierde inmediatamente el acceso al portal de AWS acceso y se le pide que vuelva a iniciar sesión para iniciar una nueva sesión de aplicación o rol de IAM. El usuario perderá el acceso a las sesiones de la aplicación existentes en 30 minutos. Todas las sesiones de rol de IAM existentes continuarán en función de la duración de la sesión configurada en el conjunto de permisos del Centro de Identidad de IAM. La duración máxima de la sesión puede ser de 12 horas.

En la siguiente tabla se resumen los comportamientos del IAM Identity Center descritos anteriormente:

| Acción                | El usuario pierde el acceso al centro de identidad de IAM | El usuario no puede crear nuevas sesiones de aplicación | El usuario no puede acceder a las sesiones de aplicación existentes | El usuario pierde el acceso a las Cuenta de AWS sesiones existentes                                |
|-----------------------|-----------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| Usuario deshabilitado | Con efecto inmediato                                      | Con efecto inmediato                                    | En 30 minutos                                                       | Dentro de 12 horas o menos. La duración depende de la duración de caducidad de la sesión de rol de |

|                            |                                                                  |                                                         |                                                                     |                                                                                                                                                  |
|----------------------------|------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Acción                     | El usuario pierde el acceso al centro de identidad de IAM        | El usuario no puede crear nuevas sesiones de aplicación | El usuario no puede acceder a las sesiones de aplicación existentes | El usuario pierde el acceso a las Cuenta de AWS sesiones existentes                                                                              |
|                            |                                                                  |                                                         |                                                                     | IAM configurada para el conjunto de permisos.                                                                                                    |
| Usuario eliminado          | Con efecto inmediato                                             | Con efecto inmediato                                    | En 30 minutos                                                       | Dentro de 12 horas o menos. La duración depende de la duración de caducidad de la sesión de rol de IAM configurada para el conjunto de permisos. |
| Sesión de usuario revocada | El usuario debe volver a iniciar sesión para recuperar el acceso | Con efecto inmediato                                    | En 30 minutos                                                       | Dentro de 12 horas o menos. La duración depende de la duración de caducidad de la sesión de rol de IAM configurada para el conjunto de permisos. |

| Acción                   | El usuario pierde el acceso al centro de identidad de IAM        | El usuario no puede crear nuevas sesiones de aplicación | El usuario no puede acceder a las sesiones de aplicación existentes | El usuario pierde el acceso a las Cuenta de AWS sesiones existentes                                                                              |
|--------------------------|------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| El usuario cierra sesión | El usuario debe volver a iniciar sesión para recuperar el acceso | Con efecto inmediato                                    | En 30 minutos                                                       | Dentro de 12 horas o menos. La duración depende de la duración de caducidad de la sesión de rol de IAM configurada para el conjunto de permisos. |

Cuando un administrador del Centro de Identidad de IAM [elimina el acceso a las aplicaciones](#), el usuario pierde el acceso a las aplicaciones existentes. El acceso del usuario a las aplicaciones existentes se pierde una hora después de eliminar el acceso a la aplicación. Todas las sesiones de rol de IAM existentes continuarán en función de la duración de la sesión configurada en el conjunto de permisos del Centro de Identidad de IAM. La duración máxima de la sesión puede ser de 12 horas.

En la siguiente tabla se resumen los comportamientos del IAM Identity Center descritos anteriormente:

| Acción                                       | El usuario pierde el acceso al centro de identidad de IAM | El usuario no puede crear nuevas sesiones de aplicación | El usuario no puede acceder a las sesiones de aplicación existentes | El usuario pierde el acceso a las Cuenta de AWS sesiones existentes |
|----------------------------------------------|-----------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|---------------------------------------------------------------------|
| Se ha eliminado la aplicación o el Cuenta de | No, el usuario puede seguir accediendo                    | Con efecto inmediato                                    | Dentro de 1 hora                                                    | Dentro de 12 horas o menos. La duración                             |

| Acción                                                                         | El usuario pierde el acceso al centro de identidad de IAM            | El usuario no puede crear nuevas sesiones de aplicación | El usuario no puede acceder a las sesiones de aplicación existentes | El usuario pierde el acceso a las Cuenta de AWS sesiones existentes                                                                              |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| AWS acceso del usuario                                                         | al Centro de identidad de IAM                                        |                                                         |                                                                     | depende de la duración de caducidad de la sesión de rol de IAM configurada para el conjunto de permisos.                                         |
| Usuario eliminado del grupo al que se le asignó una aplicación o Cuenta de AWS | No: el usuario puede seguir accediendo al Centro de identidad de IAM | En menos de 1 hora                                      | Dentro de 2 horas                                                   | Dentro de 12 horas o menos. La duración depende de la duración de caducidad de la sesión de rol de IAM configurada para el conjunto de permisos. |
| Se ha eliminado la aplicación o el Cuenta de AWS acceso del grupo              | No, el usuario puede seguir accediendo al Centro de identidad de IAM | Con efecto inmediato                                    | Dentro de 1 hora                                                    | Dentro de 12 horas o menos. La duración depende de la duración de caducidad de la sesión de rol de IAM configurada para el conjunto de permisos. |



# Revocar el acceso a los usuarios eliminados

Para revocar inmediatamente el acceso para realizar llamadas a la API autorizadas cuando un usuario del Centro de Identidad de IAM esté deshabilitado o eliminado, puede:

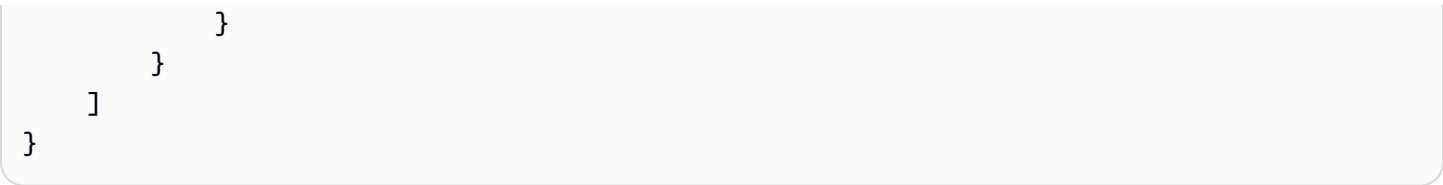
1. Añada o actualice la política integrada de los conjuntos de permisos asignados al usuario añadiendo un Deny efecto explícito a todas las acciones que se realicen en todos los recursos.
2. Especifique la clave de `identitystore:user_id` condición `aws:user_id` or.

Como alternativa, puedes usar una [política de control de servicios](#) para revocar el acceso del usuario a todas las cuentas de los miembros de tu organización.

## Example SCPs para revocar el acceso

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:UserId": "*:deleteduser@domain.com"
        }
      }
    }
  ]
}
```

```
{
  "Version": "2012-10-17",
  "Statement" : [
    {
      "Effect": "Deny",
      "Action": "*",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "identitystore:UserId": "DELETEDUSER_ID"
        }
      }
    }
  ]
}
```



# Conecte a los usuarios del personal

IAM Identity Center es la AWS solución de para conectar a su personal con aplicaciones AWS administradas de, como Amazon Q Developer y Amazon QuickSight, y otros AWS recursos de. Puede conectar su proveedor de identidad actual y sincronizar los usuarios y grupos de su directorio, o bien crear y gestionar sus usuarios directamente en el IAM Identity Center.

¿Ya utilizas IAM para acceder a? Cuentas de AWS

No necesita realizar ningún cambio en sus Cuenta de AWS flujos de trabajo de actuales para utilizar el Centro de identidades de IAM y acceder a las aplicaciones AWS administradas de. Si utiliza la [federación con IAM](#) o usuarios de IAM para el Cuenta de AWS acceso a, sus usuarios pueden seguir Cuentas de AWS accediendo a de la misma manera que siempre lo han hecho y usted puede seguir utilizando sus flujos de trabajo actuales para gestionar ese acceso.

## Temas

- [Usuarios, grupos y aprovisionamiento en IAM Identity Center](#)
- [Administración de su fuente de identidad](#)
- [Uso del portal de AWS acceso](#)
- [Autenticación multifactor para usuarios de Identity Center](#)

## Usuarios, grupos y aprovisionamiento en IAM Identity Center

El Centro de identidades de IAM le permite controlar quién puede iniciar sesión y a qué recursos puede acceder. Se debe aprovisionar a un usuario para iniciar sesión. A continuación, puede asignar el acceso solo a los usuarios o grupos aprovisionados.

Obtenga información sobre el aprovisionamiento de usuarios y grupos, ya sea que provengan de un proveedor de identidad externo o se hayan creado directamente en el IAM Identity Center.

## Exclusividad del nombre de usuario y de la dirección de correo electrónico

El Centro de Identidad de IAM requiere que cada usuario tenga un nombre de usuario único. El nombre de usuario es el identificador principal del usuario. El nombre de usuario no tiene que coincidir con la dirección de correo electrónico del usuario. IAM Identity Center exige que todos los

nombres de usuario y direcciones de correo electrónico de sus usuarios no sean nulos y que sean únicos.

## Grupos

Los grupos son una combinación lógica de usuarios que usted define. Puede crear grupos y agregar usuarios a los grupos. IAM Identity Center no admite grupos anidados (un grupo dentro de otro grupo). Los grupos son útiles a la hora de asignar el acceso a las Cuentas de AWS y a las aplicaciones. En lugar de asignarlo a cada usuario de manera individual, concede permisos a un grupo. Más adelante, al agregar o eliminar usuarios de un grupo, el usuario obtiene o pierde de forma dinámica el acceso a las cuentas y aplicaciones que haya asignado al grupo.

## Aprovisionamiento de usuarios y grupos

El aprovisionamiento es el proceso de poner la información de usuarios y grupos a disposición de IAM Identity Center y de las aplicaciones administradas por o las aplicaciones AWS administradas por el cliente. Puede crear usuarios y grupos directamente en IAM Identity Center o conectar su fuente de identidad a IAM Identity Center. Con el Centro de identidad de IAM, puede asignar a los usuarios y grupos el acceso a las aplicaciones conectadas y. Cuentas de AWS

El aprovisionamiento en IAM Identity Center varía en función de la fuente de identidades que utilice. Para obtener más información, consulte [Administración de su fuente de identidad](#).

## Desaprovisionamiento de usuarios y grupos

El desaprovisionamiento es el proceso de eliminar la información de usuarios y grupos del Centro de identidades de IAM.

Si utiliza Active Directory o un proveedor de identidades externo con IAM Identity Center, debe eliminar usuarios y grupos de estas fuentes de identidad de IAM en lugar de IAM Identity Center. La eliminación de los usuarios y grupos de IAM Identity Center no los eliminará por completo si su fuente de identidad es Active Directory o un proveedor de identidades externo. Si ha configurado el aprovisionamiento automático de los usuarios de su IdP al Centro de Identidad de IAM, estos usuarios y grupos previamente eliminados se volverán a aprovisionar en el Centro de Identidad de IAM.

Si necesita desaprovisionar usuarios o grupos del IAM Identity Center, primero debe [eliminar cualquier asignación de conjuntos de permisos](#) o aplicaciones a los usuarios o grupos que desee

desaprovisionar. De lo contrario, tendrá conjuntos de permisos y asignaciones de aplicaciones sin asignar en su centro de identidad de IAM.

## Administración de su fuente de identidad

Su origen de identidad en IAM Identity Center define dónde se administran sus usuarios y grupos. Después de configurar la fuente de identidad, puede buscar usuarios o grupos para concederles acceso de inicio de sesión único a Cuentas de AWS las aplicaciones o a ambos.

Solo puede tener una fuente de identidad por organización en AWS Organizations. Puede elegir una de las siguientes opciones como origen de identidad:

- **Proveedor de identidad externo:** elija esta opción si desea administrar los usuarios en un proveedor de identidad externo (IdP), como Okta o Microsoft Entra ID.
- **Active Directory:** elija esta opción si desea seguir administrando los usuarios de su AWS Managed Microsoft AD directorio mediante AWS Directory Service o del directorio autogestionado de Active Directory (AD).
- **Directorio de Identity Center:** cuando se activa IAM Identity Center por primera vez, se configura de manera automática con un directorio de Identity Center como fuente de identidad predeterminada. Con el directorio de Identity Center, puede crear sus usuarios y grupos y asignar su nivel de acceso a sus aplicaciones Cuentas de AWS y a las suyas.

### Note

El Centro de Identidad de IAM no SAMBA4 admite Simple AD como fuente de identidad.

### Temas

- [Consideraciones para cambiar la fuente de identidad](#)
- [Cambiar su fuente de identidad](#)
- [Administre el inicio de sesión y el uso de atributos para todos los tipos de fuentes de identidad](#)
- [Administración de identidades en IAM Identity Center](#)
- [Conexión un directorio Microsoft AD](#)
- [Administrar un proveedor de identidades externo](#)

## Consideraciones para cambiar la fuente de identidad

Aunque puede cambiar su fuente de identidad en cualquier momento, le recomendamos que considere cómo este cambio podría afectar a su implementación actual.

Si ya administra usuarios y grupos en un origen de identidad, cambiar a un origen de identidad diferente podría eliminar todas las asignaciones de usuarios y grupos que configuró en IAM Identity Center. Si esto ocurre, todos los usuarios, incluido el usuario administrativo del Centro de identidades de IAM, perderán el acceso de inicio de sesión único a sus Cuentas de AWS aplicaciones.

No cambie la fuente de identidad de IAM Identity Center sin revisar las siguientes consideraciones antes de proceder. Si desea continuar con el cambio de la fuente de identidad, consulte [Cambiar su fuente de identidad](#) para obtener más información.

### Cambiar entre el directorio del Centro de Identidad de IAM y Active Directory

Si ya administra usuarios y grupos en Active Directory, le recomendamos que considere la posibilidad de conectar su directorio al habilitar IAM Identity Center y elegir su fuente de identidad. Esto debe hacerse antes de crear usuarios y grupos en el directorio predeterminado de Identity Center y de realizar cualquier asignación.

Si ya administra usuarios y grupos en el directorio predeterminado de Identity Center, tenga en cuenta lo siguiente:

- **Asignaciones, usuarios y grupos eliminados:** al cambiar la fuente de identidad a Active Directory, se eliminan los usuarios y grupos del directorio de Identity Center. Este cambio también elimina las asignaciones. En este caso, después de cambiar a Active Directory, debe sincronizar los usuarios y grupos de Active Directory con el directorio de Identity Center y, a continuación, volver a aplicar sus asignaciones.

Si decide no usar Active Directory, debe crear los usuarios y grupos en el directorio de Identity Center y, a continuación, realizar las asignaciones.

- **Las asignaciones no se eliminan cuando se eliminan las identidades:** cuando se eliminan las identidades del directorio de Identity Center, las asignaciones correspondientes también se eliminan en IAM Identity Center. Sin embargo, cuando se eliminan las identidades (ya sea en Active Directory o en las identidades sincronizadas) en Active Directory, las asignaciones correspondientes no se eliminan.
- **Sin sincronización saliente para APIs:** si utiliza Active Directory como fuente de identidad, le recomendamos que utilice las opciones de [creación, actualización y eliminación APIs con](#)

[precaución](#). El Centro de identidades de IAM no admite la sincronización saliente, por lo que su fuente de identidad no se actualiza automáticamente con los cambios que realiza en los usuarios o grupos que la utilizan. APIs

- La URL del portal de acceso cambiará: al cambiar la fuente de identidad entre el IAM Identity Center y Active Directory, también se cambiará la URL del portal de acceso. AWS
- Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs, los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Autenticación mediante el IAM Identity Center](#).

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Conexión un directorio Microsoft AD](#).

## Cómo cambiar de IAM Identity Center a un IdP externo

Si cambia la fuente de identidad de IAM Identity Center a un proveedor de identidades (IdP) externo, tenga en cuenta lo siguiente:

- Las asignaciones y las membresías funcionan con las aserciones correctas: las asignaciones de usuario, las asignaciones grupales y las pertenencias a grupos seguirán funcionando siempre y cuando el nuevo IdP envíe las aserciones correctas (por ejemplo, el nombre SAML). IDs Estas confirmaciones deben coincidir con los nombres de usuario y grupos de IAM Identity Center.
- No hay sincronización saliente: IAM Identity Center no admite la sincronización saliente, por lo que su IdP externo no se actualizará automáticamente con los cambios en los usuarios y grupos que realice en IAM Identity Center.
- Aprovisionamiento de SCIM: si está usando el aprovisionamiento de SCIM, los cambios en los usuarios y grupos de su proveedor de identidades solo se reflejan en IAM Identity Center después de que su proveedor de identidades los envíe a IAM Identity Center. Consulte [Consideraciones para utilizar el aprovisionamiento automático](#).
- Retroceso: puede volver a utilizar su fuente de identidad para que utilice el IAM Identity Center en cualquier momento. Consulte [Cambiar de un IdP externo a IAM Identity Center](#).
- Las sesiones de usuario existentes se revocan al expirar la duración de la sesión: una vez que cambia su fuente de identidad a un proveedor de identidad externo, las sesiones de usuario activas se conservan durante el resto de la duración máxima de sesión configurada en la consola. Por ejemplo, si la duración de la sesión del portal de AWS acceso está establecida en ocho horas y cambiaste la fuente de identidad en la cuarta hora, las sesiones de usuario activas se

mantendrán durante cuatro horas más. Para revocar las sesiones de usuario, consulte [Elimine las sesiones de usuario activas del portal de AWS acceso y las aplicaciones AWS integradas](#).

- Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs, los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Autenticación mediante el IAM Identity Center](#).

 Note

No podrá revocar las sesiones de los usuarios desde la consola del IAM Identity Center después de eliminar el usuario.

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Administrar un proveedor de identidades externo](#).

## Cambiar de un IdP externo a IAM Identity Center

Si cambia la fuente de identidad de un proveedor de identidades (IdP) externo a IAM Identity Center, tenga en cuenta lo siguiente:

- IAM Identity Center conserva todas sus asignaciones.
- Forzar el restablecimiento de la contraseña: los usuarios que tenían contraseñas en IAM Identity Center pueden seguir iniciando sesión con sus contraseñas anteriores. Para los usuarios que estaban en el IdP externo y no en IAM Identity Center, el administrador debe forzar el restablecimiento de la contraseña.
- Las sesiones de usuario existentes se revocan al expirar la duración de la sesión: una vez que cambie su fuente de identidad al IAM Identity Center, las sesiones de usuario activas se conservan durante el resto de la duración máxima de sesión configurada en la consola. Por ejemplo, si la duración de la sesión del portal de AWS acceso es de ocho horas y ha cambiado la fuente de identidad a la cuarta hora, las sesiones de usuario activas seguirán ejecutándose durante cuatro horas más. Para revocar las sesiones de usuario, consulte [Elimine las sesiones de usuario activas del portal de AWS acceso y las aplicaciones AWS integradas](#).
- Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs, los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Autenticación mediante el IAM Identity Center](#).



 Note

No podrá revocar las sesiones de los usuarios desde la consola del IAM Identity Center después de eliminar el usuario.

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Administración de identidades en IAM Identity Center](#).

## Cambiar de un IdP externo a otro IdP externo

Si ya utiliza un IdP externo como fuente de identidad para IAM Identity Center y cambia a un IdP externo diferente, tenga en cuenta lo siguiente:

- Las asignaciones y las membresías funcionan con las confirmaciones correctas: IAM Identity Center conserva todas sus tareas. Las asignaciones de usuarios, las asignaciones de grupos y las pertenencias a grupos seguirán funcionando siempre que el nuevo IdP envíe las afirmaciones correctas (por ejemplo, el nombre SAML). IDs

Estas confirmaciones deben coincidir con los nombres de usuario de IAM Identity Center cuando los usuarios se autentican a través del nuevo IdP externo.

- Aprovisionamiento de SCIM: si utiliza SCIM para el aprovisionamiento en IAM Identity Center, le recomendamos que revise la información específica del IdP en esta guía y la documentación proporcionada por el IdP para asegurarse de que el nuevo proveedor haga coincidir correctamente los usuarios y los grupos cuando SCIM esté habilitado.
- Las sesiones de usuario existentes se revocan al expirar la duración de la sesión: una vez que cambie su fuente de identidad a otro proveedor de identidad externo, las sesiones de usuario activas se conservan durante el tiempo restante de la duración máxima de sesión configurada en la consola. Por ejemplo, si la duración de la sesión del portal de AWS acceso es de ocho horas y cambiaste la fuente de identidad a las cuatro horas, las sesiones de usuario activas se mantendrán durante cuatro horas más. Para revocar las sesiones de usuario, consulte [Elimine las sesiones de usuario activas del portal de AWS acceso y las aplicaciones AWS integradas](#).
- Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs, los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Autenticación mediante el IAM Identity Center](#).

 Note

No podrá revocar las sesiones de los usuarios desde la consola del IAM Identity Center después de eliminar el usuario.

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Administrar un proveedor de identidades externo](#).

## Cambiar de Active Directory a un IdP externo

Si cambia la fuente de identidad de un IdP externo a Active Directory o de Active Directory a un IdP externo, tenga en cuenta lo siguiente:

- Se eliminan los usuarios, los grupos y las asignaciones: todos los usuarios, grupos y asignaciones se eliminan de IAM Identity Center. Ninguna información de usuario o grupo se ve afectada ni en el IdP externo ni en Active Directory.
- Aprovisionamiento de usuarios: si cambia a un IdP externo, debe configurar IAM Identity Center para aprovisionar a los usuarios. Como alternativa, debe aprovisionar manualmente los usuarios y grupos para el IdP externo antes de poder configurar las asignaciones.
- Creación de asignaciones y grupos: si cambia a Active Directory, debe crear asignaciones con los usuarios y grupos que se encuentran en el directorio de Active Directory.
- Si los usuarios se eliminan o deshabilitan en la consola del IAM Identity Center mediante Identity Store APIs, los usuarios con sesiones activas pueden seguir accediendo a las aplicaciones y cuentas integradas. Para obtener información sobre la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Autenticación mediante el IAM Identity Center](#).

Para obtener información sobre cómo IAM Identity Center aprovisiona usuarios y grupos, consulte [Conexión un directorio Microsoft AD](#).

## Cambiar su fuente de identidad

El siguiente procedimiento describe cómo cambiar de un directorio que proporciona IAM Identity Center (el directorio predeterminado de Identity Center) a Active Directory o a un proveedor de identidad externo, o viceversa. Antes de continuar, revise la información incluida en [Consideraciones para cambiar la fuente de identidad](#). Para completar este procedimiento, necesitará una instancia

de organización de IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

 Warning

En función de su implementación actual, este cambio elimina cualquier asignación de usuarios y grupos que haya configurado en el Centro de identidades de IAM. Este cambio también eliminará sus funciones de IAM establecidas en el conjunto de permisos. Cuentas de AWS En consecuencia, es posible que deba actualizar sus políticas de recursos y asegurarse de que esto no interrumpa su acceso a AWS KMS las claves y a los clústeres de Amazon EKS. Para obtener más información, consulte [Hacer referencia a conjuntos de permisos en políticas de recursos, mapas de configuración de Amazon EKS Cluster y políticas AWS KMS clave](#).

Cuando esto ocurra, todos los usuarios y grupos, incluido el usuario administrativo del Centro de Identidad de IAM, perderán el acceso de inicio de sesión único a sus Cuentas de AWS aplicaciones.

Cómo cambiar la fuente de identidad:

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de Configuración, seleccione la pestaña Origen de la identidad. Elija Acciones y, a continuación, elija Cambiar fuente de identidad.
4. En Elegir fuente de identidad, seleccione la fuente a la que desee cambiar y, a continuación, seleccione Siguiente.

Si va a cambiar a Active Directory, elija el directorio disponible en el menú de la página siguiente.

 Important

Al cambiar la fuente de identidad a o desde Active Directory, se eliminan los usuarios y grupos del directorio de Identity Center. Este cambio también elimina cualquier asignación que haya configurado en IAM Identity Center.

Si va a cambiar a un proveedor de identidad externo, recomendamos que siga los pasos descritos en [Cómo conectarse a un proveedor de identidades externo](#).

5. Cuando haya leído el aviso legal y esté listo para continuar, introduzca Aceptar.
6. Elija Cambiar fuente de identidad. Si va a cambiar su fuente de identidad a Active Directory, vaya al siguiente paso.
7. Si cambia la fuente de identidad a Active Directory, accederá a la página de Configuración. Utilice la página de configuración para realizar cualquiera de las siguientes operaciones:
  - Seleccione Iniciar la configuración guiada. Para obtener información sobre cómo completar el proceso de configuración guiada, consulte [Configuración guiada](#).
  - En la sección Fuente de identidad, elija Acciones y, a continuación, elija Administrar la sincronización para configurar el Alcance de la sincronización, la lista de usuarios y grupos que se van a sincronizar.

## Administre el inicio de sesión y el uso de atributos para todos los tipos de fuentes de identidad

El IAM Identity Center permite a los administradores controlar el uso del portal de AWS acceso, establecer la duración de las sesiones para los usuarios del portal de AWS acceso y sus aplicaciones, y utilizar atributos para el control de acceso. Estas características funcionan con un directorio de Identity Center o con un proveedor de identidad externo como su fuente de identidad.

### Atributos de usuario y grupo compatibles en IAM Identity Center

Los atributos son fragmentos de información que le ayudan a definir e identificar a usuarios individuales o a agrupar objetos, como `name`, `email` o `members`. IAM Identity Center admite los atributos más utilizados, independientemente de si se introducen de forma manual durante la creación del usuario o si se aprovisionan de forma automática mediante un motor de sincronización, como el definido en la especificación del sistema de administración de identidades entre dominios (SCIM).

- [Para obtener más información sobre la especificación del Sistema de gestión de identidades entre dominios \(SCIM\), consulte /rfc7642. <https://tools.ietf.org/html>](#)
- Para obtener más información sobre el aprovisionamiento manual y automático, consulte [Aprovisionamiento cuando los usuarios provienen de un IdP externo](#).

- Para obtener más información acerca de la asignación de atributos, consulte [Asignaciones de atributos entre Centro de identidades de IAM y directorio de proveedores de identidades externos](#).

Dado que IAM Identity Center admite el SCIM para los casos de uso del aprovisionamiento automático, el directorio de Identity Center admite todos los mismos atributos de usuario y grupo que figuran en la especificación del SCIM, con algunas excepciones. En las siguientes secciones, se describen los atributos que IAM Identity Center no admite.

### Objetos del usuario

El almacén de identidades del IAM Identity Center admite todos los atributos del esquema de usuario del SCIM (<https://tools.ietf.org/html/rfc7643#section-8.3>), excepto los siguientes:

- password
- ims
- photos
- entitlements
- x509Certificates

Se admiten todos los subatributos de los usuarios, excepto los siguientes:

- Subatributo 'display' de cualquier atributo con valores múltiples (por ejemplo, emails o phoneNumbers)
- Subatributo 'version' del atributo 'meta'

### Agrupar objetos

[Se admiten todos los atributos del esquema de grupo SCIM \(/rfc7643#section-8.4\). https://tools.ietf.org/html](#)

Se admiten todos los subatributos de los grupos, excepto los siguientes:

- Subatributo 'display' de cualquier atributo con valores múltiples (por ejemplo, miembros).

### Temas

- [Configure la duración de la sesión del portal de acceso AWS y de las aplicaciones integradas del IAM Identity Center](#)

- [Elimine las sesiones de usuario activas del portal de AWS acceso y las aplicaciones AWS integradas](#)

## Configure la duración de la sesión del portal de acceso AWS y de las aplicaciones integradas del IAM Identity Center

El administrador del IAM Identity Center puede configurar la duración de la sesión tanto para las aplicaciones integradas con el IAM Identity Center como para Portal de acceso a AWS. La duración de la sesión de autenticación en las aplicaciones integradas en el IAM Identity Center Portal de acceso a AWS y en las aplicaciones integradas es el tiempo máximo que un usuario puede iniciar sesión sin volver a autenticarse. El administrador del IAM Identity Center puede finalizar una sesión activa en el portal de AWS acceso y, al hacerlo, también finalizar las sesiones de las aplicaciones integradas.

De forma predeterminada, la sesión es de 8 horas. El IAM Identity Center puede especificar una duración diferente, que puede variar entre un mínimo de 15 minutos y un máximo de 90 días. El valor de duración personalizado debe introducirse en minutos y debe estar comprendido entre 15 y 10080 minutos (7 días). Para obtener más información acerca de la duración de la sesión de autenticación y el comportamiento de los usuarios, consulte [Autenticación mediante el IAM Identity Center](#).

### Note

La AWS modificación de la duración de la sesión del portal de AWS acceso y la finalización de las sesiones del portal de acceso no afectan a la duración de la AWS Management Console sesión que defina en sus conjuntos de permisos.

En los temas siguientes se proporciona información sobre la configuración de la duración de la sesión del portal de acceso AWS y de las aplicaciones integradas del IAM Identity Center.

### Requisitos y consideraciones previos

Los siguientes son los requisitos previos y las consideraciones para configurar la duración de la sesión para el portal de AWS acceso y las aplicaciones integradas del IAM Identity Center.

### Proveedores de identidades externos

El IAM Identity Center utiliza los atributos de `SessionNotOn0rAfter` de las aserciones de SAML para ayudar a determinar durante cuánto tiempo puede ser válida la sesión.

- Si `SessionNotOnOrAfter` se incluye en una afirmación de SAML, la duración de una sesión del portal de AWS acceso no se ve afectada por la duración de la sesión de IdP externa. Por ejemplo, si la duración de su sesión de IdP es de 24 horas y ha establecido una duración de sesión de 18 horas en el Centro de identidad de IAM, sus usuarios deberán volver a autenticarse en el AWS portal de acceso después de 18 horas.
- Si `SessionNotOnOrAfter` se incluye en una afirmación de SAML, el valor de duración de la sesión se establece en la duración de la sesión del portal de AWS acceso y la duración de la sesión de IDP de SAML, que sea menor. Si establece una duración de sesión de 72 horas en el Centro de identidades de IAM y su IdP tiene una duración de sesión de 18 horas, sus usuarios tendrán acceso a los AWS recursos durante las 18 horas definidas en su IdP.
- Si la duración de la sesión de su IdP es superior a la establecida en el IAM Identity Center, sus usuarios podrán iniciar una nueva sesión en el IAM Identity Center sin tener que volver a introducir sus credenciales, en función de la sesión de inicio de sesión aún válida con su IdP.

## AWS CLI y sesiones de SDK

Si utiliza los AWS Command Line Interface kits de desarrollo de AWS software (SDKs) u otras herramientas de AWS desarrollo para acceder a los AWS servicios mediante programación, debe cumplir los siguientes requisitos previos para establecer la duración de la sesión para el portal de AWS acceso y las aplicaciones integradas del IAM Identity Center.

- Debe [configurar la duración de la sesión del portal de AWS acceso](#) en la consola del IAM Identity Center.
- Debe definir un perfil para la configuración de inicio de sesión único en su archivo de configuración compartido de AWS . Este perfil se utiliza para conectarse al portal de AWS acceso. Le recomendamos que utilice la configuración del proveedor de tokens de SSO. Con esta configuración, el AWS SDK o la herramienta pueden recuperar automáticamente los tokens de autenticación actualizados. Para obtener más información, consulte [Configuración del proveedor de tokens de SSO](#) en la Guía de referencia de los SDK y las herramientas de AWS .
- Los usuarios deben ejecutar una versión del SDK AWS CLI o una versión que sea compatible con la administración de sesiones.

## Versiones mínimas de la AWS CLI que admiten la administración de sesiones

Las siguientes son las versiones mínimas de las AWS CLI que admiten la administración de sesiones.

- AWS CLI V2 2.9 o posterior
- AWS CLI V1 1.27.10 o posterior

Para obtener información sobre cómo instalar o actualizar la última AWS CLI versión, consulte [Instalación o actualización de la última versión de AWS CLI](#).

Si sus usuarios están ejecutando el conjunto de permisos AWS CLI, si actualiza el conjunto de permisos justo antes de que caduque la sesión del Centro de Identidad de IAM y la duración de la sesión se establece en 20 horas, mientras que la duración del conjunto de permisos se establece en 12 horas, la AWS CLI sesión se prolongará durante un máximo de 20 horas más 12 horas para un total de 32 horas. Para obtener más información sobre la CLI de IAM Identity Center, consulte [Referencia de comandos de la AWS CLI](#).

Estas versiones como mínimo SDKs admiten la gestión de sesiones del IAM Identity Center

Las siguientes son las versiones mínimas de las SDKs que admiten la gestión de sesiones del IAM Identity Center.

| SDK     | Versión mínima                                                                                  |
|---------|-------------------------------------------------------------------------------------------------|
| Python  | 1.26.10                                                                                         |
| PHP     | 3,245.0                                                                                         |
| Ruby    | aws-sdk-core 3.167,0                                                                            |
| Java V2 | AWS SDK para Java v2 (2.18.13)                                                                  |
| Go V2   | SDK completo: versión 11/11/2022 y módulos Go específicos: 1.18.0 credentials/v1.13.0, config/v |
| JS V2   | 2.1253.0                                                                                        |
| JS V3   | v3.210.0                                                                                        |
| C++     | 1.9.372                                                                                         |
| .NET    | v3.7.400.0                                                                                      |



## Temas

- [Cómo configurar la duración de sesiones de la aplicación](#)
- [Cómo extender la duración de la sesión para Amazon Q Developer](#)

### Cómo configurar la duración de sesiones de la aplicación

Los administradores del IAM Identity Center pueden ampliar la duración de las sesiones en función de las necesidades empresariales específicas, por ejemplo, adaptarse a tareas de larga duración y minimizar la necesidad de que los usuarios se vuelvan a autenticar.

Utilice el siguiente procedimiento para configurar la duración de la sesión del portal de AWS acceso y de las aplicaciones integradas de IAM Identity Center.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de Configuración, seleccione la pestaña Autenticación.
4. En Autenticación, junto a Configuración de sesión, elija Configurar. Aparecerá el cuadro de diálogo Configurar los ajustes de la sesión.
5. En el cuadro de diálogo Establecer la configuración, elija la duración máxima de la sesión en minutos, horas y días para sus usuarios a través de la flecha desplegable. Elija la duración de la sesión y, a continuación, seleccione Guardar. Vuelva a la página Configuración.

### Cómo extender la duración de la sesión para Amazon Q Developer

Si sus desarrolladores utilizan Amazon Q Developer como parte de un entorno de desarrollo integrado (IDE), puede establecer la duración de la sesión para Amazon Q Developer en 90 días. En función de cuándo haya activado el IAM Identity Center, es posible que la duración prolongada de la sesión para Amazon Q Developer esté habilitada de forma predeterminada. Esta sesión extendida no afecta a la duración de la sesión Portal de acceso a AWS ni a la de otras aplicaciones integradas del IAM Identity Center.

#### Note

Se puede acceder a Amazon Q Developer desde consolas configuradas como comerciales Regiones de AWS que están habilitadas de forma predeterminada. Si su instancia del IAM Identity Center se encuentra en una región en la que actualmente no se puede acceder a

Amazon Q Developer, habilitar una duración de sesión prolongada de 90 días no anulará la configuración predeterminada. Esto significa que la duración de la sesión permanece inalterada, independientemente de si habilita una duración de sesión prolongada de 90 días o no. Para obtener más información, consulte [Regiones compatibles con Amazon Q Developer](#).

Habilitar o deshabilitar la duración prolongada de la sesión de 90 días para Amazon Q Developer.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de Configuración, seleccione la pestaña Autenticación.
4. En Autenticación, junto a Configuración de sesión, elija Configurar. Aparecerá el cuadro de diálogo Configurar los ajustes de la sesión.
5. En el cuadro de diálogo Configurar los ajustes de sesión, seleccione la casilla Habilitar sesiones extendidas para Amazon Q Developer. Desactive la casilla de verificación para deshabilitar la duración prolongada de la sesión.
6. Pulse Guardar para volver a la página de configuración.

## Elimine las sesiones de usuario activas del portal de AWS acceso y las aplicaciones AWS integradas

Los administradores del IAM Identity Center pueden eliminar las sesiones de usuario activas. La eliminación de las sesiones de usuario permite a los administradores revocar el acceso y eliminar las sesiones obsoletas cuando los usuarios ya no necesitan o no deben mantener su estado de autenticación actual, por ejemplo, cuando un empleado deja la organización o sus permisos cambian.

Utilice el siguiente procedimiento para ver y eliminar las sesiones activas de un usuario en el IAM Identity Center.

### Note

Al eliminar una sesión activa de un usuario del Centro de Identidad de IAM, no se elimina ninguna sesión de rol de IAM activa en el AWS Management Console quirófano. AWS CLI

Para eliminar una sesión activa del portal de AWS acceso y de las aplicaciones integradas en el Centro de Identidad de IAM

1. Abra la [consola de IAM Identity Center](#).
2. Seleccione Usuarios.
3. En la página Usuarios, elija el nombre de usuario cuyas sesiones desee administrar. Esto lo dirigirá a una página con la información del usuario.
4. En la página del usuario, elija la pestaña Sesiones activas. El número entre paréntesis junto a Sesiones activas indica el número de sesiones activas actuales de este usuario.
5. Seleccione las casillas de verificación situadas junto a las identidades que desea eliminar y elija Eliminar sesión. Aparecerá un cuadro de diálogo que confirma que está eliminando las sesiones activas de este usuario. Lea la información en el cuadro de diálogo y, si desea continuar, elija Eliminar sesión.
6. Se le devuelve a la página del usuario. Aparecerá una barra de flash verde para indicar que las sesiones seleccionadas se eliminaron correctamente.

Para obtener más información sobre el comportamiento de las sesiones de autenticación revocadas, consulte [Sesiones de autenticación](#).

## Administración de identidades en IAM Identity Center

IAM Identity Center ofrece las siguientes funciones para sus usuarios y grupos:

- Cree sus usuarios y grupos.
- Añada sus usuarios como miembros a los grupos.
- Asignación de los grupos con el nivel de acceso deseado a sus Cuentas de AWS y aplicaciones.

Para administrar los usuarios y los grupos en el almacén de IAM Identity Center, AWS es compatible con las operaciones de la API que se indican en [Identity Center Actions](#).

## Aprovisionamiento cuando los usuarios están en IAM Identity Center

Al crear usuarios y grupos directamente en IAM Identity Center, el aprovisionamiento es automático. Estas identidades están disponibles de inmediato para su uso al realizar asignaciones y para que las utilicen las aplicaciones. Para obtener más información, consulte [Aprovisionamiento de usuarios y grupos](#).

## Cambio de su fuente de identidad

Si prefiere administrar los usuarios en AWS Managed Microsoft AD, puede dejar de usar el directorio de Identity Center en cualquier momento y, en su lugar, conectar IAM Identity Center al directorio de Microsoft AD mediante AWS Directory Service. Para obtener información, consulte las consideraciones para [Cambiar entre el directorio del Centro de Identidad de IAM y Active Directory](#).

Si prefiere administrar los usuarios en un proveedor de identidades (IdP) externo, puede conectar IAM Identity Center a su IdP y habilitar el aprovisionamiento automático. Para obtener información, consulte las consideraciones para [Cómo cambiar de IAM Identity Center a un IdP externo](#).

### Temas

- [Agregue usuarios a su directorio de Identity Center](#)
- [Agregue grupos al directorio del Identity Center](#)
- [Agregar usuarios a grupos](#)
- [Eliminación de grupos de IAM Identity Center](#)
- [Eliminación de usuarios del IAM Identity Center](#)
- [Elimine usuarios de los grupos](#)
- [Inhabilitar el acceso de usuarios a Cuentas de AWS y aplicaciones en IAM Identity Center](#)
- [Editar las propiedades de los usuarios del directorio de IAM Identity Center](#)
- [Restablecimiento de la contraseña de usuario de IAM Identity Center para un usuario final](#)
- [Envíe por correo electrónico una contraseña de un solo uso a los usuarios creados con la API o la CLI](#)
- [Requisitos de contraseñas para administrar identidades en IAM Identity Center](#)

## Agregue usuarios a su directorio de Identity Center

Los usuarios y grupos que cree en su directorio de Identity Center solo estarán disponibles en IAM Identity Center. Siga el procedimiento que se detalla para añadir usuarios al directorio Identity Center. Como alternativa, puede llamar a la operación de AWS API [CreateUser](#) para añadir usuarios.

### Console

Para añadir un usuario

1. Abra la consola de [IAM Identity Center](#).

2. Seleccione Usuarios.
3. Elija Agregar usuario, y proporcione la siguiente información necesaria:
  - a. Nombre de usuario: este nombre de usuario es obligatorio para iniciar sesión en el portal de AWS acceso y no se puede modificar más tarde. Debe tener entre 1 y 100 caracteres de longitud.
  - b. Contraseña: puede enviar un correo electrónico con las instrucciones de configuración de la contraseña (esta es la opción predeterminada) o generar una contraseña de un solo uso. Si va a crear un usuario administrativo y envía un correo electrónico, asegúrese de especificar una dirección de correo electrónico a la que pueda acceder.
    - i. Enviar un correo electrónico a este usuario con instrucciones de configuración de contraseña: esta opción envía automáticamente al usuario una dirección de correo electrónico de Amazon Web Services, con el asunto Invitación para unirse a AWS IAM Identity Center. El correo electrónico invita al usuario, en nombre de su empresa, a acceder al portal de acceso AWS de IAM Identity Center y registrar una contraseña. La invitación por correo electrónico caducará en siete días. Si esto ocurre, para volver a enviar el correo electrónico, seleccione Restablecer contraseña y, a continuación, Enviar un correo electrónico al usuario con instrucciones para restablecer la contraseña. Antes de que el usuario acepte la invitación, verá el enlace Enviar correo electrónico de verificación, que sirve para verificar su dirección de correo electrónico. Sin embargo, este paso es opcional y desaparecerá cuando el usuario acepte la invitación y registre una contraseña.

 Note

En algunas regiones, IAM Identity Center envía correos electrónicos a los usuarios que utilizan Amazon Simple Email Service desde otra Región de AWS. Para obtener información sobre cómo se envían los correos electrónicos, consulte [Correos electrónicos entre regiones con Amazon SES](#).

Todos los correos electrónicos enviados por el servicio de IAM Identity Center procederán de una de estas direcciones: `no-reply@signin.aws.com` o `no-reply@login.awsapps.com`. Le recomendamos que configure su sistema de correo electrónico para que

acepte los mensajes con estas direcciones de correo electrónico como remitente y no los trate como correo basura o no deseado.

- ii. Generar una contraseña de un solo uso que pueda compartir con este usuario: esta opción le proporcionará la URL del portal de AWS acceso y los detalles de la contraseña que puede enviar manualmente al usuario desde su dirección de correo electrónico. El usuario tendrá que verificar su dirección de correo electrónico. Puede iniciar el proceso si selecciona el enlace Enviar correo electrónico de verificación. El enlace de verificación por correo electrónico caducará en siete días. Si esto ocurre, para volver a enviar el enlace de verificación por correo electrónico, seleccione Restablecer contraseña y, a continuación, Generar una contraseña de un solo uso y compartir la contraseña con el usuario.
- c. Correo electrónico: la dirección de correo electrónico debe ser única.
- d. Confirmación de la dirección de correo electrónico
- e. Nombre: debe introducir un nombre aquí para que funcione el aprovisionamiento automático. Para obtener más información, consulte [Aprovisionamiento de un proveedor de identidad externo al IAM Identity Center mediante SCIM](#).
- f. Apellido: debe introducir un nombre aquí para que funcione el aprovisionamiento automático.
- g. Display name (Nombre de visualización)

 Note

(Opcional) Si corresponde, puede especificar valores para atributos adicionales, como el ID inmutable de Microsoft 365 del usuario, para ayudar a proporcionarle acceso de inicio de sesión único a determinadas aplicaciones empresariales.

4. Elija Siguiente.
5. Si corresponde, seleccione uno o más grupos a los que desee añadir al usuario y elija Siguiente.
6. Revise la información que especificó para el paso 1: especificar los detalles del usuario y el paso 2: agregar el usuario a los grupos (opcional). Elija Editar en uno de los pasos para realizar cualquier cambio. Tras confirmar que se ha especificado la información correcta para ambos pasos, elija Añadir usuario.

## AWS CLI

Para añadir un usuario

El siguiente `create-user` comando crea un nuevo usuario en el directorio de Identity Center.

```
aws identitystore create-user \  
  --identity-store-id d-1234567890 \  
  --user-name johndoe \  
  --name "GivenName=John,FamilyName=Doe" \  
  --display-name "John Doe" \  
  --emails "Type=work,Value=johndoe@example.com"
```

Salida:

```
{  
  "UserId": "1234567890-abcdef",  
  "IdentityStoreId": "d-1234567890"  
}
```

### Note

Al crear usuarios con el comando `create-user` CLI o la operación de [CreateUser](#) API, los usuarios no tienen contraseñas. Puede actualizar la configuración del Centro de identidad de IAM para enviar a estos usuarios un correo electrónico de verificación tras su primer intento de inicio de sesión para que puedan configurar una contraseña. Si no habilita esta configuración, debe generar y compartir una contraseña de un solo uso con el usuario. Para obtener más información, consulte [Envíe por correo electrónico una contraseña de un solo uso a los usuarios creados con la API o la CLI](#).

## Agregue grupos al directorio del Identity Center

Siga el procedimiento que se detalla para agregar grupos al directorio Identity Center. Como alternativa, puede llamar a la operación de la AWS API [CreateGroup](#) para agregar grupos.

### Console

Para añadir un grupo

1. Abrir la consola de [IAM Identity Center](#).

2. Elija Grupos.
3. Elija Crear grupo.
4. Introduzca un nombre y una descripción del grupo (opcional). La descripción debe proporcionar detalles sobre qué permisos se han asignado o se asignará al grupo. En Añadir usuarios al grupo: opcional, busque los usuarios que desea añadir como miembros. A continuación, seleccione la casilla de verificación situada junto a cada uno de ellos.
5. Elija Crear grupo.

## AWS CLI

Para añadir un grupo

El siguiente `create-group` comando crea un grupo nuevo en el directorio de Identity Center.

```
aws identitystore create-group \  
  --identity-store-id d-1234567890 \  
  --display-name "Developers" \  
  --description "Group that contains all developers"
```

Salida:

```
{  
  "GroupId": "1a2b3c4d-5e6f-7g8h-9i0j-1k2l3m4n5o6p",  
  "IdentityStoreId": "d-1234567890"  
}
```

Tras añadir este grupo al directorio de Identity Center, puede asignar el acceso de inicio de sesión único al grupo. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

## Agregar usuarios a grupos

Utilice el siguiente procedimiento para agregar usuarios como miembros de un grupo que ha creado anteriormente en el directorio de Identity Center. Como alternativa, puede llamar a la operación de la AWS API [CreateGroupMembership](#) para agregar un usuario como miembro de un grupo.



## Console

### Cómo añadir un usuario como miembro de un grupo

1. Abra la consola de [IAM Identity Center](#).
2. Elija Grupos.
3. Elija el nombre de grupo que desea actualizar.
4. En la página de detalles del grupo, en Usuarios de este grupo, elija Añadir usuarios al grupo.
5. En la página Añadir usuarios al grupo, en Otros usuarios, localice los usuarios que desea añadir como miembros. A continuación, marque la casilla de verificación situada junto a cada uno de ellos.
6. Elija Agregar usuarios.

## AWS CLI

### Cómo añadir un usuario como miembro de un grupo

El siguiente `create-group-membership` comando agrega un usuario a un grupo al directorio Identity Center.

```
aws identitystore create-group-membership \
  --identity-store-id d-1234567890 \
  --group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222 \
  --member-id UserId=a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Salida:

```
{
  "MembershipId": "a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  "IdentityStoreId": "d-1234567890"
}
```

## Eliminación de grupos de IAM Identity Center

Al eliminar un grupo del directorio de IAM Identity Center, se elimina el acceso a las Cuentas de AWS y a las aplicaciones para todos los usuarios que son miembros de este grupo. Una vez que se elimina un grupo, no se puede deshacer la acción. Siga el procedimiento que se detalla para eliminar un grupo al directorio Identity Center.

 Important

Las instrucciones de esta página se aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo eliminar grupos en IAM, consulte [Eliminar un grupo de usuarios de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

## Console

Para eliminar un grupo

1. Abra la [consola de IAM Identity Center](#).
2. Elija Grupos.
3. Hay 2 formas de eliminar un grupo:
  - En la página Grupos, puede seleccionar varios grupos para su eliminación. Elija el nombre de grupo que desee eliminar y seleccione Eliminar grupo.
  - Elija el nombre de grupo que desea eliminar. En la página de detalles del grupo, elija Eliminar grupo.
4. Es posible que se le pida que confirme su intención de eliminar el grupo.
  - Si elimina varios grupos a la vez, confírmelo escribiendo **Delete** en el cuadro de diálogo Eliminar grupo.
  - Si elimina un solo grupo que contiene usuarios, confirme su intención escribiendo el nombre del grupo que desea eliminar en el cuadro de diálogo Eliminar grupo.
5. Elija Eliminar grupo. Si ha seleccionado varios grupos para eliminarlos, elija Eliminar # grupos.

## AWS CLI

Para eliminar un grupo

El siguiente delete-group comando elimina el grupo especificado del directorio de Identity Center.

```
aws identitystore delete-group \
```

```
--identity-store-id d-1234567890 \  
--group-id a1b2c3d4-5678-90ab-cdef-EXAMPLE22222
```

## Eliminación de usuarios del IAM Identity Center

Al eliminar un usuario del directorio de IAM Identity Center, se elimina el acceso a las Cuentas de AWS y a las aplicaciones. Tras eliminar un usuario, no podrá deshacer esta acción. Siga el procedimiento que se detalla para eliminar un usuario al directorio Identity Center.

### Note

Si deshabilita el acceso de un usuario o lo elimina en IAM Identity Center, se impedirá inmediatamente a ese usuario iniciar sesión en el portal de AWS acceso y no podrá crear nuevas sesiones de inicio de sesión en IAM Identity Center. Para obtener más información, consulte [Sesiones de autenticación](#).

### Important

Las instrucciones de esta página se aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo eliminar usuarios en IAM, consulte [Eliminar un usuario de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

## Console

### Cómo eliminar un usuario

1. Abra la [consola de IAM Identity Center](#).
2. Seleccione Usuarios.
3. Hay 2 formas de eliminar un usuario:
  - En la página Usuarios, puede seleccionar varios usuarios para su eliminación. Seleccione el nombre de usuario que desee eliminar y seleccione Eliminar usuarios.

- Elija el nombre de usuario que desea eliminar. En la página de detalles del usuario, vaya a la pestaña Eliminar usuario.
4. Si elimina varios usuarios a la vez, confirme su intención escribiendo **Delete** en el cuadro de diálogo Eliminar usuario.
  5. Seleccione Eliminar usuario(s). Si ha seleccionado varios usuarios para eliminarlos, elija Eliminar # usuarios.

## AWS CLI

### Cómo eliminar un usuario

El siguiente `delete-user` comando elimina un usuario del directorio del Centro de identidad.

```
aws identitystore delete-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

## Elimine usuarios de los grupos

Utilice el siguiente procedimiento para quitar los miembros de un grupo. Como alternativa, puede llamar a la operación de la AWS API [DeleteGroupMembership](#) para eliminar un usuario de un grupo.

### Console

#### Eliminación de un usuario de un grupo

1. Abra la [consola de IAM Identity Center](#).
2. Elija Grupos.
3. Elija al grupo que desee actualizar.
4. En la página de detalles del grupo, en Usuarios de este grupo, elija los usuarios que desee eliminar.
5. Seleccione Eliminar usuarios del grupo.
6. En el cuadro de diálogo Eliminar usuarios, elija Eliminar usuarios del grupo para comprobar que desea eliminar el acceso de los usuarios a la cuenta y a las aplicaciones asignadas al grupo.

## AWS CLI

### Eliminación de un usuario de un grupo

El siguiente `delete-group-membership` comando elimina un miembro de un grupo.

```
aws identitystore delete-group-membership
--identity-store-id d-1234567890 \
--membership-id a1b2c3d4-5678-90ab-cdef-EXAMPLE33333
```

## Inhabilitar el acceso de usuarios a Cuentas de AWS y aplicaciones en IAM Identity Center

Cuando deshabilita un acceso de usuario en su directorio IAM Identity Center, no puede editar sus detalles de usuario, restablecer su contraseña, agregar el usuario a un grupo ni ver los grupos a los que pertenece. Al inhabilitar el acceso de los usuarios, estos no podrán iniciar sesión en el portal de AWS acceso y dejarán de tener acceso a las asignadas Cuentas de AWS y a las aplicaciones.

Siga el procedimiento que se detalla a continuación para deshabilitar el acceso de los usuarios al directorio de Identity Center mediante la consola de IAM Identity Center.

### Note

Si deshabilita el acceso de un usuario o lo elimina en IAM Identity Center, se impedirá inmediatamente a ese usuario iniciar sesión en el portal de AWS acceso y no podrá crear nuevas sesiones de inicio de sesión en IAM Identity Center. Para obtener más información, consulte [Sesiones de autenticación](#).

### Cómo inhabilitar el acceso de usuarios de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).

### Important

Las instrucciones de esta página se aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales

de usuario de IAM. Si busca instrucciones sobre cómo deshabilitar en IAM, consulte [Administrar usuarios de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

2. Seleccione Usuarios.
3. Seleccione el nombre de usuario del usuario cuyo acceso desee deshabilitar.
4. Debajo del nombre de usuario de la persona cuyo acceso desee inhabilitar, en la sección Información general, elija Inhabilitar el acceso del usuario.
5. En el cuadro de diálogo Desactivar el acceso de usuarios, seleccione Desactivar el acceso de usuarios.

## Editar las propiedades de los usuarios del directorio de IAM Identity Center

Siga el procedimiento que se detalla para modificar las propiedades de un usuario al directorio Identity Center. Como alternativa, puede llamar a la operación de la AWS API [UpdateUser](#) para actualizar las propiedades del usuario.

### Console

#### Cómo editar las propiedades de los usuarios de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Seleccione Usuarios.
3. Elija el usuario que desee editar.
4. En la página Perfil, al lado de Detalles del perfil seleccione Editar.
5. En la página Editar detalles del perfil, actualice las propiedades que corresponda. A continuación, elija Save changes (Guardar cambios).

#### Note

(Opcional) Puede modificar atributos adicionales como el número de empleado y la ID inmutable de Office 365 para ayudar a asignar la identidad del usuario en IAM Identity Center a determinadas aplicaciones empresariales que los usuarios necesiten utilizar.

 Note

El atributo Correo electrónico es un campo editable y el valor que proporcione debe ser único.

## AWS CLI

### Cómo editar las propiedades de los usuarios de IAM Identity Center

El siguiente `update-user` comando actualiza el apodo del usuario.

```
aws identitystore update-user \  
  --identity-store-id d-1234567890 \  
  --user-id a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
  --operations '{"AttributePath":"nickName","AttributeValue":"Johnny"}'
```

## Restablecimiento de la contraseña de usuario de IAM Identity Center para un usuario final

Este procedimiento es para los administradores que necesitan restablecer la contraseña de un usuario del directorio de IAM Identity Center. Utilizará la consola de IAM Identity Center para restablecer las contraseñas.

### Consideraciones sobre los proveedores de identidad y los tipos de usuario

- Microsoft Active Directory o un proveedor externo: si va a conectar IAM Identity Center a Microsoft Active Directory o a un proveedor externo, las contraseñas de usuario se deben restablecer desde Active Directory o desde el proveedor externo. Esto significa que las contraseñas de esos usuarios no se pueden restablecer desde la consola de IAM Identity Center.
- Usuarios del directorio de IAM Identity Center: si es usuario de IAM Identity Center, puede restablecer su propia contraseña de IAM Identity Center. Para ello, consulte [Restablecer la contraseña de usuario del portal de AWS acceso](#).

## Cómo restablecer la contraseña de un usuario final de IAM Identity Center

### Important

Las instrucciones de esta página se aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo cambiar contraseñas para usuarios de IAM, consulte [Administración de contraseñas para usuarios de IAM](#) en la Guía del usuario de AWS Identity and Access Management .

1. Abra la [consola de IAM Identity Center](#).
2. Seleccione Usuarios.
3. Elija el nombre del usuario cuya contraseña desea restablecer.
4. En la página de detalles del usuario, vaya a la pestaña Restablecer contraseña.
5. En el cuadro de diálogo Restablecer contraseña, seleccione una de las siguientes opciones y después elija Restablecer contraseña:
  - a. Enviar un correo electrónico al usuario con instrucciones para restablecer la contraseña: esta opción envía automáticamente al usuario una dirección de correo electrónico de Amazon Web Services que le explica cómo restablecer su contraseña.

### Warning

Como práctica recomendada de seguridad, compruebe que la dirección de correo electrónico de este usuario sea correcta antes de seleccionar esta opción. Si el correo electrónico de restablecimiento de contraseña se enviara a una dirección de correo electrónico incorrecta o mal configurada, un destinatario malintencionado podría usarlo para obtener acceso no autorizado a su AWS entorno de.

- b. Generar una contraseña de un solo uso y compartirla con el usuario: esta opción le proporcionará los detalles de la contraseña que puede enviar manualmente al usuario desde su dirección de correo electrónico.



Envíe por correo electrónico una contraseña de un solo uso a los usuarios creados con la API o la CLI

Al crear usuarios con la operación de [CreateUser](#) API o el comando `create-user` CLI, los usuarios no tienen contraseñas. Puede actualizar la configuración de IAM Identity Center para enviar a estos usuarios un correo electrónico de verificación después de que intenten iniciar sesión por primera vez, si especificó un correo electrónico para el usuario cuando se creó. Tras recibir el correo electrónico de verificación, el usuario debe establecer una contraseña para iniciar sesión.

Si no habilita esta configuración, debe [generar y compartir una contraseña de un solo uso](#) con los usuarios que cree mediante el comando de la `CreateUser` API o la `create-user` CLI.

Cómo enviar un correo electrónico de verificación de dirección de correo electrónico a los usuarios creados con el comando de la `CreateUser` API o la **`create-user`** CLI

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación estándar, selecciona Configurar.
5. En el cuadro de diálogo Configurar la autenticación estándar, active la casilla Enviar correo electrónico OTP. A continuación, elija Guardar. El estado pasa de Deshabilitado a Habilitado.

## Requisitos de contraseñas para administrar identidades en IAM Identity Center

### Note

Estos requisitos se aplican únicamente a los usuarios creados en el directorio de Identity Center. Si ha configurado una fuente de identidad distinta de IAM Identity Center para la autenticación, como [Active Directory](#) o un [proveedor de identidad externo](#), las políticas de contraseñas para sus usuarios se definen y aplican en esos sistemas, no en IAM Identity Center. Si su fuente de identidad es AWS Managed Microsoft AD, consulte [Administrar las políticas de contraseñas AWS Managed Microsoft AD para](#) obtener más información.

Al utilizar IAM Identity Center como fuente de identidad, los usuarios deben cumplir los siguientes requisitos de contraseña para establecer o cambiar su contraseña:

- Las contraseñas distinguen entre mayúsculas y minúsculas.
- Las contraseñas deben tener una longitud de entre 8 y 64 caracteres.
- También deben contener al menos un carácter de cada una de las siguientes cuatro categorías:
  - Letras minúsculas (a-z)
  - Letras mayúsculas (A-Z)
  - Números (0-9)
  - Caracteres no alfanuméricos (~!@#\$%^&\* \_-+=`|\\(){}[];:'"<>,.?/)
- Las tres últimas contraseñas no se pueden volver a utilizar.
- No se pueden usar contraseñas que se conozcan públicamente a través de un conjunto de datos que haya obtenido cualquier tercero mediante una filtración de datos.

## Conexión un directorio Microsoft AD

Con AWS IAM Identity Center, puede conectarse a un directorio autoadministrado en Active Directory (AD) o un directorio en AWS Managed Microsoft AD mediante AWS Directory Service. Este directorio de Microsoft AD define el grupo de identidades que los administradores pueden extraer al utilizar la consola de Centro de identidades de IAM para asignar el acceso de inicio de sesión único. Tras conectar su directorio corporativo al Centro de identidades de IAM, podrá conceder a sus usuarios o grupos de AD acceso a las Cuentas de AWS, a las aplicaciones o a ambas opciones.

AWS Directory Service le ayuda a configurar y ejecutar un AWS Managed Microsoft AD directorio independiente alojado en. Nube de AWS También puede utilizar AWS Directory Service para conectar sus AWS recursos de con un AD autoadministrado existente. Para configurar AWS Directory Service para que funcione con su servicio autogestionado Active Directory, primero debe configurar relaciones de confianza para llevar la autenticación a la nube.

Centro de identidades de IAM utiliza la conexión proporcionada por AWS Directory Service para realizar la autenticación de transferencia a la instancia de AD de origen. Si utiliza AWS Managed Microsoft AD como fuente de identidad, Centro de identidades de IAM puede funcionar con usuarios de AWS Managed Microsoft AD o de cualquier dominio conectado a través de una relación de confianza de AD. Si desea ubicar a sus usuarios en 4 o más dominios, los usuarios deben usar la sintaxis de DOMAIN\user como nombre de usuario al iniciar sesión en Centro de identidades de IAM.

### Notas

- Como paso previo, asegúrese de que su AD Connector o directorio en en AWS Managed Microsoft AD en AWS Directory Service reside en su cuenta AWS Organizations de administración.
- Centro de identidades de IAM no admite Simple AD basado en SAMBA 4 como directorio conectado.

Para ver una demostración del proceso de uso de Active Directory como fuente de identidad para Centro de identidades de IAM, consulte el siguiente YouTube vídeo:

[Uso de Active Directory como fuente de identidad para AWS IAM Identity Center | Amazon Web Services](#)

## Consideraciones sobre el uso de Active Directory

Si quiere utilizar Active Directory como origen de identidad, la configuración debe cumplir los siguientes requisitos previos:

- Si está usando AWS Managed Microsoft AD, debe habilitar Centro de identidades de IAM en la misma Región de AWS donde su AWS Managed Microsoft AD directorio está configurado. Centro de identidades de IAM almacena los datos de asignación en la misma región que el directorio. Para administrar Centro de identidades de IAM, es posible que deba cambiarse a la región en la que está configurado Centro de identidades de IAM. Además, tenga en cuenta que el portal de AWS acceso de utiliza la misma URL de acceso que su directorio.
- Utilice un Active Directory que resida en la cuenta de administración:

Debe tener un conector de AD existente o AWS Managed Microsoft AD directorio de configurado en AWS Directory Service, que debe residir dentro de su cuenta AWS Organizations de administración. Solo puede conectarse a un directorio de AD Connector o un directorio AWS Managed Microsoft AD en a la vez. Si necesita admitir varios dominios o bosques, utilice AWS Managed Microsoft AD. Para obtener más información, consulte:

- [Conectar un directorio en AWS Managed Microsoft AD al Centro de identidades de IAM](#)
- [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#)
- Utilice un Active Directory que resida en la cuenta de administrador delegada:

Si planea habilitar la administración delegada de Centro de identidades de IAM y usar Active Directory como fuente de identidad de Centro de identidades de IAM, puede usar un conector de AD existente o AWS Managed Microsoft AD directorio de configurado en el directorio de que reside en AWS la cuenta de administrador delegado.

Si decide cambiar la fuente de identidad de Centro de identidades de IAM de cualquier otra fuente a Active Directory o cambiarla de Active Directory a cualquier otra fuente, el directorio debe residir (ser propiedad de) la cuenta de miembro administrador delegado de Centro de identidades de IAM si existe; de lo contrario, debe estar en la cuenta de administración.

## Conexión de Active Directory y especificación de un usuario

Si ya utiliza Active Directory, los siguientes temas lo ayudarán a prepararse para conectar su directorio al Centro de identidades de IAM.

Puede conectar un AWS Managed Microsoft AD directorio de o un directorio autoadministrado de Active Directory con Centro de identidades de IAM.

### Note

Centro de identidades de IAM no admite SAMBA4 Simple AD como fuente de identidad.

## AWS Managed Microsoft AD

1. Revise la guía en [Conexión un directorio Microsoft AD](#).
2. Siga los pasos de [Conectar un directorio en AWS Managed Microsoft AD al Centro de identidades de IAM](#).
3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM. Para obtener más información, consulte [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

## Directorio autogestionado en Active Directory

1. Revise la guía en [Conexión un directorio Microsoft AD](#).
2. Siga los pasos de [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#).

3. Configure Active Directory para sincronizar el usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM. Para obtener más información, consulte [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

## IdP externo

1. Revise la guía en [Administrar un proveedor de identidades externo](#).
2. Siga los pasos de [Cómo conectarse a un proveedor de identidades externo](#).
3. Configure su IdP para aprovisionar usuarios al Centro de identidades de IAM.

### Note

Antes de configurar el aprovisionamiento automático y basado en grupos de todas las identidades de sus empleados desde su IdP al Centro de identidades de IAM, le recomendamos que sincronice el único usuario al que quiere conceder permisos administrativos en Centro de identidades de IAM.

## Sincronice un usuario administrativo en el Centro de identidades de IAM

Tras conectar Active Directory al Centro de identidades de IAM, puede especificar el usuario al que quiere conceder permisos administrativos y, a continuación, sincronizar ese usuario del directorio con el Centro de identidades de IAM.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de Administrar sincronización, elija la pestaña Usuarios y, continuación, seleccione Añadir usuarios y grupos.
5. En la pestaña Usuarios, en Usuario, introduzca el nombre de usuario exacto y seleccione Añadir.
6. En Usuarios y grupos añadidos, haga lo siguiente:
  - a. Confirme que se ha especificado el usuario a quien desea conceder permisos administrativos.
  - b. Seleccione la casilla de verificación que hay junto al nombre del archivo.

c. Elija Enviar

7. En la página Administrar sincronización, el usuario que especificó aparece en la lista de Ámbito de usuarios sincronizados.
8. En el panel de navegación, seleccione Usuarios.
9. En la página Usuarios, es posible que el usuario que especificó tarde algún tiempo en aparecer en la lista. Seleccione el icono de actualización para actualizar la lista de usuarios.

En este momento, el usuario no tiene acceso a la cuenta de administración. Para configurar el acceso administrativo a esta cuenta, debe crear un conjunto de permisos administrativos y asignar el usuario a ese conjunto de permisos. Para obtener más información, consulte [Crea un conjunto de permisos](#).

## Aprovisionamiento cuando los usuarios provienen de Active Directory

Centro de identidades de IAM utiliza la conexión proporcionada por AWS Directory Service para sincronizar la información de usuarios, grupos y miembros del directorio de origen de Active Directory con el almacén de identidades de Centro de identidades de IAM Identity Center. La información de la contraseña no se sincroniza con Centro de identidades de IAM, ya que la autenticación de los usuarios se realiza directamente desde el directorio de origen de Active Directory. Las aplicaciones utilizan estos datos de identidad para facilitar los escenarios de búsqueda, autorización y colaboración dentro de la aplicación sin devolver la actividad de LDAP al directorio de origen de Active Directory.

Para obtener más información sobre aprovisionamiento, consulte [Aprovisionamiento de usuarios y grupos](#).

### Temas

- [Conectar un directorio en AWS Managed Microsoft AD al Centro de identidades de IAM](#)
- [Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM](#)
- [Asignaciones de atributos entre Centro de identidades de IAM y directorio de proveedores de identidades externos](#)
- [Centro de identidades de IAM y sincronización de AD configurable](#)

# Conectar un directorio en AWS Managed Microsoft AD al Centro de identidades de IAM

Utilice el siguiente procedimiento para conectar un directorio en AWS Managed Microsoft AD administrado por AWS Directory Service al Centro de identidades de IAM.

Cómo conectar AWS Managed Microsoft AD al Centro de identidades de IAM

1. Abra la [consola de Centro de identidades de IAM](#).

## Note

Antes de continuar con el paso siguiente, compruebe que la consola de Centro de identidades de IAM utiliza alguna de las regiones donde se encuentra su directorio de AWS Managed Microsoft AD .

2. Elija Configuración.
3. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, Cambiar fuente de identidad.
4. En Elegir origen de identidad, seleccione Active Directory y, a continuación, seleccione Siguiente.
5. En Conectar Active Directory, elija un directorio AWS Managed Microsoft AD de la lista y, a continuación, Siguiente.
6. En Confirmar el cambio, revise la información; cuando esté todo listo, escriba ACEPTAR y, a continuación, elija Cambiar fuente de identidad.

## Important

Para especificar un usuario de Active Directory como usuario administrativo en Centro de identidades de IAM, primero debe sincronizar el usuario al que desea conceder permisos administrativos desde Active Directory con Centro de identidades de IAM. Para ello, siga los pasos que se indican en [Sincronice un usuario administrativo en el Centro de identidades de IAM](#).

## Conexión de un directorio autoadministrado de Active Directory a Centro de identidades de IAM

Los usuarios del directorio autoadministrado de Active Directory (AD) también pueden tener acceso mediante inicio de sesión único a las Cuentas de AWS y a las aplicaciones del AWS portal de acceso. Para configurar el acceso de inicio de sesión único para estos usuarios, puede realizar una de las siguientes acciones:

- Crear una relación de confianza bidireccional: las relaciones de confianza bidireccionales creadas entre AWS Managed Microsoft AD y un Active Directory permiten a los usuarios iniciar sesión con sus credenciales corporativas en varios AWS servicios de y aplicaciones empresariales. Las relaciones de confianza unidireccionales no funcionan con Centro de identidades de IAM.

AWS IAM Identity Center requiere una relación de confianza bidireccional para tener permisos de leer la información de usuarios y grupos de su dominio a fin de sincronizar los metadatos de usuarios y grupos. Centro de identidades de IAM utiliza estos metadatos al asignar el acceso a conjuntos de permisos o aplicaciones. Las aplicaciones también utilizan los metadatos de usuarios y grupos para colaborar como, por ejemplo, cuando se comparte un panel con otro usuario o grupo. La confianza de AWS Directory Service Microsoft Active Directory en su dominio permite que Centro de identidades de IAM confíe en su dominio para la autenticación. La confianza en la dirección opuesta otorga AWS permisos para leer los metadatos de los usuarios y grupos.

Para obtener más información acerca de la configuración de una relación de confianza bidireccional, consulte [Cuándo crear una relación de confianza](#) en la Guía de administración de AWS Directory Service .

### Note

Para poder utilizar AWS aplicaciones, como Centro de identidades de IAM y leer los usuarios del AWS Directory Service directorio de dominios de confianza, las AWS Directory Service cuentas de requieren permisos para el userAccountControl atributo de los usuarios de confianza. Sin permisos de lectura para este atributo, las aplicaciones de AWS no pueden determinar si la cuenta está habilitada o deshabilitada.

El acceso de lectura a este atributo se proporciona de forma predeterminada cuando se crea una confianza. Si deniega el acceso a este atributo (no se recomienda), impedirá que aplicaciones como Identity Center puedan leer a los usuarios de confianza. La solución



consiste en permitir específicamente el acceso de lectura al `userAccountControl` atributo de las cuentas de AWS servicio de de la OU AWS reservada (con el prefijo `AWS_`).

- Crear un conector AD: Un conector AD es una puerta de enlace de directorio que puede redirigir solicitudes del directorio al Active Directory autoadministrado sin almacenar en caché la información que hay en la nube. Para obtener más información, consulte [Conectarse a un directorio](#) en la Guía de administración de AWS Directory Service . A continuación, se presentan las consideraciones a tener en cuenta al usar el Conector AD:
  - Si va a conectar Centro de identidades de IAM a un directorio de un conector AD, cualquier restablecimiento de contraseñas de usuario en el futuro deberá realizarse desde AD. Esto significa que los usuarios no podrán restablecer sus contraseñas desde el portal de AWS acceso.
  - Si utiliza un conector AD para conectar el servicio de dominio de Active Directory al Centro de identidades de IAM, Centro de identidades de IAM solo tiene acceso a los usuarios y grupos del dominio único al que se conecta el conector AD. Si necesita admitir varios dominios o bosques, utilice AWS Directory Service para Microsoft Active Directory.

 Note

Centro de identidades de IAM no funciona con los directorios Simple AD SAMBA4 basados en.

## Asignaciones de atributos entre Centro de identidades de IAM y directorio de proveedores de identidades externos

Las asignaciones de atributos se utilizan para asignar los tipos de atributos que existen en Centro de identidades de IAM con atributos similares en sus fuentes de identidad externas, como Google Workspace, Microsoft Active Directory (AD) y Okta. Centro de identidades de IAM recupera los atributos de usuario de la fuente de identidad y los asigna a los atributos de usuario de Centro de identidades de IAM.

Si su centro de identidad de IAM está sincronizado para usar un proveedor de identidad (IdP) externo, por ejemplo Google Workspace Okta, o Ping como fuente de identidad, tendrá que mapear sus atributos en su IdP.

Centro de identidades de IAM rellena previamente un conjunto de atributos en la pestaña Mapeos de atributos de su página de configuración. Centro de identidades de IAM utiliza estos atributos

de usuario para rellenar las aserciones de SAML (como atributos de SAML) que se envían a la aplicación. Estos atributos de usuario se recuperan, a su vez, de su fuente de identidad. Cada aplicación determina la lista de atributos de SAML 2.0 que necesita para un inicio de sesión único correcto. Para obtener más información, consulte [Asignación de atributos de su aplicación con atributos de IAM Identity Center](#).

Centro de identidades de IAM también administra un conjunto de atributos en la sección Mapeos de atributos de la página de configuración de Active Directory si utiliza Active Directory como fuente de identidad. Para obtener más información, consulte [Asignación de los atributos de usuario entre IAM Identity Center y directorio Microsoft AD](#).

### Atributos de proveedores de identidad externos compatibles

En la siguiente tabla se enumeran todos los atributos del proveedor de identidades (IdP) externo compatibles y se pueden asignar a los atributos que se pueden utilizar al configurar [Atributos para controlar el acceso](#) en Centro de identidades de IAM. Al usar aserciones de SAML, puede usar cualquier atributo que admita su IdP.

#### Atributos compatibles en su IdP

```
${path:userName}
```

```
${path:name.familyName}
```

```
${path:name.givenName}
```

```
${path:displayName}
```

```
${path:nickName}
```

```
${path:emails[primary eq true].value}
```

```
${path:addresses[type eq "work"].streetAddress}
```

```
${path:addresses[type eq "work"].locality}
```

```
${path:addresses[type eq "work"].region}
```

```
${path:addresses[type eq "work"].postalCode}
```

```
${path:addresses[type eq "work"].country}
```

## Atributos compatibles en su IdP

`${path:addresses[type eq "work"].formatted}``${path:phoneNumbers[type eq "work"].value}``${path:userType}``${path:title}``${path:locale}``${path:timezone}``${path:enterprise.employeeNumber}``${path:enterprise.costCenter}``${path:enterprise.organization}``${path:enterprise.division}``${path:enterprise.department}``${path:enterprise.manager.value}`

## Mapeos predeterminados entre Centro de identidades de IAM y Microsoft AD

En la tabla siguiente se muestran las asignaciones predeterminadas de los atributos de usuario de Centro de identidades de IAM a los atributos de usuario del directorio Microsoft AD. Centro de identidades de IAM solo admite la lista de atributos de la columna Atributo de usuario en Centro de identidades de IAM.

| Atributo de usuario en Centro de identidades de IAM | Se asigna a este atributo en su Active Directory |
|-----------------------------------------------------|--------------------------------------------------|
| displayname                                         | <code>\${displayname}</code>                     |
| emails[?primary].value *                            | <code>\${mail}</code>                            |

| Atributo de usuario en Centro de identidades de IAM | Se asigna a este atributo en su Active Directory |
|-----------------------------------------------------|--------------------------------------------------|
| externalid                                          | \${objectguid}                                   |
| name.givenname                                      | \${givenname}                                    |
| name.familyname                                     | \${sn}                                           |
| name.middlename                                     | \${initials}                                     |
| username                                            | \${userprincipalname}                            |

\* El atributo de correo electrónico de Centro de identidades de IAM debe ser único en el directorio.

| Atributo de grupo en Centro de identidades de IAM | Se asigna a este atributo en su Active Directory |
|---------------------------------------------------|--------------------------------------------------|
| externalid                                        | \${objectguid}                                   |
| description                                       | \${description}                                  |
| displayname                                       | \${samaccountname}@{associateddomain}            |

## Consideraciones

- Si no tiene ninguna asignación para sus usuarios y grupos en Centro de identidades de IAM cuando habilite la sincronización de AD configurable, se utilizan las asignaciones predeterminadas de las tablas anteriores. Para obtener información acerca de cómo personalizar estas asignaciones, consulte [Configuración de las asignaciones de atributos para su sincronización](#).
- Algunos atributos de Centro de identidades de IAM no se pueden modificar porque son inmutables y se asignan de forma predeterminada a atributos de directorio específicos de Microsoft AD.

Por ejemplo, el “nombre de usuario” es un atributo obligatorio en el IAM Identity Center. Si asigna “nombre de usuario” a un atributo del directorio de AD con un valor vacío, el IAM Identity Center considerará el valor windowsUpn como el valor predeterminado de “nombre de usuario”. Si desea

cambiar la asignación de atributos de “nombre de usuario” de la asignación actual, confirme que los flujos del IAM Identity Center que dependen del “nombre de usuario” sigan funcionando según lo previsto antes de realizar el cambio.

## Microsoft AD Atributos compatibles para Centro de identidades de IAM

En la siguiente tabla se proporciona la lista completa de los atributos del directorio Microsoft AD admitidos y que se pueden asignar a atributos de usuario de Centro de identidades de IAM.

### Atributos admitidos en el directorio de Microsoft AD

`${samaccountname}`

`${description}`

`${objectguid}`

`${givenname}`

`${sn}`

`${initials}`

`${mail}`

`${userprincipalname}`

`${displayname}`

`${distinguishedname}`

`${proxyaddresses[?type == "SMTP"].value}`

`${proxyaddresses[?type == "smtp"].value}`

`${useraccountcontrol}`

`${associateddomain}`

## Consideraciones

- Puede especificar cualquier combinación de atributos de Microsoft AD directorio compatibles para asignarlos a un único atributo de Centro de identidades de IAM.

### Atributos de Centro de identidades de IAM compatibles para Microsoft AD

En la siguiente tabla se proporciona la lista completa de los atributos de Centro de identidades de IAM admitidos y que se pueden asignar a atributos de usuario del directorio Microsoft AD. Posteriormente, cuando configure las asignaciones de los atributos de la aplicación podrá usar estos mismos atributos de Centro de identidades de IAM para asignarlos con los atributos reales utilizados por dicha aplicación.

#### Atributos compatibles en Centro de identidades de IAM para Active Directory

`${user:AD_GUID}`

`${user:email}`

`${user:familyName}`

`${user:givenName}`

`${user:middleName}`

`${user:name}`

`${user:preferredUsername}`

`${user:subject}`

### Asignación de los atributos de usuario entre IAM Identity Center y directorio Microsoft AD

Puede utilizar el siguiente procedimiento para especificar cómo deben asignarse sus atributos de usuario de Centro de identidades de IAM con los atributos correspondientes de su Microsoft AD directorio.

#### Cómo asignar atributos de Centro de identidades de IAM a atributos de su directorio

1. Abra la [consola de Centro de identidades de IAM](#).

2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Atributos para el control de acceso y, a continuación, elija Administrar atributos.
4. En la página Gestionar asignaciones de atributos para el control de acceso, busque el atributo en Centro de identidades de IAM que desea asignar y, a continuación, escriba un valor en el cuadro de texto. Por ejemplo, es posible que desee asignar el atributo de usuario **email** de Centro de identidades de IAM al atributo del directorio de Microsoft AD **mail**.
5. Seleccione Save changes (Guardar cambios).

## Centro de identidades de IAM y sincronización de AD configurable

La sincronización con Active Directory (AD) configurable de Centro de identidades de IAM le permite configurar de forma explícita las identidades de Microsoft Active Directory que se sincronizan automáticamente en Centro de identidades de IAM y controlar el proceso de sincronización.

- Con este método de sincronización, puede hacer lo siguiente:
  - Controle los límites de los datos definiendo explícitamente los usuarios y grupos de Microsoft Active Directory que se sincronizan automáticamente en Centro de identidades de IAM. Puede [añadir usuarios y grupos](#) o [eliminar usuarios y grupos](#) para cambiar el alcance de la sincronización en cualquier momento.
  - Asigne a los usuarios y grupos sincronizados [acceso mediante inicio de sesión único a Cuentas de AWS](#) o [acceso a las aplicaciones](#). Las aplicaciones pueden ser aplicaciones AWS administradas por o aplicaciones administradas por el cliente.
  - Controle el proceso de sincronización [pausando y reanudando la sincronización](#) según sea necesario. Esto le ayuda a regular la carga de los sistemas de producción.

### Requisitos y consideraciones previos

Antes de utilizar la sincronización de AD configurable, tenga en cuenta los siguientes requisitos y consideraciones:

- Especificación de usuarios y grupos de Active Directory para la sincronización

Antes de poder utilizar Centro de identidades de IAM para asignar a nuevos usuarios y grupos el acceso a Cuentas de AWS y a aplicaciones AWS administradas por o aplicaciones administradas

por el cliente, debe especificar los usuarios y grupos de Active Directory que desee sincronizar y, a continuación, sincronizarlos en Centro de identidades de IAM.

- **Sincronización de AD configurable:** Centro de identidades de IAM no busca usuarios y grupos directamente en el controlador de dominio. En su lugar, primero debe especificar la lista de usuarios y grupos que desea sincronizar. Puede configurar esta lista, también conocida como ámbito de sincronización, de una de las siguientes maneras, en función de si tiene usuarios y grupos que ya están sincronizados en Centro de identidades de IAM o si tiene nuevos usuarios y grupos que vaya a sincronizar por primera vez mediante la sincronización configurable de AD.
- **Usuarios y grupos existentes:** si tiene usuarios y grupos que ya están sincronizados en Centro de identidades de IAM, el ámbito de sincronización de la sincronización configurable de AD se rellena previamente con una lista de esos usuarios y grupos. Para asignar nuevos usuarios o grupos, debe añadirlos específicamente al ámbito de sincronización. Para obtener más información, consulte [Añadir usuarios y grupos a su ámbito de sincronización](#).
- **Nuevos usuarios y grupos:** si quiere asignar a nuevos usuarios y grupos el acceso a las aplicaciones y Cuentas de AWS, debe especificar qué usuarios y grupos quiere añadir al ámbito de sincronización en la sincronización configurable de AD antes de poder utilizar Centro de identidades de IAM para realizar la asignación. Para obtener más información, consulte [Añadir usuarios y grupos a su ámbito de sincronización](#).

#### • Asignaciones a grupos anidados en Active Directory

Los grupos que son miembros de otros grupos se llaman grupos anidados (o grupos secundarios).

- **Sincronización AD configurable:** el uso de la sincronización de AD configurable para realizar asignaciones a un grupo de Active Directory que contiene otros grupos anidados puede aumentar el número de usuarios que tienen acceso a Cuentas de AWS o las aplicaciones. En este caso, la asignación se aplica a todos los usuarios, incluidos los de los grupos anidados. Por ejemplo, si asigna el acceso al grupo A y el grupo B es miembro del grupo A, los miembros del grupo B también consiguen el acceso.
- **Actualización de los flujos de trabajo automatizados**

Si tiene flujos de trabajo automatizados que utilizan las acciones de la API del almacén de identidades de Centro de identidades de IAM y las acciones de la API de asignación de Centro de identidades de IAM para asignar a los nuevos usuarios y grupos el acceso a las cuentas y a las aplicaciones y sincronizarlos en Centro de identidades de IAM, debe ajustar esos flujos de trabajo antes del 15 de abril de 2022 para que funcionen según lo previsto con la sincronización



AD configurable. La sincronización de AD configurable cambia el orden en que se realizan la asignación y el aprovisionamiento de usuarios y grupos, así como la forma en que se realizan las consultas.

- Sincronización AD configurable: el aprovisionamiento se produce primero y no se realiza automáticamente. En su lugar, primero debe añadir usuarios y grupos de forma explícita al almacén de identidades, agregándolos a su ámbito de sincronización. Para obtener información sobre los pasos recomendados para automatizar la configuración de sincronización para una sincronización AD configurable, consulte [Automatizar la configuración de sincronización para una sincronización AD configurable](#).

## Temas

- [Cómo funciona la sincronización de AD configurable](#)
- [Configuración de la primera sincronización de Active Directory a IAM Identity Center](#)
- [Añadir usuarios y grupos a su ámbito de sincronización](#)
- [Eliminación de usuarios y grupos de su ámbito de sincronización](#)
- [Pausa y reanudación de la sincronización](#)
- [Configuración de las asignaciones de atributos para su sincronización](#)
- [Automatizar la configuración de sincronización para una sincronización AD configurable](#)

## Cómo funciona la sincronización de AD configurable

Centro de identidades de IAM actualiza los datos de identidad basados en anuncios en el almacén de identidades mediante el siguiente proceso. Para obtener más información acerca de los requisitos previos, consulte [Requisitos y consideraciones previos](#).

## Creación

Tras conectar el directorio autoadministrado de Active Directory o su AWS Managed Microsoft AD directorio administrado por AWS Directory Service al Centro de identidades de IAM, puede configurar de forma explícita los usuarios y grupos de Active Directory que desee sincronizar en el almacén de identidades de Centro de identidades de IAM. Las identidades que elija se sincronizarán aproximadamente cada 3 horas en el almacén de identidades de Centro de identidades de IAM. Según el tamaño del directorio, el proceso de sincronización puede tardar más.

Los grupos que son miembros de otros grupos (llamados grupos anidados o grupos secundarios) también se escriben en el almacén de identidades.

Solo puede asignar el acceso a nuevos usuarios o grupos después de que estén sincronizados en el almacén de identidades de Centro de identidades de IAM.

## Actualización

Los datos de identidad del almacén de identidades de Centro de identidades de IAM se mantienen actualizados al leer periódicamente los datos del directorio de origen de Active Directory. De forma predeterminada, IAM Identity Center sincroniza los datos de su Active Directory cada hora en un ciclo de sincronización. Los datos pueden tardar entre 30 minutos y 2 horas en sincronizarse con el IAM Identity Center, según el tamaño de su Active Directory.

Los objetos de usuario y grupo que se encuentran en el ámbito de la sincronización y sus pertenencias se crean o actualizan en Centro de identidades de IAM para asignarlos a los objetos correspondientes del directorio de origen de Active Directory. En el caso de los atributos de usuario, solo el subconjunto de atributos que aparece en la sección Atributos para controlar el acceso de la consola de Centro de identidades de IAM se actualiza en Centro de identidades de IAM. Las actualizaciones de atributos que realice en Active Directory pueden tardar un ciclo de sincronización en reflejarse en el IAM Identity Center.

También puede actualizar el subconjunto de usuarios y grupos que sincroniza en el almacén de identidades de Centro de identidades de IAM. Puede optar por añadir nuevos usuarios o grupos a este subconjunto o eliminarlos. Todas las identidades que añada se sincronizarán en la próxima sincronización programada. Las identidades que elimine del subconjunto dejarán de actualizarse en el almacén de identidades de Centro de identidades de IAM. Los usuarios que no estén sincronizados durante más de 28 días quedarán inhabilitados en el almacén de identidades de Centro de identidades de IAM. Los objetos de usuario correspondientes se deshabilitarán automáticamente en el almacén de identidades de Centro de identidades de IAM durante el siguiente ciclo de sincronización, a menos que formen parte de otro grupo que siga formando parte del ámbito de sincronización.

## Eliminación

Los usuarios y grupos se eliminan del almacén de identidades de Centro de identidades de IAM cuando los objetos de usuario o grupo correspondientes se eliminan del directorio de origen de Active Directory. Como alternativa, puede eliminar de forma explícita los objetos de usuario del almacén de identidades de Centro de identidades de IAM mediante la consola de Centro de identidades de IAM. Si utiliza la consola de Centro de identidades de IAM, también debe eliminar los usuarios del ámbito de sincronización para garantizar que no se vuelvan a sincronizar con Centro de identidades de IAM durante el siguiente ciclo de sincronización.

También puede pausar y reiniciar la sincronización en cualquier momento. Si pausa la sincronización durante más de 28 días, se deshabilitarán todos los usuarios.

## Configuración de la primera sincronización de Active Directory a IAM Identity Center

Si va a sincronizar sus usuarios y grupos de Active Directory con Centro de identidades de IAM por primera vez, siga estos pasos. Como alternativa, puede seguir los pasos descritos en [Cambiar su fuente de identidad](#) para cambiar la fuente de identidad de Centro de identidades de IAM a Active Directory.

### Configuración guiada

1. Abra la [consola de Centro de identidades de IAM](#).

#### Note

Antes de continuar con el paso siguiente, compruebe que la consola de Centro de identidades de IAM utiliza alguna de las Regiones de AWS donde se encuentra su AWS Managed Microsoft AD directorio.

2. Elija Configuración.
3. En la parte superior de la página, en el mensaje de notificación, seleccione Iniciar configuración guiada.
4. En el paso 1 (opcional): configurar las asignaciones de atributos, revise las asignaciones de atributos de usuario y grupo predeterminadas. Si no es necesario realizar cambios, seleccione Siguiente. Si es necesario realizar cambios, realice los cambios y, a continuación, seleccione Guardar cambios.
5. En el paso 2 (opcional): configurar el alcance de la sincronización, seleccione la pestaña Usuarios. A continuación, introduzca el nombre de usuario exacto del usuario que quiere añadir a su ámbito de sincronización y seleccione Añadir. Seleccione la pestaña Grupos. A continuación, introduzca el nombre de grupo exacto del grupo que quiere añadir a su ámbito de sincronización y seleccione Añadir. A continuación, elija Siguiente. Si quiere añadir usuarios y grupos a su ámbito de sincronización más adelante, no realice ningún cambio y seleccione Siguiente.
6. En el paso 3: revisar y guardar la configuración, confirme las asignaciones de atributos en el paso 1: asignaciones de atributos y sus usuarios y grupos en el paso 2: ámbito de sincronización. Seleccione Guardar configuración. Esto le llevará a la página Administrar sincronización.

## Añadir usuarios y grupos a su ámbito de sincronización

Agregue sus usuarios y grupos de Active Directory al IAM Identity Center siguiendo estos pasos.

Para agregar usuarios

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de Administrar sincronización, elija la pestaña Usuarios y, continuación, seleccione Añadir usuarios y grupos.
5. En la pestaña Usuarios, en Usuario, introduzca el nombre de usuario exacto y seleccione Añadir.
6. En Usuarios y grupos agregados, revise el usuario que desea agregar.
7. Elija Enviar.
8. En el panel de navegación, seleccione Usuarios. Si el usuario que ha especificado no se muestra en la lista, elija el icono de actualización para actualizar la lista de usuarios.

Cómo añadir grupos:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En la página de administrar la sincronización, elija la pestaña Grupos y, continuación, seleccione Añadir usuarios y grupos.
5. Seleccione la pestaña Groups (Grupos). En Grupo, introduzca el nombre exacto del grupo y seleccione Añadir.
6. En Usuarios y grupos añadidos, revise el grupo que desea agregar.
7. Elija Enviar.
8. En el panel de navegación, elija Grupos. Si el grupo que ha especificado no se muestra en la lista, seleccione el icono de actualización para actualizar la lista de grupos.

## Eliminación de usuarios y grupos de su ámbito de sincronización

Para obtener más información sobre lo que ocurre cuando elimina usuarios y grupos del ámbito de sincronización, consulte [Cómo funciona la sincronización de AD configurable](#).

Cómo eliminar usuarios:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. Elija la pestaña Users.
5. En Usuarios en el ámbito de sincronización, seleccione la casilla de verificación situada junto al usuario que desea eliminar. Para eliminar todos los usuarios, seleccione la casilla de verificación situada junto al nombre de usuario.
6. Elija Eliminar.

Cómo eliminar grupos:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. Seleccione la pestaña Groups (Grupos).
5. En Grupos en el ámbito de sincronización, seleccione la casilla de verificación situada junto al usuario que desea eliminar. Para eliminar todos los grupos, seleccione la casilla de verificación situada junto al nombre del grupo.
6. Elija Eliminar.

## Pausa y reanudación de la sincronización

Al pausar la sincronización, se pausan todos los ciclos de sincronización futuros e impide que los cambios que realice en los usuarios y grupos de Active Directory se reflejen en Centro de identidades de IAM. Tras reanudar la sincronización, el ciclo de sincronización recoge los cambios de la siguiente sincronización programada.

## Cómo pausar la sincronización:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En Administrar la sincronización, seleccione Pausar la sincronización.

## Cómo reanudar la sincronización:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En Administrar la sincronización, seleccione Reanudar la sincronización.

### Note

Si aparece Pausar la sincronización en lugar de Reanudar la sincronización, significa que la sincronización de Active Directory con Centro de identidades de IAM ya se ha reanudado.

## Configuración de las asignaciones de atributos para su sincronización

Cómo obtener más información acerca de los atributos disponibles, consulte [Asignaciones de atributos entre Centro de identidades de IAM y directorio de proveedores de identidades externos](#).

## Cómo configurar las asignaciones de atributos de Centro de identidades de IAM a su directorio:

1. Abra la [consola del Centro de identidades de IAM](#).
2. Elija Configuraciones.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar sincronización.
4. En Administrar sincronización, seleccione Ver asignaciones de atributos.

5. En Atributos de usuario de Active Directory, configure los atributos del almacén de identidades de Centro de identidades de IAM y los atributos de usuario de Active Directory. Por ejemplo, puede que desee asignar el atributo `email` del almacén de identidades de Centro de identidades de IAM al atributo `${objectguid}` del directorio de usuarios de Active Directory.

 Note

En Atributos de grupo, no se pueden cambiar los atributos del almacén de identidades de Centro de identidades de IAM ni los atributos de grupo de Active Directory.

6. Seleccione **Save changes** (Guardar cambios). Esto le llevará a la página de **Administrar sincronización**.

## Automatizar la configuración de sincronización para una sincronización AD configurable

Para garantizar que su flujo de trabajo automatizado funcione según lo esperado con la sincronización de AD configurable, le recomendamos que realice los siguientes pasos para automatizar la configuración de la sincronización.

Cómo automatizar la configuración de sincronización para una sincronización AD configurable:

1. En Active Directory, cree un Grupo de sincronización principal que contenga todos los usuarios y grupos que desee sincronizar en Centro de identidades de IAM. Por ejemplo, puede asignar un nombre al grupo `IAMIdentityCenterAllUsersAndGroups`.
2. En Centro de identidades de IAM, añada el grupo de sincronización principal a su lista de sincronización configurable. Centro de identidades de IAM sincronizará todos los usuarios, grupos, subgrupos y miembros de todos los grupos incluidos en el grupo de sincronización principal.
3. Use las acciones de la API de administración de usuarios y grupos de Active Directory proporcionadas por Microsoft para añadir o eliminar usuarios y grupos del grupo de sincronización principal.

## Administrar un proveedor de identidades externo

Con IAM Identity Center, puede conectar las identidades de sus empleados existentes de proveedores de identidad externos (IdPs) mediante el lenguaje de marcado de aserciones de seguridad (SAML) 2.0 y los protocolos del Sistema de gestión de identidades entre dominios

(SCIM). Esto permite a los usuarios iniciar sesión en el portal de acceso AWS con sus credenciales corporativas. A continuación, pueden acceder a sus cuentas, funciones y aplicaciones asignadas alojadas en un servidor externo. IdPs

Por ejemplo, puede conectar un IdP externo como Okta o Microsoft Entra ID, al centro de identidad de IAM. A continuación, sus usuarios pueden iniciar sesión en el portal de AWS acceso con los que ya tienen Okta o Microsoft Entra ID credenciales. Para controlar lo que pueden hacer sus usuarios una vez que han iniciado sesión, puede asignarles permisos de acceso de forma centralizada en todas las cuentas y aplicaciones de su AWS organización. Además, los desarrolladores pueden simplemente iniciar sesión en AWS Command Line Interface (AWS CLI) con sus credenciales actuales y beneficiarse de la generación y rotación automáticas de credenciales a corto plazo.

Si utiliza un directorio autogestionado en Active Directory o un directorio AWS Managed Microsoft AD, consulte. [Conexión un directorio Microsoft AD](#)

#### Note

El protocolo SAML no proporciona una forma de consultar al IdP para obtener información sobre los usuarios y los grupos. Por lo tanto, debe hacer que IAM Identity Center conozca a esos usuarios y grupos aprovisionándolos en IAM Identity Center.

## Aprovisionamiento cuando los usuarios provienen de un IdP externo

Al utilizar un IdP externo, debe aprovisionar todos los usuarios y grupos aplicables en el Centro de Identidad de IAM antes de poder realizar cualquier asignación o aplicación. Cuentas de AWS Para ello, puede configurar el [Aprovisionamiento de un proveedor de identidad externo al IAM Identity Center mediante SCIM](#) para sus usuarios y grupos o bien utilizar el [Aprovisionamiento manual](#). Independientemente de cómo aprovisiona a los usuarios, IAM Identity Center redirige la AWS Management Console interfaz de línea de comandos y la autenticación de la aplicación a su IdP externo. A continuación, IAM Identity Center concede el acceso a esos recursos en función de las políticas que cree en IAM Identity Center. Para obtener más información sobre la capacidad aprovisionada, consulte [Aprovisionamiento de usuarios y grupos](#).

### Temas

- [Cómo conectarse a un proveedor de identidades externo](#)
- [Cómo cambiar los metadatos de un proveedor de identidades externo en IAM Identity Center](#)
- [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#)



- [Perfil SCIM e implementación de SAML 2.0](#)

## Cómo conectarse a un proveedor de identidades externo

Existen diferentes requisitos previos, consideraciones y procedimientos de aprovisionamiento para el dispositivo externo compatible. IdPs Hay step-by-step tutoriales disponibles para varios: IdPs

- [CyberArk](#)
- [Google Workspace](#)
- [JumpCloud](#)
- [Microsoft Entra ID](#)
- [Okta](#)
- [OneLogin](#)
- [Ping Identity](#)

Para obtener más información sobre las consideraciones externas IdPs que admite IAM Identity Center, consulte [Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos](#).

En el siguiente procedimiento se proporciona una descripción general del procedimiento que se utiliza con todos los proveedores de identidades externos.

### Cómo conectarse a un proveedor de identidades externo

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, elija la pestaña Fuente de identidad, elija Acciones y, a continuación, Cambiar fuente de identidad.
4. En Elegir la fuente de identidad, seleccione Proveedor de identidades externo y, a continuación, Siguiente.
5. En Configurar un proveedor de identidad externo, haga lo siguiente:
  - a. En Metadatos del proveedor de servicios, seleccione Descargar archivo de metadatos para descargar el archivo de metadatos y guardarlo en el sistema. El proveedor de identidades externo necesita el archivo de metadatos SAML de IAM Identity Center.

- b. En Metadatos del proveedor de identidad, elija Elegir archivo y busque el archivo de metadatos que descargó de su proveedor de identidades externo. A continuación, cargue el archivo. Este archivo de metadatos contiene el certificado x509 público necesario que se utiliza para confiar en los mensajes que se envían desde el IdP.
- c. Elija Siguiente.

 Important

Al cambiar la fuente a o desde Active Directory, se eliminan todas las asignaciones de usuarios y grupos existentes. Debe volver a aplicar las asignaciones manualmente una vez que haya cambiado correctamente la fuente.

6. Cuando haya leído el aviso legal, introduzca ACCEPT para continuar.
7. Elija Cambiar fuente de identidad. Un mensaje de estado le informa de que ha cambiado correctamente el origen de identidad.

## Cómo cambiar los metadatos de un proveedor de identidades externo en IAM·Identity·Center

Puede cambiar los metadatos de su proveedor de identidades externo que proporcionó con anterioridad a IAM·Identity·Center. Estos cambios afectan a la capacidad de los usuarios para iniciar sesión y acceder a los AWS recursos a través del Centro de identidades de IAM. El siguiente procedimiento describe cómo actualizar los metadatos del IdP externo que están almacenados en el IAM·Identity·Center. Para completar este procedimiento, necesitará una instancia organizativa del IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

### Cómo eliminar los metadatos de un proveedor de identidades externo

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de Configuración, seleccione la pestaña Origen de la identidad. Elija Acciones y luego Administrar autenticación.
4. En la sección Metadatos del proveedor de identidad, seleccione Editar metadatos del IdP. Puede realizar los cambios en la URL de inicio de sesión del IdP o en la URL del emisor del IdP para

su IdP externo en esta página. Seleccione Guardar cambios cuando haya realizado todos los cambios necesarios.

## Uso de la federación de identidades SAML y SCIM con proveedores de identidad externos

IAM Identity Center implementa los siguientes protocolos basados en estándares para la federación de identidades:

- SAML 2.0 para la autenticación de usuarios
- SCIM para el aprovisionamiento

Se espera que cualquier proveedor de identidades (IdP) que implemente estos protocolos estándar interactúe correctamente con IAM Identity Center, teniendo en cuenta las siguientes consideraciones especiales:

- SAML
  - IAM Identity Center requiere un formato de identificador de nombre SAML para la dirección de correo electrónico (es decir, `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`).
  - [El valor del campo NameID en las aserciones debe ser una cadena \(/rfc2822 #section -3.4.1\) que cumpla con las especificaciones addr-spec \(«»\) \(https://tools.ietf.org/html/rfc2822 -3.4.1\). name@domain.com https://tools.ietf.org/html](https://tools.ietf.org/html/rfc2822-3.4.1)
  - El archivo de metadatos no puede tener más de 75 000 caracteres.
  - Los metadatos deben contener un ID de entidad, un certificado X509 y formar parte de la URL de inicio de sesión. SingleSignOnService
  - No se admite el cifrado SSE-KMS.
- SCIM
  - [La implementación del SCIM del IAM Identity Center se basa en los SCIM RFCs 7642 \(https://tools.ietf.org/html/rfc7642\), 7643 \(/rfc7643\) y 7644 \(https://tools.ietf.org/html/rfc7644\) y en los requisitos de interoperabilidad establecidos en el borrador de marzo de 2020 del Perfil SCIM https://tools.ietf.org/htmlbásico 1.0 \(#rfc .section.4\). FastFed https://openid.net/specs/fastfed-scim-1\\_0-02.html](https://tools.ietf.org/html/rfc7642) Las diferencias entre estos documentos y la implementación actual en IAM

Identity Center se describen en la sección [Operaciones de API compatibles](#) de la Guía para desarrolladores de implementación del SCIM de IAM Identity Center.

IdPs no se admiten aquellos que no se ajusten a los estándares y consideraciones mencionados anteriormente. Póngase en contacto con su IdP si cualquier pregunta o necesita más información sobre la conformidad de sus productos con estas normas y consideraciones.

Si tiene problemas para conectar su IdP al IAM Identity Center, compruebe lo siguiente:

- AWS CloudTrail se registra filtrando por el nombre del evento ExternalIdDirectoryIniciar sesión
- Registros específicos de IdP o registros de depuración
- [Resolución de problemas de IAM Identity Center](#)

#### Note

Algunas IdPs, como las del [Tutoriales de fuentes de identidad de IAM Identity Center](#), ofrecen una experiencia de configuración simplificada para el IAM Identity Center en forma de «aplicación» o «conector» creado específicamente para el IAM Identity Center. Si su IdP ofrece esta opción, le recomendamos que la utilice, teniendo cuidado al elegir el elemento creado específicamente para IAM Identity Center. Otros elementos denominados «AWS», «AWS federación» o nombres genéricos similares de «»AWS pueden utilizar otros enfoques de federación o puntos finales, y es posible que no funcionen como se esperaba con el IAM Identity Center.

## Perfil SCIM e implementación de SAML 2.0

Tanto SCIM como SAML son consideraciones importantes a la hora de configurar IAM Identity Center.

### Implementación de SAML 2.0

IAM Identity Center admite la federación de identidades con [lenguaje de marcado para confirmaciones de seguridad SAML](#) 2.0. Esto permite al IAM Identity Center autenticar las identidades de proveedores de identidad externos (). IdPs SAML 2.0 es un estándar abierto que se utiliza para intercambiar aserciones de SAML de forma segura. SAML 2.0 transfiere información sobre un usuario entre una autoridad de SAML (denominada proveedor de identidades o IdP) y un consumidor de SAML (denominado proveedor de servicios o SP). El servicio de IAM Identity Center

utiliza esta información para proporcionar un inicio de sesión único federado. El inicio de sesión único permite a los usuarios acceder a las aplicaciones Cuentas de AWS y configurarlas en función de sus credenciales de proveedor de identidad existentes.

El Centro de identidad de IAM añade las capacidades de IdP de SAML a su almacén del Centro de identidades de IAM o a un proveedor AWS Managed Microsoft AD de identidad externo. A continuación, los usuarios pueden iniciar sesión de forma única en los servicios compatibles con SAML, incluidas las aplicaciones y las de terceros, como AWS Management Console Microsoft 365, Concur, y Salesforce.

Sin embargo, el protocolo SAML no proporciona ninguna forma de consultar al IdP para obtener información sobre los usuarios y los grupos. Por lo tanto, debe hacer que IAM Identity Center conozca a esos usuarios y grupos aprovisionándolos en IAM Identity Center.

## Perfil SCIM

IAM Identity Center es compatible con el estándar Sistema de la administración de identidades entre dominios (SCIM) v2.0. El SCIM mantiene las identidades de su IAM Identity Center sincronizadas con las identidades de su IdP. Esto incluye cualquier aprovisionamiento, actualización y desaprovisionamiento de usuarios entre su IdP y IAM Identity Center.

Para obtener más información acerca de cómo implementar una capa personalizada, consulte [Aprovisionamiento de un proveedor de identidad externo al IAM Identity Center mediante SCIM](#). Para obtener más información sobre la implementación del SCIM de IAM Identity Center, consulte la [Guía para desarrolladores de implementación de IAM Identity Center SCIM](#).

## Temas

- [Aprovisionamiento de un proveedor de identidad externo al IAM Identity Center mediante SCIM](#)
- [Rotar certificados SAML 2.0](#)

## Aprovisionamiento de un proveedor de identidad externo al IAM Identity Center mediante SCIM

IAM Identity Center admite el aprovisionamiento automático (sincronización) de la información de usuarios y grupos de su proveedor de identidades (IdP) a IAM Identity Center mediante el protocolo Sistema de administración de identidades entre dominios (SCIM) v2.0. Al configurar la sincronización de SCIM, crea una asignación de los atributos de usuario del proveedor de identidades (IdP) con los atributos nombrados en IAM Identity Center. Esto hace que los atributos esperados coincidan entre IAM Identity Center y su IdP. Esta conexión se configura en el IdP mediante el punto de conexión de SCIM para IAM Identity Center y un token de portador que se crea en IAM Identity Center.

## Temas

- [Consideraciones para utilizar el aprovisionamiento automático](#)
- [Cómo monitorizar la caducidad del token de acceso](#)
- [Habilitar el aprovisionamiento automático](#)
- [Deshabilitar el aprovisionamiento automático](#)
- [Generar un token de acceso](#)
- [Eliminar un token de acceso](#)
- [Rotar un token de acceso](#)
- [Aprovisionamiento manual](#)

## Consideraciones para utilizar el aprovisionamiento automático

Antes de comenzar a implementar el SCIM, le recomendamos revisar primero las siguientes consideraciones importantes sobre su funcionamiento con IAM Identity Center. Para conocer otras consideraciones de aprovisionamiento, consulte los [Tutoriales de fuentes de identidad de IAM Identity Center](#) aplicables a su IdP.

- Si va a aprovisionar una dirección de correo electrónico principal, el valor de este atributo debe ser único para cada usuario. En algunos casos IdPs, es posible que la dirección de correo electrónico principal no sea una dirección de correo electrónico real. Por ejemplo, puede ser un nombre principal universal (UPN) que solo se parece a un correo electrónico. Es IdPs posible que tengan una dirección de correo electrónico secundaria o «otra» que contenga la dirección de correo electrónico real del usuario. Debe configurar SCIM en su IdP para asignar la dirección de correo electrónico única no nula al atributo de dirección de correo electrónico principal de IAM Identity Center. Además, debe asignar el identificador de inicio de sesión único no nulo del usuario al atributo de nombre de usuario de IAM Identity Center. Compruebe si su IdP tiene un valor único que sea tanto el identificador de inicio de sesión como el nombre de correo electrónico del usuario. Si es así, puede asignar ese campo de IdP al correo electrónico principal de IAM Identity Center y al nombre de usuario de IAM Identity Center.
- Para que la sincronización de SCIM funcione, cada usuario debe tener un nombre, apellidos, nombre de usuario y nombre para mostrar especificados. Si falta alguno de estos valores en un usuario, este no se aprovisionará.
- Si necesita utilizar aplicaciones de terceros, primero tendrá que asignar el atributo de asunto de SAML saliente al atributo de nombre de usuario. Si la aplicación de terceros necesita una dirección de correo electrónico enrutable, debe proporcionar el atributo de correo electrónico a su IdP.

- El proveedor de identidades controla los intervalos de aprovisionamiento y actualización de SCIM. Los cambios en los usuarios y grupos de su proveedor de identidades solo se reflejan en IAM Identity Center después de que su proveedor de identidades los envíe a IAM Identity Center. Consulte con su proveedor de identidades para obtener más información sobre la frecuencia de las actualizaciones de usuarios y grupos.
- Actualmente, SCIM no proporciona atributos con varios valores (como varios correos electrónicos o números de teléfono para un usuario determinado). Los intentos de sincronizar atributos con varios valores en IAM Identity Center con SCIM fallarán. Para evitar errores, asegúrese de que solo se pase un valor único para cada atributo. Si tiene usuarios con atributos de varios valores, elimine o modifique las asignaciones de atributos duplicadas en SCIM en su IdP para la conexión con IAM Identity Center.
- Compruebe que el mapeo SCIM de `externalId` en su IdP corresponde a un valor que sea único, que esté siempre presente y que tenga menos probabilidades de cambiar para sus usuarios. Por ejemplo, su IdP puede proporcionar un `objectId` garantizado u otro tipo de identificador que no se vea afectado por los cambios en los atributos del usuario, como el nombre y el correo electrónico. Si es así, puede asignar ese valor al campo `externalId` de SCIM. Esto garantiza que tus usuarios no pierdan sus AWS derechos, asignaciones o permisos si necesitas cambiarles el nombre o el correo electrónico.
- Usuarios que aún no se han asignado a una aplicación o que no se Cuenta de AWS pueden aprovisionar en el Centro de identidades de IAM. Para sincronizar usuarios y grupos, asegúrese de que estén asignados a la aplicación u otra configuración que represente la conexión de su IdP a IAM Identity Center.
- El comportamiento de desaprovisionamiento de los usuarios lo administra el proveedor de identidades y puede variar según su implementación. Consulte con su proveedor de identidades para obtener más información sobre el desaprovisionamiento de usuarios.
- Tras configurar el aprovisionamiento automático con SCIM para su IdP, ya no podrá añadir ni editar usuarios en la consola de IAM Identity Center. Si necesita agregar o modificar un usuario, debe hacerlo desde su IdP externo o fuente de identidad.

Para obtener más información sobre la implementación de SCIM de IAM Identity Center, consulte la [guía para desarrolladores de implementación de IAM Identity Center SCIM](#).

## Cómo monitorizar la caducidad del token de acceso

Los tokens de acceso SCIM se generan con una validez de un año. Cuando tu token de acceso SCIM caduque en 90 días o menos, te AWS envía recordatorios a la consola del IAM Identity

Center y al AWS Health panel de control para ayudarte a cambiar el token. Al rotar el token de acceso de SCIM antes de que caduque, asegura de forma continua el aprovisionamiento automático de la información de usuarios y grupos. Si el token de acceso SCIM caduca, se interrumpe la sincronización de la información de usuarios y grupos de su proveedor de identidades con IAM Identity Center, por lo que el aprovisionamiento automático ya no puede realizar actualizaciones ni crear y eliminar información. La interrupción del aprovisionamiento automático puede aumentar los riesgos de seguridad y afectar al acceso a sus servicios.

Los recordatorios de la consola de Identity Center persisten hasta que rote el token de acceso SCIM y elimine los tokens de acceso no utilizados o vencidos. Los eventos del AWS Health panel de control se renuevan semanalmente entre 90 y 60 días, dos veces por semana entre 60 y 30 días, tres veces por semana entre 30 y 15 días y todos los días desde 15 días hasta que caduquen los tokens de acceso del SCIM.

### Habilitar el aprovisionamiento automático

Siga el siguiente procedimiento para habilitar el aprovisionamiento automático de usuarios y grupos desde su IdP a IAM Identity Center mediante el protocolo SCIM.

#### Note

Antes de comenzar con este procedimiento, le recomendamos que revise primero las consideraciones de aprovisionamiento aplicables a su IdP. Para obtener más información, consulte [Tutoriales de fuentes de identidad de IAM Identity Center](#) de su IdP.

### Cómo habilitar el aprovisionamiento automático en IAM Identity Center

1. Una vez que haya completado los requisitos previos, abra la consola de [IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, busque el cuadro de información sobre el aprovisionamiento automático y, a continuación, seleccione Habilitar. Esto habilita inmediatamente el aprovisionamiento automático en IAM Identity Center y muestra la información necesaria sobre el punto de conexión del SCIM y el token de acceso.
4. En el cuadro de diálogo de aprovisionamiento automático entrante, copie el punto final y el token de acceso del SCIM. Deberá pegarlos más adelante cuando configure el aprovisionamiento en su IdP.



- a. Punto final de SCIM: por ejemplo, `https://scim.us-east-2.amazonaws.com/scim/v21111111111-2222-3333-4444-55555555555`
- b. Token de acceso: seleccione Mostrar token para copiar el valor.

 Warning

Esta es la única vez en la que puede obtener el punto de conexión y el token de acceso de SCIM. Asegúrese de copiar estos valores antes de continuar. Introducirá estos valores para configurar el aprovisionamiento automático en su IdP más adelante en este tutorial.

5. Seleccione Cerrar.

Después de completar este procedimiento, debe configurar el aprovisionamiento automático en su IdP. Para obtener más información, consulte [Tutoriales de fuentes de identidad de IAM Identity Center](#) de su IdP.

### Deshabilitar el aprovisionamiento automático

Siga el siguiente procedimiento para desactivar el aprovisionamiento automático en la consola de IAM Identity Center.

 Important

Debe eliminar el token de acceso antes de iniciar este procedimiento. Para obtener más información, consulte [Eliminar un token de acceso](#).

Siga el siguiente procedimiento para desactivar el aprovisionamiento automático en la consola de IAM Identity Center.

1. En la [consola de IAM Identity Center](#), elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar el aprovisionamiento.
3. En la página de aprovisionamiento automático, seleccione Deshabilitar.

4. En el cuadro de diálogo Desactivar el aprovisionamiento automático, revise la información, escriba DISABLE y, a continuación, elija Deshabilitar el aprovisionamiento automático.

## Generar un token de acceso

Siga el siguiente procedimiento para generar un nuevo token de acceso en la consola de IAM Identity Center.

### Note

Este procedimiento requiere que haya habilitado previamente el aprovisionamiento automático. Para obtener más información, consulte [Habilitar el aprovisionamiento automático](#).

## Cómo generar un nuevo token de acceso

1. En la [consola de IAM Identity Center](#), elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página de aprovisionamiento automático, en Tokens de acceso, seleccione Generar token.
4. En el cuadro de diálogo Generar un nuevo token de acceso, copie el nuevo token de acceso y guárdelo en un lugar seguro.
5. Seleccione Cerrar.

## Eliminar un token de acceso

Siga el procedimiento que se detalla a continuación para eliminar un token de acceso actual de la consola de IAM Identity Center.

## Cómo eliminar una clave de acceso

1. En la [consola de IAM Identity Center](#), elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.

3. En la página de aprovisionamiento automático, en Tokens de acceso, seleccione el token de acceso que desee eliminar y, a continuación, Eliminar.
4. En el cuadro de diálogo Eliminar el token de acceso, revise la información, escriba ELIMINAR y, a continuación, elija Eliminar el token de acceso.

## Rotar un token de acceso

Un directorio de IAM Identity Center admite hasta 2 tokens de acceso a la vez. Para generar un token de acceso adicional antes de cualquier rotación, elimine los tokens de acceso caducados o no utilizados.

Si su token de acceso SCIM está a punto de caducar, puede seguir el procedimiento que se describe a continuación para rotar un token de acceso existente en la consola de IAM Identity Center.

## Cómo eliminar un token de acceso

1. En la [consola de IAM Identity Center](#), elija Configuración en el panel izquierdo de navegación del servicio.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página de aprovisionamiento automático, en Tokens de acceso, anote el ID del token que desee rotar.
4. Siga los pasos que encontrará en [Generar un token de acceso](#) para crear un nuevo token. Si ya ha creado el número máximo de tokens de acceso a SCIM, primero tendrá que eliminar uno de los tokens actuales.
5. Vaya al sitio web de su proveedor de identidades y configure el nuevo token de acceso para el aprovisionamiento de SCIM y, a continuación, pruebe la conectividad con IAM Identity Center con el nuevo token de acceso de SCIM. Una vez que haya confirmado que el aprovisionamiento funciona correctamente con el nuevo token, continúe con el siguiente paso de este procedimiento.
6. Siga los pasos que se indican en [Eliminar un token de acceso](#) para eliminar el token de acceso que anotó anteriormente. También puede usar la fecha de creación del token como una pista sobre qué token eliminar.

## Aprovisionamiento manual

Algunos IdPs no son compatibles con el Sistema de Gestión de Identidad entre Dominios (SCIM) o tienen una implementación de SCIM incompatible. En esos casos, puede aprovisionar usuarios manualmente a través de la consola de IAM Identity Center. Cuando añada usuarios a IAM Identity Center, asegúrese de configurar el nombre de usuario para que sea idéntico al nombre de usuario que tiene en su IdP. Como mínimo, debe tener una dirección de correo electrónico y un nombre de usuario únicos. Para obtener más información, consulte [Exclusividad del nombre de usuario y de la dirección de correo electrónico](#).

También debe gestionar todos los grupos manualmente en IAM Identity Center. Para ello, debe crear los grupos y añadirlos mediante la consola de IAM Identity Center. No es necesario que estos grupos coincidan con los que existen en su IdP. Para obtener más información, consulte [Grupos](#).

## Rotar certificados SAML 2.0

IAM Identity Center utiliza certificados para establecer una relación de confianza de SAML entre IAM Identity Center y su proveedor de identidades (IdP) externo. Al añadir un IdP externo a IAM Identity Center, también debe obtener al menos un certificado SAML 2.0 X.509 público del IdP externo. Por lo general, ese certificado se instala automáticamente durante el intercambio de metadatos SAML del IdP durante la creación de relaciones de confianza.

Como administrador de IAM Identity Center, en ocasiones tendrá que sustituir los certificados de IdP antiguos por otros más nuevos. Por ejemplo, debe sustituir un certificado cuando se aproxime la fecha de vencimiento del certificado. El proceso de sustituir un certificado antiguo por uno más nuevo se denomina rotación de certificados.

## Temas

- [Rotar un certificado SAML 2.0](#)
- [Indicadores de estado de caducidad de certificados](#)

## Rotar un certificado SAML 2.0

Es posible que tenga que importar certificados periódicamente para rotar los certificados no válidos o vencidos emitidos por su proveedor de identidades. Esto ayuda a evitar la interrupción de la autenticación o el tiempo de inactividad. Todos los certificados importados se activan automáticamente. Los certificados solo se deben eliminar después de asegurarse de que ya no se utilizan con el proveedor de identidades asociado.

También debes tener en cuenta que es IdPs posible que algunos no admitan varios certificados. En este caso, el hecho de rotar los certificados con ellos IdPs podría suponer una interrupción temporal del servicio para los usuarios. El servicio se restablece cuando la confianza con ese IdP se ha restablecido correctamente. Si es posible, planifique esta operación cuidadosamente durante las horas de menor actividad.

 Note

Como práctica recomendada de seguridad, ante cualquier indicio de que un certificado SAML existente está en peligro o se está usando de forma incorrecta, debe retirarlo inmediatamente y cambiarlo.

La rotación de un certificado de IAM Identity Center es un proceso de varios pasos que incluye lo siguiente:

- Obtención de un nuevo certificado del IdP
- Importación del nuevo certificado a IAM Identity Center
- Activación del nuevo certificado en el IdP
- Eliminación del certificado anterior

Siga todos los procedimientos que se detallan a continuación para completar el proceso de rotación del certificado y, al mismo tiempo, evitar cualquier tiempo de inactividad de la autenticación.

#### Paso 1: obtención de un nuevo certificado del IdP

Vaya al sitio web del IdP y descargue su certificado SAML 2.0. Asegúrese de que el archivo del certificado se descargue en formato codificado PEM. La mayoría de los proveedores le permiten crear varios certificados SAML 2.0 en el IdP. Es probable que se marquen como deshabilitados o inactivos.

#### Paso 2: importación del nuevo certificado a IAM Identity Center

Siga el procedimiento que se detalla a continuación para importar el nuevo certificado mediante la consola de IAM Identity Center.

1. En la [consola de IAM Identity Center](#), elija Configuración.

2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página Administrar certificados SAML 2.0, seleccione Importar certificado.
4. En el cuadro de diálogo Importar certificado SAML 2.0, seleccione Elegir archivo, navegue hasta el archivo de certificado, selecciónelo y, a continuación, elija Importar certificado.

En este punto, IAM Identity Center confiará en todos los mensajes SAML entrantes firmados desde los 2 certificados que haya importado.

### Paso 3: activación del nuevo certificado en el IdP

Regrese al sitio web del IdP y marque el nuevo certificado que creó anteriormente como principal o activo. En este punto, todos los mensajes SAML firmados por el IdP deberían usar el nuevo certificado.

### Paso 4: eliminación del certificado anterior

Siga el procedimiento que se detalla para completar el proceso de rotación de certificados para su IdP. Siempre debe haber al menos un certificado válido en la lista y no se puede eliminar.

#### Note

Asegúrese de que su proveedor de identidades ya no firme las respuestas de SAML con este certificado antes de eliminarlo.

1. En la página Administrar certificados SAML 2.0, seleccione el certificado que desea eliminar. Elija Eliminar.
2. En el cuadro de diálogo Eliminar el certificado SAML 2.0, escriba **DELETE** para confirmarlo y, a continuación, elija Eliminar.
3. Regrese al sitio web del IdP y lleve a cabo los pasos necesarios para eliminar el certificado inactivo anterior.

### Indicadores de estado de caducidad de certificados

La página Administrar certificados SAML 2.0 muestra iconos indicadores de estado en colores en la columna Fecha de caducidad situada junto a cada certificado de la lista. A continuación, se describen los criterios que IAM Identity Center utiliza para determinar qué icono se muestra en cada certificado.

- Rojo: indica que un certificado está caducado.
- Amarillo: indica que un certificado caducará en 90 días o menos.
- Verde: indica que un certificado es válido y seguirá siendo válido durante al menos 90 días más.

Cómo comprobar el estado de la renovación de un certificado:

1. En la [consola de IAM Identity Center](#), elija Configuración.
2. En la página de configuración, elija la pestaña Fuente de identidad y, a continuación, Acciones > Administrar aprovisionamiento.
3. En la página Administrar la autenticación de SAML 2.0, en Administrar certificados de SAML 2.0, consulte el estado de los certificados de la lista tal y como se indica en la columna Caduca el.

## Uso del portal de AWS acceso

El portal de AWS acceso proporciona a los usuarios acceso de inicio de sesión único a todas sus Cuentas de AWS y aplicaciones en la nube más utilizadas, como Office 365, Concur, Salesforce y muchas más. Puede lanzar rápidamente varias aplicaciones. Solo tiene que elegir el icono de la Cuenta de AWS o de la aplicación en el portal. La presencia de iconos de aplicación en su portal de AWS acceso significa que un administrador de su empresa le ha otorgado acceso a dichas Cuentas de AWS o aplicaciones. También significa que puede acceder a todas esas cuentas o aplicaciones desde el portal de AWS acceso sin tener que realizar inicios de sesión adicionales.

Póngase en contacto con su administrador o con el servicio de asistencia para solicitar acceso adicional en las siguientes situaciones:

- Cuando no ve una cuenta Cuenta de AWS o una aplicación de la que necesita acceder.
- Si el acceso que tiene a una cuenta o aplicación determinada no es el previsto.

### Temas

- [Activar el portal de AWS acceso para usuarios que acceden por primera vez al IAM Identity Center](#)
- [Cómo iniciar sesión en el portal de AWS acceso de.](#)
- [Restablecer la contraseña de usuario del portal de AWS acceso:](#)
- [Obtención de las credenciales de usuario de IAM Identity Center para la AWS CLI o AWS SDKs](#)
- [Crear enlaces de acceso directo a los AWS Management Console destinos de](#)

- [Registro de un dispositivo para MFA](#)
- [Personalización de la URL del portal de AWS acceso](#)

## Activar el portal de AWS acceso para usuarios que acceden por primera vez al IAM Identity Center

Si es la primera vez que intenta iniciar sesión en el portal de AWS acceso, consulte su correo electrónico para obtener instrucciones sobre cómo activar sus credenciales de usuario.

Para activar las credenciales de usuario

1. Según el correo electrónico que haya recibido de su empresa, elija uno de los siguientes métodos para activar sus credenciales de usuario para que pueda comenzar a utilizar el portal de AWS usuarios de.
  - a. Si ha recibido un correo electrónico con el asunto Invitación a unirse a AWS IAM Identity Center, ábralo y seleccione Aceptar invitación. En la página de Registro de usuarios nuevos, introduzca y confirme una contraseña y, a continuación, seleccione Establecer nueva contraseña. Deberá utilizar esa contraseña cada vez que inicie sesión en el portal.
  - b. Si fue el equipo de asistencia de TI o el administrador de TI de la empresa el que le envió el correo electrónico, siga las instrucciones proporcionadas para activar sus credenciales de usuario.
2. Una vez que active sus credenciales de usuario proporcionando una nueva contraseña, se inicia sesión AWS en el portal de usuarios de forma automática. Si esto no ocurre, puede iniciar sesión manualmente en el portal de usuarios AWS usando las instrucciones que se indican en el siguiente paso.

## Cómo iniciar sesión en el portal de AWS acceso de.

El portal de AWS acceso proporciona a los usuarios de IAM Identity Center un acceso de inicio de sesión único a todas sus Cuentas de AWS y aplicaciones asignadas a través de un portal web. A continuación, se describe cómo iniciar sesión en el portal de AWS acceso, consejos para iniciar sesión y cómo cerrar sesión en el AWS portal de acceso. Para obtener información sobre cómo iniciar sesión en el portal de AWS acceso como usuario del Centro de identidad de IAM, consulte [Iniciar sesión en el portal de AWS acceso en la](#) Guía de inicio de AWS sesión.

### Requisitos previos



El Centro de identidad de IAM debe estar habilitado para usar el AWS portal de acceso. Para obtener más información, consulte [Activar IAM Identity Center](#)

 Note

Tras iniciar sesión, la duración predeterminada de la sesión del portal de AWS acceso es de 8 horas. Tenga en cuenta que un administrador puede [cambiar la duración](#) de esta sesión.

## Inicie sesión en el portal de AWS acceso de.

Los siguientes pasos son para que el administrador de IAM Identity Center confirme que el usuario de IAM Identity Center puede iniciar sesión en el portal de AWS acceso de y acceder a la. Cuenta de AWS

Inicie sesión en el portal de AWS acceso de.

1. Realice una de estas 2 operaciones para iniciar sesión en la AWS Management Console.
  - Primera vez que AWS utiliza (usuario raíz): inicie sesión como propietario de cuenta; para ello, elija Usuario raíz de la e ingrese la dirección de Cuenta de AWS correo electrónico de. En la siguiente página, escriba su contraseña.
  - Ya utiliza AWS (credenciales de IAM): inicie sesión con sus credenciales de IAM y seleccione un rol administrativo.
2. Abra la [consola de IAM Identity Center](#).
3. En el panel de navegación, elija Panel.
4. En la página del panel de control, en el resumen de la configuración, selecciona la URL del portal de AWS acceso.
5. Inicie sesión mediante cualquiera de las siguientes opciones:
  - Si utiliza Active Directory o un proveedor de identidades (IdP) externo como origen de identidad, inicie sesión con las credenciales del usuario de Active Directory o IdP.
  - Si utiliza el directorio predeterminado de Identity Center como origen de identidad, inicie sesión con el nombre de usuario que especificó al crear el usuario y la nueva contraseña que especificó para el usuario.
6. En la pestaña Cuentas, localice la su Cuenta de AWS y amplíela.

7. Se mostrarán los roles que tiene disponibles. Por ejemplo, si se le asigna tanto el conjunto de `AdministratorAccess` permisos como los conjuntos de permisos `Billing`, esos roles se muestran en el portal de AWS acceso de. Seleccione el nombre del rol de IAM que desee usar para la sesión.
8. Si se le redirige a la Consola AWS de administración de, significa que ha terminado de configurar correctamente el acceso a la Cuenta de AWS.

 Note

Si no ve Cuentas de AWS en la lista, es probable que aún no se le haya asignado al usuario un conjunto de permisos para esa cuenta. Para obtener instrucciones sobre cómo asignar usuarios a un conjunto de permisos, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

Ahora que ha confirmado que puede iniciar sesión con las credenciales de IAM Identity Center, cambie al navegador que utilizó para iniciar sesión en la AWS Management Console y cierre la sesión de las credenciales del usuario raíz o del usuario de IAM.

 Important

Le recomendamos encarecidamente que utilice las credenciales del usuario administrativo de IAM Identity Center al iniciar sesión en el portal de AWS acceso para realizar tareas administrativas en lugar de utilizar credenciales de usuario de IAM o usuario raíz. Proteja las credenciales del usuario raíz y utilícelas sólo para las tareas que el usuario raíz pueda realizar. Para permitir que otros usuarios accedan a sus cuentas y aplicaciones, y para administrar IAM Identity Center, cree y asigne conjuntos de permisos únicamente a través de IAM Identity Center.

## Dispositivos de confianza

Después de seleccionar la opción *Este es un dispositivo de confianza* en la página de inicio de sesión, IAM Identity Center considerará que todos los inicios de sesión futuros desde ese dispositivo están autorizados. Esto significa que IAM Identity Center no ofrecerá la opción de introducir un código MFA mientras utilice ese dispositivo de confianza. Sin embargo, hay algunas excepciones, como iniciar sesión desde un navegador nuevo o cuando el dispositivo recibe una dirección IP desconocida.

## Consejos para iniciar sesión en el portal de AWS acceso

Estos son algunos consejos que le ayudarán a administrar su experiencia con el portal de AWS acceso.

- En alguna ocasión, es posible que tenga que cerrar la sesión del portal de usuario e AWS iniciarla de nuevo. Esto puede ser necesario para poder acceder a las nuevas aplicaciones que el administrador le haya asignado recientemente. Sin embargo, no será necesario, ya que todas las nuevas aplicaciones se actualizan cada hora.
- Al iniciar sesión en el portal de AWS acceso, puede abrir cualquiera de las aplicaciones que se enumeran en el portal eligiendo el icono de la aplicación. En cuanto haya terminado de usar la aplicación, puede o bien cerrar la aplicación o bien cerrar la sesión del portal de AWS acceso. Al cerrar la aplicación solo finaliza la sesión de la aplicación en cuestión. Las demás aplicaciones que haya abierto desde el portal de AWS usuario seguirán abiertas y en funcionamiento.
- Antes de iniciar sesión con otro usuario, primero debe cerrar la sesión del portal de usuario AWS . El cierre de sesión del portal elimina por completo sus credenciales de la sesión del navegador.
- Una vez que inicie sesión en el portal de AWS acceso, podrá cambiar a un rol. Esto anula temporalmente los permisos de usuario originales y, en su lugar, le otorga los permisos asignados al rol. Para obtener más información, consulte [Cambiar a un rol \(consola\)](#).

## Cerrar sesión en el portal de AWS acceso de.

Al cerrar sesión del portal, se eliminan por completo sus credenciales de la sesión del navegador. Para obtener más información, [consulte Cerrar sesión en el portal de AWS acceso](#) en la AWS Sign-In guía.

## Cerrar sesión en el portal de AWS acceso de.

- En el portal de AWS acceso, seleccione Cerrar sesión en la barra de navegación.

### Note

Antes de iniciar sesión con otro usuario, primero debe cerrar la sesión del portal de usuario AWS .

## Restablecer la contraseña de usuario del portal de AWS acceso:

El portal de AWS acceso proporciona a los usuarios de [IAM Identity Center](#) un acceso de inicio de sesión único a todas sus AWS cuentas asignadas y aplicaciones en la nube a través de un portal web. El portal de AWS acceso es diferente de la [AWS Management Console](#), que es un conjunto de consolas de servicio para gestionar AWS los recursos de.

Siga este procedimiento para restablecer la contraseña de usuario de IAM Identity Center para el portal de AWS acceso. Más información sobre los [tipos de usuario](#) en la Guía del usuario de AWS Sign-In .

### Consideraciones

La función de restablecimiento de la contraseña para el portal de AWS acceso solo está disponible para los usuarios de las instancias de Identity Center que utilizan el directorio de Identity Center o [AWS Managed Microsoft AD](#) como fuente de identidad. Si el usuario está conectado a un proveedor de identidad externo o a [AD Connector](#), el restablecimiento de la contraseña del usuario debe realizarse desde el proveedor de identidad externo o estar conectado a Active Directory.

- Si su fuente de identidad es un directorio del IAM Identity Center, consulte [Requisitos de contraseñas para administrar identidades en IAM Identity Center](#).
- Si su fuente de identidad es una AWS Managed Microsoft AD, consulte [Requisitos de contraseña al restablecer una contraseña en AWS Managed Microsoft AD](#).

### Cómo restablecer la contraseña del portal de AWS acceso:

1. Abra un navegador y vaya a la página de inicio de sesión del portal de AWS usuarios.

Si no tiene la URL del portal de AWS acceso, compruebe su correo electrónico. Debería haber recibido por correo electrónico una invitación para unirse a AWS IAM Identity Center que incluye una URL de inicio de sesión específica en el AWS portal de acceso. Como alternativa, es posible que su administrador le haya proporcionado directamente una contraseña de un solo uso y la URL del portal de AWS acceso. Si no encuentra esta información, pida al administrador que se la envíe.

Para obtener más información sobre cómo iniciar sesión en el portal de AWS acceso, consulte [Iniciar sesión en el portal de AWS acceso](#) en la Guía del AWS Sign-In usuario de.

2. Escriba su nombre y, a continuación, elija Siguiente.

3. En Contraseña, seleccione He olvidado la contraseña.

Proporcione su nombre de usuario y escriba los caracteres de la imagen para confirmar que no es un robot. A continuación, elija Siguiente. Es posible que tenga que deshabilitar el software bloqueador de anuncios si no puede introducir caracteres.

4. Aparecerá un mensaje para confirmar que se envió un correo electrónico para restablecer la contraseña. Elija Continuar.
5. Recibirá un correo electrónico de `no-reply@signin.aws` con el asunto Se solicita el restablecimiento de la contraseña. En el correo electrónico, seleccione Restablecer contraseña.
6. En la página Restablecer la contraseña, compruebe su nombre de usuario, especifique una nueva contraseña para el portal de AWS acceso y, a continuación, seleccione Establecer nueva contraseña.
7. Recibirá un correo electrónico de `no-reply@signin.aws` con el asunto Se solicita el restablecimiento de la contraseña.

 Note

Un administrador puede restablecer su contraseña enviándole un correo electrónico con instrucciones para restablecerla o generando una contraseña de un solo uso y compartiéndola con usted. Si es un administrador, consulte [Restablecimiento de la contraseña de usuario de IAM Identity Center para un usuario final](#).

## Obtención de las credenciales de usuario de IAM Identity Center para la AWS CLI o AWS SDKs

Puede acceder a AWS los servicios de mediante programación usando los kits de desarrollo de AWS software (SDKs) de la AWS Command Line Interface o de con credenciales de usuario de IAM Identity Center. En este tema se describe cómo obtener credenciales temporales para un usuario en IAM Identity Center.

El portal de AWS acceso proporciona a los usuarios de IAM Identity Center un acceso único a sus aplicaciones Cuentas de AWS y la nube de. Tras iniciar sesión en el portal de AWS acceso como usuario de IAM Identity Center, podrá obtener credenciales temporales. A continuación, puede utilizar las credenciales, también denominadas credenciales de usuario de IAM Identity Center, en la AWS CLI o AWS SDKs para acceder a los recursos de una Cuenta de AWS.

Si utiliza la AWS CLI para acceder a los AWS servicios de mediante programación, puede utilizar los procedimientos de este tema para iniciar el acceso a la. AWS CLI Para obtener información sobre el AWS CLI, consulte la Guía del [AWS Command Line Interface usuario](#).

Si utiliza la AWS SDKs para acceder a los AWS servicios de mediante programación, seguir los procedimientos de este tema también establece directamente la autenticación de la. AWS SDKs Para obtener información acerca de AWS SDKs, consulte la Guía de [referencia de herramientas AWS SDKs y herramientas](#).

#### Note

Los usuarios de IAM Identity Center son diferentes a los [usuarios de IAM](#). Los usuarios de IAM reciben credenciales a largo plazo para AWS los recursos de. Los usuarios de IAM Identity Center reciben credenciales temporales. Le recomendamos que utilice credenciales temporales como práctica recomendada de seguridad para acceder a sus, Cuentas de AWS ya que estas credenciales se generan cada vez que inicia sesión.

## Requisitos previos

Para obtener credenciales temporales para su usuario de IAM Identity Center, necesitará lo siguiente:

- Un usuario de IAM Identity Center: iniciará sesión en el portal de acceso AWS como este usuario. Usted o su administrador pueden crearlo. Para obtener información sobre cómo activar IAM Identity Center y crear un usuario de IAM Identity Center, consulte [Getting started with IAM Identity Center](#).
- Acceso de usuario a una Cuenta de AWS: para conceder permiso a un usuario de IAM Identity Center para que recupere sus credenciales temporales, usted o un administrador deben asignar al usuario de IAM Identity Center un conjunto de [permisos](#). Los conjuntos de permisos se guardan en IAM Identity Center y definen el nivel de acceso que tienen los usuarios y grupos de una Cuenta de AWS. Si su administrador creó el usuario de IAM Identity Center por usted, pídale que añada este acceso. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).
- AWS CLI La instalada: para usar las credenciales temporales, debe instalar la AWS CLI. Para obtener instrucciones de instalación, consulte [Instalar o actualizar la última versión de la AWS CLI](#) en la Guía del usuario de AWS CLI .

## Consideraciones

Antes de completar los pasos para obtener credenciales temporales para el usuario de IAM Identity Center, tenga en cuenta los siguientes aspectos:

- IAM Identity Center crea roles de IAM: cuando se asigna a un usuario de IAM Identity Center un conjunto de permisos, IAM Identity Center crea un rol de IAM correspondiente a partir del conjunto de permisos. Los roles de IAM creados mediante conjuntos de permisos se diferencian de los roles de IAM creados AWS Identity and Access Management en los siguientes aspectos:
  - IAM Identity Center posee y protege los roles creados por los conjuntos de permisos. Solo IAM Identity Center puede modificar estos roles.
  - Solo los usuarios de IAM Identity Center pueden asumir los roles que corresponden a sus conjuntos de permisos asignados. No puede asignar el acceso a los conjuntos de permisos a los usuarios de IAM, a los usuarios federados de IAM ni a las cuentas de servicio.
  - No puede modificar una política de confianza de roles en estos roles para permitir el acceso a [entidades principales](#) fuera de IAM Identity Center.

Para obtener información sobre cómo obtener credenciales temporales para un rol que cree en IAM, consulte [Uso de credenciales de seguridad temporales con la AWS CLI](#) en la Guía del usuario de AWS Identity and Access Management .

- Puede configurar la duración de la sesión para los conjuntos de permisos: tras iniciar sesión en el portal de AWS acceso, el conjunto de permisos al que está asignado su usuario de IAM Identity Center aparecerá como rol disponible. IAM Identity Center crea una sesión independiente para este rol. Esta sesión puede durar de una a 12 horas según la duración de la sesión configurada para el conjunto de permisos. De forma predeterminada, la sesión durará 1 hora. Para obtener más información, consulte [Definir la duración de la sesión para Cuentas de AWS](#).

## Obtención y actualización de credenciales temporales

Puede obtener y actualizar credenciales temporales de su usuario de IAM Identity Center de forma automática o manual.

### Temas

- [Actualización automática de credenciales \(recomendada\)](#)
- [Actualización manual de credenciales](#)

## Actualización automática de credenciales (recomendada)

La actualización automática de credenciales utiliza el estándar de autorización de código de dispositivo Open ID Connect (OIDC)). Con este método, se inicia el acceso directamente mediante el comando `aws configure sso` en la AWS CLI. Puede usar este comando para acceder automáticamente a cualquier rol que esté asociado a cualquier conjunto de permisos al que esté asignado para cualquier Cuenta de AWS.

Para acceder al rol creado para su usuario de IAM Identity Center, ejecute el `aws configure sso` comando y, a continuación, autorice la AWS CLI desde una ventana del navegador. Mientras tenga una sesión activa en el portal de AWS acceso, la AWS CLI recuperará automáticamente las credenciales temporales y las actualizará automáticamente.

Para obtener más información, consulte [Configurar el perfil con el `aws configure sso wizard`](#) en la Guía del usuario AWS Command Line Interface .

Cómo obtener credenciales temporales que se actualicen automáticamente:

1. El administrador o el empleado del AWS servicio de asistencia proporcionan el portal de acceso o la URL de inicio de sesión específica. Si creó el usuario de IAM Identity Center, AWS envió una invitación por correo electrónico con la URL de inicio de sesión. Para obtener más información, consulte [Iniciar sesión en el portal de AWS acceso en la Guía del](#) usuario de AWS inicio de sesión.
2. En la pestaña Cuentas, localice Cuenta de AWS la para la que desee recuperar las credenciales. Al seleccionar la cuenta, aparecerán el nombre y el ID de la cuenta y la dirección de correo electrónico asociados a la cuenta.

### Note

Si no ve ninguna Cuentas de AWS en la lista, es probable que aún no se le haya asignado un conjunto de permisos dicha cuenta o cuentas. En este caso, póngase en contacto con su administrador y pídale que añada este acceso. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

3. Debajo del nombre de la cuenta, los permisos al que está asignado el usuario de IAM Identity Center aparecen como un rol disponible. Por ejemplo, si a su usuario del Centro de Identidad de IAM se le asigna el conjunto de `PowerUserAccess` permisos de la cuenta, el rol aparecerá en el portal de AWS acceso como `PowerUserAccess`.



4. Según la opción que elija junto al nombre del rol, elija Claves de acceso o Línea de comandos o acceso mediante programación.
5. En el cuadro de diálogo Obtener credenciales, elija macOS y Linux, Windows o PowerShell, según el sistema operativo en el que haya instalado el AWS CLI.
6. En Credenciales de IAM Identity Center de AWS (recomendadas), se muestran sus credenciales de SSO Start URL y SSO Region. Estos valores son necesarios para configurar un perfil habilitado para IAM Identity Center y sso-session para la AWS CLI Para completar esta configuración, siga las instrucciones de [Configurar el perfil con el aws configure sso wizard](#) en la Guía del usuario de AWS Command Line Interface .

Continúe utilizando la para su cuenta de AWS CLI mientras la Cuenta de AWS necesite hasta que caduquen las credenciales.

### Actualización manual de credenciales

Puede usar el método de actualización manual de credenciales para obtener credenciales temporales para un rol que esté asociado a un conjunto de permisos específico en una Cuenta de AWS específica. Para ello, debe copiar y pegar los comandos necesarios para las credenciales temporales. Con este método, debe actualizar las credenciales temporales manualmente.

Puede ejecutar AWS CLI comandos de la hasta que caduquen sus credenciales temporales.

### Cómo obtener credenciales que se actualizan manualmente

1. El administrador o el empleado del AWS servicio de asistencia proporcionan el portal de acceso o la URL de inicio de sesión específica. Si creó el usuario de IAM Identity Center, AWS envió una invitación por correo electrónico con la URL de inicio de sesión. Para obtener más información, consulte [Iniciar sesión en el portal de AWS acceso en la Guía del](#) usuario de AWS inicio de sesión.
2. En la pestaña Cuentas, localice la para la que desea recuperar las credenciales Cuenta de AWS de acceso y amplíela para mostrar el nombre del rol de IAM (por ejemplo, Administrador). Según la opción que elija junto al nombre del rol de IAM, elija Claves de acceso o Línea de comandos o acceso mediante programación.

#### Note

Si no ve ninguna Cuentas de AWS en la lista, es probable que aún no se le haya asignado un conjunto de permisos dicha cuenta o cuentas. En este caso, póngase

en contacto con su administrador y pídale que añada este acceso. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

3. En el cuadro de diálogo Obtener credenciales, elija macOS y Linux, Windows o PowerShell, según el sistema operativo en el que haya instalado el AWS CLI.

4. Elija una de las siguientes opciones:

- Opción 1: definir las variables de AWS entorno

Elija esta opción para anular toda la configuración de credenciales, incluida la configuración de los archivos `credentials` y `config`. Para obtener más información, consulte [Variables de entorno para configurar la AWS CLI](#) en la Guía del usuario de AWS CLI .

Para usar esta opción, copie los comandos en el portapapeles, péguelos en la ventana del AWS CLI terminal de la y, a continuación, presione Entrar para configurar las variables de entorno necesarias.

- Opción 2: agregue un perfil al archivo de AWS credenciales de

Elija esta opción para ejecutar comandos con diferentes conjuntos de credenciales.

Para usar esta opción, copie los comandos en el portapapeles y, a continuación, péguelos en los AWS `credentials` archivos compartidos de para configurar un nuevo perfil con nombre. Para obtener más información, consulte los [archivos de configuración y credenciales compartidos](#) en la Guía de referencia de herramientas AWS SDKs y herramientas. Para usar esta credencial, especifique la `--profile` opción en el AWS CLI comando de la. Esto afecta a todos los símbolos del sistema que utilicen el mismo archivo de credenciales.

- Opción 3: utilice valores individuales en su cliente AWS de servicio de

Elija esta opción para acceder a AWS los recursos de de de un cliente AWS de servicio de. Para obtener más información, consulte [Herramientas para crear en AWS](#).

Para usar esta opción, copie los valores en el portapapeles, péguelos en el código y asígnelos a las variables adecuadas para su SDK. Para obtener más información, consulte la documentación específica de su específico SDK API.

## Crear enlaces de acceso directo a los AWS Management Console destinos de

Los enlaces de acceso directo creados en el portal de AWS acceso llevan a los usuarios de IAM Identity Center a un destino específico en la AWS Management Console, con un conjunto de permisos específico y en una específica Cuenta de AWS.

Los enlaces de acceso directo le ahorran tiempo a usted y a sus colaboradores. En lugar de navegar hasta la URL de destino deseada en AWS Management Console (por ejemplo, una página de instancia de bucket de Amazon S3) a través de varias páginas, incluido el portal de AWS acceso, puede utilizar un enlace de acceso directo para llegar al mismo destino automáticamente.

### Opciones de destino del enlace de acceso directo

Los enlaces de acceso directo tienen tres opciones de destino, que se enumeran aquí por prioridad:

- (Opcional) Cualquier URL de destino en la AWS Management Console especificada en el enlace de acceso directo. Por ejemplo, la página de instancias de bucket de Amazon S3.
- (Opcional) URL de estado de retransmisión configurada por el administrador para el conjunto de permisos en cuestión. Para obtener más información sobre el estado de retransmisión, consulte [Configure el estado de la retransmisión para acceder rápidamente a AWS Management Console](#).
- AWS Management Console casa. El destino por defecto si no especifica ninguna.

#### Note

La navegación automática a un destino solo se realiza correctamente si se ha autenticado en el IAM Identity Center y se ha asignado el conjunto de permisos necesario para la AWS cuenta y la URL de destino.

El portal de AWS acceso incluye un botón Crear acceso directo que le ayuda a crear un enlace de acceso directo que se pueda compartir. Si tiene pensado especificar una URL de destino (la primera opción de la lista anterior), puede copiar la URL en un portapapeles para compartirla.

### Cree un enlace de acceso directo en el portal de AWS acceso

1. Con la sesión iniciada en el portal de AWS acceso, seleccione la pestaña Cuentas y, a continuación, pulse el botón Crear acceso directo.

## 2. En el cuadro de diálogo:

- a. Elija una Cuenta de AWS con el ID o el nombre de la cuenta. A medida que escribe, un menú desplegable muestra la cuenta IDs y los nombres correspondientes a los que puedes acceder. Puede elegir solo una cuenta a la que tenga acceso.
- b. Si lo desea, elija un rol de IAM de la lista desplegable. Estos son los conjuntos de permisos que se le han asignado para la cuenta seleccionada. Si omite la elección del rol, se le pide a los usuarios que seleccionen uno que se les haya asignado para la cuenta elegida al utilizar el enlace de acceso directo.

### Note

No puede conceder nuevos accesos con los enlaces de acceso directo. Los enlaces de acceso directo solo funcionan con los conjuntos de permisos ya asignados al usuario. Si el usuario no tiene asignados los conjuntos de permisos necesarios para la cuenta y la URL de destino, se le deniega el acceso.

- c. Si lo desea, introduzca la URL de destino del portal de AWS acceso. Si omite introducir una URL, el destino se determina de forma automática al utilizar el enlace de acceso directo, en función de las opciones de destino del enlace de acceso directo mencionadas anteriormente.
- d. El enlace abreviado se generará en la parte inferior del cuadro de diálogo, en función de lo que introduzca. Pulse el botón Copiar URL. Ahora puede crear un marcador con el enlace de acceso directo copiado o compartirlo con sus colaboradores que tengan acceso a la misma cuenta con el mismo conjunto de permisos o con otro conjunto de permisos suficiente.

## Crear enlaces de AWS Management Console acceso directo de seguros con codificación de URL

Todos los valores de los parámetros de la URL, incluidos el ID de cuenta, el nombre del conjunto de permisos y la URL de destino, deben estar codificados en URL.

Los enlaces de AWS acceso directo amplían la URL del portal de acceso con la siguiente ruta:

/#/console?

account\_id=[*account\_ID*]&role\_name=[*permission\_set\_name*]&destination=[*destination*]

La URL completa de la AWS partición de clásica sigue este patrón:

```
https://[your_subdomain].awsapps.com/start/#/console?  
account_id=[account_ID]&role_name=[permission_set_name]&destination=[destination]
```

Este es un ejemplo de enlace de acceso directo que permite a un usuario acceder a una cuenta 123456789012 con el conjunto de permisos de S3FullAccess y acceder a la página de inicio de la consola S3:

- `https://example.awsapps.com/start/#/console?  
account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.aws.amazon.com%2Fs3%2Fhome`
- (AWS GovCloud (US) Region) `https://start.us-gov-west-1.us-gov-home.awsapps.com/directory/example/#/console?  
account_id=123456789012&role_name=S3FullAccess&destination=https%3A%2F%2Fconsole.amazonaws-us-gov.com%2Fs3%2Fhome`

## Registro de un dispositivo para MFA

Siga el siguiente procedimiento en el portal de AWS acceso para registrar el nuevo dispositivo para la autenticación multifactor (MFA).

### Note

Le recomendamos que primero descargue la aplicación de autenticación adecuada en su dispositivo antes de iniciar los pasos de este procedimiento. Para obtener una lista de las aplicaciones probadas que puede utilizar con dispositivos de MFA, consulte [Aplicaciones de autenticación virtual](#).

### Cómo registrar el dispositivo para su uso con MFA

1. Inicio de sesión en el portal de AWS acceso. Para obtener más información, consulte [Cómo iniciar sesión en el portal de AWS acceso de..](#)
2. Cerca de la parte superior derecha de la página, seleccione dispositivos MFA.
3. En la página Dispositivos de autenticación multifactor (MFA), seleccione Registrar dispositivo.

 Note

Si la opción Registrar dispositivo MFA aparece atenuada, póngase en contacto con el administrador para que le ayude a registrar el dispositivo.

4. En la página Registrar dispositivo MFA, seleccione uno de los siguientes tipos de dispositivos MFA y siga las instrucciones:

- Aplicación de autenticación

1. En la página Configurar la aplicación de autenticación, IAM Identity Center muestra la información de configuración del nuevo dispositivo de MFA, incluido un gráfico de código QR. El gráfico es una representación de la clave secreta que se puede introducir manualmente en dispositivos que no admiten códigos QR.
2. Con el dispositivo de MFA físico, haga lo siguiente:
  - a. Abra una aplicación de autenticación MFA compatible. Para obtener una lista de las aplicaciones probadas que puede utilizar con dispositivos de MFA, consulte [Aplicaciones de autenticación virtual](#). Si la aplicación de MFA admite varias cuentas (varios dispositivos de MFA), elija la opción para crear una nueva cuenta (un nuevo dispositivo de MFA).
  - b. Determine si la aplicación de MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones de la página Configurar la aplicación de autenticación.
    - i. Elija Mostrar código QR y, a continuación, utilice la aplicación para escanear el código QR. Por ejemplo, puede elegir el icono de la cámara o una opción similar a Escanear código. A continuación, use la cámara del dispositivo para escanear el código.
    - ii. Seleccione Mostrar clave secreta y, a continuación, introduzca esa clave secreta en su aplicación de MFA.

 Important

Cuando configure un dispositivo MFA para que funcione con IAM Identity Center, recomendamos que guarde una copia del código QR o la clave secreta en un lugar seguro. Esto puede ayudarle si pierde el teléfono o tiene que volver a instalar la aplicación de autenticación MFA. Si ocurre alguna de

estas cosas, puede volver a configurar rápidamente la aplicación para que utilice la misma configuración de MFA.

3. En la página Configurar la aplicación de Authenticator, en Código de autenticación, escriba la contraseña de uso único que aparece actualmente en el dispositivo MFA físico.

 Important

Envíe su solicitud inmediatamente después de generar el código. Si genera el código y después espera demasiado tiempo a enviar la solicitud, el dispositivo MFA se asociará correctamente a su usuario, pero no estará sincronizado. Esto ocurre porque las contraseñas temporales de un solo uso (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo.

4. Elija Asignar MFA. Ahora, el dispositivo MFA puede empezar a generar contraseñas de un solo uso y ya se puede usar con. AWS

- Llave de seguridad o autenticador integrado

1. En la página Registrar la clave de seguridad de su usuario, siga las instrucciones que le dé su navegador o plataforma.

 Note

La experiencia varía según el navegador o la plataforma. Una vez que el dispositivo se haya registrado correctamente, podrá asociar un nombre descriptivo al dispositivo recién inscrito. Si desea cambiarlo, seleccione Cambiar nombre, escriba el nuevo nombre y, a continuación, seleccione Guardar.

## Personalización de la URL del portal de AWS acceso

De forma predeterminada, puede acceder al portal de AWS acceso mediante una URL que siga este formato: `d-xxxxxxxxxx.awsapps.com/start`. Puede personalizar el complemento del modo siguiente: `your_subdomain.awsapps.com/start`.

 Important

Si cambia la URL del portal de AWS acceso, no podrá editarla más adelante.

### Cómo personalizar la URL

1. Abre la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En la consola de IAM Identity Center, elija Panel en el panel de navegación y localice la sección Resumen de configuración.
3. Pulse el botón Personalizar debajo de la URL de su portal de AWS acceso.

 Note

Si el botón Personalizar no aparece, significa que el portal de acceso AWS ya se ha personalizado. La personalización de la URL del portal de AWS acceso es una operación que se realiza una sola vez y no se puede revertir.

4. Introduzca el nombre de subdominio que desee y pulse Guardar.

Ahora puede iniciar sesión en la AWS consola de a través de su portal de AWS acceso con su URL personalizada.

## Autenticación multifactor para usuarios de Identity Center

El IAM Identity Center viene preconfigurado con la autenticación multifactor (MFA) activada de forma predeterminada, de modo que todos los usuarios deben iniciar sesión con la MFA además de su nombre de usuario y contraseña. Esto garantiza que los usuarios deban iniciar sesión en el portal de AWS acceso mediante los dos factores siguientes:

- Su nombre de usuario y contraseña. Este es el primer factor y es un elemento que los usuarios saben.
- Ya sea un código, una clave de seguridad o datos biométricos. Este es el segundo factor y es un elemento que los usuarios tienen (posesión) o son (biométrico). El segundo factor puede ser un código de autenticación generado desde su dispositivo móvil, una clave de seguridad conectada a su ordenador o el escaneo biométrico del usuario.



En conjunto, estos múltiples factores proporcionan una mayor seguridad al impedir el acceso no autorizado a sus AWS recursos, a menos que se haya completado correctamente una impugnación de MFA válida.

Cada usuario puede registrar hasta 2 aplicaciones de autenticación virtual, que son aplicaciones de autenticación de contraseñas de un solo uso instaladas en su dispositivo móvil o tableta, y 6 autenticadores FIDO, que incluyen autenticadores y claves de seguridad integrados, para un total de 8 dispositivos MFA. Obtener más información sobre [Tipos de MFA disponibles para IAM Identity Center](#).

## Temas

- [Tipos de MFA disponibles para IAM Identity Center](#)
- [Configuración de MFA en el centro de identidad de IAM](#)
- [Registre un dispositivo MFA para usuarios](#)
- [Cambiar el nombre y eliminar dispositivos MFA en IAM Identity Center](#)

## Tipos de MFA disponibles para IAM Identity Center

La autenticación multifactor (MFA) es un mecanismo simple y eficaz para mejorar la seguridad de los usuarios. El primer factor del usuario, su contraseña, es un secreto que debe memorizar, también conocido como factor de conocimiento. Otros factores pueden ser factores de posesión (algo que posea, como una clave de seguridad) o factores inherentes (algo que sea suyo y solo suyo, como un escaneo biométrico). Se recomienda encarecidamente que configure una MFA para agregar una capa adicional para la seguridad de su cuenta.

La MFA de IAM Identity Center admite los siguientes tipos de dispositivos: Todos los tipos de MFA se admiten tanto para el acceso a la consola desde un navegador como para el uso de la AWS CLI versión 2 con IAM Identity Center.

- [FIDO2 autenticadores](#), incluidos los autenticadores y las claves de seguridad integrados
- [Aplicaciones de autenticación virtual](#)
- Su propia implementación conectada a través de [MFA en RADIUS](#) AWS Managed Microsoft AD

Un usuario puede tener hasta ocho dispositivos MFA, que incluyen hasta dos aplicaciones de autenticación virtual y seis autenticadores FIDO, registrados en uno. Cuenta de AWS También puede configurar los ajustes de MFA para que requieran la MFA siempre que intenten iniciar sesión desde

un nuevo dispositivo o navegador, o cuando inicien sesión desde una dirección IP desconocida. Para obtener más información sobre cómo configurar los ajustes de MFA para los usuarios, consulte [Elegir tipos de MFA para la autenticación de usuarios](#) y [Configurar la aplicación de dispositivos MFA](#).

## FIDO2 autenticadores

[FIDO2](#) es un estándar que incluye CTAP2 [WebAuthn](#) y se basa en la criptografía de clave pública. Las credenciales FIDO son eficaces ante intentos de suplantación de identidad porque son exclusivas del sitio web en el que se crearon, por ejemplo AWS.

AWS admite los dos factores de forma más comunes para los autenticadores FIDO: los autenticadores integrados y las claves de seguridad. Consulte la sección que aparece a continuación para obtener más información sobre los tipos más comunes de autenticadores FIDO.

### Temas

- [Autenticadores integrados](#)
- [Claves de seguridad](#)
- [Administradores de contraseñas, proveedores de claves de acceso y otros autenticadores FIDO](#)

### Autenticadores integrados

Algunos ordenadores y teléfonos móviles actuales tienen autenticadores integrados, como el TouchID del MacBook o una cámara compatible con Windows Hello. Si su dispositivo tiene un autenticador integrado compatible con FIDO, puede usar su huella digital, su rostro o el PIN del dispositivo como segundo factor.

### Claves de seguridad

Las llaves de seguridad son autenticadores de hardware externos compatibles con FIDO que puede comprar y conectar a su dispositivo a través de USB, BLE o NFC. Cuando se le pida la MFA, solo tiene que realizar un gesto con el sensor de la tecla. Algunos ejemplos de claves de seguridad incluyen las claves feitianas, YubiKeys y las claves de seguridad más comunes crean credenciales FIDO vinculadas al dispositivo. Para obtener una lista de todas las llaves de seguridad certificadas por FIDO, consulte los [productos certificados por FIDO](#).

### Administradores de contraseñas, proveedores de claves de acceso y otros autenticadores FIDO

Existen varios proveedores externos que admiten la autenticación FIDO en las aplicaciones móviles, como características disponibles en administradores de contraseñas, tarjetas inteligentes con modo

FIDO y otros formatos. Estos dispositivos compatibles con FIDO pueden funcionar con IAM Identity Center, pero le recomendamos que pruebe usted mismo un autenticador FIDO antes de activar esta opción como MFA.

#### Note

Algunos autenticadores FIDO pueden crear credenciales FIDO reconocibles, conocidas como claves de acceso. Las claves de acceso pueden estar vinculadas al dispositivo que las crea o pueden sincronizarse y guardarse copias de seguridad en una nube. Por ejemplo, se puede registrar una clave de acceso con el Apple Touch ID en un MacBook compatible y, a continuación, iniciar sesión en un sitio desde un portátil Windows con Google Chrome con la clave de acceso en iCloud siguiendo las instrucciones que aparecen en pantalla al iniciar sesión. Para obtener más información sobre qué dispositivos admiten claves de acceso sincronizables y la interoperabilidad actual de claves entre sistemas operativos y navegadores, consulte [Asistencia para dispositivos](#) en [passkeys.dev](https://passkeys.dev), un recurso proporcionado por la Alianza FIDO y el Consorcio World Wide Web (W3C).

## Aplicaciones de autenticación virtual

Las aplicaciones de autenticación son autenticadores de terceros basados en contraseñas de un solo uso (OTP). Puede utilizar una aplicación de autenticación instalada en su dispositivo móvil o tableta como dispositivo MFA autorizado. La aplicación de autenticación de terceros debe cumplir con RFC 6238, que es un algoritmo de contraseña temporal de un solo uso (TOTP) basado en estándares y capaz de generar códigos de autenticación de seis dígitos.

Cuando se le pida la MFA, el usuario debe introducir un código válido de su aplicación de autenticación en el cuadro de entrada que aparece. Cada dispositivo MFA asignado a un usuario debe ser único. Se pueden registrar dos aplicaciones de autenticación para un usuario determinado.

### Aplicaciones de autenticación probada

Cualquier aplicación compatible con TOTP funcionará con la MFA de IAM Identity Center. La siguiente tabla muestra las aplicaciones de autenticación de terceros conocidas que puede elegir.

| Sistema operativo | Aplicación de autenticación probada                                                                                                 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| Android           | <a href="#">Authy</a> , <a href="#">Duo Mobile</a> , <a href="#">Microsoft Authenticator</a> , <a href="#">Google Authenticator</a> |

| Sistema operativo | Aplicación de autenticación probada                                                                                                 |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------|
| iOS               | <a href="#">Authy</a> , <a href="#">Duo Mobile</a> , <a href="#">Microsoft Authenticator</a> , <a href="#">Google Authenticator</a> |

## MFA en RADIUS

El [servicio de autenticación remota para usuarios por acceso telefónico \(RADIUS\)](#) es un protocolo cliente-servidor estándar del sector que proporciona administración de autenticación, autorización y contabilidad para que los usuarios puedan conectarse a los servicios de red. AWS Directory Service incluye un cliente RADIUS que se conecta al servidor RADIUS en el que ha implementado la solución de MFA. Para obtener más información, consulte [Activar autenticación multifactor de AWS Managed Microsoft AD](#).

Puede utilizar MFA en RADIUS o MFA en IAM Identity Center para los inicios de sesión de los usuarios en el portal de usuarios, pero no en ambos. La MFA en IAM Identity Center es una alternativa a la MFA RADIUS en los casos en que desee una autenticación AWS nativa de dos factores para acceder al portal.

Al habilitar la MFA en IAM Identity Center, los usuarios necesitan un dispositivo de MFA para iniciar sesión en el portal de acceso AWS. Si ya había utilizado MFA RADIUS, la activación de la MFA en IAM Identity Center anula de manera efectiva el MFA RADIUS para los usuarios que inician sesión en el portal de acceso. AWS Sin embargo, la MFA de RADIUS sigue siendo un desafío para los usuarios cuando inician sesión en todas las demás aplicaciones con las que funcionan AWS Directory Service, como Amazon RDS for SQL Server.

Si el MFA está deshabilitado en la consola del IAM Identity Center y ha configurado el MFA RADIUS con él, el MFA RADIUS rige el inicio de sesión en el AWS Directory Service portal de acceso. AWS Esto significa que IAM Identity Center recurre a la configuración de MFA en RADIUS si la MFA está deshabilitada.

## Configuración de MFA en el centro de identidad de IAM

Puede configurar las capacidades de MFA en el Centro de Identidad de IAM cuando su fuente de identidad esté configurada con el almacén de identidades del Centro de Identidad de IAM, o AWS Managed Microsoft AD AD Connector. Actualmente, los [proveedores de identidad externos](#) no admiten la MFA en IAM Identity Center.

Las siguientes son recomendaciones generales de MFA, en función de la configuración del centro de identidad de IAM y de las preferencias organizativas.

- Se recomienda a los usuarios que registren varios autenticadores de respaldo para todos los tipos de MFA habilitados. Esta práctica puede evitar la pérdida de acceso en caso de que un dispositivo MFA se rompa o se pierda.
- No elija la opción Exigirles que proporcionen una contraseña de un solo uso enviada por correo electrónico si sus usuarios deben iniciar sesión en el portal de acceso para AWS acceder a su correo electrónico. Por ejemplo, sus usuarios podrían utilizar Microsoft 365 el portal de AWS acceso para leer su correo electrónico. En este caso, los usuarios no podrán recuperar el código de verificación ni podrán iniciar sesión en el portal de AWS acceso. Para obtener más información, consulte [Configurar la aplicación de dispositivos MFA](#).
- Si ya utiliza el MFA RADIUS con el que configuró AWS Directory Service, no necesita habilitar el MFA en IAM Identity Center. La MFA de IAM Identity Center es una alternativa a la MFA en RADIUS para los usuarios de Microsoft Active Directory de IAM Identity Center. Para obtener más información, consulte [MFA en RADIUS](#).
- El siguiente YouTube vídeo ofrece una descripción general del Centro de identidades de MFA e IAM:

[IAM Identity Center: la autenticación multifactorial es la opción predeterminada para las instancias nuevas](#)

## Temas

- [Solicitar MFA a los usuarios](#)
- [Elegir tipos de MFA para la autenticación de usuarios](#)
- [Configurar la aplicación de dispositivos MFA](#)
- [Permita a los usuarios registrar sus propios dispositivos MFA](#)

## Solicitar MFA a los usuarios

Puede seguir los siguientes pasos para determinar con qué frecuencia se solicita a los usuarios de la fuerza laboral la autenticación multifactor (MFA) cada vez que intentan iniciar sesión en el portal de acceso AWS . Antes de comenzar, le recomendamos que comprenda los [Tipos de MFA disponibles para IAM Identity Center](#).

 Important

Las instrucciones figuran en esta sección aplican a [AWS IAM Identity Center](#). No se aplican a [AWS Identity and Access Management](#) (IAM). Los usuarios, grupos y credenciales de usuario de IAM Identity Center son diferentes de los usuarios, grupos y credenciales de usuario de IAM. Si busca instrucciones sobre cómo desactivar la MFA para los usuarios de IAM, consulte [Desactivación de dispositivos de MFA](#) en la Guía del usuario de AWS Identity and Access Management .

 Note

Si utiliza un IdP externo, la sección de Autenticación multifactor no estará disponible. Su IdP externo gestiona la configuración de MFA en lugar de IAM Identity Center.

## Para configurar MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.
5. En la página Configurar la autenticación multifactor, en Solicitar MFA a los usuarios, elija uno de los siguientes modos de autenticación en función del nivel de seguridad que necesite su empresa:

- Cada vez que inician sesión (siempre activo)

En este modo (la configuración predeterminada), el Centro de identidad de IAM requiere que se pregunte a los usuarios con un dispositivo MFA registrado cada vez que inicien sesión. Esta es la configuración más segura y garantiza que se apliquen las políticas organizativas o de cumplimiento al exigir que se utilice la MFA cada vez que inicien sesión en el portal de AWS acceso. Por ejemplo, PCI DSS recomienda encarecidamente la MFA durante cada inicio de sesión para acceder a las aplicaciones que admiten transacciones de pago de alto riesgo.

- Solo cuando su contexto de inicio de sesión cambie (en función del contexto)

En este modo, el Centro de identidad de IAM ofrece a los usuarios la opción de confiar en su dispositivo durante el inicio de sesión. Cuando un usuario indica que quiere confiar en un dispositivo, IAM Identity Center solicita al usuario la MFA una vez y analiza el contexto de inicio de sesión (como el dispositivo, el navegador y la ubicación) para los siguientes inicios de sesión del usuario. Para los inicios de sesión posteriores, IAM Identity Center determina si el usuario inicia sesión con un contexto en el que anteriormente se confiaba. Si el contexto de inicio de sesión del usuario cambia, IAM Identity Center solicita al usuario la MFA además de sus credenciales de dirección de correo electrónico y contraseña.

Este modo facilita su uso a los usuarios que inician sesión con frecuencia desde su lugar de trabajo, pero es menos seguro que la opción siempre activa. A los usuarios solo se les solicita el MFA si cambia su contexto de inicio de sesión.

- Nunca (desactivado)

Mientras estén en este modo, todos los usuarios iniciarán sesión únicamente con su nombre de usuario y contraseña estándar. La elección de esta opción desactiva el MFA de IAM Identity Center y no se recomienda.

Si bien la MFA está deshabilitada en el directorio de usuarios de Identity Center, no puede administrar los dispositivos MFA en sus detalles de usuario y los usuarios del directorio de Identity Center no pueden administrar los dispositivos MFA desde el portal de acceso. AWS

 Note

Si ya utiliza el MFA RADIUS y desea seguir utilizándolo como el tipo de MFA predeterminado, puede dejar el modo de autenticación desactivado para omitir las capacidades de MFA en IAM Identity Center. AWS Directory Service Al cambiar del modo Desactivada al modo En función del contexto o Siempre activo, se anulará la configuración de MFA en RADIUS existente. Para obtener más información, consulte [MFA en RADIUS](#).

6. Elija Save changes (Guardar cambios).

Temas relacionados

- [Elegir tipos de MFA para la autenticación de usuarios](#)
- [Configurar la aplicación de dispositivos MFA](#)

- [Permita a los usuarios registrar sus propios dispositivos MFA](#)

## Elegir tipos de MFA para la autenticación de usuarios

Utilice el siguiente procedimiento para elegir los tipos de dispositivos con los que los usuarios pueden autenticarse cuando se les solicite el MFA en AWS el portal de acceso.

Cómo configurar los tipos de MFA para sus usuarios

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.
5. En la página Configurar la autenticación multifactor, en Los usuarios pueden autenticarse con estos tipos de MFA, elija uno de los siguientes tipos de MFA en función de las necesidades de su empresa. Para obtener más información, consulte [Tipos de MFA disponibles para IAM Identity Center](#).
  - Claves de seguridad y autenticadores integrados
  - Aplicaciones de autenticación
6. Seleccione Save changes (Guardar cambios).

## Configurar la aplicación de dispositivos MFA

Siga el procedimiento que se indica a continuación para determinar si los usuarios deben tener un dispositivo MFA registrado al iniciar sesión en el portal de acceso AWS .

Para obtener información sobre MFA en IAM, consulte [AWS Autenticación multifactor en IAM](#).

Cómo configurar la aplicación de dispositivos de MFA para sus usuarios

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.



5. En la página Configurar la autenticación multifactor, en Si un usuario aún no tiene un dispositivo MFA registrado, elija una de las siguientes opciones en función de las necesidades de su empresa:

- Exija que registren un dispositivo MFA al iniciar sesión

Esta es la configuración predeterminada al configurar MFA por primera vez para IAM Identity Center. Utilice esta opción cuando desee solicitar a los usuarios que aún no tengan un dispositivo MFA registrado que autoinscriban un dispositivo durante el inicio de sesión tras una autenticación con contraseña correcta. Esto le permite proteger los AWS entornos de su organización con MFA sin tener que inscribir y distribuir individualmente los dispositivos de autenticación a sus usuarios. Durante la inscripción automática, sus usuarios pueden registrar cualquier dispositivo de los [Tipos de MFA disponibles para IAM Identity Center](#) disponibles que haya activado anteriormente. Tras completar el registro, los usuarios tienen la opción de asignar un nombre descriptivo a su dispositivo MFA recién inscrito, tras lo cual IAM Identity Center redirige al usuario a su destino original. Si el dispositivo del usuario se pierde o se lo roban, solo tiene que eliminarlo de su cuenta y IAM Identity Center le pedirá que registre automáticamente un dispositivo nuevo la próxima vez que inicie sesión.

- Solicite que proporcionen una contraseña de un solo uso enviada por correo electrónico para iniciar sesión

Use esta opción si desea que los códigos de verificación se envíen a los usuarios por correo electrónico. Como el correo electrónico no está enlazado a un dispositivo específico, esta opción no cumple con los requisitos de autenticación multifactor estándar del sector. Sin embargo, mejora la seguridad en comparación con tener solo una contraseña. La verificación por correo electrónico solo se solicitará si el usuario no ha registrado un dispositivo MFA. Si se ha habilitado el método de autenticación Dependiente del contexto, el usuario tendrá la oportunidad de marcar el dispositivo en el que recibe el correo electrónico como de confianza. Posteriormente, no se les pedirá que verifiquen un código de correo electrónico en futuros inicios de sesión desde esa combinación de dispositivo, navegador y dirección IP.

 Note

Si utiliza Active Directory como fuente de identidad habilitada para IAM Identity Center, la dirección de correo electrónico siempre se basará en el atributo de Active Directory email. Las asignaciones personalizadas de atributos de Active Directory no anularán este comportamiento.

- Bloquear su inicio de sesión

Utilice la opción Bloquear su inicio de sesión cuando desee obligar a todos los usuarios a utilizar MFA antes de que puedan iniciar sesión en AWS.

 Important

Si el método de autenticación está configurado como En función del contexto, el usuario puede seleccionar la casilla Este es un dispositivo de confianza en la página de inicio de sesión. En ese caso, no se le solicitará la MFA a ese usuario aunque tenga habilitada la configuración Bloquear su inicio de sesión. Si desea que se les pregunte a estos usuarios, cambie el método de autenticación a Siempre activo.

- Permitirles iniciar sesión

Utilice esta opción para indicar que los dispositivos MFA no son necesarios para que los usuarios inicien sesión en el portal de AWS acceso. A los usuarios que hayan decidido registrar dispositivos MFA se les seguirá solicitando la MFA.

6. Seleccione Save changes (Guardar cambios).

## Permita a los usuarios registrar sus propios dispositivos MFA

Los administradores de IAM Identity Center pueden permitir que los usuarios registren automáticamente sus propios dispositivos MFA.

Cómo permitir a los usuarios registrar sus propios dispositivos MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En la sección Autenticación multifactor, seleccione Configurar.
5. En la página Configurar la autenticación multifactor, en Quién puede administrar los dispositivos MFA, elija Los usuarios pueden agregar y administrar sus propios dispositivos MFA.
6. Seleccione Save changes (Guardar cambios).

**Note**

Tras configurar el registro automático de los usuarios, es posible que desee enviarles un enlace al procedimiento de [Registro de un dispositivo para MFA](#). En este tema se proporcionan instrucciones sobre cómo configurar sus propios dispositivos de MFA.

## Registre un dispositivo MFA para usuarios

Los administradores de IAM Identity Center pueden configurar un nuevo dispositivo MFA al que pueda acceder un usuario específico en la consola de IAM Identity Center. Deben tener acceso físico al dispositivo de MFA del usuario para poder registrarlo. Por ejemplo, si configura la MFA para un usuario que use un dispositivo de MFA que se ejecute en un smartphone, necesitará acceso físico al teléfono inteligente para completar el proceso de registro. También puede permitir a los usuarios configurar y administrar sus propios dispositivos MFA. Para obtener más información, consulte [Permita a los usuarios registrar sus propios dispositivos MFA](#).

### Cómo registrar un dispositivo MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Usuarios. Elija un usuario de la lista. No seleccione la casilla de verificación situada junto al usuario para este paso.
3. En la página de detalles del usuario, vaya a la pestaña Dispositivos MFA y, a continuación, elija Registrar dispositivo MFA.
4. En la página Registrar dispositivo MFA, seleccione uno de los siguientes tipos de dispositivos MFA y siga las instrucciones:
  - Aplicación de autenticación
    1. En la página Configurar la aplicación de autenticación, IAM Identity Center muestra la información de configuración del nuevo dispositivo de MFA, incluido un gráfico de código QR. El gráfico es una representación de la clave secreta que se puede introducir manualmente en dispositivos que no admiten códigos QR.
    2. Con el dispositivo de MFA físico, haga lo siguiente:
      - a. Abra una aplicación de autenticación MFA compatible. Para obtener una lista de las aplicaciones probadas que puede utilizar con dispositivos de MFA, consulte [Aplicaciones de autenticación virtual](#). Si la aplicación de MFA admite varias cuentas

- (varios dispositivos de MFA), elija la opción para crear una nueva cuenta (un nuevo dispositivo de MFA).
- b. Determine si la aplicación de MFA admite códigos QR y, a continuación, lleve a cabo alguna de las siguientes operaciones de la página Configurar la aplicación de autenticación.
    - i. Elija Mostrar código QR y, a continuación, utilice la aplicación para escanear el código QR. Por ejemplo, puede elegir el icono de la cámara o una opción similar a Escanear código. A continuación, use la cámara del dispositivo para escanear el código.
    - ii. Seleccione Mostrar clave secreta y, a continuación, introduzca esa clave secreta en su aplicación de MFA.

 Important

Cuando configure un dispositivo MFA para que funcione con IAM Identity Center, recomendamos que guarde una copia del código QR o la clave secreta en un lugar seguro. Esto puede ayudar si el usuario asignado pierde el teléfono o tiene que volver a instalar la aplicación de autenticación MFA. Si ocurre alguna de estas cosas, puede volver a configurar rápidamente la aplicación para que utilice la misma configuración de MFA. Así evita tener que crear un nuevo dispositivo MFA en IAM Identity Center para el usuario.

3. En la página Configurar la aplicación de autenticación, en Código de autenticación, escriba la contraseña de uso único que aparece actualmente en el dispositivo MFA físico.

 Important

Envíe su solicitud inmediatamente después de generar el código. Si genera el código y después espera demasiado tiempo a enviar la solicitud, el dispositivo MFA está correctamente asociado al usuario. Sin embargo, el dispositivo MFA no está sincronizado. Esto ocurre porque las contraseñas temporales de un solo uso (TOTP) caducan tras un corto periodo de tiempo. Si esto ocurre, puede volver a sincronizar el dispositivo.

4. Elija Asignar MFA. El dispositivo MFA ahora puede empezar a generar contraseñas de un solo uso y ya está listo para usarse con ellas. AWS

- Clave de seguridad
  1. En la página Registrar la clave de seguridad de su usuario, siga las instrucciones que le dé su navegador o plataforma.

 Note

La experiencia aquí varía en función de los distintos sistemas operativos y navegadores, así que sigue las instrucciones que se muestran en su navegador o plataforma. Una vez que el dispositivo de su usuario se haya registrado correctamente, tendrá la opción de asociar un nombre descriptivo para mostrar al dispositivo recién inscrito del usuario. Si desea cambiarlo, seleccione Cambiar nombre, escriba el nuevo nombre y, a continuación, seleccione Guardar. Si ha activado la opción que permite a los usuarios gestionar sus propios dispositivos, el usuario verá este nombre descriptivo en el portal de acceso AWS .

## Cambiar el nombre y eliminar dispositivos MFA en IAM Identity Center

Los administradores de IAM Identity Center pueden utilizar los siguientes procedimientos para cambiar el nombre o eliminar el dispositivo MFA de un usuario.

### Cómo cambiar el nombre de un dispositivo de MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Usuarios. Elija el usuario en la lista. No seleccione la casilla de verificación situada junto al usuario para este paso.
3. En la página de detalles del usuario, vaya a la pestaña Dispositivos MFA y, a continuación, elija Cambiar nombre.
4. Cuando se le solicite, introduzca el nuevo nombre y, a continuación, seleccione Cambiar nombre.

### Para eliminar un dispositivo MFA

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación izquierdo, elija Usuarios. Elija el usuario en la lista.

3. En la página de detalles del usuario, vaya a la pestaña Dispositivos MFA y, a continuación, elija Eliminar.
4. Elija Eliminar y luego, Eliminar para confirmar la acción.

# Acceso de aplicaciones

Con él AWS IAM Identity Center, puede controlar quién puede tener acceso mediante un inicio de sesión único a sus aplicaciones. Los usuarios obtienen acceso estable a estas aplicaciones en cuanto usan las credenciales de directorio para iniciar sesión.

IAM Identity Center se comunica de forma segura con estas aplicaciones a través de una relación de confianza entre IAM Identity Center y el proveedor de servicios de la aplicación. Esta confianza se puede crear de diferentes maneras, según el tipo de aplicación.

IAM Identity Center admite dos tipos de aplicaciones: aplicaciones administradas y [aplicaciones AWS administradas por el cliente](#). AWS las aplicaciones gestionadas se configuran directamente desde las consolas de aplicaciones correspondientes o a través de la aplicación APIs. Debe agregar las aplicaciones administradas por el cliente a la consola de IAM Identity Center y configurarlas con los metadatos correspondientes tanto para IAM Identity Center como para el proveedor de servicios.

Tras configurar las aplicaciones para que funcionen con IAM Identity Center, puede administrar los usuarios o grupos que acceden a las aplicaciones. De forma predeterminada, no hay ningún usuario asignado a las aplicaciones.

También puede conceder a sus empleados el AWS Management Console acceso a una instancia específica Cuenta de AWS de su organización. Para obtener más información, consulte [Cuenta de AWS acceso](#).

## Temas

- [AWS aplicaciones gestionadas](#)
- [Aplicaciones administradas por el cliente](#)
- [Descripción general de la propagación de identidades de confianza](#)
- [Rotación de certificados de IAM Identity Center](#)
- [Entender las propiedades de la aplicación en la consola de IAM Identity Center](#)
- [Asignar el acceso de los usuarios a las aplicaciones en la consola de IAM Identity Center](#)
- [Eliminar el acceso de los usuarios a las aplicaciones de SAML 2.0](#)
- [Asignación de atributos de su aplicación con atributos de IAM Identity Center](#)

## AWS aplicaciones gestionadas

AWS IAM Identity Center agiliza y simplifica la tarea de conectar a los usuarios de su fuerza laboral con aplicaciones AWS gestionadas, como Amazon Q Developer y Amazon. QuickSight Con IAM Identity Center, puede conectar su proveedor de identidades existente una vez y sincronizar usuarios y grupos de su directorio, o crear y administrar sus usuarios directamente en IAM Identity Center. Al proporcionar un punto de federación, IAM Identity Center elimina la necesidad de configurar la federación o la sincronización de usuarios y grupos para cada aplicación y reduce el esfuerzo administrativo. También obtiene una [visión común de las asignaciones de usuarios y grupos](#).

Para ver una tabla de AWS aplicaciones que funcionan con el Centro de identidades de IAM, consulte. [AWS aplicaciones gestionadas que puede utilizar con el Centro de identidades de IAM](#)

## Controlar el acceso a las aplicaciones AWS gestionadas

El acceso a las aplicaciones AWS gestionadas se controla de dos maneras:

- Entrada inicial a la aplicación

IAM Identity Center administra esto mediante asignaciones a la aplicación. De forma predeterminada, las asignaciones son obligatorias para las aplicaciones AWS administradas. Si es administrador de aplicaciones, puede elegir si desea solicitar asignaciones a una aplicación.

Si las asignaciones son obligatorias, cuando un usuario inicie sesión en Portal de acceso a AWS, solo verá el icono de la aplicación si está asignado a la aplicación directamente o mediante una asignación de grupo.

Si las asignaciones no son obligatorias, puede permitir que todos los usuarios de IAM Identity Center entren en la aplicación. En este caso, la aplicación administra el acceso a los recursos y todos los usuarios que visitan Portal de acceso a AWS.

### Important

Si es administrador del IAM Identity Center, puede utilizar la consola del IAM Identity Center para eliminar las asignaciones a las aplicaciones AWS gestionadas. Antes de eliminar las asignaciones, le recomendamos que colabore con el administrador de la aplicación. También debe colaborar con el administrador de la aplicación si tiene previsto modificar la configuración que determina si las asignaciones son obligatorias o automatizar las asignaciones de la aplicación.



- Acceso a los recursos de la aplicación

La aplicación administra esto mediante asignaciones de recursos independientes que controla.

AWS las aplicaciones gestionadas proporcionan una interfaz de usuario administrativa que puede utilizar para gestionar el acceso a los recursos de la aplicación. Por ejemplo, QuickSight los administradores pueden asignar a los usuarios el acceso a los paneles en función de la pertenencia a un grupo. La mayoría de las aplicaciones AWS administradas también ofrecen una AWS Management Console experiencia que permite asignar usuarios a la aplicación. La experiencia de la consola de estas aplicaciones podría integrar ambas funciones para combinar las capacidades de asignación de usuarios con la capacidad de administrar el acceso a los recursos de la aplicación.

## Compartición de información de identidad

### Consideraciones para compartir información de identidad en Cuentas de AWS

IAM Identity Center admite los atributos más utilizados en todas las aplicaciones. Estos atributos pueden ser el nombre y apellido, el número de teléfono, la dirección de correo electrónico, la dirección y el idioma preferido. Considere detenidamente qué aplicaciones y qué cuentas pueden utilizar esta información de identificación personal.

Puede controlar el acceso a esta información de cualquiera de las siguientes maneras:

- Puede optar por habilitar el acceso solo en la cuenta AWS Organizations de administración o en todas las cuentas de AWS Organizations.
- Como alternativa, puede usar las políticas de control de servicios (SCPs) para controlar qué aplicaciones pueden acceder a la información en qué cuentas se encuentran AWS Organizations.

Por ejemplo, si solo habilita el acceso a la cuenta AWS Organizations de administración, las aplicaciones de las cuentas de los miembros no tendrán acceso a la información. Sin embargo, si habilita el acceso en todas las cuentas, puede impedir SCPs el acceso a todas las aplicaciones, excepto a las que desee permitir.

Las políticas de control de servicios son una característica de AWS Organizations. Para obtener instrucciones sobre cómo conectar una SCP, consulte [Asociar y desasociar políticas de control de servicios](#) en la Guía del usuario de AWS Organizations .

## Configuración de IAM Identity Center para compartir información de las identidades

IAM Identity Center proporciona un almacén de identidades que contiene los atributos de usuario y grupo, sin incluir las credenciales de inicio de sesión. Puede utilizar cualquiera de los siguientes métodos para mantener actualizados a los usuarios y grupos de su almacén de identidades de IAM Identity Center:

- Utilice el almacén de identidades de IAM Identity Center como fuente de identidades principal. Si elige este método, gestiona los usuarios, sus credenciales de inicio de sesión y los grupos desde la consola de IAM Identity Center o AWS Command Line Interface (AWS CLI). Para obtener más información, consulte [Administración de identidades en IAM Identity Center](#).
- Configure el aprovisionamiento (sincronización) de los usuarios y grupos procedentes de cualquiera de las siguientes fuentes de identidad en el almacén de identidades de IAM Identity Center:
  - Active Directory: para más información, consulte [Conexión un directorio Microsoft AD](#).
  - Proveedor de identidades externo: para más información, consulte [Administrar un proveedor de identidades externo](#).

Si elige este método de aprovisionamiento, seguirá administrando sus usuarios y grupos desde su origen de identidad y esos cambios se sincronizarán con el almacén de identidades de IAM Identity Center.

Sea cual sea la fuente de identidad que elija, el Centro de Identidad de IAM puede compartir la información del usuario y del grupo con AWS las aplicaciones gestionadas. De esta forma, puede conectar un origen de identidad a IAM Identity Center una vez y, a continuación, compartir la información de identidad con varias aplicaciones en la Nube de AWS. De este modo, se elimina la necesidad de configurar el aprovisionamiento de identidades y federaciones de forma independiente con cada aplicación. Esta característica de uso compartido también facilita el acceso de los usuarios a muchas aplicaciones en diferentes Cuentas de AWS.

## Restringir el uso de aplicaciones gestionadas AWS

Cuando habilita el Centro de Identidad de IAM por primera vez, estará disponible como fuente de identidad para las aplicaciones AWS gestionadas en todas sus cuentas. AWS Organizations Para restringir las aplicaciones, debe implementar políticas de control de servicios (SCP). SCPs son una función AWS Organizations que puede utilizar para controlar de forma centralizada el número máximo de permisos que pueden tener las identidades (usuarios y roles) de su organización.

Puede utilizarlas SCPs para bloquear el acceso a la información de usuarios y grupos del Centro de Identidad de IAM e impedir que se inicie la aplicación, excepto en las cuentas designadas. Para obtener más información, consulte [las políticas de control de servicios \(SCPs\)](#) en la Guía del AWS Organizations usuario.

El siguiente ejemplo de SCP bloquea el acceso a la información de usuarios y grupos del Centro de Identidad de IAM e impide que se inicie la aplicación, excepto en las cuentas designadas (191111 y 222222222222):

```
{
  "Sid": "DenyIdCExceptInDesignatedAWSAccounts",
  "Effect": "Deny",
  "Action": [
    "identitystore:*",
    "sso:*",
    "sso-directory:*",
    "sso-oauth:*"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalAccount": [
        "111111111111",
        "222222222222"
      ]
    }
  }
}
```

## AWS aplicaciones gestionadas que puede utilizar con el Centro de identidades de IAM

El Centro de identidades de IAM le permite conectar su fuente de identidad existente o crear usuarios una sola vez, lo que permite a los propietarios de las aplicaciones gestionar el acceso a las siguientes aplicaciones AWS gestionadas sin necesidad de federaciones independientes ni de sincronizar usuarios y grupos por separado.

## AWS aplicaciones gestionadas que se integran con el IAM Identity Center

| AWS aplicación gestionada | Integración con <a href="#">instancias de organización de IAM Identity Center</a> | Integración con <a href="#">instancias de cuenta de IAM Identity Center</a> | Permite una <a href="#">propagación de identidad confiable</a> a través de IAM Identity Center |
|---------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Amazon AppStream 2.0      | Sí                                                                                | No                                                                          | No                                                                                             |
| Amazon Athena SQL         | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| Amazon CodeCatalyst       | Sí                                                                                | Sí                                                                          | No                                                                                             |
| Amazon Connect            | Sí                                                                                | No                                                                          | No                                                                                             |
| Amazon DataZone           | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| Amazon EMR en Amazon EC2  | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| Amazon EMR Studio         | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| Amazon Kendra             | Sí                                                                                | No                                                                          | No                                                                                             |
| Amazon Managed Grafana    | Sí                                                                                | No                                                                          | No                                                                                             |
| Amazon Monitron           | Sí                                                                                | No                                                                          | No                                                                                             |

| AWS aplicación gestionada                                   | Integración con <a href="#">instancias de organización de IAM Identity Center</a> | Integración con <a href="#">instancias de cuenta de IAM Identity Center</a> | Permite una <a href="#">propagación de identidad confiable</a> a través de IAM Identity Center |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| OpenSearch Servicio Amazon                                  | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| OpenSearch Servicio Amazon Serverless Service               | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| OpenSearch user interface (Dashboards)                      | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| Amazon Q Business                                           | Sí                                                                                | Sí                                                                          | No                                                                                             |
| Amazon Q Developer                                          | Sí                                                                                | Sí*                                                                         | No                                                                                             |
| Investigaciones operativas para desarrolladores de Amazon Q | Sí                                                                                | No                                                                          | No                                                                                             |
| Amazon QuickSight                                           | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| Amazon Redshift                                             | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| Amazon S3 Access Grants                                     | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| Amazon SageMaker AI Studio                                  | Sí                                                                                | No                                                                          | No                                                                                             |
| Amazon WorkMail                                             | Sí                                                                                | Sí                                                                          | Sí                                                                                             |

| AWS aplicación gestionada        | Integración con <a href="#">instancias de organización de IAM Identity Center</a> | Integración con <a href="#">instancias de cuenta de IAM Identity Center</a> | Permite una <a href="#">propagación de identidad confiable</a> a través de IAM Identity Center |
|----------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| Amazon WorkSpaces                | Sí                                                                                | Sí                                                                          | No                                                                                             |
| Amazon WorkSpaces Secure Browser | Sí                                                                                | No                                                                          | No                                                                                             |
| AWS App Studio                   | Sí                                                                                | Sí                                                                          | No                                                                                             |
| AWS Client VPN                   | Sí                                                                                | No                                                                          | No                                                                                             |
| AWS CLI                          | Sí                                                                                | No                                                                          | No                                                                                             |
| AWS Deadline Cloud               | Sí                                                                                | Sí                                                                          | No                                                                                             |
| AWS IoT Events                   | Sí                                                                                | No                                                                          | No                                                                                             |
| AWS IoT Fleet Hub                | Sí                                                                                | No                                                                          | No                                                                                             |
| AWS IoT SiteWise                 | Sí                                                                                | No                                                                          | No                                                                                             |
| AWS Lake Formation               | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| AWS re:Post Private              | Sí                                                                                | Sí                                                                          | No                                                                                             |

| AWS aplicación gestionada            | Integración con <a href="#">instancias de organización de IAM Identity Center</a> | Integración con <a href="#">instancias de cuenta de IAM Identity Center</a> | Permite una <a href="#">propagación de identidad confiable</a> a través de IAM Identity Center |
|--------------------------------------|-----------------------------------------------------------------------------------|-----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|
| AWS Supply Chain                     | Sí                                                                                | Sí                                                                          | No                                                                                             |
| AWS Systems Manager                  | Sí                                                                                | No                                                                          | No                                                                                             |
| AWS Transfer Family aplicaciones web | Sí                                                                                | Sí                                                                          | Sí                                                                                             |
| AWS Transformación                   | Sí                                                                                | Sí                                                                          | No                                                                                             |
| Acceso verificado de AWS             | Sí                                                                                | No                                                                          | No                                                                                             |
| Aprobación multipartita              | Sí                                                                                | No                                                                          | Sí                                                                                             |

\* Para Amazon Q Developer, se admiten las instancias de cuenta del IAM Identity Center, a menos que los usuarios necesiten acceder al conjunto completo de funciones de Amazon Q Developer en los AWS sitios web. Para obtener más información, consulte [Configuración de Amazon Q Developer](#) en la Guía del usuario de Amazon Q Developer.

## Inicio rápido: configuración del centro de identidad de IAM para probar las aplicaciones gestionadas AWS

Si su administrador aún no le ha dado acceso al Centro de identidad de IAM, puede seguir los pasos de este tema para configurar el Centro de identidades de IAM para probar AWS las aplicaciones gestionadas. Aprenderá a activar el Centro de identidad de IAM, a crear un usuario directamente en el Centro de identidades de IAM y a asignar ese usuario a una aplicación gestionada. AWS

En este tema se proporcionan pasos de inicio rápido sobre cómo habilitar el Centro de Identidad de IAM de cualquiera de las siguientes maneras:

- Con AWS Organizations: si elige esta opción, se crea una instancia de organización del Centro de identidades de IAM.
- Solo en su entorno específico Cuenta de AWS: si elige esta opción, se crea una instancia de cuenta del IAM Identity Center.

Para obtener información sobre estos tipos de instancias, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Requisitos previos

Antes de activar el Centro de identidades de IAM, confirme lo siguiente:

- Tiene una Cuenta de AWS: si no la tiene, consulte [Cómo empezar con una Cuenta de AWS](#) en la Guía de referencia sobre la gestión de AWS cuentas.
- La aplicación AWS gestionada funciona con el Centro de identidades de IAM: consulte la lista [AWS aplicaciones gestionadas que puede utilizar con el Centro de identidades de IAM](#) para confirmar que la aplicación AWS gestionada que desea probar funciona con el Centro de identidades de IAM.
- Ha revisado las consideraciones regionales: asegúrese de que la aplicación AWS gestionada que desea probar es compatible con el Región de AWS lugar donde habilita el Centro de Identidad de IAM. Para obtener más información, consulte la documentación de la aplicación AWS gestionada.

### Note

Debe implementar la aplicación AWS gestionada en la misma región en la que planea habilitar el IAM Identity Center.



## Configuración de una instancia organizativa del IAM Identity Center para probar las aplicaciones gestionadas AWS

### Note

En este tema se describe cómo habilitar el Centro de Identidad de IAM AWS Organizations, que es la forma recomendada de habilitar el Centro de Identidad de IAM.

### Confirme sus permisos

Para habilitar el IAM Identity Center AWS Organizations, debe iniciar sesión en la consola AWS de administración de una de las siguientes maneras:

- Un usuario con permisos administrativos en el Cuenta de AWS lugar donde se habilitará el Centro de Identidad de IAM. AWS Organizations
- El usuario raíz (no se recomienda a menos que no existan otros usuarios administrativos).

### Important

El usuario raíz tiene acceso a todos los AWS servicios y recursos de la cuenta. Como práctica recomendada de seguridad, a menos que no tengas otras credenciales, no utilices las credenciales raíz de tu cuenta para acceder a AWS los recursos. Estas credenciales proporcionan acceso ilimitado a la cuenta y son difíciles de revocar.

### Paso 1. Habilite IAM Identity Center con AWS Organizations

1. Realice una de las siguientes acciones para iniciar sesión en. AWS Management Console
  - Nuevo para AWS (usuario root): inicia sesión como propietario de la cuenta; para ello, selecciona Usuario root e introduce tu dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
  - Si ya lo AWS utilizas de forma independiente Cuenta de AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
2. En la página de inicio de la consola de AWS administración, seleccione el servicio IAM Identity Center o vaya a la consola de [IAM](#) Identity Center.

3. Seleccione Activar y active IAM Identity Center con. AWS Organizations Al hacerlo, está creando una [instancia organizativa](#) del IAM Identity Center.

## Paso 2. Cree un usuario administrativo en el Centro de identidades de IAM

En este procedimiento se describe cómo crear un usuario directamente en el directorio integrado del Centro de identidades. Este directorio no está conectado a ningún otro directorio que su administrador pueda usar para administrar los usuarios de la fuerza laboral. Tras crear el usuario en el Centro de identidades de IAM, especificará las nuevas credenciales para este usuario. Cuando inicie sesión como este usuario para probar su aplicación AWS gestionada, iniciará sesión con las nuevas credenciales, no con las credenciales existentes que utilice para acceder a los recursos corporativos.

### Note

Le recomendamos que utilice este método para crear usuarios únicamente con fines de prueba.

1. En el panel de navegación de la consola de IAM Identity Center, elija Usuarios y, a continuación, elija Agregar usuario.
2. Siga las instrucciones de la consola para añadir el usuario. Mantenga seleccionada la opción Enviar un correo electrónico a este usuario con las instrucciones de configuración de la contraseña y asegúrese de especificar una dirección de correo electrónico a la que tenga acceso.
3. En el panel de navegación, elija Cuentas de AWS, active la casilla de verificación situada junto a su cuenta y elija Asignar usuarios o grupos.
4. Seleccione la pestaña Usuarios, active la casilla de verificación situada junto al usuario que acaba de agregar y elija Siguiente.
5. Seleccione Crear conjunto de permisos y siga las instrucciones de la consola para crear el conjunto de permisos AdministratorAccess predefinido.
6. Cuando haya terminado, el nuevo conjunto de permisos aparecerá en la lista. Cierre la pestaña Conjuntos de permisos en la ventana del navegador, vuelva a la pestaña Asignar usuarios y grupos y elija el icono de actualización situado junto a Crear conjunto de permisos.

7. En la pestaña del navegador Asignar usuarios y grupos, el nuevo conjunto de permisos aparece en la lista. Active la casilla de verificación situada junto al nombre del conjunto de permisos, elija Siguiente y, a continuación, elija Enviar.
8. Cierre la sesión de la consola de .

### Paso 3. Inicie sesión en el portal de AWS acceso como usuario administrativo

El portal de AWS acceso es un portal web que proporciona al usuario que ha creado acceso a la consola AWS de administración. Antes de iniciar sesión en el portal de AWS acceso, debe aceptar la invitación para unirse al Centro de identidades de IAM y activar sus credenciales de usuario.

1. Compruebe en su correo electrónico el asunto Invitación a unirse al Centro de Identidad de AWS IAM.
2. Selecciona Aceptar invitación y sigue las instrucciones de la página de registro para establecer una nueva contraseña, iniciar sesión y registrar un dispositivo de MFA para tu usuario.
3. Después de registrar su dispositivo MFA, se abre el portal de AWS acceso.
4. En el portal de AWS acceso, seleccione el suyo Cuenta de AWS y elija AdministratorAccess. Se le redirigirá a la consola AWS de administración.

### Paso 4. Configure la aplicación AWS gestionada para que utilice IAM Identity Center

1. Con la sesión iniciada en la consola AWS de administración, abra la consola de la aplicación AWS gestionada que vaya a utilizar.
2. Siga las instrucciones de la consola para configurar la aplicación AWS gestionada para que utilice el IAM Identity Center. Durante este proceso, puede asignar el usuario que creó a la aplicación.

## Configuración de una instancia de cuenta del IAM Identity Center para probar las aplicaciones AWS gestionadas

#### Note

Una instancia de cuenta de IAM Identity Center limita la implementación a una sola Cuenta de AWS. Debe habilitar esta instancia en el mismo lugar Región de AWS que en la AWS aplicación que desee probar.

## Confirma tu aplicación

Todas las aplicaciones AWS gestionadas que funcionan con el IAM Identity Center se pueden utilizar con las instancias organizativas del IAM Identity Center. Sin embargo, solo algunas de estas aplicaciones se pueden usar con instancias de cuentas del IAM Identity Center. Revise la lista de.

[AWS aplicaciones gestionadas que puede utilizar con el Centro de identidades de IAM](#)

### Paso 1. Habilite una instancia de cuenta de IAM Identity Center

1. Realice una de las siguientes acciones para iniciar sesión en AWS Management Console
  - Nuevo para AWS (usuario root): inicia sesión como propietario de la cuenta; para ello, selecciona Usuario root e introduce tu dirección de Cuenta de AWS correo electrónico. En la siguiente página, escriba su contraseña.
  - Si ya lo AWS utilizas de forma independiente Cuenta de AWS (credenciales de IAM): inicia sesión con tus credenciales de IAM con permisos administrativos.
2. En la página de inicio de la consola de AWS administración, seleccione el servicio IAM Identity Center o vaya a la consola de [IAM](#) Identity Center.
3. Seleccione Habilitar.
4. En la AWS Organizations página Habilitar el centro de identidad de IAM con, seleccione habilitar una instancia de cuenta del Centro de identidades de IAM.
5. En la página Habilitar la instancia de cuenta del Centro de Identidad de IAM, revise la información y, si lo desea, añada las etiquetas que desee asociar a esta instancia de cuenta. A continuación, elija Enable.

### Paso 2. Cree un usuario en el Centro de identidades de IAM

En este procedimiento se describe cómo crear un usuario directamente en el directorio integrado del Centro de identidades. Este directorio no está conectado a ningún otro directorio que su administrador pueda usar para administrar los usuarios de la fuerza laboral. Tras crear el usuario en el Centro de identidades de IAM, especificará las nuevas credenciales para este usuario. Cuando inicie sesión como este usuario para probar su aplicación AWS gestionada, iniciará sesión con las nuevas credenciales. Las nuevas credenciales no le permitirán acceder a otros recursos corporativos.

 Note

Le recomendamos que utilice este método para crear usuarios únicamente con fines de prueba.

1. En el panel de navegación de la consola de IAM Identity Center, elija Usuarios y, a continuación, elija Agregar usuario.
2. Siga las instrucciones de la consola para añadir el usuario. Mantenga seleccionada la opción Enviar un correo electrónico a este usuario con las instrucciones de configuración de la contraseña y asegúrese de especificar una dirección de correo electrónico a la que tenga acceso.
3. Cierre la sesión de la consola de .

### Paso 3. Inicie sesión en el portal de AWS acceso como usuario del IAM Identity Center

El portal de AWS acceso es un portal web que proporciona al usuario que ha creado acceso a la consola AWS de administración. Antes de iniciar sesión en el portal de AWS acceso, debe aceptar la invitación para unirse al Centro de identidades de IAM y activar sus credenciales de usuario.

1. Compruebe en su correo electrónico el asunto Invitación a unirse al Centro de Identidad de AWS IAM.
2. Selecciona Aceptar invitación y sigue las instrucciones de la página de registro para establecer una nueva contraseña, iniciar sesión y registrar un dispositivo de MFA para tu usuario.
3. Después de registrar su dispositivo MFA, se abre el portal de AWS acceso. Cuando haya solicitudes disponibles, las encontrará en la pestaña Aplicaciones.

 Note

AWS las aplicaciones que admiten instancias de cuentas permiten a los usuarios iniciar sesión en las aplicaciones sin necesidad de permisos adicionales. Por lo tanto, la pestaña Cuentas permanecerá vacía.

## Paso 4. Configure la aplicación AWS gestionada para que utilice IAM Identity Center

1. Con la sesión iniciada en la consola AWS de administración, abra la consola de la aplicación AWS gestionada que vaya a utilizar.
2. Siga las instrucciones de la consola para configurar la aplicación AWS gestionada para que utilice el IAM Identity Center. Durante este proceso, puede asignar el usuario que creó a la aplicación.

## Ver y cambiar los detalles de una aplicación AWS gestionada

Tras conectar una aplicación AWS gestionada al IAM Identity Center mediante la consola o APIs para la aplicación, la aplicación se registra en el IAM Identity Center. Una vez registrada una aplicación en IAM Identity Center, puede ver y cambiar detalles sobre la aplicación en la consola de IAM Identity Center.

La información sobre la aplicación incluye si son obligatorias las asignaciones de usuarios y grupos y, si corresponde, los usuarios y grupos asignados y las aplicaciones de confianza para la propagación de identidades. Para obtener más información acerca de la propagación de identidades de confianza, consulte [Descripción general de la propagación de identidades de confianza](#).

Para ver y cambiar la información sobre una aplicación AWS gestionada en la consola del IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada de AWS .
4. Elija el enlace de la aplicación administrada que desee abrir y ver.
5. Si desea cambiar la información sobre una aplicación AWS gestionada, seleccione Acción y, a continuación, seleccione Editar detalles.
6. Puede cambiar el nombre mostrado y la descripción de la aplicación, así como el método de asignación de usuarios y grupos.
  - a. Para cambiar el nombre para mostrar, introduzca el nombre deseado en el campo Nombre para mostrar y seleccione Guardar cambios.
  - b. Para cambiar la descripción, introduzca la descripción deseada en el campo Descripción y seleccione Guardar cambios.

- c. Para cambiar el método de asignación de usuarios y grupos, realice el cambio deseado y seleccione Guardar cambios. Para obtener más información, consulte [the section called “Usuarios, grupos y aprovisionamiento”](#).

## Deshabilitar una aplicación AWS gestionada

Para evitar que los usuarios se autenticuen en una aplicación AWS gestionada, puede inhabilitar la aplicación en la consola del IAM Identity Center.

Para deshabilitar una aplicación gestionada AWS

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la página Aplicaciones, en Aplicaciones administradas por AWS , seleccione la aplicación que desee deshabilitar.
4. Con la aplicación seleccionada, seleccione Acciones y, a continuación, seleccione Deshabilitar.
5. En el cuadro de diálogo Desactivar aplicación, seleccione Desactivar.
6. En la lista Aplicaciones administradas por AWS , el estado de la aplicación aparece como Inactiva.

### Note

Si una aplicación AWS gestionada está deshabilitada, puede restaurar la capacidad de los usuarios de autenticarse en la aplicación seleccionando Acciones y, a continuación, Activar.

## Habilitar sesiones de consola con identidad mejorada

Una sesión de consola con identidad mejorada mejora la sesión de AWS consola del usuario al proporcionar un contexto de usuario adicional para personalizar la experiencia de ese usuario. Actualmente, esta capacidad es compatible con los usuarios de Amazon Q Developer Pro de [Amazon Q en aplicaciones y sitios web de AWS](#).

Puede habilitar sesiones de consola con identidad mejorada sin realizar ningún cambio en los patrones de acceso existentes ni en la federación en la consola. AWS Si sus usuarios inician sesión

en la AWS consola con IAM (por ejemplo, si inician sesión como usuarios de IAM o mediante un acceso federado con IAM), pueden seguir utilizando estos métodos. Si sus usuarios inician sesión en el portal de AWS acceso, pueden seguir utilizando sus credenciales de usuario del IAM Identity Center.

## Temas

- [Requisitos y consideraciones previos](#)
- [¿Cómo habilitar las sesiones identity-enhanced-console](#)
- [Cómo funcionan las sesiones de consola con identidad mejorada](#)

## Requisitos y consideraciones previos

Antes de habilitar las sesiones de consola con identidad mejorada, revise los siguientes requisitos previos y consideraciones:

- Si sus usuarios acceden a Amazon Q en AWS aplicaciones y sitios web a través de una suscripción a Amazon Q Developer Pro, debe habilitar las sesiones de consola con identidad mejorada.

### Note

Los usuarios de Amazon Q Developer pueden acceder a Amazon Q sin sesiones con identidad mejorada, pero no tendrán acceso a sus suscripciones a Amazon Q Developer Pro.

- Las sesiones de consola con identidad mejorada requieren una [instancia organizativa](#) del IAM Identity Center.
- La integración con Amazon Q no se admite si habilita IAM Identity Center en una Región de AWS opcional.
- Para habilitar las sesiones de consola con identidad mejorada, debe tener los siguientes permisos:
  - `sso:CreateApplication`
  - `sso:GetSharedSsoConfiguration`
  - `sso:ListApplications`
  - `sso:PutApplicationAssignmentConfiguration`
  - `sso:PutApplicationAuthenticationMethod`



- `sso:PutApplicationGrant`
- `sso:PutApplicationAccessScope`
- `signin:CreateTrustedIdentityPropagationApplicationForConsole`
- `signin:ListTrustedIdentityPropagationApplicationsForConsole`
- Para permitir que sus usuarios utilicen sesiones de consola con identidad mejorada, debe concederles el `sts:setContext` permiso en virtud de una política basada en la identidad. Para obtener más información, consulte [Conceder a los usuarios permisos para usar](#) sesiones de consola con identidad mejorada.

## ¿Cómo habilitar las sesiones identity-enhanced-console

Puede habilitar sesiones de consola con identidad mejorada en la consola de Amazon Q o en la consola de IAM Identity Center.

Habilite sesiones de consola con identidad mejorada en la consola Amazon Q

Antes de habilitar las sesiones de consola con identidad mejorada, debe tener una instancia organizativa del IAM Identity Center con una fuente de identidad conectada. Si ya ha configurado IAM Identity Center, vaya al paso 3.

1. Abra la consola del IAM Identity Center. Seleccione Activar y cree una instancia de organización de IAM Identity Center. Para obtener información, consulte [Activar IAM Identity Center](#).
2. Conecte su fuente de identidad a IAM Identity Center y aprovisiona usuarios a IAM Identity Center. Puede conectar su fuente de identidad actual a IAM Identity Center o utilizar el directorio del Identity Center si aún no utiliza otra fuente de identidad. Para obtener más información, consulte [Tutoriales de fuentes de identidad de IAM Identity Center](#).
3. Cuando termine de configurar IAM Identity Center, abra la consola de Amazon Q y siga los pasos de [Suscripciones](#) de la Guía de usuario de Amazon Q Developer. Asegúrese de habilitar las sesiones de consola con identidad mejorada.

### Note

Si no tiene los permisos suficientes para habilitar las sesiones de consola con identidad mejorada, puede que tenga que pedirle a un administrador del Centro de Identidad de IAM que realice esta tarea por usted en la consola del Centro de Identidad de IAM. Para obtener más información, consulte el siguiente procedimiento.

## Habilite las sesiones de consola con identidad mejorada en la consola de IAM Identity Center

Si es administrador del IAM Identity Center, es posible que otro administrador le pida que habilite las sesiones de consola con identidad mejorada en la consola del IAM Identity Center.

1. Abra la consola de IAM Identity Center.
2. En el panel de navegación, seleccione Configuración.
3. En Habilitar sesiones con identidad mejorada, seleccione Habilitar.
4. En el segundo mensaje, seleccione Activar.
5. Cuando termine de habilitar las sesiones de consola con identidad mejorada, aparecerá un mensaje de confirmación en la parte superior de la página de configuración.
6. En la sección Detalles, el estado de las sesiones con identidad mejorada es Habilitado.

## Cómo funcionan las sesiones de consola con identidad mejorada

IAM Identity Center mejora la sesión de consola actual del usuario para incluir el ID de usuario activo de IAM Identity Center y el ID de sesión de IAM Identity Center.

Las sesiones de consola con identidad mejorada incluyen los tres valores siguientes:

- ID de usuario del almacén de identidades ([almacén de identidades: UserId](#)): este valor se utiliza para identificar de forma exclusiva a un usuario en la fuente de identidad que está conectada a IAM Identity Center.
- Directorio de almacenes de identidades ARN ([almacén de identidades: IdentityStoreArn](#)): este valor es el ARN del almacén de identidades que está conectado a IAM Identity Center y en el que puede buscar los atributos para `identitystore:UserId`.
- ID de sesión del IAM Identity Center: este valor indica si la sesión del usuario en IAM Identity Center sigue siendo válida.

Los valores son los mismos, pero se obtienen de formas distintas y se añaden en distintos puntos del proceso, en función de cómo inicie sesión el usuario:

- Centro de identidad de IAM (portal de AWS acceso): en este caso, los valores de ID de usuario y ARN del almacén de identidades del usuario ya se proporcionan en la sesión activa del Centro de identidades de IAM. IAM Identity Center mejora la sesión actual al añadir únicamente el ID de sesión.

- Otros métodos de inicio de sesión: si el usuario inicia sesión en AWS como usuario de IAM, con un rol de IAM o como usuario federado con IAM, no se proporciona ninguno de estos valores. IAM Identity Center mejora la sesión actual al añadir el ID de usuario del almacén de identidades, el ARN del directorio del almacén de identidades y el ID de sesión.

## Aplicaciones administradas por el cliente

IAM Identity Center actúa como un servicio de identidades central para los usuarios y grupos de su fuerza laboral. Si ya utiliza un proveedor de identidades (IdP), IAM Identity Center puede integrarse con su IdP para que pueda aprovisionar sus usuarios y grupos en IAM Identity Center y utilizar su IdP para la autenticación. Con una sola conexión, IAM Identity Center representa su IdP frente a Servicios de AWS varios y permite que OAuth sus aplicaciones 2.0 soliciten acceso a los datos de estos servicios en nombre de sus usuarios. También puede utilizar IAM Identity Center para asignar a sus usuarios el acceso a las aplicaciones de [SAML 2.0](#).

- Si su aplicación es compatible con los JSON Web Tokens (JWTs), puede utilizar la fiable función de propagación de identidades del Centro de Identidad de IAM para permitir que la aplicación solicite acceso a los datos Servicios de AWS en nombre de sus usuarios. La propagación fiable de la identidad se basa en el marco de autorización OAuth 2.0 e incluye una opción para que las aplicaciones intercambien los identificadores de identidad procedentes de un servidor de autorización OAuth 2.0 externo por símbolos emitidos por el IAM Identity Center y reconocidos por. Servicios de AWS Para obtener más información, consulte [Casos de uso de propagación de identidades de confianza](#).
- Si su aplicación es compatible con SAML 2.0, puede conectarla a una instancia [organizativa de IAM Identity Center](#). Puede utilizar IAM Identity Center para asignar acceso a su aplicación SAML 2.0.

### Temas

- [Acceso mediante inicio de sesión único a las aplicaciones SAML 2.0 y 2.0 OAuth](#)
- [Configuración de aplicaciones de SAML 2.0 administradas por el cliente](#)

# Acceso mediante inicio de sesión único a las aplicaciones SAML 2.0 y 2.0 OAuth

El Centro de identidades de IAM le permite ofrecer a sus usuarios un acceso de inicio de sesión único a las aplicaciones SAML 2.0 o 2.0. OAuth Los siguientes temas proporcionan una descripción general de alto nivel de SAML 2.0 y 2.0. OAuth

## Temas

- [SAML 2.0](#)
- [OAuth 2.0](#)

## SAML 2.0

SAML 2.0 es un estándar del sector utilizado para intercambiar de forma segura aserciones de SAML que transmiten información sobre un usuario entre una autoridad de SAML (denominada proveedor de identidades o IdP) y un consumidor de SAML 2.0 (denominado proveedor de servicios o SP). El Centro de Identidad de IAM utiliza esta información para proporcionar un acceso de inicio de sesión único federado a los usuarios que están autorizados a utilizar las aplicaciones del portal de acceso. AWS

## OAuth 2.0

OAuth 2.0 es un protocolo que permite a las aplicaciones acceder a los datos de los usuarios y compartirlos de forma segura sin compartir contraseñas. Esta capacidad proporciona a los usuarios una forma segura y estandarizada de permitir que las aplicaciones accedan a sus recursos. El acceso se ve facilitado por diferentes flujos de subvenciones OAuth 2.0.

El IAM Identity Center permite a las aplicaciones que se ejecutan en clientes públicos recuperar credenciales temporales de acceso Cuentas de AWS y servicios mediante programación en nombre de sus usuarios. Los clientes públicos suelen ser computadoras de escritorio, portátiles u otros dispositivos móviles que se utilizan para ejecutar aplicaciones de forma local. Entre los ejemplos de AWS aplicaciones que se ejecutan en clientes públicos se incluyen los kits de desarrollo de AWS software AWS Command Line Interface (AWS CLI) y (). AWS Toolkit SDKs Para permitir que estas aplicaciones obtengan credenciales, IAM Identity Center admite partes de los siguientes flujos OAuth 2.0:

- Concesión de códigos de autorización con clave de prueba para el intercambio de códigos (PKCE) ([RFC 6749](#) y [RFC 7636](#))

- Concesión de autorización de dispositivo ([RFC 8628](#))

 Note

Estos tipos de subvenciones solo se pueden utilizar si Servicios de AWS admiten esta capacidad. Es posible que estos servicios no admitan este tipo de concesión en todas Regiones de AWS. Consulte la documentación relevante Servicios de AWS para conocer las diferencias regionales.

OpenID Connect (OIDC) es un protocolo de autenticación que se basa en el marco 2.0. OAuth El OIDC especifica cómo utilizar la versión 2.0 para la autenticación. OAuth A través del [servicio OIDC del IAM Identity Center APIs](#), una aplicación registra un cliente OAuth 2.0 y utiliza uno de estos flujos para obtener un token de acceso que permite proteger el IAM Identity Center. APIs Una aplicación especifica los [ámbitos de acceso](#) para declarar el usuario de API al que va dirigido. Una vez que usted, como administrador de IAM Identity Center, haya configurado su fuente de identidad, los usuarios finales de la aplicación deberán completar un proceso de inicio de sesión, si aún no lo han hecho. A continuación, los usuarios finales deben dar su consentimiento para permitir que la aplicación realice llamadas a la API. Estas llamadas a la API se realizan con los permisos de los usuarios. En respuesta, IAM Identity Center devuelve un token de acceso a la aplicación que contiene los ámbitos de acceso a los que los usuarios dieron su consentimiento.

### Uso de un flujo de concesión 2.0 OAuth

OAuth Los flujos de subvenciones 2.0 solo están disponibles a través de aplicaciones AWS gestionadas que admiten los flujos. Para utilizar un flujo OAuth 2.0, su instancia de IAM Identity Center y cualquier aplicación AWS gestionada compatible que utilice deben desplegarse en una sola Región de AWS instancia. Consulte la documentación de cada una de ellas Servicio de AWS para determinar la disponibilidad regional de las aplicaciones AWS gestionadas y la instancia del IAM Identity Center que desea utilizar.

Para utilizar una aplicación que utilice un flujo OAuth 2.0, el usuario final debe introducir la URL a la que se conectará la aplicación y registrarse en su instancia de IAM Identity Center. En función de la aplicación, como administrador, debe proporcionar a sus usuarios la URL del portal de acceso AWS o la URL del emisor de su instancia de IAM Identity Center. Puede encontrar estos dos ajustes en la página de Configuración de la [consola de IAM Identity Center](#). Para obtener información adicional sobre la configuración de una aplicación cliente, consulte la documentación de esa aplicación.

La experiencia del usuario final a la hora de iniciar sesión en una aplicación y dar su consentimiento depende de si la aplicación utiliza [Concesión de código de autorización con PKCE](#) o [Concesión de autorización de dispositivo](#).

### Concesión de código de autorización con PKCE

Este flujo lo utilizan las aplicaciones que se ejecutan en un dispositivo que tiene un navegador.

1. Se abre una ventana del navegador.
2. Si el usuario no se ha autenticado, el navegador lo redirige para completar la autenticación del usuario.
3. Tras la autenticación, se presenta al usuario una pantalla de consentimiento que muestra la siguiente información:
  - El nombre de la aplicación
  - Los ámbitos de acceso para los que la aplicación solicita el consentimiento
4. El usuario puede cancelar el proceso de consentimiento o puede dar su consentimiento y la aplicación procederá al acceso en función de los permisos del usuario.

### Concesión de autorización de dispositivo

Las aplicaciones que se ejecutan en un dispositivo con o sin navegador pueden utilizar este flujo. Cuando la aplicación inicia el flujo, presenta una URL y un código de usuario que el usuario debe verificar más adelante en el flujo. El código de usuario es necesario porque la aplicación que inicia el flujo puede estar ejecutándose en un dispositivo diferente al dispositivo en el que el usuario da su consentimiento. El código garantiza que el usuario dé su consentimiento al flujo que inició en el otro dispositivo.

#### Note

Si tiene clientes que la utilizan `device.sso.region.amazonaws.com`, debe actualizar su flujo de autorización para usar Proof Key for Code Exchange (PKCE). Para obtener más información, consulte [Configuración de la autenticación del IAM Identity Center AWS CLI en la Guía del AWS Command Line Interface usuario](#).

1. Cuando el flujo se inicia desde un dispositivo con un navegador, se abre una ventana del navegador. Cuando el flujo se inicia desde un dispositivo sin navegador, el usuario debe abrir un navegador en un dispositivo diferente e ir a la URL que presentó la aplicación.
2. En cualquier caso, si el usuario no se ha autenticado, el navegador lo redirige para completar la autenticación del usuario.
3. Tras la autenticación, se presenta al usuario una pantalla de consentimiento que muestra la siguiente información:
  - El nombre de la aplicación
  - Los ámbitos de acceso para los que la aplicación solicita el consentimiento
  - El código de usuario que la aplicación presentó al usuario
4. El usuario puede cancelar el proceso de consentimiento o puede dar su consentimiento y la aplicación procederá al acceso en función de los permisos del usuario.

## Ámbitos de acceso

Un ámbito define el acceso a un servicio al que se puede acceder a través de un flujo OAuth 2.0. Los ámbitos permiten al servicio, también denominado servidor de recursos, agrupar los permisos relacionados con las acciones y los recursos del servicio, y especifican las operaciones más generales que OAuth pueden solicitar los clientes de la versión 2.0. Cuando un cliente OAuth 2.0 se registra en el [servicio OIDC del IAM Identity Center](#), el cliente especifica los ámbitos para declarar las acciones que pretende realizar, para lo cual el usuario debe dar su consentimiento.

OAuth Los clientes 2.0 utilizan scope los valores definidos en la [sección 3.3 de la OAuth versión 2.0 \(RFC 6749\)](#) para especificar qué permisos se solicitan para un token de acceso. Los clientes pueden especificar un máximo de 25 ámbitos al solicitar un token de acceso. Cuando un usuario da su consentimiento durante una concesión de código de autorización con el PKCE o el flujo de concesión de autorización de un dispositivo, IAM Identity Center codifica los ámbitos en el token de acceso que devuelve.

AWS añade ámbitos al Centro de Identidad de IAM para que sean compatibles. Servicios de AWS En la siguiente tabla, se enumeran los ámbitos que admite el servicio OIDC de IAM Identity Center al registrar un cliente público.

## Ámbitos de acceso compatibles con el servicio OIDC de IAM Identity Center al registrar a un cliente público

| Alcance                                          | Descripción                                                                                                      | Servicios admitidos por                                |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| <code>sso:account:access</code>                  | Acceda a las cuentas administradas y a los conjuntos de permisos de IAM Identity Center.                         | IAM Identity Center                                    |
| <code>codewhisperer:analysis</code>              | Habilite el acceso al análisis de código de Amazon Q Developer.                                                  | ID de creador de AWS y el Centro de identidades de IAM |
| <code>codewhisperer:completions</code>           | Habilite el acceso a las sugerencias de código en línea de Amazon Q.                                             | ID de creador de AWS y el Centro de Identidad de IAM   |
| <code>codewhisperer:conversations</code>         | Habilite el acceso al chat de Amazon Q.                                                                          | ID de creador de AWS y el Centro de Identidad de IAM   |
| <code>codewhisperer:taskassist</code>            | Habilite el acceso al agente de Amazon Q Developer para el desarrollo de software.                               | ID de creador de AWS y el Centro de Identidad de IAM   |
| <code>codewhisperer:transformations</code>       | Habilite el acceso al agente de Amazon Q Developer para la transformación de código.                             | ID de creador de AWS y el Centro de Identidad de IAM   |
| <code>codecatalyst:read_write</code>             | Lee y escribe en tus CodeCatalyst recursos de Amazon, lo que te permite acceder a todos tus recursos existentes. | ID de creador de AWS y el Centro de Identidad de IAM   |
| <code>verified_access:application:connect</code> | Habilitar Acceso verificado de AWS                                                                               | Acceso verificado de AWS                               |



| Alcance                                      | Descripción                                                                | Servicios admitidos por |
|----------------------------------------------|----------------------------------------------------------------------------|-------------------------|
| <code>redshift:connect</code>                | Connect a Amazon Redshift                                                  | Amazon Redshift         |
| <code>datazone:domain:access</code>          | Acceda a su función DataZone de ejecución de dominios                      | Amazon DataZone         |
| <code>nosqlworkbench:datamodeladviser</code> | Crea y lee modelos de datos                                                | NoSQL Workbench         |
| <code>transform:read_write</code>            | Habilite el acceso a AWS Transform Agent para la transformación del código | AWS Transformación      |

## Configuración de aplicaciones de SAML 2.0 administradas por el cliente

Si usa aplicaciones administradas por el cliente que admiten [SAML 2.0](#), puede federar su IdP a IAM Identity Center mediante SAML 2.0 y usar IAM Identity Center para administrar el acceso de los usuarios a esas aplicaciones. Puede seleccionar una aplicación de SAML 2.0 de un catálogo de aplicaciones de uso frecuente en la consola de IAM Identity Center o puede configurar su propia aplicación de SAML 2.0.

### Note

Si tiene aplicaciones gestionadas por clientes compatibles con la OAuth versión 2.0 y sus usuarios necesitan acceder a ellas desde esas aplicaciones Servicios de AWS, puede utilizar la propagación de identidades fiable. Con una propagación de identidad fiable, un usuario puede iniciar sesión en una aplicación y esa aplicación puede transmitir la identidad de los usuarios en las solicitudes de acceso a los datos Servicios de AWS.

## Temas

- [Configuración de una aplicación del catálogo de aplicaciones de IAM Identity Center](#)
- [Configuración de su propia aplicación de SAML 2.0](#)

## Configuración de una aplicación del catálogo de aplicaciones de IAM Identity Center

Puede utilizar el catálogo de aplicaciones de la consola de IAM Identity Center para agregar muchas aplicaciones de SAML 2.0 de uso común que funcionan con IAM Identity Center. Algunos ejemplos son Salesforce, Box y Microsoft 365.

La mayoría de aplicaciones proporcionan información detallada sobre cómo configurar la confianza entre IAM Identity Center y el proveedor de servicios de la aplicación. Esta información está disponible en la página de configuración de la aplicación, después de seleccionarla en el catálogo. Tras configurar la aplicación, puede asignar el acceso a los usuarios o grupos de IAM Identity Center según sea necesario.

Utilice este procedimiento para configurar una relación de confianza de SAML 2.0 entre IAM Identity Center y el proveedor de servicios de la aplicación.

Antes de comenzar este procedimiento, resulta útil disponer del archivo de intercambio de metadatos del proveedor de servicios para que pueda configurar la relación de confianza de manera más eficiente. Aunque no disponga de este archivo, puede utilizar este procedimiento para configurar la confianza manualmente.

Para añadir y configurar una aplicación del catálogo de aplicaciones

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, elija Deseo seleccionar una aplicación del catálogo.
6. En Catálogo de aplicaciones, empiece a escribir el nombre de la aplicación que desea agregar en el cuadro de búsqueda.
7. Elija el nombre de la aplicación en la lista cuando aparezca en los resultados de la búsqueda y, a continuación, seleccione Siguiente.
8. En la página Configurar aplicación, los campos Nombre de visualización y Descripción se rellenan automáticamente con los detalles correspondientes de la aplicación. Puede modificar esta información.
9. En Metadatos de IAM Identity Center, haga lo siguiente:

- a. En el Archivo de metadatos del SAML de IAM Identity Center, elija Descargar para descargar los metadatos del proveedor de identidad.
- b. En el Certificado de IAM Identity Center, elija Descargar certificado para descargar el certificado del proveedor de identidad.

 Note

Necesitará estos archivos más tarde al configurar la aplicación desde el sitio web del proveedor de servicios. Siga las instrucciones de dicho proveedor.

10. (Opcional) En Propiedades de la aplicación, puede especificar URL de inicio de aplicación, Estado de retransmisión y Duración de la sesión. Para obtener más información, consulte [Entender las propiedades de la aplicación en la consola de IAM Identity Center](#).
11. En Metadatos de la aplicación, realice una de las siguientes acciones:
  - a. Si tiene un archivo de metadatos, seleccione Cargar archivo de metadatos de SAML de la aplicación. A continuación, seleccione Elegir archivo para buscar y seleccionar el archivo de metadatos.
  - b. Si no tiene un archivo de metadatos, elija Escribir manualmente los valores de los metadatos y, a continuación, proporcione los valores de URL de ACS de la aplicación y Audiencia de SAML de la aplicación.
12. Elija Enviar. Accederá a la página de detalles de la aplicación que acaba de añadir.

## Configuración de su propia aplicación de SAML 2.0

Puede configurar sus propias aplicaciones que permitan la federación de identidades mediante SAML 2.0 y agregarlas a IAM Identity Center. La mayoría de los pasos para configurar sus propias aplicaciones de SAML 2.0 son los mismos que para configurar una aplicación de SAML 2.0 desde el catálogo de aplicaciones de la consola de IAM Identity Center. Sin embargo, también debe proporcionar más asignaciones de atributos de SAML para sus aplicaciones de SAML 2.0. Estas asignaciones permiten que IAM Identity Center rellene correctamente la aserción de SAML 2.0 para su aplicación. Puede proporcionar esta asignación de atributos SAML adicionales cuando configure la aplicación por primera vez. También puede proporcionar asignaciones de atributos de SAML 2.0 en la página de detalles de la aplicación de la consola de IAM Identity Center.

Utilice el siguiente procedimiento para configurar una relación de confianza de SAML 2.0 entre IAM Identity Center y el proveedor de servicios de la aplicación de SAML 2.0. Antes de comenzar este procedimiento, asegúrese de que dispone del certificado y del archivo de intercambio de metadatos del proveedor de servicios para que pueda completar la configuración de la relación de confianza.

Para configurar su propia aplicación de SAML 2.0

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, seleccione Tengo una aplicación que quiero configurar.
6. En Tipo de aplicación, seleccione SAML 2.0.
7. Elija Siguiente.
8. En la página Configurar aplicación, en Configurar aplicación, introduzca un nombre para mostrar para la aplicación, por ejemplo **MyApp**. Escriba una descripción en Descripción.
9. En Metadatos de IAM Identity Center, haga lo siguiente:
  - a. En a Archivo de metadatos del SAML de IAM Identity Center, elija Descargar para descargar los metadatos del proveedor de identidad.
  - b. Junto a Certificado de IAM Identity Center, seleccione Descargar para descargar el certificado del proveedor de identidades.

 Note

Necesitará estos archivos más tarde al configurar la aplicación personalizada desde el sitio web del proveedor de servicios.

10. (Opcional) En Propiedades de la aplicación, también puede especificar los valores de URL de inicio de aplicación, Estado de retransmisión y Duración de la sesión. Para obtener más información, consulte [Entender las propiedades de la aplicación en la consola de IAM Identity Center](#).

11. En Metadatos de la aplicación, elija Escribir manualmente los valores de los metadatos. A continuación, proporcione valores para la URL de ACS de la aplicación y la audiencia de SAML de la aplicación.
12. Elija Enviar. Accederá a la página de detalles de la aplicación que acaba de añadir.

## Descripción general de la propagación de identidades de confianza

La propagación fiable de la identidad es una función del Centro de Identidad de IAM que permite Servicios de AWS a los administradores conceder permisos en función de los atributos de los usuarios, como las asociaciones de grupos. Con la propagación de identidades fiable, el contexto de identidad se añade a una función de IAM para identificar al usuario que solicita acceso a AWS los recursos. Este contexto se propaga a otros. Servicios de AWS

El contexto de identidad comprende la información que se Servicios de AWS utiliza para tomar decisiones de autorización cuando reciben solicitudes de acceso. Esta información incluye los metadatos que identifican al solicitante (por ejemplo, un usuario del Centro de Identidad de IAM), el lugar Servicio de AWS al que se solicita el acceso (por ejemplo, Amazon Redshift) y el ámbito del acceso (por ejemplo, el acceso de solo lectura). El destinatario Servicio de AWS utiliza este contexto y cualquier permiso asignado al usuario para autorizar el acceso a sus recursos.

## Ventajas de una propagación de identidad fiable

La propagación fiable de la identidad permite Servicios de AWS a los administradores conceder permisos a los recursos, como los datos, utilizando las identidades corporativas de sus empleados. Además, pueden auditar quién accedió a qué datos consultando los registros de servicio o AWS CloudTrail. Si es administrador del IAM Identity Center, es posible que otros Servicio de AWS administradores le pidan que habilite la propagación de identidades de forma fiable.

## Habilitar la propagación de identidades de forma fiable

El proceso de habilitar la propagación de identidades confiables implica los dos pasos siguientes:

1. Activa el Centro de Identidad de IAM y conecta tu fuente de identidades actual al Centro de Identidad de IAM. Seguirás gestionando las identidades de tus empleados en tu fuente de identidades actual; al conectarlo al Centro de Identidad de IAM, se crea una referencia a tu personal que todos los que quieras compartir Servicios de AWS en tu caso práctico. También está disponible para que los propietarios de los datos la utilicen en futuros casos de uso.

2. Conéctelo Servicios de AWS en su caso de uso al Centro de identidad de IAM: el administrador de cada uno Servicio de AWS de los casos de uso de propagación de identidad confiable sigue las instrucciones de la documentación de servicio correspondiente para conectar el servicio al Centro de identidad de IAM.

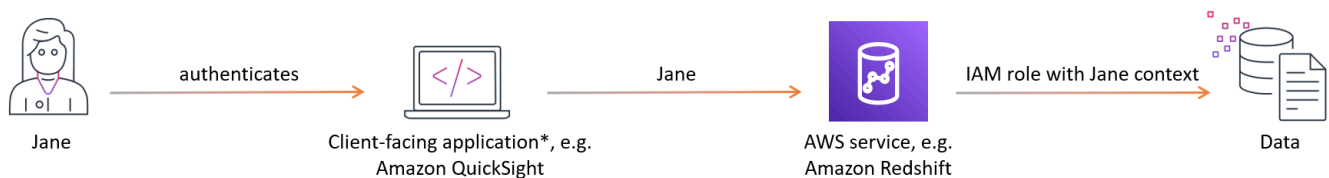
### Note

Si su caso de uso involucra una aplicación desarrollada por terceros o por un cliente, habilite la propagación de identidades confiable configurando una relación de confianza entre el proveedor de identidades que autentica a los usuarios de la aplicación y el Centro de Identidad de IAM. Esto permite que su aplicación aproveche el flujo de propagación de identidad confiable descrito anteriormente.

Para obtener más información, consulte [Uso de aplicaciones con un emisor de tokens de confianza](#).

## Cómo funciona la propagación de identidades confiable

El siguiente diagrama muestra el flujo de trabajo de alto nivel para la propagación de identidades confiables:



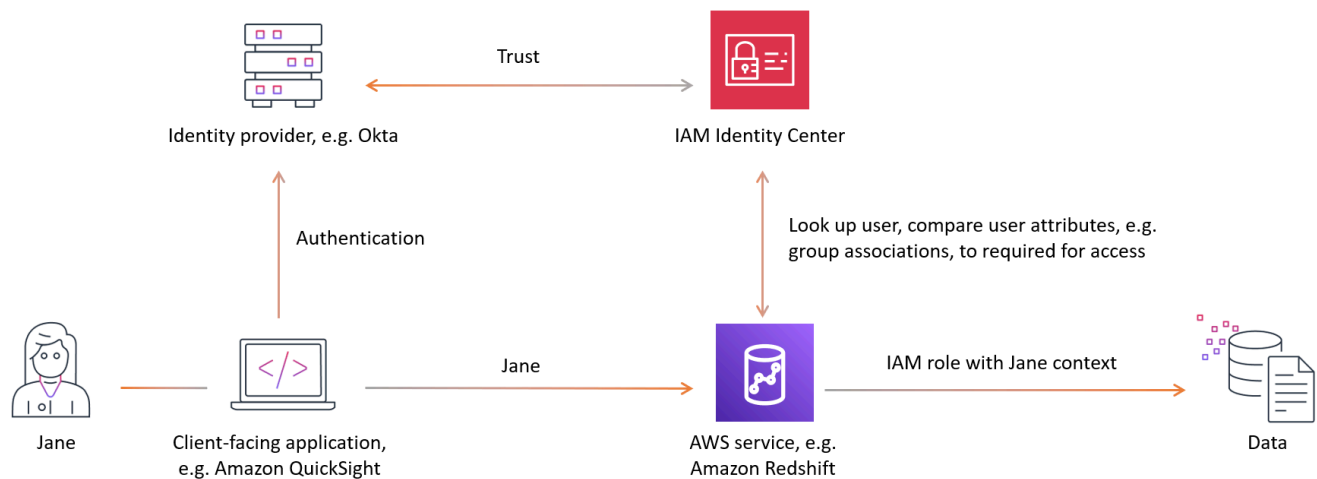
1. Los usuarios se autentican con una aplicación orientada al cliente, por ejemplo. QuickSight
2. La aplicación orientada al cliente solicita acceso para utilizarlos y Servicio de AWS consultarlos e incluye información sobre el usuario.

### Note

Algunos casos de uso fiables de la propagación de identidades implican herramientas que interactúan con el Servicios de AWS uso de controladores de servicio. Puedes averiguar si esto se aplica a tu caso de uso en la [guía de casos de uso](#).

3. Servicio de AWS Verifica la identidad del usuario con el Centro de Identidad de IAM y compara los atributos del usuario, como sus asociaciones grupales, con los necesarios para el acceso. Servicio de AWS Autoriza el acceso siempre que el usuario o su grupo tengan los permisos necesarios.
4. Servicios de AWS puede registrar el identificador de usuario AWS CloudTrail y en sus registros de servicio. Consulte la documentación del servicio para obtener más información.

La siguiente imagen proporciona una descripción general de los pasos descritos anteriormente en el flujo de trabajo de propagación de identidad confiable:



## Temas

- [Requisitos y consideraciones previos](#)
- [Casos de uso de propagación de identidades de confianza](#)
- [Uso de la propagación de identidades de confianza con aplicaciones administradas por el cliente](#)

## Requisitos y consideraciones previos

Antes de configurar la propagación de identidades de confianza, revise los siguientes requisitos previos y consideraciones.

## Temas

- [Requisitos previos](#)
- [Consideraciones](#)
- [Consideraciones sobre las aplicaciones administradas por el cliente](#)

## Requisitos previos

Para utilizar una propagación de identidad confiable, asegúrese de que su entorno cumpla los siguientes requisitos previos:

- Habilite y aprovisione el centro de identidad de IAM
  - Para utilizar la propagación de identidades fiable, debe habilitar el Centro de Identidad de IAM en el mismo Región de AWS lugar donde están habilitadas las AWS aplicaciones y los servicios a los que accederán sus usuarios. Para obtener información, consulte [Activar IAM Identity Center](#).
  - Se recomienda utilizar una instancia de organización del IAM Identity Center. Le recomendamos que utilice una [instancia de organización](#) del IAM Identity Center que esté habilitada en la cuenta de administración de la empresa. AWS Organizations Puede [delegar la administración](#) de una instancia organizativa del IAM Identity Center a una cuenta de miembro. Si elige una [instancia de cuenta](#) del IAM Identity Center, todas las cuentas a las Servicios de AWS que desee que accedan los usuarios con una propagación de identidad fiable deberán residir en el mismo Cuenta de AWS lugar en el que habilite el IAM Identity Center. Para obtener más información, consulte [Instancias de cuenta de IAM Identity Center](#).
  - Conecte su proveedor de identidad actual al Centro de identidades de IAM y aprovisiona sus usuarios y grupos al Centro de identidades de IAM. Para obtener más información, consulte [Tutoriales de fuentes de identidad de IAM Identity Center](#).
- Conecte las aplicaciones y los servicios AWS gestionados de su caso de uso de propagación de identidades de confianza al IAM Identity Center. Para utilizar una propagación de identidad fiable, las aplicaciones AWS gestionadas deben estar conectadas al Centro de identidades de IAM.

## Consideraciones

Tenga en cuenta las siguientes consideraciones al configurar y utilizar la propagación de identidades fiable:

- Organización frente a instancia de cuenta de IAM Identity Center
  - Una [instancia organizativa](#) de IAM Identity Center le proporcionará el mayor control y flexibilidad para ampliar sus casos de uso a varios Cuentas de AWS usuarios y. Servicios de AWS Si no puede utilizar una instancia de organización, es posible que su caso de uso sea compatible con las instancias de cuentas de IAM Identity Center. Para obtener más información sobre qué instancias Servicios de AWS de cuentas del IAM Identity Center son compatibles con su caso de



uso, consulte. [AWS aplicaciones gestionadas que puede utilizar con el Centro de identidades de IAM](#)

- No se requieren permisos de varias cuentas (conjuntos de permisos)
- La propagación de identidades de confianza no requiere que configure [permisos de varias cuentas](#) (conjuntos de permisos). Puede habilitar IAM Identity Center y utilizarlo únicamente para la propagación de identidades de confianza.

## Consideraciones sobre las aplicaciones administradas por el cliente

Su personal puede beneficiarse de una propagación de identidad fiable incluso si sus usuarios interactúan con aplicaciones orientadas al cliente que no están gestionadas, por ejemplo AWS, por sus aplicaciones Tableau desarrolladas a medida. Es posible que los usuarios de estas aplicaciones no estén aprovisionados en el IAM Identity Center. Para permitir el reconocimiento y la autorización sin problemas del acceso de los usuarios a AWS los recursos, el Centro de Identidad de IAM le permite configurar una relación de confianza entre el proveedor de identidades que autentica a sus usuarios y el Centro de Identidad de IAM. Para obtener más información, consulte [Uso de aplicaciones con un emisor de tokens de confianza](#).

Además, para configurar la propagación de identidades fiable para su aplicación, será necesario:

- La aplicación debe utilizar el marco OAuth 2.0 para la autenticación. La propagación de identidades confiable no admite las integraciones de SAML 2.0.
- El Centro de Identidad de IAM debe reconocer su aplicación. Siga las instrucciones específicas para su [caso de uso](#).

## Casos de uso de propagación de identidades de confianza

Como administrador del Centro de Identidad de IAM, es posible que se le pida que ayude a configurar la propagación fiable de la identidad desde las aplicaciones orientadas a los usuarios hasta las aplicaciones. Servicios de AWS Para respaldar esta solicitud, necesitará la siguiente información:

- ¿Con qué aplicación orientada al cliente interactuarán sus usuarios?
- ¿ Servicios de AWS Cuáles se utilizan para consultar los datos y autorizar el acceso a los datos?
- ¿ Servicio de AWS Quién autoriza el acceso a los datos?

Su función a la hora de facilitar los casos de uso de la propagación de identidades confiables que no involucren aplicaciones de terceros o aplicaciones desarrolladas a medida consiste en:

1. [Habilite el Centro de Identidad de IAM.](#)
2. [Conecte su fuente de identidades existente al Centro de identidades de IAM.](#)

Los pasos restantes de la configuración de la identidad confiable para estos casos de uso se llevan a cabo dentro de las aplicaciones conectadas Servicios de AWS y. Los administradores de las aplicaciones conectadas Servicios de AWS o conectadas deben consultar las guías de usuario correspondientes para obtener una guía completa sobre los servicios específicos.

Su función a la hora de posibilitar la propagación fiable de identidades en los casos de uso relacionados con aplicaciones de terceros o aplicaciones desarrolladas a medida incluye los pasos necesarios para [conectar su fuente de identidades Activar IAM Identity Center y conectarla](#), así como:

1. Configurar la conexión de su proveedor de identidad (IdP) con la aplicación de terceros o desarrollada a medida.
2. Permitir que el Centro de Identidad de IAM reconozca la aplicación de terceros o desarrollada a medida.
3. Configuración de su IdP como emisor de token de confianza en el IAM Identity Center. Para obtener más información, consulte [Uso de aplicaciones con un emisor de tokens de confianza](#).

Los administradores de las aplicaciones conectadas Servicios de AWS deben consultar las guías de usuario correspondientes para obtener una guía completa sobre los servicios específicos.

## Casos de uso de datos y análisis

Puede habilitar los casos de uso de propagación confiables con los siguientes servicios de análisis:

- Amazon Redshift: para obtener orientación, consulte. [Propagación de identidad fiable con Amazon Redshift](#)
- Amazon EMR: para obtener orientación, consulte. [Propagación de identidad fiable con Amazon EMR](#)
- Amazon Athena: para obtener orientación, consulte. [Propagación de identidad confiable con Amazon Athena](#)

## Casos de uso adicionales

Puede activar el Centro de Identidad de IAM y la propagación de identidades confiables con estas opciones adicionales Servicios de AWS:

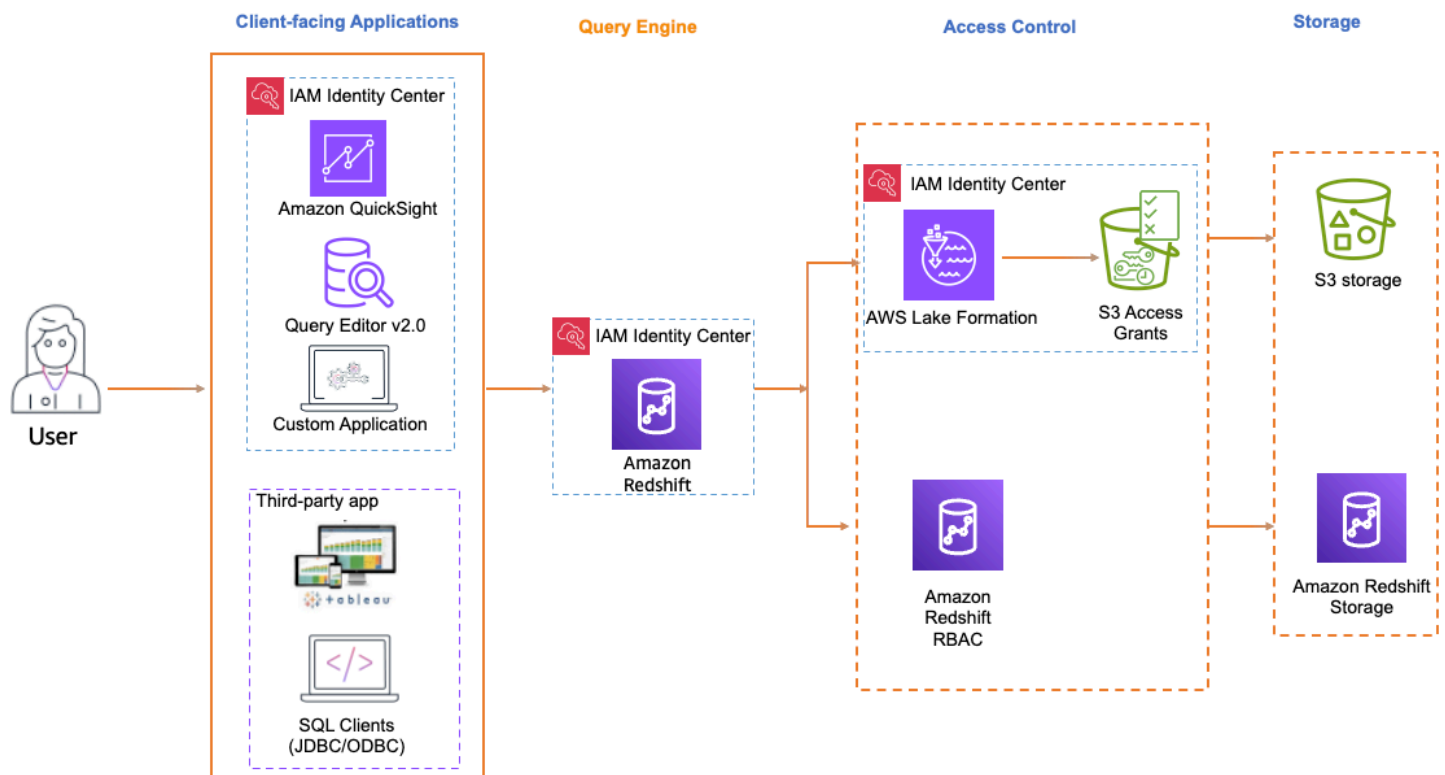
- Amazon Q Business: para obtener orientación, consulte:
  - [Administra el flujo de trabajo de las aplicaciones que utilizan IAM Identity Center.](#)
  - [Configuración de una aplicación Amazon Q Business mediante el Centro de identidad de IAM.](#)
  - [Configure Amazon Q Business con la propagación de identidad fiable de IAM Identity Center.](#)
- Amazon OpenSearch Service: para obtener información, consulta:
  - [IAM Identity Center Trusted Identity Propagation Support for Amazon OpenSearch Service.](#)
  - [Interfaz OpenSearch de usuario centralizada \(paneles de control\) con Amazon OpenSearch Service.](#)
- AWS Transfer Family- para obtener orientación, consulte:
  - [Aplicaciones web Transfer Family.](#)

## Temas

- [Propagación de identidad fiable con Amazon Redshift](#)
- [Propagación de identidad fiable con Amazon EMR](#)
- [Propagación de identidad confiable con Amazon Athena](#)
- [Servicios de autorización](#)

## Propagación de identidad fiable con Amazon Redshift

Los pasos para habilitar la propagación de identidades confiable dependen de si los usuarios interactúan con las aplicaciones administradas o con las aplicaciones AWS administradas por el cliente. El siguiente diagrama muestra una configuración de propagación de identidad confiable para aplicaciones orientadas al cliente, AWS administradas o externas, que consultan datos de Amazon Redshift con el control de acceso proporcionado por Amazon Redshift o por servicios de autorización, como Amazon S3. AWS Lake Formation Access Grants



Cuando la propagación de identidades de confianza a Amazon Redshift está habilitada, los administradores de Redshift pueden configurar Redshift para que cree automáticamente funciones para el Centro de identidades de IAM como proveedor de identidades, asignar las funciones de Redshift a los grupos del Centro de identidades de IAM y utilizar el control de acceso basado en funciones de Redshift para conceder el acceso.

Aplicaciones orientadas al cliente compatibles

AWS aplicaciones gestionadas

Las siguientes aplicaciones AWS gestionadas orientadas al cliente admiten la propagación de identidades de confianza en Amazon Redshift:

- [Amazon Redshift Query Editor V2](#)
- [QuickSight](#)

 Note

Si utiliza Amazon Redshift Spectrum para acceder a bases de datos o tablas AWS Glue Data Catalog externas, considere la posibilidad de [configurar Lake](#) Formation [y Amazon Access Grants](#) S3 para proporcionar un control de acceso detallado.

## Aplicaciones administradas por el cliente

Las siguientes aplicaciones administradas por el cliente permiten la propagación de identidades de confianza en Amazon Redshift:

- Tableau incluidos Tableau Desktop TableauServer, y Tableau Prep
  - Para habilitar la propagación de identidades fiable para los usuarios de Tableau, consulte [Integrar Tableau y Okta con Amazon Redshift mediante IAM Identity Center](#) en el blog sobre AWS macrodatos.
- Clientes SQL (y) DBeaver DBVisualizer
  - Para permitir la propagación de identidades confiable para los usuarios de SQL Clients (DBeaver y DBVisualizer), consulte [Integrar el proveedor de identidad \(IdP\) con Amazon Redshift Query Editor V2 y SQL Client mediante IAM Identity Center para lograr un inicio de sesión único sin problemas en el blog sobre](#) big data.AWS

## Configuración de la propagación de identidades de confianza con Amazon Redshift Query Editor V2

El siguiente procedimiento explica cómo lograr una propagación de identidades fiable desde Amazon Redshift Query Editor V2 a Amazon Redshift.

### Requisitos previos

Antes de empezar con este tutorial, tendrá que configurar lo siguiente:

1. [Habilite el Centro de identidades de IAM](#). Se recomienda [una instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).
2. [Aprovisione los usuarios y grupos de su fuente de identidades en el Centro de identidades de IAM](#).

La activación de la propagación de identidades de confianza incluye las tareas realizadas por un administrador del Centro de Identidad de IAM en la consola del Centro de Identidad de IAM y las tareas realizadas por un administrador de Amazon Redshift en la consola de Amazon Redshift.

## Tareas realizadas por el administrador del Centro de Identidad de IAM

El administrador del Centro de Identidad de IAM debía realizar las siguientes tareas:

1. Cree un [rol de IAM](#) en la cuenta en la que se encuentre el clúster o la instancia Serverless de Amazon Redshift con la siguiente política de permisos. Para obtener más información, consulte [Creación de roles de IAM](#).

  - Los siguientes ejemplos de políticas incluyen los permisos necesarios para completar este tutorial. Para usar esta política, sustituya *italicized placeholder text* la política del ejemplo por su propia información. Para obtener instrucciones adicionales, consulte [Crear una política](#) o [Editar una política](#).

Política de permisos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowRedshiftApplication",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowIDCPermissions",
      "Effect": "Allow",
      "Action": [
        "sso:DescribeApplication",
        "sso:DescribeInstance"
      ],
      "Resource": [
        "arn:aws:sso:::instance/Your-IAM-Identity-Center-Instance ID",
```

```

        "arn:aws:sso::Your-AWS-Account-ID:application/Your-IAM-Identity-Center-Instance-ID/*"
    ]
}

```

Política de confianza:

```

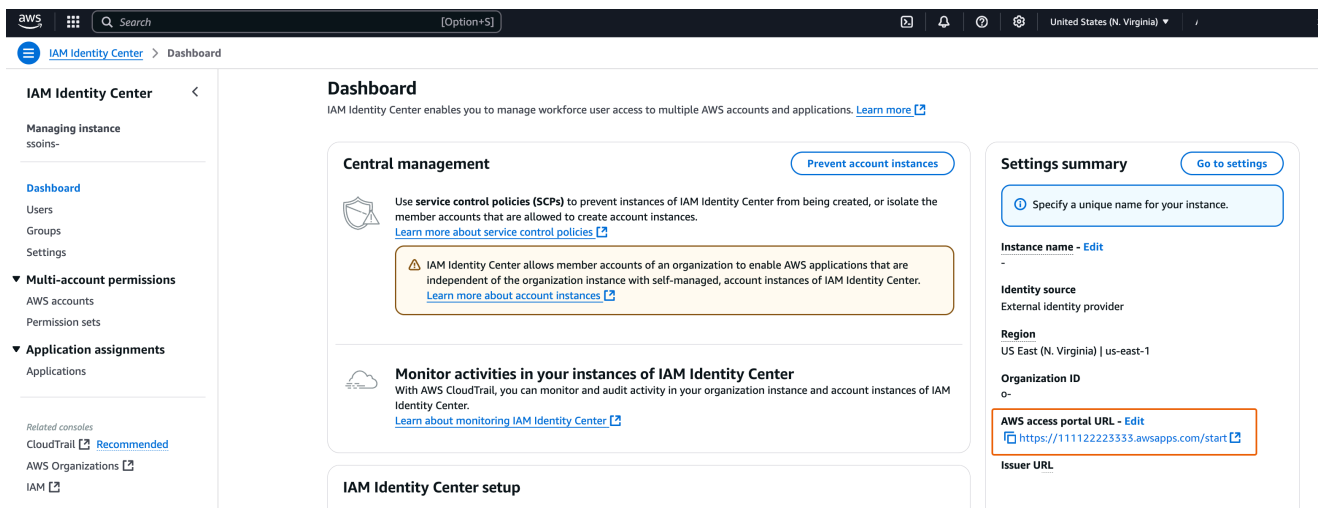
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "redshift-serverless.amazonaws.com",
          "redshift.amazonaws.com"
        ]
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}

```

2. Cree un conjunto de permisos en la cuenta AWS Organizations de administración en la que esté activado el Centro de identidades de IAM. Lo usará en el siguiente paso para permitir que los usuarios federados accedan a Redshift Query Editor V2.
  - a. Vaya a la consola del IAM Identity Center y, en Permisos para varias cuentas, seleccione Conjuntos de permisos.
  - b. Elija Crear conjunto de permisos.
  - c. Elija Conjunto de permisos personalizado y, a continuación, elija Siguiente.
  - d. En Políticas AWS administradas, selecciona **AmazonRedshiftQueryEditorV2ReadSharing**.
  - e. En Política en línea, agrega la siguiente política:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": [
        "redshift:DescribeQev2IdcApplications",
        "redshift-serverless:ListNamespaces",
        "redshift-serverless:ListWorkgroups",
        "redshift-serverless:GetWorkgroup"
      ],
      "Resource": "*"
    }
  ]
}
```

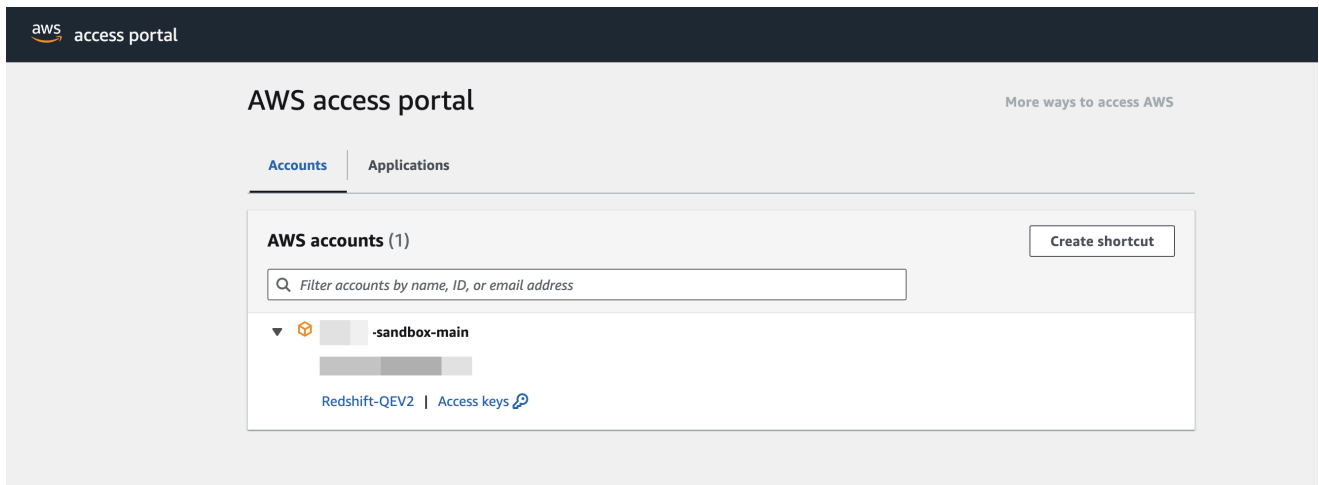
- f. Seleccione Siguiente y, a continuación, proporcione un nombre para el nombre del conjunto de permisos. Por ejemplo, **Redshift-Query-Editor-V2**.
- g. En Estado de retransmisión (opcional), defina el estado de retransmisión predeterminado en la URL de Query Editor V2, con el formato: `https://your-region.console.aws.amazon.com/sqlworkbench/home`.
- h. Revise la configuración y seleccione Crear.
- i. Vaya al panel de control del IAM Identity Center y copie la URL del portal de AWS acceso de la sección Resumen de la configuración.



- j. Abre una nueva ventana del navegador de incógnito y pega la URL.



Esto lo llevará a su portal de AWS acceso y se asegurará de que está iniciando sesión con un usuario del IAM Identity Center.



Para obtener más información sobre el conjunto de permisos, consulte [Administre Cuentas de AWS con conjuntos de permisos](#).

3. Permita que los usuarios federados accedan a Redshift Query Editor V2.
  - a. En la cuenta AWS Organizations de administración, abra la consola de IAM Identity Center.
  - b. En el panel de navegación, en Permisos para varias cuentas, elija Cuentas de AWS.
  - c. En la Cuentas de AWS página, seleccione Cuenta de AWS aquella a la que desee asignar el acceso.
  - d. Seleccione Asignar usuarios o grupos.
  - e. En la página Asignar usuarios y grupos, elija los usuarios o grupos para los que desee crear el conjunto de permisos. A continuación, elija Siguiente.
  - f. En la página Asignar conjuntos de permisos, elija el conjunto de permisos que creó en el paso anterior. A continuación, elija Siguiente.
  - g. En la página Revisar y enviar tareas, revise sus selecciones y pulse Enviar.

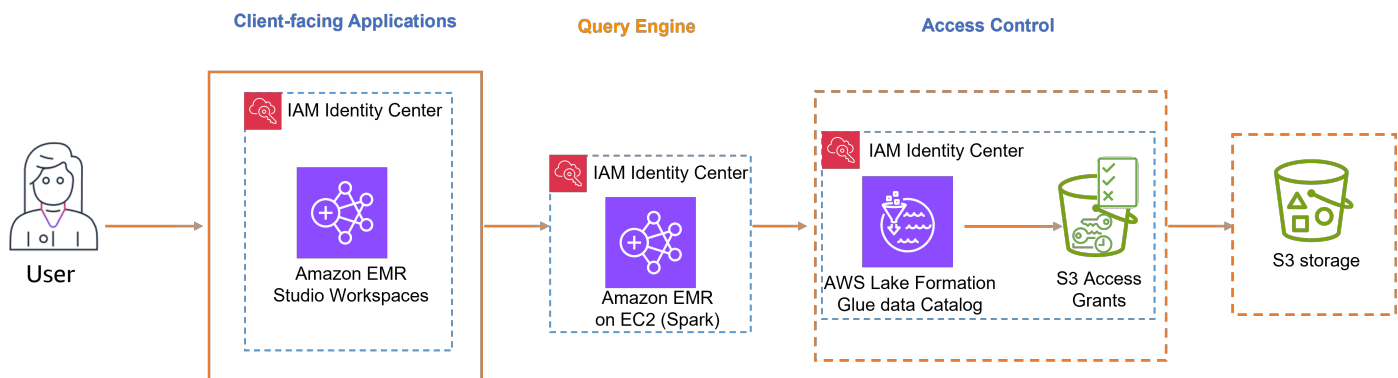
### Tareas realizadas por un administrador de Amazon Redshift

Para habilitar la propagación de identidades de confianza en Amazon Redshift, es necesario que un administrador de clústeres de Amazon Redshift o un administrador de Amazon Redshift Serverless realice una serie de tareas en la consola de Amazon Redshift. Para obtener más información, consulte [Integrar el proveedor de identidad \(IdP\) con Amazon Redshift Query Editor V2 y SQL Client](#)

[mediante IAM Identity Center para lograr un inicio de sesión único sin problemas](#) en el blog sobre big data.AWS

## Propagación de identidad fiable con Amazon EMR

El siguiente diagrama muestra una configuración de propagación de identidad fiable para Amazon EMR Studio mediante Amazon EMR en Amazon EC2 con el control de acceso proporcionado por AWS Lake Formation Amazon S3. Access Grants



### Aplicaciones orientadas al cliente compatibles

- Amazon EMR Studio

Para habilitar la propagación de identidades confiable, siga estos pasos:

- [Configure Amazon EMR Studio](#) como la aplicación orientada al cliente para el clúster de Amazon EMR.
- Configure [Amazon EMR Cluster en Amazon EC2](#) con. Apache Spark
- Recomendado: [AWS Lake Formationy Amazon S3 Access Grants](#) para proporcionar un control de acceso detallado a las ubicaciones de datos subyacentes AWS Glue Data Catalog y a las ubicaciones de datos subyacentes en S3.

### Configuración de la propagación de identidades de confianza con Amazon EMR Studio

El siguiente procedimiento explica cómo configurar Amazon EMR Studio para la propagación de identidades de confianza en consultas realizadas en grupos de trabajo de Amazon Athena o clústeres de Amazon EMR en ejecución. Apache Spark

## Requisitos previos

Antes de empezar con este tutorial, tendrá que configurar lo siguiente:

1. [Habilite el Centro de identidades de IAM](#). Se recomienda [una instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).
2. [Aprovisione los usuarios y grupos de su fuente de identidades en el Centro de identidades de IAM](#).

Para completar la configuración de la propagación de identidades de confianza desde Amazon EMR Studio, el administrador de EMR Studio debe realizar los siguientes pasos.

### Paso 1. Cree las funciones de IAM necesarias para EMR Studio

En este paso, el Studio administrador de Amazon EMR crea un rol de servicio de IAM y un rol de usuario de IAM para EMR Studio

1. [Cree una función de servicio de EMR Studio: EMR Studio asume esta función](#) de IAM para gestionar de forma segura los espacios de trabajo y las libretas, conectarse a clústeres y gestionar las interacciones de datos.
  - a. Navegue hasta la consola de IAM (<https://console.aws.amazon.com/iam/>) y cree un rol de IAM.
  - b. Seleccione Servicio de AWS como entidad de confianza y, a continuación, elija Amazon EMR. Adjunte las siguientes políticas para definir los permisos y la relación de confianza del rol.

Para usar estas políticas, sustituya *italicized placeholder text* la política del ejemplo por su propia información. Para obtener instrucciones adicionales, consulte [Crear una política](#) o [Editar una política](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectActions",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
```

```

        "s3:DeleteObject"
    ],
    "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio/*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
    }
},
{
    "Sid": "BucketActions",
    "Effect": "Allow",
    "Action": [
        "s3:ListBucket",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": [
        "arn:aws:s3:::Your-S3-Bucket-For-EMR-Studio"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "Your-AWS-Account-ID"
        }
    }
}
]
}

```

Para obtener una referencia de todos los permisos de rol de servicio, consulte [Permisos de rol de servicio de EMR Studio](#).

2. [Cree un rol de usuario de EMR Studio para la autenticación del Centro de identidad de IAM:](#)

EMR Studio asume este rol cuando un usuario inicia sesión a través del Centro de identidades de IAM para administrar espacios de trabajo, clústeres de EMR, trabajos y repositorios de git. Esta función se utiliza para iniciar el flujo de trabajo de propagación de identidades fiables.

 Note

El rol de usuario de EMR Studio no necesita incluir permisos para acceder a las ubicaciones de Amazon S3 de las tablas del catálogo. AWS Glue AWS Lake Formation

los permisos y las ubicaciones de lagos registradas se utilizarán para recibir permisos temporales.

El siguiente ejemplo de política se puede utilizar en un rol que permita a un usuario de EMR Studio utilizar los grupos de trabajo de Athena para ejecutar consultas.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDefaultEC2SecurityGroupsCreationInVPCWithEMRTags",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:vpc/*"
      ],
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/for-use-with-amazon-emr-managed-policies":
            "true"
        }
      }
    },
    {
      "Sid": "AllowAddingEMRTagsDuringDefaultSecurityGroupCreation",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags"
      ],
      "Resource": "arn:aws:ec2:*:*:security-group/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/for-use-with-amazon-emr-managed-policies":
            "true",
          "ec2:CreateAction": "CreateSecurityGroup"
        }
      }
    }
  ]
}
```

```

        "Sid": "AllowSecretManagerListSecrets",
        "Action": [
            "secretsmanager:ListSecrets"
        ],
        "Resource": "*",
        "Effect": "Allow"
    },
    {
        "Sid": "AllowSecretCreationWithEMRTagsAndEMRStudioPrefix",
        "Effect": "Allow",
        "Action": "secretsmanager:CreateSecret",
        "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*",
        "Condition": {
            "StringEquals": {
                "aws:RequestTag/for-use-with-amazon-emr-managed-policies":
"true"
            }
        }
    },
    {
        "Sid": "AllowAddingTagsOnSecretsWithEMRStudioPrefix",
        "Effect": "Allow",
        "Action": "secretsmanager:TagResource",
        "Resource": "arn:aws:secretsmanager:*:*:secret:emr-studio-*"
    },
    {
        "Sid": "AllowPassingServiceRoleForWorkspaceCreation",
        "Action": "iam:PassRole",
        "Resource": [
            "arn:aws:iam::Your-AWS-Account-ID:role/service-
role/AmazonEMRStudio_ServiceRole_Name"
        ],
        "Effect": "Allow"
    },
    {
        "Sid": "AllowS3ListAndLocationPermissions",
        "Action": [
            "s3:ListAllMyBuckets",
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": "arn:aws:s3:::*",
        "Effect": "Allow"
    },

```

```

    {
      "Sid": "AllowS3ReadOnlyAccessToLogs",
      "Action": [
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3::aws-logs-Your-AWS-Account-ID-Region/elasticmapreduce/
* "
      ],
      "Effect": "Allow"
    },
    {
      "Sid": "AllowAthenaQueryExecutions",
      "Effect": "Allow",
      "Action": [
        "athena:StartQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:StopQueryExecution",
        "athena:ListQueryExecutions",
        "athena:GetQueryResultsStream",
        "athena:ListWorkGroups",
        "athena:GetWorkGroup",
        "athena:CreatePreparedStatement",
        "athena:GetPreparedStatement",
        "athena>DeletePreparedStatement"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowGlueSchemaManipulations",
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabase",
        "glue:GetDatabases",
        "glue:GetTable",
        "glue:GetTables",
        "glue:GetPartition",
        "glue:GetPartitions"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowQueryEditorToAccessWorkGroup",

```

```

    "Effect": "Allow",
    "Action": "athena:GetWorkGroup",
    "Resource": "arn:aws:athena:*:Your-AWS-Account-ID:workgroup*"
  },
  {
    "Sid": "AllowConfigurationForWorkspaceCollaboration",
    "Action": [
      "elasticmapreduce:UpdateEditor",
      "elasticmapreduce:PutWorkspaceAccess",
      "elasticmapreduce>DeleteWorkspaceAccess",
      "elasticmapreduce:ListWorkspaceAccessIdentities"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "elasticmapreduce:ResourceTag/creatorUserId": "${aws:userId}"
      }
    }
  },
  {
    "Sid": "DescribeNetwork",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeVpcs",
      "ec2:DescribeSubnets",
      "ec2:DescribeSecurityGroups"
    ],
    "Resource": "*"
  },
  {
    "Sid": "ListIAMRoles",
    "Effect": "Allow",
    "Action": [
      "iam:ListRoles"
    ],
    "Resource": "*"
  },
  {
    "Sid": "AssumeRole",
    "Effect": "Allow",
    "Action": [
      "sts:AssumeRole"
    ],

```



```
        "Resource": "*"
      }
    ]
  }
}
```

La siguiente política de confianza permite a EMR Studio asumir la función:

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "elasticmapreduce.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

#### Note

Se necesitan permisos adicionales para aprovechar EMR Studio Workspaces y EMR Notebooks. Consulte [Crear políticas de permisos para los usuarios de EMR Studio](#) para obtener más información.

Puede encontrar más información en los siguientes enlaces:

- [Defina los permisos de IAM personalizados con políticas administradas por el cliente](#)
- [Permisos de rol de servicio de EMR Studio](#)

## Paso 2. Cree y configure su EMR Studio

En este paso, creará un Amazon EMR Studio en la consola de EMR Studio y utilizará las funciones de IAM en las que creó. [Paso 1. Cree las funciones de IAM necesarias para EMR Studio](#)

1. Navegue hasta la consola de EMR Studio, seleccione Crear estudio y la opción Configuración personalizada. Puede crear un nuevo depósito de S3 o utilizar uno existente. Puede marcar la casilla Cifrar los archivos del espacio de trabajo con sus propias claves de KMS. Para obtener más información, consulte [AWS Key Management Service](#).

**Create a Studio** [Info](#)

**Setup options** [Info](#)

☐ Interactive workloads
 ☐ Batch jobs
 ☒ Custom

**Studio settings** [Info](#)

**Studio name**

Studio\_1

Use up to 256 characters (alphanumeric, hyphens, or underscores).

**Description - optional**

The description below will be visible to your studio teams.

Describe the Studio

256 characters maximum

**S3 location for Workspace storage**

Specify an Amazon S3 location where Workspace work will be saved.

☒ Create new bucket
 ☐ Select existing location

We'll create a new bucket and use the location `s3://aws-emr-studio-225989353012-us-east-1/1735848818523`.

☐ Encrypt Workspace files with your own AWS KMS key  
 EMR Studio automatically uses the S3 location's encryption configuration. Choose this option if you want to override the S3 location's encryption configuration with your own AWS KMS key. This key information will not be editable past Studio creation.

2. En Función de servicio para permitir que Studio acceda a sus recursos, seleccione la función de servicio creada en el [Paso 1. Cree las funciones de IAM necesarias para EMR Studio](#) menú.
3. Elija IAM Identity Center en Autenticación. Seleccione el rol de usuario creado en [Paso 1. Cree las funciones de IAM necesarias para EMR Studio](#).

**Service role to let Studio access your AWS resources**

AmazonEMRStudio\_ [View permission details](#)

**Authentication** [Info](#)

**Authentication**

Choose an authentication method for your Studio.

☐ AWS Identity and Access Management (IAM)  
 Authenticate with single sign-on using IAM Identity federation or IAM credentials.

☒ IAM Identity Center (AWS Single Sign-On)  
 Authenticate with single sign-on using IAM Identity Center (recommended to centrally manage access permissions for multiple AWS accounts).

**User role**

Each Studio will have a default set of user roles. You can further refine user permissions once you have created a Studio. To create an additional set of permission use [AWS IAM](#)

emrstudio-userrole-ids [Create IAM role](#)

**Connect EMR Studio to IAM Identity Center**

Instance of IAM Identity Center

Manage access to EMR Studio by assigning users and groups from your Identity Center directory.

arn:aws:sso::instance/ssolns-

4. Marque la casilla Propagación de identidad confiable. Seleccione Solo usuarios y grupos asignados en la sección Acceso a la aplicación, lo que le permitirá permitir el acceso a este estudio únicamente a usuarios y grupos autorizados.
5. (Opcional): puede configurar la VPC y la subred si utiliza este estudio con clústeres de EMR.

**Trusted identity propagation** [Info](#)  
Control and log the access that a user has across connected applications.

☒ **Enable trusted identity propagation**  
When users make requests to applications that are connected through Identity Center, share their user identity information from EMR Studio. This setting applies for the lifetime of the Studio. You can't turn it off later.

ⓘ The following features aren't supported from a Studio with trusted identity propagation: creating EMR on EC2 clusters without a template, using EMR Serverless applications, launching EMR on EKS clusters, using a runtime role, and enabling SQL Explorer or Workspace collaboration.

**Application access** [Info](#)  
**Choose who can access your application**  
Specify whether only assigned users and groups can access your application.

☒ **Only assigned users and groups**  
Only the users and groups that you specify from your Identity Center directory can access this application.

☐ **All users and groups**  
Any user or group from your IAM Identity Center directory can access this application.

▼ **Networking and security - optional**

**VPC** [Info](#)  
Select a VPC for your Studio to use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag the VPC with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

Select a VPC

**Subnets** [Info](#)  
Select the subnets that your Studio can use when it communicates with EMR clusters. To use condition keys like those in the example [service role policies for Amazon EMR](#), you must tag each subnet with the `for-use-with-amazon-emr-managed-policies` key and value `true`. To manage tags, use [VPC Dashboard](#).

6. Revise todos los detalles y seleccione Create Studio.
7. Tras configurar un clúster de Athena WorkGroup o EMR, inicie sesión en la URL de Studio para:
  - a. Ejecute consultas de Athena con el editor de consultas.
  - b. Ejecuta los trabajos de Spark en el espacio de trabajo con un Jupyter bloc de notas.

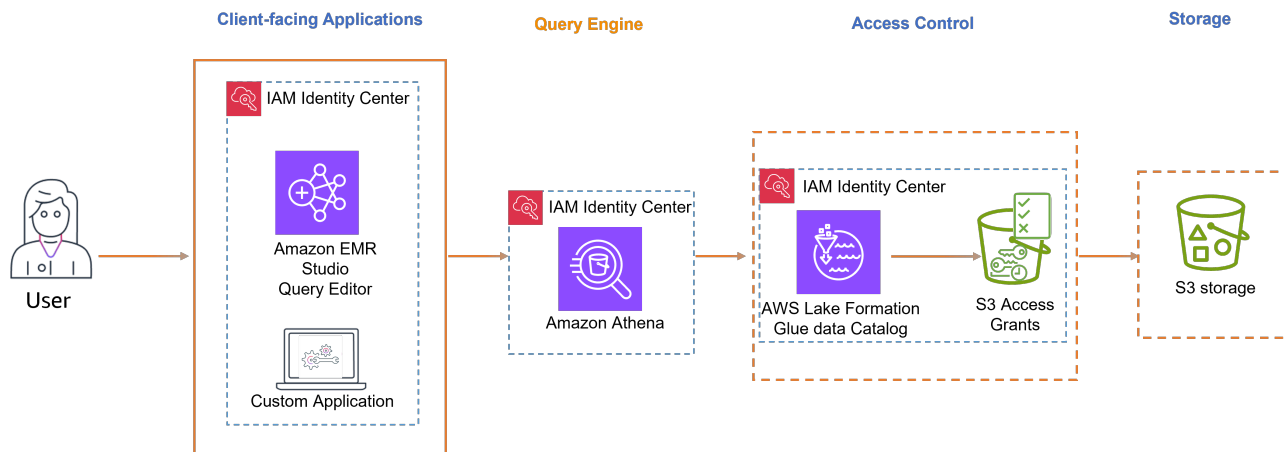
## Propagación de identidad confiable con Amazon Athena

Los pasos para permitir una propagación de identidad confiable dependen de si sus usuarios interactúan con las aplicaciones administradas o con las aplicaciones AWS administradas por los clientes. El siguiente diagrama muestra una configuración de propagación de identidad confiable para aplicaciones orientadas al cliente, AWS administradas o externas, que utilizan Amazon Athena para AWS consultar datos de Amazon S3 con el control de acceso proporcionado por AWS Lake Formation Amazon S3. Access Grants

### Note

- La propagación de identidades de confianza con Amazon Athena requiere el uso de Trino.

- No se admiten los clientes Apache Spark y SQL conectados a Amazon Athena mediante controladores ODBC y JDBC.



## AWS aplicaciones gestionadas

La siguiente aplicación AWS gestionada orientada al cliente admite la propagación de identidades de confianza con Athena:

- Amazon EMR Studio

Para habilitar la propagación de identidades confiable, siga estos pasos:

- [Configure Amazon EMR Studio](#) como la aplicación orientada al cliente para Athena. El editor de consultas de EMR Studio es necesario para ejecutar Athena Queries cuando la propagación de identidad confiable está habilitada.
- [Configure Athena Workgroup](#).
- Se ha [configurado AWS Lake Formation](#) para permitir un control de acceso detallado para AWS Glue las tablas en función del usuario o grupo del IAM Identity Center.
- [Configure Amazon S3 Access Grants](#) para permitir el acceso temporal a las ubicaciones de datos subyacentes en S3.

 Note

Tanto Lake Formation como Amazon S3 Access Grants son necesarios para el control de acceso AWS Glue Data Catalog y para los resultados de las consultas de Athena en Amazon S3.

## Aplicaciones administradas por el cliente

Para permitir la propagación de identidades confiable para los usuarios de aplicaciones desarrolladas a medida, consulte [Acceder mediante Servicios de AWS programación mediante la propagación de identidades confiable en](#) el blog de seguridad.AWS

## Configuración de la propagación de identidades de confianza con los grupos de trabajo de Amazon Athena

El siguiente procedimiento le explica cómo configurar los grupos de trabajo de Amazon Athena para la propagación de identidades de confianza.

### Requisitos previos

Antes de empezar con este tutorial, tendrá que configurar lo siguiente:

1. [Habilite el Centro de identidades de IAM](#). Se recomienda [una instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).
2. [Aprovisione los usuarios y grupos de su fuente de identidades en el Centro de identidades de IAM](#).
3. Esta configuración requiere [Amazon EMR Studio](#) y [Amazon S3 Access](#) Grants. [AWS Lake Formation](#)

## Configuración de una propagación de identidad fiable con Athena

Para configurar la propagación de identidades de confianza con Athena, el administrador de Athena debe:

1. Revise [las consideraciones y limitaciones del uso de grupos de trabajo de Athena habilitados para IAM Identity Center](#).
2. [Cree un grupo de trabajo de Athena habilitado para el Centro de Identidad de IAM](#).

## Servicios de autorización

En todos los [casos de uso relacionados con el análisis y el almacenamiento de datos](#), puede lograr controles de acceso detallados mediante:

- AWS Lake Formation - para obtener orientación, consulte [Configuración AWS Lake Formation con IAM Identity Center](#)
- Amazon S3Access Grants: para obtener orientación, consulte [Configuración de las concesiones de acceso a Amazon S3 con el centro de identidad de IAM](#).

### Configuración AWS Lake Formation con IAM Identity Center

[AWS Lake Formation](#) es un servicio gestionado que simplifica la creación y la gestión de los lagos de datos en él. AWS Automatiza la recopilación, la catalogación y la seguridad de los datos, y proporciona un repositorio centralizado para almacenar y analizar diversos tipos de datos. Lake Formation ofrece controles de acceso detallados y se integra con varios servicios de AWS análisis, lo que permite a las organizaciones configurar, proteger y obtener información de manera eficiente de sus lagos de datos.

Siga estos pasos para permitir que Lake Formation conceda permisos de datos en función de la identidad del usuario mediante el IAM Identity Center y la propagación de identidades confiable.

### Requisitos previos

Antes de empezar con este tutorial, tendrás que configurar lo siguiente:

- [Habilite el Centro de identidades de IAM](#). Se recomienda [una instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).

### Pasos para configurar una propagación de identidad confiable

1. Integre IAM Identity Center AWS Lake Formation siguiendo las instrucciones de [Connecting Lake Formation con IAM Identity Center](#).

#### Important

Si no tiene AWS Glue Data Catalog tablas, debe crearlas para poder AWS Lake Formation utilizarlas para conceder acceso a los usuarios y grupos del IAM Identity

Center. Consulte [Crear objetos en AWS Glue Data Catalog](#) para obtener más información.

## 2. Registre las ubicaciones de los lagos de datos.

[Registre las ubicaciones S3 en](#) las que se almacenan los datos de las tablas de Glue. De este modo, Lake Formation proporcionará acceso temporal a las ubicaciones de S3 requeridas cuando se consulten las tablas, lo que eliminará la necesidad de incluir los permisos de S3 en la función de servicio (por ejemplo, la función de servicio de Athena configurada en WorkGroup la).

- Diríjase a las ubicaciones de los lagos de datos en la sección Administración del panel de navegación de la AWS Lake Formation consola. Seleccione Registrar ubicación.

Esto permitirá a Lake Formation proporcionar credenciales de IAM temporales con los permisos necesarios para acceder a las ubicaciones de datos de S3.

The screenshot shows the AWS Lake Formation console interface for registering a location. The breadcrumb navigation at the top indicates the path: AWS Lake Formation > Data lake locations > Register location. The main content area is titled 'Register location' and includes the following sections:

- Amazon S3 location:** A section with the instruction 'Register an Amazon S3 path as the storage location for your data lake.' It contains an 'Amazon S3 path' label and a text input field with the value 's3://awsids-albi-sandbox-storage'. A 'Browse' button is located to the right of the input field.
- Review location permissions - strongly recommended:** A section with a note about reviewing permissions and a 'Review location permissions' button.
- IAM role:** A section with a note about adding or updating data and a dropdown menu showing 'LakeFormationDataLocationRole'.
- Permission mode:** A section with a note about selecting a permission mode and two radio buttons: 'Hybrid access mode' (selected) and 'Lake Formation'.

At the bottom right of the form, there are 'Cancel' and 'Register location' buttons.

- Introduzca la ruta S3 de las ubicaciones de los datos de las AWS Glue tablas en el campo de ruta de Amazon S3.
- En la sección de funciones de IAM, no seleccione la función vinculada al servicio si quiere utilizarla con una propagación de identidades fiable. Cree un rol independiente con los siguientes permisos.

Para usar estas políticas, sustituya *italicized placeholder text* la política del ejemplo por su propia información. Para obtener instrucciones adicionales, consulte [Crear una política](#) o [Editar una política](#). La política de permisos debe permitir el acceso a la ubicación de S3 especificada en la ruta:

## i. Política de permisos:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3",
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket/*"
      ]
    },
    {
      "Sid": "LakeFormationDataAccessPermissionsForS3ListBucket",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::Your-S3-Bucket"
      ]
    },
    {
      "Sid": "LakeFormationDataAccessServiceRolePolicy",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ]
    }
  ]
}
```

- ii. Relación de confianza: debe incluir lo siguiente `sts:SectContext`, lo cual es obligatorio para la propagación de identidades confiables.



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "lakeformation.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetContext"
      ]
    }
  ]
}
```

 Note

La función de IAM creada por el asistente es una función vinculada a un servicio y no se incluye `sts:SetContext`

- d. Tras crear el rol de IAM, seleccione Registrar ubicación.

## Propagación de identidad confiable con Lake Formation across Cuentas de AWS

AWS Lake Formation admite el uso de [AWS Resource Access Manager \(RAM\)](#) para compartir tablas Cuentas de AWS y funciona con la propagación de identidades confiable cuando la cuenta del otorgante y la cuenta del concesionario están en la misma Región de AWS, en la misma instancia de la organización y comparten la misma instancia AWS Organizations organizativa del Centro de Identidad de IAM. Consulte [Intercambio de datos entre cuentas en Lake Formation](#) para obtener más información.

## Configuración de las concesiones de acceso a Amazon S3 con el centro de identidad de IAM

[Amazon S3 Access Grants](#) ofrece la flexibilidad necesaria para conceder un control de acceso detallado basado en la identidad a las ubicaciones de S3. Puede usar Amazon S3 Access Grants para conceder acceso al bucket de Amazon S3 directamente a sus usuarios y grupos corporativos.

Siga estos pasos para habilitar S3 Access Grants con el Centro de Identidad de IAM y lograr una propagación de identidades fiable.

## Requisitos previos

Antes de empezar con este tutorial, tendrás que configurar lo siguiente:

- [Habilite el Centro de identidades de IAM](#). Se recomienda [una instancia de organización](#). Para obtener más información, consulte [Requisitos y consideraciones previos](#).

Configurar S3 Access Grants para una propagación de identidad fiable a través del IAM Identity Center

Si ya tiene una Access Grants instancia de Amazon S3 con una ubicación registrada, siga estos pasos:

1. [Asocie su instancia de IAM Identity Center](#).
2. [Cree una subvención](#).

Si Access Grants aún no ha creado un Amazon S3, siga estos pasos:

1. [Crear una Access Grants instancia S3](#): puede crear una Access Grants instancia S3 por cada instancia Región de AWS. Cuando cree la Access Grants instancia S3, asegúrese de marcar la casilla Añadir instancia de IAM Identity Center y de proporcionar el ARN de su instancia de IAM Identity Center. Seleccione Siguiente.

La siguiente imagen muestra la página Crear Access Grants instancia S3 en la Access Grants consola de Amazon S3:

Step 1: Create S3 Access Grants instance

Step 2: Register S3 Buckets or prefixes as locations

Step 3: Create grant

Step 4: Review and finish

### Create S3 Access Grants instance

When you create your S3 Access Grants instance, you can use identities from your corporate directory or you can use IAM users and roles. This Access Grants instance serves as the container for your individual grants.

**S3 Access Grants instance**

**AWS Region**  
You can create one S3 Access Grants instance per AWS Region per account.  
US East (N. Virginia) us-east-1

☒ Add IAM Identity Center instance in US East (N. Virginia) us-east-1 - optional  
You can use an IAM Identity Center instance to specify identities from corporate directories. If you don't have an existing IAM Identity Center instance, you can add one after creating your S3 Access Grants instance.

**IAM Identity Center instance ARN**  
You can find the IAM Identity Center instance ARN in the [IAM Identity Center console](#).  
Enter IAM Identity Center instance ARN  
Format: arn:aws:sso::instance/<instanceid>

Choosing Next will create the S3 Access Grants instance and proceed to the next step.

Cancel Next

- Registrar una ubicación: después de crear y [crear una Access Grants instancia de Amazon S3](#) Región de AWS en una de su cuenta, [registra una ubicación S3](#) en esa instancia. Una Access Grants ubicación de S3 asigna la región S3 predeterminada (S3://), un depósito o un prefijo a un rol de IAM. S3 Access Grants asume esta función de Amazon S3 para vender credenciales temporales al concesionario que accede a esa ubicación en particular. Primero debe registrar al menos una ubicación en su Access Grants instancia de S3 antes de poder crear una concesión de acceso.

Para el ámbito de ubicaciones `s3://`, especifique, que incluye todos los depósitos de esa región. Este es el ámbito de ubicación recomendado para la mayoría de los casos de uso. Si tiene un caso de uso de administración de acceso avanzada, puede establecer el ámbito de ubicación en un depósito específico `s3://bucket` o en un prefijo dentro de un depósitos `s3://bucket/prefix-with-path`. Para obtener más información, consulte [Registrar una ubicación](#) en la Guía del usuario de Amazon Simple Storage Service.

#### Note

Asegúrese de que las ubicaciones S3 de las AWS Glue tablas a las que desea conceder acceso estén incluidas en esta ruta.

El procedimiento requiere que configure un rol de IAM para la ubicación. Esta función debe incluir permisos para acceder al ámbito de la ubicación. Puede usar el asistente de la consola S3 para crear el rol. Deberá especificar el ARN de su Access Grants instancia S3 en las políticas

de este rol de IAM. El valor predeterminado del ARN de la Access Grants instancia S3 es.  
`arn:aws:s3:Your-Region:Your-AWS-Account-ID:access-grants/default`

El siguiente ejemplo de política de permisos otorga a Amazon S3 permisos para el rol de IAM que ha creado. Y el ejemplo de política de confianza que aparece a continuación permite que el director del Access Grants servicio de S3 asuma la función de IAM.

a. Política de permisos

Para usar estas políticas, sustituya *italicized placeholder text* la política del ejemplo por su propia información. Para obtener instrucciones adicionales, consulte [Crear una política](#) o [Editar una política](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ObjectLevelReadPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:GetObjectVersion",
        "s3:GetObjectAcl",
        "s3:GetObjectVersionAcl",
        "s3:ListMultipartUploadParts"
      ],
      "Resource": [
        "arn:aws:s3:::*"
      ],
      "Condition": {
        "StringEquals": { "aws:ResourceAccount": "Your-AWS-Account-ID" },
        "ArnEquals": {
          "s3:AccessGrantsInstanceArn": [ "Your-Custom-Access-Grants-Location-ARN" ]
        }
      }
    },
    {
      "Sid": "ObjectLevelWritePermissions",
      "Effect": "Allow",
      "Action": [
```

```

        "s3:PutObject",
        "s3:PutObjectAcl",
        "s3:PutObjectVersionAcl",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:AbortMultipartUpload"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": { "aws:ResourceAccount": "Your-AWS-Account-ID" },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": ["Your-Custom-Access-Grants-Location-ARN"]
        }
    }
},
{
    "Sid": "BucketLevelReadPermissions",
    "Effect": "Allow",
    "Action": [
        "s3:ListBucket"
    ],
    "Resource": [
        "arn:aws:s3:::*"
    ],
    "Condition": {
        "StringEquals": { "aws:ResourceAccount": "Your-AWS-Account-ID" },
        "ArnEquals": {
            "s3:AccessGrantsInstanceArn": ["Your-Custom-Access-Grants-Location-ARN"]
        }
    }
},
//Optionally add the following section if you use SSE-KMS encryption
{
    "Sid": "KMSPermissions",
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": [

```

```

        "*"
    ]
}
]
}

```

## b. Política de confianza

En la política de confianza del rol de IAM, proporcione al servicio de Concesiones de acceso a Amazon S3 acceso de entidad principal (access-grants.s3.amazonaws.com) al rol de IAM que ha creado. Para ello, puede crear un archivo JSON que contenga las siguientes instrucciones. Para agregar la política de confianza a su cuenta, consulte [Creación de un rol mediante políticas de confianza personalizadas](#).

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1234567891011",
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": [
        "sts:AssumeRole",
        "sts:SetSourceIdentity"
      ],
      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "Your-AWS-Account-ID",
          "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
        }
      }
    },
    {
      "Sid": "Stmt1234567891012",
      "Effect": "Allow",
      "Principal": {
        "Service": "access-grants.s3.amazonaws.com"
      },
      "Action": "sts:SetContext",
      "Condition": {

```

```
    "StringEquals": {
      "aws:SourceAccount": "Your-AWS-Account-ID",
      "aws:SourceArn": "Your-Custom-Access-Grants-Location-ARN"
    },
    "ForAllValues:ArnEquals": {
      "sts:RequestContextProviders": "arn:aws:iam::aws:contextProvider/
IdentityCenter"
    }
  }
}
```

## Crear una concesión de acceso a Amazon S3

Si tiene una Access Grants instancia de Amazon S3 con una ubicación registrada y ha asociado su instancia del IAM Identity Center a ella, puede [crear una concesión](#). En la página de creación de subvenciones de la consola S3, complete lo siguiente:

### Crear una concesión

1. Seleccione la ubicación creada en el paso anterior. Puede reducir el alcance de la subvención añadiendo un subprefijo. El subprefijo puede ser un bucketbucket/prefix, o un objeto del depósito. Para obtener más información, consulte [Subprefijo](#) en la Guía del usuario de Amazon Simple Storage Service.
2. En Permisos y acceso, selecciona Leer o Escribir según tus necesidades.
3. En Tipo de otorgante, elija Identidad de directorio en el Centro de identidades de IAM.
4. Proporcione el ID de usuario o grupo del IAM Identity Center. Puede encontrar el usuario y el grupo IDs en la consola del IAM Identity Center, en las secciones [Usuario y Grupo](#). Seleccione Siguiente.
5. En la página Revisar y finalizar, revise la configuración del S3 Access Grant y, a continuación, seleccione Crear subvención.

La siguiente imagen muestra la página Create Grant en la Access Grants consola de Amazon S3:

**Create Grant** [Info](#)

**Grant** [Info](#)  
Grant a user or role a specific level of access to your S3 data.

**Grant scope**  
The grant scope is a combination of the location and the subprefix. Choose a registered location or register a new location. To narrow the scope, specify a subprefix. If you use the default "s3://" location, you must specify a subprefix.

**Location**  
s3:// [Browse locations](#) [Register location](#) [IAM role](#) [Info](#)  
[s3accessgrants\\_role\\_for\\_location\\_for\\_awsids-aiib-sandbox-storage](#)

**Subprefix - optional** [Info](#)  
Further scope the grant to a bucket, prefix, or an individual object.  
Format for bucket: <bucket>/\*  
Format for prefix: <bucket>/<prefix-with-path>/\*  
Format for object: <bucket>/<prefix-with-path>/<object>

**Grant scope** [Info](#)  
s3:// ☐ The grant scope is an object

**Permissions and access**  
Grant a user or role a specific level of access to your S3 data.  

The S3 console can't be used to access the data specified in the grant scope. To access the data, the grantee must do so through the AWS CLI, the application, or other AWS services.

**Permissions**  
☒ Read  
☐ Write

**Gantee type** [Info](#)  
☒ Directory identity from IAM Identity Center  
☐ IAM principal

**Directory identity type** [Info](#)  
☐ User  
☒ Group

**IAM Identity Center group ID** [Info](#)  
The group that you want to grant this level of access to. You can find the ID in the [IAM Identity Center console](#).

## Uso de la propagación de identidades de confianza con aplicaciones administradas por el cliente

La propagación de identidad confiable permite que una aplicación administrada por el cliente solicite acceso a los datos de AWS los servicios en nombre de un usuario. La administración del acceso a los datos se basa en la identidad del usuario, por lo que los administradores pueden conceder el acceso en función de la pertenencia actual de los usuarios a grupos y usuarios. La identidad del usuario, las acciones realizadas en su nombre y otros eventos se registran en registros y CloudTrail eventos específicos del servicio.

Con una propagación de identidad fiable, un usuario puede iniciar sesión en una aplicación gestionada por el cliente y esa aplicación puede transmitir la identidad del usuario en las solicitudes de acceso a los datos. Servicios de AWS

### Important

Para acceder a una Servicio de AWS, las aplicaciones gestionadas por el cliente deben obtener un token de un emisor de token de confianza, que sea externo al Centro de Identidad de IAM. Un emisor de tokens de confianza es un servidor de autorización OAuth 2.0 que crea tokens firmados. Estos tokens autorizan las aplicaciones que inician solicitudes de acceso a



Servicios de AWS (aplicaciones receptoras). Para obtener más información, consulte [Uso de aplicaciones con un emisor de tokens de confianza](#).

## Temas

- [Configure aplicaciones OAuth 2.0 administradas por el cliente para una propagación de identidad confiable](#)
- [Especificación de las aplicaciones de confianza](#)
- [Uso de aplicaciones con un emisor de tokens de confianza](#)

## Configure aplicaciones OAuth 2.0 administradas por el cliente para una propagación de identidad confiable

Para configurar una aplicación OAuth 2.0 gestionada por el cliente para la propagación de identidades de forma fiable, primero debe añadirla al Centro de identidades de IAM. Siga el procedimiento que se indica a continuación para agregar su aplicación a IAM Identity Center.

## Temas

- [Paso 1: selección del tipo de aplicación](#)
- [Paso 2: especificación de los detalles de la aplicación](#)
- [Paso 3: especificación de la configuración de autenticación](#)
- [Paso 4: especificación de las credenciales de la aplicación](#)
- [Paso 5: revisión y configuración](#)

### Paso 1: selección del tipo de aplicación

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.
4. Elija Agregar aplicación.
5. En la página Seleccionar el tipo de aplicación, en Preferencia de configuración, seleccione Tengo una aplicación que quiero configurar.
6. En Tipo de aplicación, elija OAuth 2.0.

7. Seleccione Siguiente para continuar a la página siguiente, [Paso 2: especificación de los detalles de la aplicación](#).

## Paso 2: especificación de los detalles de la aplicación

1. En la página Especificar detalles de la aplicación, en Nombre y descripción de la aplicación, ingrese un Nombre de visualización para la aplicación, como **MyApp**. Escriba una descripción en Descripción.
2. En Método de asignación de usuarios y grupos, seleccione una de las siguientes opciones:
  - Requerir asignaciones: permita que solo los usuarios y grupos de IAM Identity Center que estén asignados a esta aplicación accedan a la aplicación.

Visibilidad del mosaico de la aplicación: solo los usuarios que estén asignados a la aplicación directamente o mediante una asignación grupal pueden ver el mosaico de la aplicación en el portal de AWS acceso, siempre que la visibilidad de la aplicación en el portal de AWS acceso esté establecida en Visible.

- No requerir asignaciones: permita que todos los usuarios y grupos autorizados de IAM Identity Center accedan a esta aplicación.

Visibilidad del mosaico de la aplicación: el mosaico de la aplicación es visible para todos los usuarios que inician sesión en el portal de AWS acceso, a menos que la visibilidad de la aplicación en el portal de AWS acceso esté configurada como No visible.

3. En el portal de AWS acceso, introduzca la URL desde la que los usuarios pueden acceder a la aplicación y especifique si el icono de la aplicación estará visible o no en el portal de AWS acceso. Si selecciona No visible, ni siquiera los usuarios asignados podrán ver el icono de la aplicación.
4. Expanda Etiquetas (opcional), seleccione Agregar etiqueta nueva y especifique los valores de Clave y Valor (opcional).

Para obtener más información acerca de las etiquetas, consulte [Recursos de etiquetado AWS IAM Identity Center](#).

5. Seleccione Siguiente y pase a la página siguiente, [Paso 3: especificación de la configuración de autenticación](#).

### Paso 3: especificación de la configuración de autenticación

Para añadir una aplicación gestionada por el cliente que sea compatible con la OAuth versión 2.0 al IAM Identity Center, debe especificar un emisor de token de confianza. Un emisor de tokens de confianza es un servidor de autorización OAuth 2.0 que crea tokens firmados. Estos tokens autorizan a las aplicaciones que inician solicitudes (aplicaciones solicitantes) de acceso a aplicaciones administradas por AWS (aplicaciones receptoras).

1. En la página Especificar configuración de autenticación, en Emisores de tokens de confianza, realice una de las siguientes acciones:

- Para usar un emisor de tokens de confianza existente:

Seleccione la casilla de verificación situada junto al nombre del emisor de tokens de confianza que desea usar.

- Para agregar un nuevo emisor de tokens de confianza:

1. Seleccione Crear emisor de tokens de confianza.
2. Se abrirá una nueva pestaña del navegador. Siga los pasos del 5 al 8 que se indican en [Cómo agregar un emisor de tokens de confianza a la consola de IAM Identity Center](#).
3. Tras completar estos pasos, regrese a la ventana del navegador que está utilizando para configurar la aplicación y seleccione el emisor de tokens de confianza que acaba de agregar.
4. En la lista de emisores de tokens de confianza, seleccione la casilla de verificación situada junto al nombre del emisor de tokens de confianza que acaba de agregar.

Tras seleccionar un emisor de tokens de confianza, aparece la sección Configurar los emisores de tokens de confianza seleccionados.

2. En Configurar los emisores de tokens de confianza seleccionados, ingrese la notificación de audiencia. La notificación de audiencia identifica a la audiencia objetivo (destinatarios) del token que ha generado el emisor de tokens de confianza. Para obtener más información, consulte [Notificación de audiencia](#).
3. Para evitar que sus usuarios tengan que volver a autenticarse cuando utilicen esta aplicación, seleccione Habilitar la concesión de tokens de actualización. Si está seleccionada, esta opción actualiza el token de acceso de la sesión cada 60 minutos, hasta que la sesión caduque o el usuario la finalice.
4. Seleccione Siguiente y pase a la página siguiente, [Paso 4: especificación de las credenciales de la aplicación](#).

## Paso 4: especificación de las credenciales de la aplicación

Complete los pasos de este procedimiento para especificar las credenciales que la aplicación utilizará para realizar acciones de intercambio de tokens con aplicaciones de confianza. Estas credenciales se utilizan en una política basada en recursos. La política requiere que especifique una entidad principal que tenga permisos para realizar las acciones que se especifican en la política. Debe especificar una entidad principal, incluso si las aplicaciones de confianza se encuentran en la misma Cuenta de AWS.

### Note

Cuando establezca permisos con políticas, conceda solo los permisos necesarios para llevar a cabo una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos.

Esta política requiere la acción `sso-oauth:CreateTokenWithIAM`.

1. En la página Especificar las credenciales de la aplicación, lleve a cabo una de las siguientes acciones:
  - Para especificar rápidamente uno o varios roles de IAM:
    1. Seleccione Ingresar uno o más roles de IAM.
    2. En Ingresar roles de IAM, especifique el nombre de recurso de Amazon (ARN) de un rol de IAM existente. Para especificar el ARN, utilice la siguiente sintaxis. La parte de la región del ARN está en blanco porque los recursos de IAM son globales.

```
arn:aws:iam::account:role/role-name-with-path
```

Para obtener más información, consulte el artículo [Acceso entre cuentas mediante políticas basadas en recursos](#) e [IAM ARNs](#) en la Guía del usuario.AWS Identity and Access Management

- Para editar la política manualmente (obligatorio si no especificas credenciales):AWS
  1. Seleccione Editar la política de la aplicación.
  2. Para modificar la política, escriba o pegue texto en el cuadro de texto JSON.

3. Resuelva las advertencias de seguridad, errores o advertencias generales que hayan surgido durante la validación de la política. Para obtener más información, consulte [Validación de políticas de IAM](#) en la Guía del usuario de AWS Identity and Access Management .
2. Seleccione Siguiente y pase a la página siguiente, [Paso 5: revisión y configuración](#).

## Paso 5: revisión y configuración

1. En la página Revisar y configurar, revise las elecciones que ha realizado. Para realizar cambios, seleccione la sección de configuración que desee, seleccione Editar y, a continuación, realice los cambios necesarios.
2. Cuando haya terminado, seleccione Agregar aplicación.
3. La aplicación que ha agregado aparece en la lista Aplicaciones administradas por el cliente.
4. Tras configurar la aplicación gestionada por el cliente en el Centro de identidades de IAM, debe especificar una o más Servicios de AWS aplicaciones de confianza para la propagación de la identidad. Esto permite a los usuarios iniciar sesión en la aplicación administrada por el cliente y acceder a los datos de la aplicación de confianza.

Para obtener más información, consulte [Especificación de las aplicaciones de confianza](#) .

## Especificación de las aplicaciones de confianza

Tras [configurar la aplicación gestionada por el cliente](#), debe especificar uno o más AWS servicios o aplicaciones de confianza para la propagación de la identidad. Especifique un AWS servicio que contenga datos a los que los usuarios de las aplicaciones gestionadas por el cliente necesiten acceder. Cuando los usuarios inicien sesión en la aplicación administrada por el cliente, esa aplicación transferirá la identidad de los usuarios a la aplicación de confianza.

Utilice el siguiente procedimiento para seleccionar un servicio y, a continuación, especifique las aplicaciones individuales que son de confianza para ese servicio.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. Seleccione la pestaña Administrada por el cliente.

4. En la lista de aplicaciones administradas por el cliente, seleccione la aplicación OAuth 2.0 a la que desee iniciar las solicitudes de acceso. Esta es la aplicación en la que inician sesión los usuarios.
5. En la página de detalles, en Aplicaciones de confianza para la propagación de identidades, seleccione Especificar aplicaciones de confianza.
6. En Tipo de configuración, seleccione Aplicaciones individuales y acceso específico y, a continuación, seleccione Siguiente.
7. En la página Seleccionar servicio, seleccione el servicio de AWS que tenga aplicaciones en las que la aplicación administrada por el cliente pueda confiar para propagar identidades y, a continuación, seleccione Siguiente.

El servicio que seleccione define las aplicaciones que son de confianza. Seleccionará las aplicaciones en el siguiente paso.

8. En la página Seleccionar aplicaciones, seleccione Aplicaciones individuales, active la casilla de verificación de cada aplicación que pueda recibir solicitudes de acceso y, a continuación, seleccione Siguiente.
9. En la página Configurar el acceso, en Método de configuración, realice una de las siguientes acciones:
  - Seleccionar el acceso por aplicación: seleccione esta opción para configurar diferentes niveles de acceso para cada aplicación. Seleccione la aplicación para la que desee configurar el nivel de acceso y, a continuación, seleccione Editar acceso. En Nivel de acceso que aplicar, cambie los niveles de acceso según sea necesario y, a continuación, seleccione Guardar cambios.
  - Aplicar el mismo nivel de acceso a todas las aplicaciones: seleccione esta opción si no tiene que configurar los niveles de acceso por aplicación.
10. Elija Siguiente.
11. En la página Revisar configuración, revise las elecciones que ha realizado. Para realizar cambios, seleccione la sección de configuración que desee, seleccione Editar acceso y, a continuación, realice los cambios necesarios.
12. Cuando haya terminado, seleccione Aplicaciones de confianza.

## Uso de aplicaciones con un emisor de tokens de confianza

Los emisores de tokens confiables le permiten utilizar la propagación de identidades confiable con aplicaciones que se autentican fuera de ella. AWS Con los emisores de tokens de confianza, puede

autorizar a estas aplicaciones a realizar solicitudes en nombre de sus usuarios para acceder AWS a las aplicaciones gestionadas.

En los siguientes temas se describe cómo funcionan los emisores de tokens de confianza y se proporcionan instrucciones de configuración.

## Temas

- [Descripción general de los emisores de tokens de confianza](#)
- [Requisitos previos y consideraciones para los emisores de tokens de confianza](#)
- [Detalles de la notificación de JTI](#)
- [Ajustes de configuración de un emisor de tokens de confianza](#)
- [Configuración de un emisor de tokens de confianza](#)
- [Sesiones de rol de IAM con identidad mejorada](#)

## Descripción general de los emisores de tokens de confianza

La propagación de identidades fiable proporciona un mecanismo que permite a las aplicaciones que se autentican fuera del AWS sistema realizar solicitudes en nombre de sus usuarios mediante el uso de un emisor de token de confianza. Un emisor de tokens de confianza es un servidor de autorización OAuth 2.0 que crea tokens firmados. Estos tokens autorizan a las aplicaciones que inician solicitudes (solicitudes de solicitudes) de acceso a Servicios de AWS(aplicaciones receptoras). Las aplicaciones solicitantes inician las solicitudes de acceso en nombre de los usuarios que el emisor de tokens de confianza autentica. Tanto el emisor de tokens de confianza como IAM Identity Center conocen a los usuarios.

**Servicios de AWS** Las personas que reciben solicitudes gestionan la autorización detallada de sus recursos en función de sus usuarios y de la pertenencia a grupos, tal y como se muestran en el directorio de Identity Center. Servicios de AWS no pueden usar directamente los tokens del emisor externo del token.

Para resolver este problema, IAM Identity Center proporciona una forma para que la aplicación solicitante, o un controlador de AWS que utilice la aplicación solicitante, intercambie el token que emite el emisor de tokens de confianza por un token generado por IAM Identity Center. El token que genera IAM Identity Center hace referencia al usuario correspondiente de IAM Identity Center. La aplicación solicitante, o el controlador, utiliza el nuevo token para iniciar una solicitud a la aplicación receptora. Como el nuevo token hace referencia al usuario correspondiente de IAM Identity Center,

la aplicación receptora puede autorizar el acceso solicitado en función del usuario o de su grupo, tal como se representa en IAM Identity Center.

 Important

Elegir un servidor de autorización OAuth 2.0 para añadirlo como emisor de token de confianza es una decisión de seguridad que requiere una cuidadosa consideración. Seleccione únicamente emisores de tokens de confianza para realizar las siguientes tareas:

- Autenticar al usuario especificado en el token.
- Autorizar el acceso de ese usuario a la aplicación receptora.
- Generar un token que IAM Identity Center pueda intercambiar por un token creado por IAM Identity Center.

## Requisitos previos y consideraciones para los emisores de tokens de confianza

Antes de configurar un emisor de tokens de confianza, revise los siguientes requisitos previos y consideraciones.

- Configuración de un emisor de tokens de confianza

Debe configurar un servidor de autorización OAuth 2.0 (el emisor de token de confianza). Aunque el emisor del token de confianza suele ser el proveedor de identidad que utilizas como fuente de identidad para el IAM Identity Center, no tiene por qué serlo. Para ver instrucciones sobre cómo configurar el emisor de tokens de confianza, consulte la documentación del proveedor de identidades correspondiente.

 Note

Puede configurar hasta 10 emisores de tokens de confianza para utilizarlos con IAM Identity Center, siempre que asigne la identidad de cada usuario del emisor de tokens de confianza a un usuario correspondiente de IAM Identity Center.

- El servidor de autorización OAuth 2.0 (el emisor del token de confianza) que crea el token debe tener un punto final de descubrimiento [OpenID Connect \(OIDC\)](#) que IAM Identity Center pueda utilizar para obtener claves públicas para verificar las firmas del token. Para obtener más información, consulte [URL del punto de conexión de detección de OIDC \(URL del emisor\)](#).



- Tokens emitidos por el emisor de tokens de confianza

Los tokens del emisor de tokens de confianza deben cumplir los siguientes requisitos:

- El token debe estar firmado y en [formato JSON Web Token \(JWT\)](#) mediante el algoritmo. RS256
- El token debe contener las siguientes afirmaciones:
  - [Emisor](#) (iss): la entidad que emitió el token. Este valor debe coincidir con el valor que está configurado en el punto de conexión de detección del OIDC (URL del emisor) en el emisor del token de confianza.
  - [Sujeto](#) (sub): el usuario autenticado.
  - [Público](#) (aud): el destinatario previsto del token. Es a lo Servicio de AWS que se accederá después de cambiar el token por un token del Centro de Identidad de IAM. Para obtener más información, consulte [Notificación de audiencia](#).
  - [Tiempo de caducidad](#) (exp): el tiempo después del cual caduca el token.
- El token puede ser un token de identidad o un token de acceso.
- El token debe tener un atributo que pueda asignarse de forma exclusiva a un usuario de IAM Identity Center.

 Note

No se admite el uso de una clave JWTs de Microsoft Entra ID firma personalizada para «from». Para usar fichas de un emisor Microsoft Entra ID de fichas de confianza, no puedes usar una clave de firma personalizada.

- Notificaciones opcionales

IAM Identity Center admite todas las notificaciones opcionales que se definen en RFC 7523. Para obtener más información, consulte la [sección 3: JWT Format and Processing Requirements](#) de esta RFC.

Por ejemplo, el token puede contener una [notificación de JTI \(ID de JWT\)](#). Esta notificación, cuando está presente, impide que los tokens que tienen el mismo JTI se reutilicen para el intercambio de tokens. Para obtener más información acerca de las notificaciones de JTI, consulte [Detalles de la notificación de JTI](#).

- Configuración de IAM Identity Center para que funcione con un emisor de tokens de confianza

También debe habilitar IAM Identity Center, configurar el origen de identidad de IAM Identity Center y aprovisionar a los usuarios que correspondan a los usuarios del directorio del emisor de tokens de confianza.

Para ello, debe hacer una de las siguientes acciones:

- Sincronice los usuarios con IAM Identity Center mediante el protocolo del sistema de administración de identidades entre dominios (SCIM) 2.0.
- Cree los usuarios directamente en IAM Identity Center.

## Detalles de la notificación de JTI

Si IAM Identity Center recibe una solicitud para intercambiar un token que IAM Identity Center ya ha intercambiado, se produce un error en la solicitud. Para detectar e impedir la reutilización de un token para los intercambios de tokens, puede incluir una notificación de JTI. IAM Identity Center protege contra la repetición de tokens en función de las notificaciones que figuran en el token.

No todos los servidores de autorización OAuth 2.0 añaden una declaración de JTI a los tokens. Es posible que algunos servidores de autorización OAuth 2.0 no te permitan añadir una JTI como afirmación personalizada. OAuth Los servidores de autorización 2.0 que admiten el uso de una declaración de JTI pueden añadir esta afirmación únicamente a los tokens de identidad, solo a los de acceso o a ambos. Para obtener más información, consulte la documentación de su servidor de autorización OAuth 2.0.

Para obtener información sobre cómo crear aplicaciones que intercambien tokens, consulte la documentación de la API de IAM Identity Center. Para obtener información sobre cómo configurar una aplicación administrada por el cliente para obtener e intercambiar los tokens correctos, consulte la documentación de la aplicación.

## Ajustes de configuración de un emisor de tokens de confianza

En las siguientes secciones se describen los ajustes necesarios para configurar y utilizar un emisor de tokens de confianza.

### Temas

- [URL del punto de conexión de detección de OIDC \(URL del emisor\)](#)
- [Mapeo de atributos](#)
- [Notificación de audiencia](#)

## URL del punto de conexión de detección de OIDC (URL del emisor)

Al agregar un emisor de tokens de confianza a la consola de IAM Identity Center, debe especificar la URL del punto de conexión de detección de OIDC. Se suele hacer referencia a esta URL por su URL relativa, `/.well-known/openid-configuration`. En la consola de IAM Identity Center, esta URL se denomina URL del emisor.

### Note

Debe pegar la URL del punto de conexión de detección hasta que no aparezca `.well-known/openid-configuration`. Si `.well-known/openid-configuration` se incluye en la URL, la configuración del emisor del token de confianza no funcionará. Como el IAM Identity Center no valida esta URL, si la URL no está formada correctamente, la configuración del emisor de token de confianza fallará sin notificación.

Solo se debe poder acceder a la URL del punto de conexión de detección del OIDC a través de los puertos 80 y 443.

IAM Identity Center utiliza esta URL para obtener información adicional sobre el emisor de tokens de confianza. Por ejemplo, IAM Identity Center utiliza esta URL para obtener la información necesaria para verificar los tokens que genera el emisor de tokens de confianza. Al agregar un emisor de tokens de confianza a IAM Identity Center, debe especificar esta URL. Para encontrar la URL, consulte la documentación del proveedor del servidor de autorización OAuth 2.0 que utilice para generar los tokens para su aplicación o póngase en contacto directamente con el proveedor para obtener ayuda.

## Mapeo de atributos

Las asignaciones de atributos permiten que IAM Identity Center vincule el usuario representado en un token emitido por un emisor de tokens de confianza con un único usuario de IAM Identity Center. Debe especificar la asignación de atributos al agregar el emisor de tokens de confianza a IAM Identity Center. Esta asignación de atributos se utiliza en una notificación del token que ha generado el emisor de tokens de confianza. El valor de la notificación se utiliza para buscar en IAM Identity Center. La búsqueda utiliza el atributo especificado para recuperar un único usuario de IAM Identity Center, que se utilizará como el usuario de AWS. La notificación que elija debe asignarse a un atributo de una lista fija de atributos disponibles en el almacén de identidades de IAM Identity Center. Puede elegir uno de los siguientes atributos del almacén de identidades de IAM Identity

Center: nombre de usuario, correo electrónico e ID externo. El valor del atributo que especifique en IAM Identity Center debe ser único para cada usuario.

## Notificación de audiencia

Las notificaciones de audiencia identifican a la audiencia (destinatarios) a la que se destina un token. Cuando la aplicación que solicita el acceso se autentica a través de un proveedor de identidades que no está federado en IAM Identity Center, dicho proveedor de identidades debe configurarse como un emisor de tokens de confianza. La aplicación que recibe la solicitud de acceso (la aplicación receptora) debe cambiar el token que ha generado el emisor de tokens de confianza por un token que haya generado IAM Identity Center.

Para obtener información sobre cómo obtener los valores de la notificación de audiencia para la aplicación receptora tal como están registrados en el emisor de tokens de confianza, consulte la documentación del emisor de tokens de confianza o póngase en contacto con el administrador del emisor de tokens de confianza para obtener ayuda.

## Configuración de un emisor de tokens de confianza

Para habilitar la propagación de identidades de confianza en una aplicación que se autentica externamente en IAM Identity Center, uno o más administradores deben configurar un emisor de tokens de confianza. Un emisor de tokens de confianza es un servidor de autorización OAuth 2.0 que emite tokens a las aplicaciones que inician solicitudes (solicitudes de solicitudes). Los tokens autorizan a estas aplicaciones a iniciar solicitudes en nombre de sus usuarios a una aplicación o aplicaciones receptoras Servicio de AWS.

## Temas

- [Coordinación de los roles y responsabilidades de administración](#)
- [Tareas para configurar un emisor de tokens de confianza](#)
- [Cómo agregar un emisor de tokens de confianza a la consola de IAM Identity Center](#)
- [Cómo ver o editar la configuración del emisor de tokens de confianza en la consola de IAM Identity Center](#)
- [Proceso de configuración y flujo de solicitud para las aplicaciones que utilizan un emisor de tokens de confianza](#)

## Coordinación de los roles y responsabilidades de administración

En algunos casos, un único administrador puede realizar todas las tareas necesarias para configurar un emisor de tokens de confianza. Si varios administradores realizan estas tareas, es necesario que haya una estrecha coordinación. En la siguiente tabla se describe cómo varios administradores pueden coordinarse para configurar un emisor de token de confianza y configurar el AWS servicio para usarlo.

### Note

La aplicación puede ser cualquier AWS servicio que esté integrado con el Centro de Identidad de IAM y permita la propagación de identidades de forma fiable.

Para obtener más información, consulte [Tareas para configurar un emisor de tokens de confianza](#).

| Rol                                                           | Realiza estas tareas                                                                                                                                                                                                                                                                                                                                    | Se coordina con                                                                                            |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| Administrador del IAM Identity Center                         | <p>Agrega el IdP externo como emisor de tokens de confianza a la consola de IAM Identity Center.</p> <p>Ayuda a configurar la asignación de atributos correcta entre IAM Identity Center y el IdP externo.</p> <p>Notifica al administrador del AWS servicio cuando el emisor del token de confianza se añade a la consola del IAM Identity Center.</p> | <p>Administrador del IdP externo (emisor de tokens de confianza)</p> <p>AWS administrador del servicio</p> |
| Administrador del IdP externo (emisor de tokens de confianza) | <p>Configura el IdP externo para emitir los tokens.</p> <p>Ayuda a configurar la asignación de atributos correcta entre IAM Identity Center y el IdP externo.</p>                                                                                                                                                                                       | <p>Administrador del IAM Identity Center</p> <p>AWS administrador de servicios</p>                         |

| Rol                            | Realiza estas tareas                                                                                                                                                                                                                                                                                                                                  | Se coordina con                                                                                                   |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
|                                | Proporciona el nombre de la audiencia (notificación de audiencia ) al administrador del servicio de AWS .                                                                                                                                                                                                                                             |                                                                                                                   |
| AWS administrador de servicios | <p>Busca en la consola AWS de servicio el emisor del token de confianza. El emisor del token de confianza estará visible en la consola de AWS servicio después de que el administrador del IAM Identity Center lo añada a la consola del IAM Identity Center.</p> <p>Configura el AWS servicio para que utilice el emisor del token de confianza.</p> | <p>Administrador del IAM Identity Center</p> <p>Administrador del IdP externo (emisor de tokens de confianza)</p> |

### Tareas para configurar un emisor de tokens de confianza

Para configurar un emisor de tokens de confianza, un administrador de IAM Identity Center, un administrador del IdP externo (emisor de tokens de confianza) y un administrador de aplicaciones deben realizar las siguientes tareas.

#### Note

La aplicación puede ser cualquier AWS servicio que esté integrado con el IAM Identity Center y permita la propagación de identidades de forma fiable.

1. Agregue el emisor de token de confianza al Centro de Identidad de IAM: el administrador del Centro de Identidad de IAM [agrega el emisor de token de confianza mediante la consola del Centro de Identidad de IAM](#) o. [APIs](#) Esta configuración requiere especificar lo siguiente:
  - El nombre del emisor de tokens de confianza.

- La URL del punto de conexión de detección de OIDC (en la consola de IAM Identity Center, esta URL se denomina URL del emisor). Solo se debe poder acceder al punto de conexión de detección a través de los puertos 80 y 443.
  - Asignación de atributos para la búsqueda de usuarios. Esta asignación de atributos se utiliza en una notificación del token que ha generado el emisor de tokens de confianza. El valor de la notificación se utiliza para buscar en IAM Identity Center. La búsqueda utiliza el atributo especificado para recuperar un único usuario en IAM Identity Center.
2. Conectar el AWS servicio al IAM Identity Center: el administrador del AWS servicio debe conectar la aplicación al IAM Identity Center mediante la consola de la aplicación o la aplicación. APIs

Una vez que el emisor del token de confianza se haya añadido a la consola del IAM Identity Center, también estará visible en la consola de AWS servicio y estará disponible para que el administrador del AWS servicio lo seleccione.

3. Configure el uso del intercambio de tokens: en la consola de AWS servicio, el administrador del AWS servicio configura el AWS servicio para que acepte los tokens emitidos por el emisor de token de confianza. Estos tokens se intercambian por tokens que ha generado IAM Identity Center. Para ello, es necesario especificar el nombre del emisor de los tokens de confianza del paso 1 y el valor de reclamación en AUD que corresponde al servicio. AWS

El emisor del token de confianza coloca el valor reclamado en AUD en el token que emite para indicar que el token está destinado a ser utilizado por el AWS servicio. Para obtener este valor, póngase en contacto con el administrador del emisor de tokens de confianza.

## Cómo agregar un emisor de tokens de confianza a la consola de IAM Identity Center

En una organización que tiene varios administradores, esta tarea la realiza un administrador de IAM Identity Center. Si es el administrador de IAM Identity Center, debe elegir qué IdP externo desea utilizar como emisor de tokens de confianza.

Para agregar un emisor de tokens de confianza a la consola de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En Emisores de tokens de confianza, seleccione Crear emisor de tokens de confianza.

5. En la página Configurar un IdP externo para emitir tokens de confianza, en Detalles del emisor del token de confianza, haga lo siguiente:
    - En la URL del emisor, especifique la [URL de detección de OIDC](#) del IdP externo que emitirá los tokens para la propagación de identidades confiables. Debe especificar la URL del punto de conexión de detección hasta el momento sin `.well-known/openid-configuration`. El administrador del IdP externo puede proporcionar esta URL.
-  **Note**

Nota: Esta URL debe coincidir con la URL de la afirmación del emisor (iss) en los tokens que se emiten para la propagación de identidades confiables.
- En Nombre del emisor de tokens de confianza, ingrese un nombre para identificar a este emisor de tokens de confianza en IAM Identity Center y en la consola de la aplicación.
6. En Asignar atributos, haga lo siguiente:
  - En Atributo de proveedor de identidad, seleccione un atributo de la lista para asignarlo a un atributo del almacén de identidades de IAM Identity Center.
  - En Atributo de IAM Identity Center, seleccione el atributo correspondiente para la asignación de atributos.
7. En Etiquetas (opcional), seleccione Agregar etiqueta nueva y especifique un valor para Clave y, si lo desea, para Valor.

Para obtener más información acerca de las etiquetas, consulte [Recursos de etiquetado AWS IAM Identity Center](#).

8. Seleccione Crear emisor de tokens de confianza.
9. Cuando termine de crear el emisor de tokens de confianza, póngase en contacto con el administrador de la aplicación para que sepa el nombre del emisor de tokens de confianza y así pueda confirmar que está visible en la consola correspondiente.
10. El administrador de la aplicación debe seleccionar este emisor de tokens de confianza en la consola correspondiente para permitir que los usuarios accedan a la aplicación desde las aplicaciones que están configuradas para la propagación de identidades de confianza.



## Cómo ver o editar la configuración del emisor de tokens de confianza en la consola de IAM Identity Center

Tras agregar un emisor de tokens de confianza a la consola de IAM Identity Center, podrá ver y editar la configuración correspondiente.

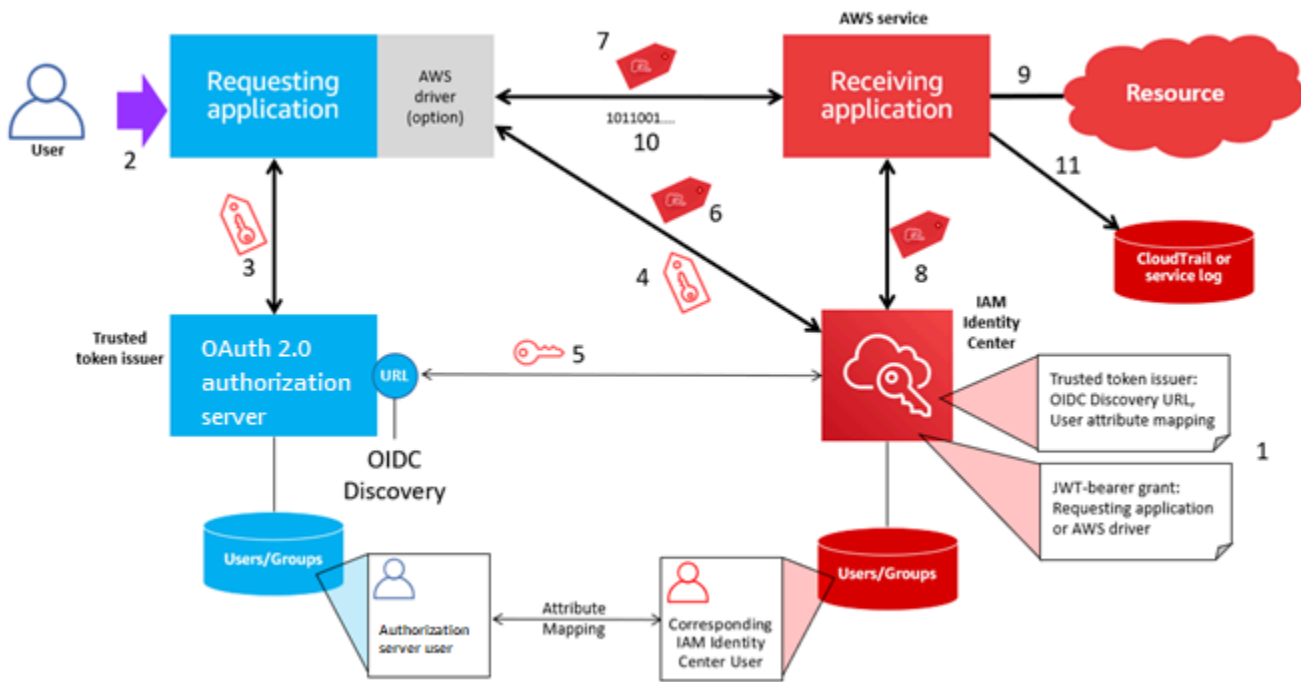
Si tiene previsto editar la configuración del emisor de tokens de confianza, tenga en cuenta que si lo hace, los usuarios podrían perder el acceso a cualquier aplicación que esté configurada para utilizar el emisor de tokens de confianza. Para evitar interrumpir el acceso de los usuarios, le recomendamos que se ponga en contacto con los administradores de cualquier aplicación que esté configurada para usar el emisor de tokens de confianza antes de editar la configuración.

Para visualizar o editar la configuración del emisor de tokens de confianza en la consola de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Autenticación.
4. En Emisores de tokens de confianza, seleccione el emisor de tokens de confianza que desee ver o editar.
5. Seleccione Acciones y, a continuación, Editar.
6. En la página Editar emisor de tokens de confianza, consulte o edite la configuración según sea necesario. Puede editar el nombre del emisor de tokens de confianza, las asignaciones de atributos y las etiquetas.
7. Seleccione Save changes (Guardar cambios).
8. En el cuadro de diálogo Editar emisor de tokens de confianza, se le pedirá que confirme que desea realizar cambios. Elija Confirmar.

## Proceso de configuración y flujo de solicitud para las aplicaciones que utilizan un emisor de tokens de confianza

En esta sección se describe el proceso de configuración y el flujo de solicitud para las aplicaciones que utilizan un emisor de tokens de confianza para la propagación de identidades de confianza. En el diagrama siguiente se proporciona una descripción general de este proceso.



En los pasos siguientes tiene más información sobre este proceso.

1. Configure el Centro de identidad de IAM y la aplicación AWS gestionada de recepción para utilizar un emisor de token de confianza. Para obtener información, consulte [Tareas para configurar un emisor de tokens de confianza](#).
2. El flujo de solicitud comienza cuando un usuario abre la aplicación solicitante.
3. La aplicación solicitante solicita un token al emisor del token de confianza para iniciar las solicitudes a la aplicación gestionada receptora AWS. Si el usuario aún no se ha autenticado, este proceso desencadena un flujo de autenticación. El token contiene la siguiente información:
  - El asunto del usuario.
  - El atributo que IAM Identity Center utiliza para buscar al usuario correspondiente en IAM Identity Center.
  - Una notificación de audiencia que contiene un valor que el emisor de tokens de confianza asocia a la aplicación administrada por AWS receptora. Si hay otras notificaciones, IAM Identity Center no las utiliza.
4. La aplicación solicitante, o el AWS controlador que utiliza, pasa el token al Centro de Identidad de IAM y solicita que se cambie por un token generado por el Centro de Identidad de IAM. Si utiliza un controlador de AWS, es posible que tenga que configurarlo para este caso de uso. Para obtener más información, consulte la documentación de la aplicación AWS gestionada correspondiente.

5. IAM Identity Center utiliza el punto de conexión de detección de OIDC para obtener la clave pública que puede utilizar para verificar la autenticidad del token. A continuación, IAM Identity Center hace lo siguiente:
  - Verifica el token.
  - Busca en el directorio de Identity Center. Para ello, IAM Identity Center utiliza el atributo asignado que se especifica en el token.
  - Verifica que el usuario está autorizado para acceder a la aplicación receptora. Si la aplicación AWS gestionada está configurada para requerir asignaciones a usuarios y grupos, el usuario debe tener una asignación directa o basada en grupos a la aplicación; de lo contrario, se deniega la solicitud. Si la aplicación AWS gestionada está configurada para no requerir asignaciones de usuarios y grupos, el procesamiento continúa.

 Note

AWS los servicios tienen una configuración predeterminada que determina si las asignaciones son necesarias para los usuarios y los grupos. Le recomendamos que no modifique la configuración Requerir asignaciones de estas aplicaciones si tiene previsto utilizarlas con la propagación de identidades de confianza. Incluso si ha configurado permisos detallados que permiten a los usuarios acceder a recursos de la aplicación específica, la modificación de la configuración Requerir asignaciones puede provocar un comportamiento inesperado, como la interrupción del acceso de los usuarios a estos recursos.

- Comprueba que la aplicación solicitante esté configurada para utilizar ámbitos válidos para la aplicación AWS gestionada receptora.
6. Si los pasos de verificación anteriores se realizan correctamente, IAM Identity Center creará un nuevo token. El nuevo token es un token opaco (cifrado) que incluye la identidad del usuario correspondiente en el Centro de Identidad de IAM, la audiencia (AUD) de la aplicación AWS gestionada receptora y los ámbitos que la aplicación solicitante puede utilizar al realizar solicitudes a la aplicación gestionada receptora. AWS
  7. La aplicación solicitante, o el controlador que utiliza, inicia una solicitud de recursos a la aplicación receptora y pasa el token que IAM Identity Center generó a la aplicación receptora.
  8. La aplicación receptora realiza llamadas a IAM Identity Center para obtener la identidad del usuario y los ámbitos codificados en el token. También puede realizar solicitudes para obtener los atributos del usuario o la pertenencia del usuario a grupos desde el directorio de Identity Center.

9. La aplicación receptora utiliza su configuración de autorización para determinar si el usuario está autorizado a acceder al recurso de la aplicación solicitado.
10. Si el usuario está autorizado a acceder al recurso de la aplicación solicitado, la aplicación receptora responde a la solicitud.
11. La identidad del usuario, las acciones realizadas en su nombre y otros eventos se registran en los registros y CloudTrail eventos de la aplicación receptora. La forma específica en que se registra esta información varía en función de la aplicación.

## Sesiones de rol de IAM con identidad mejorada

El [AWS Security Token Service](#) (STS) permite a una aplicación obtener una sesión de rol de IAM con identidad mejorada. Las sesiones de rol con identidad mejorada tienen un contexto de identidad adicional que incluye un identificador de usuario al que llaman. Servicio de AWS Servicios de AWS puede buscar las pertenencias a los grupos y los atributos del usuario en el Centro de Identidad de IAM y utilizarlos para autorizar el acceso del usuario a los recursos.

AWS las aplicaciones obtienen sesiones de roles con una identidad mejorada realizando solicitudes a la acción de la AWS STS [AssumeRole](#) API y pasando una afirmación de contexto con el identificador del usuario (userId) en el `ProvidedContexts` parámetro de la solicitud a. `AssumeRole` La afirmación de contexto se obtiene de la `idToken` reclamación recibida en respuesta a una solicitud dirigida a. SSO O IDC [CreateTokenWithIAM](#) Cuando una AWS aplicación utiliza una sesión de rol con identidad mejorada para acceder a un recurso, CloudTrail registra la `userId` sesión de inicio y la acción realizada. Para obtener más información, consulte [Registro de sesiones de rol de IAM con identidad mejorada](#).

## Temas

- [Tipos de sesiones de rol de IAM con identidad mejorada](#)
- [Registro de sesiones de rol de IAM con identidad mejorada](#)

## Tipos de sesiones de rol de IAM con identidad mejorada

AWS STS puede crear dos tipos diferentes de sesiones de rol de IAM con identidad mejorada, en función de la afirmación de contexto proporcionada a la solicitud. `AssumeRole` Las aplicaciones que hayan obtenido fichas de identificación del Centro de Identidad de IAM pueden añadir `sts:identity_context` (se recomienda) o `sts:audit_context` (se admiten por motivos de compatibilidad con versiones anteriores) a las sesiones de roles de IAM. Una sesión de rol de IAM con identidad mejorada solo puede tener una de estas afirmaciones de contexto, no ambas.

## Sesiones de rol de IAM con identidad mejorada creadas mediante **sts:identity\_context**

Cuando una sesión de rol con identidad mejorada contiene `sts:identity_context` la llamada, Servicio de AWS determina si la autorización del recurso se basa en el usuario que está representado en la sesión de rol o si se basa en el rol. Servicios de AWS que admiten la autorización basada en el usuario proporcionan al administrador de la aplicación controles para asignar el acceso al usuario o a los grupos de los que el usuario es miembro.

Servicios de AWS que no admitan la autorización basada en el usuario ignoran la.

`sts:identity_context` CloudTrail registra el `USERID` del usuario del Centro de Identidad de IAM con todas las acciones realizadas por el rol. Para obtener más información, consulte [Registro de sesiones de rol de IAM con identidad mejorada](#).

Para obtener este tipo de sesión de rol con identidad mejorada AWS STS, las aplicaciones proporcionan el valor del `sts:identity_context` campo de la solicitud mediante el parámetro de [AssumeRoles](#)solicitud. `ProvidedContexts` Utilice `arn:aws:iam::aws:contextProvider/IdentityCenter` como valor para `ProviderArn`.

Para obtener más información sobre el comportamiento de la autorización, consulte la documentación relativa a la recepción. Servicio de AWS

## Sesiones de rol de IAM con identidad mejorada creadas mediante **sts:audit\_context**

En el pasado, se `sts:audit_context` utilizaba Servicios de AWS para permitir el registro de la identidad del usuario sin utilizarla para tomar una decisión de autorización. Servicios de AWS ahora pueden usar un único contexto: `sts:identity_context` - para lograrlo y para tomar decisiones de autorización. Recomendamos utilizarla `sts:identity_context` en todas las nuevas implementaciones de propagación de identidad confiable.

### Registro de sesiones de rol de IAM con identidad mejorada

Cuando se realiza una solicitud a una Servicio de AWS sesión de rol de IAM con identidad mejorada, se inicia sesión en el elemento en el centro `userId` de identidad de IAM del usuario. CloudTrail `OnBehalfOf` La forma en que se registran los eventos CloudTrail varía en función del. Servicio de AWS No todos los Servicios de AWS registran el elemento `onBehalfOf`.

A continuación se muestra un ejemplo de cómo se inicia sesión en una sesión de rol con identidad mejorada. Servicio de AWS CloudTrail

```
"userIdentity": {
  "type": "AssumedRole",
```

```
{
  "principalId": "AROEXAMPLE:MyRole",
  "arn": "arn:aws:sts::111111111111:assumed-role/MyRole/MySession",
  "accountId": "111111111111",
  "accessKeyId": "ASIAEXAMPLE",
  "sessionContext": {
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROEXAMPLE",
      "arn": "arn:aws:iam::111111111111:role/MyRole",
      "accountId": "111111111111",
      "userName": "MyRole"
    },
    "attributes": {
      "creationDate": "2023-12-12T13:55:22Z",
      "mfaAuthenticated": "false"
    }
  },
  "onBehalfOf": {
    "userId": "11111111-1111-1111-1111-111111111111",
    "identityStoreArn": "arn:aws:identitystore::111111111111:identitystore/d-1111111111"
  }
}
```

## Rotación de certificados de IAM Identity Center

IAM Identity Center utiliza certificados para establecer una relación de confianza de SAML entre IAM Identity Center y el proveedor de servicios de la aplicación. Al añadir una aplicación al IAM Identity Center, se crea automáticamente un certificado de IAM Identity Center para usarlo con esa aplicación durante el proceso de configuración. De forma predeterminada, este certificado de IAM Identity Center generado automáticamente es válido durante un período de 5 años.

Como administrador de IAM Identity Center, en ocasiones tendrá que sustituir los certificados antiguos de una aplicación por otros más nuevos. Por ejemplo, puede que tenga que sustituir un certificado cuando se aproxime la fecha de vencimiento del certificado. El proceso de sustituir un certificado antiguo por uno más nuevo se denomina rotación de certificados.

## Consideraciones antes de rotar un certificado

Antes de iniciar el proceso de rotación de un certificado en IAM Identity Center, tenga en cuenta lo siguiente:

- El proceso de rotación de certificaciones requiere que se restablezca la relación de confianza entre IAM Identity Center y el proveedor de servicios. Para restablecer la relación de confianza, utilice los procedimientos que se proporcionan en [Rotación de un certificado de IAM Identity Center](#).
- La actualización del certificado con el proveedor de servicios puede provocar una interrupción temporal del servicio para los usuarios hasta que la relación de confianza se restablezca correctamente. Si es posible, planifique esta operación cuidadosamente durante las horas de menor actividad.

## Rotación de un certificado de IAM Identity Center

La rotación de un certificado de IAM Identity Center es un proceso de varios pasos que incluye lo siguiente:

- Generación de un nuevo certificado
- Adición del nuevo certificado al sitio web del proveedor de servicios
- Configuración del nuevo certificado como activo
- Eliminación del certificado inactivo

Utilice todos los procedimientos siguientes en el orden que se indica a continuación para completar el proceso de rotación de certificados para una solicitud determinada:

### Paso 1: generar un nuevo certificado

Los nuevos certificados de IAM Identity Center que genere se pueden configurar para que utilicen las siguientes propiedades:

- **Período de validez:** especifica el tiempo asignado (en meses) antes de que caduque un nuevo certificado de IAM Identity Center.
- **Tamaño de la clave:** determina el número de bits que debe utilizar una clave con su algoritmo criptográfico. Puede establecer este valor en RSA de 1024 bits o RSA de 2048 bits. Para obtener información general sobre cómo funcionan los tamaños de clave en criptografía, consulte [Tamaño de clave](#).
- **Algoritmo:** especifica el algoritmo que IAM Identity Center utiliza al firmar la aserción/respuesta de SAML. Puede establecer este valor en SHA-1 o SHA-256. AWS recomienda utilizar el SHA-256 siempre que sea posible, a menos que su proveedor de servicios requiera el SHA-1. Para obtener

información general sobre cómo funcionan los algoritmos de criptografía, consulte [Criptografía de clave pública](#).

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, elija la aplicación para la que desee generar un nuevo certificado.
4. En la página de detalles de la aplicación, elija la pestaña Configuración. En Metadatos de IAM Identity Center, seleccione Administrar certificado. Si no tiene una pestaña Configuración o el ajuste de configuración no está disponible, no tiene que rotar el certificado de esta aplicación.
5. En la página de certificados de IAM Identity Center, seleccione Generar un certificado nuevo.
6. En el cuadro de diálogo Generar un nuevo certificado de IAM Identity Center, especifique los valores adecuados para el período de validez, el algoritmo y el tamaño de clave. A continuación, elija Generar.

## Paso 2: actualizar el sitio web del proveedor de servicios

Utilice el siguiente procedimiento para restablecer la relación de confianza con el proveedor de servicios de la aplicación.

### Important

Al cargar el nuevo certificado al proveedor de servicios, es posible que los usuarios no puedan autenticarse. Para corregir esta situación, configure el nuevo certificado como activo como se describe en el paso siguiente.

1. En la [consola de IAM Identity Center](#), elija la aplicación para la que acaba de generar un nuevo certificado.
2. En la página de detalles de la aplicación, elija la pestaña Configuración.
3. Seleccione Ver instrucciones y, a continuación, siga las instrucciones del sitio web específico del proveedor de servicios de aplicaciones para añadir el certificado recién generado.



## Paso 3: configurar el nuevo certificado como activo

Una aplicación puede tener asignados hasta dos certificados. IAM Identity Center utilizará el certificado que esté establecido como activo para firmar todas las aserciones de SAML.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, elija su aplicación.
4. En la página de detalles de la aplicación, elija la pestaña Configuración. En los Metadatos de IAM Identity Center, seleccione Administrar certificado.
5. En la página de certificados de IAM Identity Center, seleccione el certificado que desee configurar como activo, elija Acciones y, a continuación, Establecer como activo.
6. En el cuadro de diálogo Establecer el certificado seleccionado como activo, confirme que comprende que configurar un certificado como activo puede requerir que restablezca la relación confianza y, a continuación, seleccione Activar.

## Paso 4: eliminación del certificado anterior

Use el siguiente procedimiento para completar el proceso de rotación de certificados para su aplicación. Solo puede eliminar un certificado que esté en estado inactivo.

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, elija su aplicación.
4. En la página de detalles de la aplicación, elija la pestaña Configuración. En los Metadatos de IAM Identity Center, seleccione Administrar certificado.
5. En la página de certificados de IAM Identity Center, seleccione el certificado que desee eliminar. Elija Acciones y, a continuación, elija Eliminar.
6. En el cuadro de diálogo Eliminar certificado, elija Eliminar.

## Indicadores de estado de caducidad de certificados

En la consola del IAM Identity Center, la página de aplicaciones muestra los iconos indicadores de estado en las propiedades de cada aplicación. Estos iconos aparecen en la columna Caduca el

situada junto a cada certificado de la lista. A continuación, se describen los criterios que IAM Identity Center utiliza para determinar qué icono se muestra en cada certificado.

- Rojo: indica que un certificado está caducado actualmente.
- Amarillo: indica que un certificado caducará en 90 días o menos.
- Verde: indica que un certificado es válido actualmente y seguirá siendo válido durante al menos 90 días más.

Cómo comprobar el estado de un certificado:

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de solicitudes, revise el estado de los certificados de la lista, tal y como se indica en la columna Caduca el.

## Entender las propiedades de la aplicación en la consola de IAM Identity Center

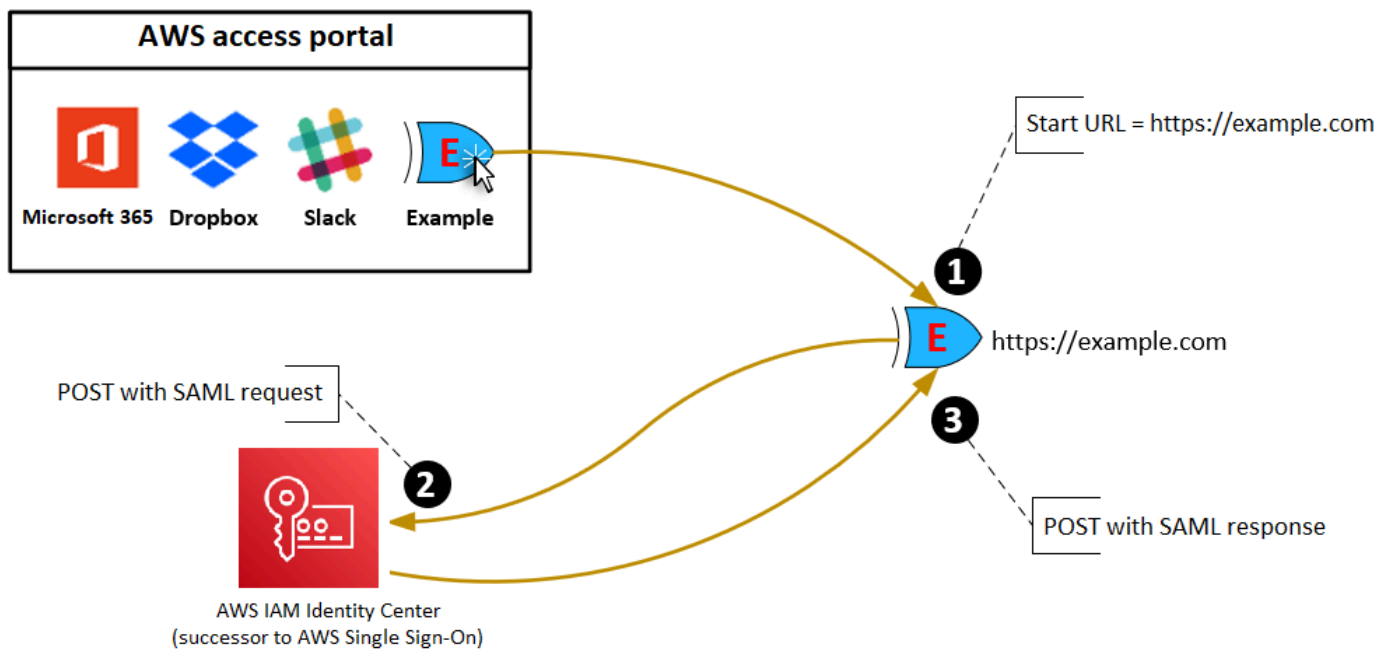
Configure la URL de inicio de la aplicación, el estado de retransmisión y la duración de la sesión en IAM Identity Center para optimizar la experiencia del usuario.

### URL de inicio de la aplicación

Utilice una URL de inicio de la aplicación para iniciar el proceso de federación con la aplicación. El uso típico es para una aplicación que solo admite una conexión iniciada por el proveedor de servicio (SP).

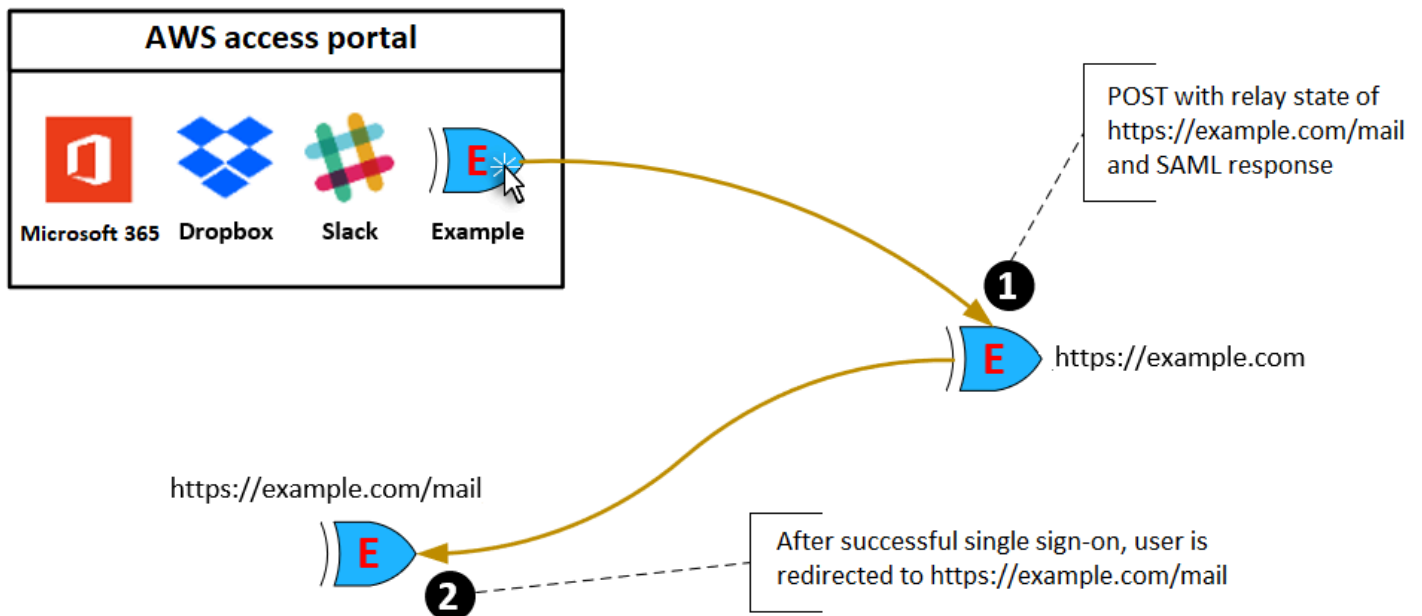
Los siguientes pasos y diagrama ilustran el flujo de trabajo de autenticación de la URL de inicio de la aplicación cuando un usuario elige una aplicación en el portal de acceso AWS :

1. El navegador del usuario redirige la solicitud de autenticación mediante el valor de la URL de inicio de la aplicación (en este caso <https://example.com>).
2. La aplicación envía un HTML POST con SAMLRequest a IAM Identity Center.
3. IAM Identity Center envía después una instrucción HTML POST con un elemento SAMLResponse a la aplicación.



## Estado de retransmisión

Durante el proceso de autenticación de la federación, el estado de retransmisión redirige a los usuarios dentro de la aplicación. Para SAML 2.0, este valor se pasa sin modificar a la aplicación. Una vez configuradas las propiedades de la aplicación, IAM Identity Center envía el valor de estado de retransmisión junto con una respuesta SAML a la aplicación.



## Duración de la sesión

La duración de la sesión es el tiempo durante el que la sesión de un usuario de la aplicación es válida. En el caso de SAML 2.0, esta duración se utiliza para definir la fecha `SessionNotOnOrAfter` del elemento de aserción de SAML `saml2:AuthNStatement`.

Las aplicaciones pueden interpretar la duración de la sesión de las siguientes formas:

- Las aplicaciones pueden utilizarla para determinar el tiempo máximo permitido para la sesión del usuario. Las aplicaciones pueden generar una sesión de usuario con una duración más corta. Esto puede ocurrir cuando la aplicación solo admite sesiones de usuario con una duración menor que la duración de la sesión configurada.
- Las aplicaciones pueden utilizarla como la duración exacta y podrían no permitir que los administradores configuren el valor. Esto puede ocurrir cuando la aplicación solo admite una duración de la sesión específica.

Para obtener más información acerca de cómo se utiliza la duración de la sesión, consulte la documentación de su aplicación específica.

## Asignar el acceso de los usuarios a las aplicaciones en la consola de IAM Identity Center

Puede asignar a los usuarios acceso mediante inicio de sesión único a las aplicaciones de SAML 2.0 del catálogo de aplicaciones o a las aplicaciones de SAML 2.0 personalizadas.

Consideraciones para las asignaciones de grupos:

- Asigne el acceso directamente a los grupos. Para simplificar la administración de los permisos de acceso, se recomienda asignar el acceso directamente a grupos en lugar de a usuarios individuales. Con los grupos puede conceder o denegar permisos para grupos de usuarios en lugar de asignar esos permisos a cada individuo. Si un usuario se muda a una organización diferente, simplemente muévelo a un grupo diferente. Así el usuario recibirá automáticamente los permisos necesarios para la nueva organización.
- No se admiten grupos anidados. Al asignar el acceso de los usuarios a las aplicaciones, IAM Identity Center no permite añadir usuarios a grupos anidados. Si añade un usuario a un grupo anidado, es posible que reciba el mensaje “No tiene ninguna aplicación” al iniciar sesión. Las asignaciones deben realizarse en función del grupo inmediato del que el usuario es miembro.

## Cómo dar acceso a una aplicación a un usuario o grupo:

### Important

En el AWS caso de las aplicaciones gestionadas, debe añadir usuarios directamente desde las consolas de aplicaciones correspondientes o a través de APIs.

1. Abra la [consola de IAM Identity Center](#).

### Note

Si administra los usuarios en AWS Managed Microsoft AD, asegúrese de que la consola del IAM Identity Center utilice la AWS región en la que se encuentra su AWS Managed Microsoft AD directorio antes de dar el siguiente paso.

2. Elija Aplicaciones.
3. En la lista de aplicaciones, seleccione el nombre de la aplicación a la que quiere asignar acceso.
4. En la página de detalles de la aplicación, en la sección Usuarios asignados, elija Asignar usuarios.
5. En el cuadro de diálogo Asignar usuarios, escriba un nombre de usuario o de grupo. Puede especificar varios usuarios o grupos seleccionando las cuentas aplicables tal y como aparecen en los resultados de búsqueda.
6. Elija Assign users (Asignar usuarios).

## Eliminar el acceso de los usuarios a las aplicaciones de SAML 2.0

Utilice este procedimiento para eliminar el acceso de los usuarios a aplicaciones de SAML 2.0 del catálogo de aplicaciones o a aplicaciones de SAML 2.0 personalizadas. Para obtener más información sobre las sesiones de autenticación y su duración, consulte [Autenticación mediante el IAM Identity Center](#).

Para eliminar el acceso de los usuarios a una aplicación

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, seleccione la aplicación cuyo acceso de usuario desea eliminar.

4. En la página de detalles de la aplicación, seleccione la pestaña Usuarios asignados, elija el usuario o grupo que desee eliminar y, a continuación, seleccione Eliminar acceso.
5. En el cuadro de diálogo Remove access (Eliminar acceso), compruebe el nombre del usuario o del grupo. A continuación, elija Remove access (Eliminar acceso).

## Asignación de atributos de su aplicación con atributos de IAM Identity Center

Algunos proveedores de servicios requieren aserciones SAML personalizadas para transferir datos adicionales acerca de los inicios de sesión de los usuarios. En ese caso, puede seguir el siguiente procedimiento para especificar cómo deben asignarse los atributos de usuarios de sus aplicaciones con los atributos correspondientes en IAM Identity Center.

Cómo asignar los atributos de la aplicación con atributos de IAM Identity Center:

1. Abra la [consola de IAM Identity Center](#).
2. Elija Aplicaciones.
3. En la lista de aplicaciones, seleccione la aplicación en la que desea mapear atributos.
4. En la página de detalles de la aplicación, seleccione Acciones y, a continuación, seleccione Editar asignación de atributos.
5. Seleccione Agregar nueva asignación de atributos.
6. En el primer cuadro de texto, escriba el atributo de la aplicación.
7. En el segundo cuadro de texto, escriba el atributo de IAM Identity Center que desea asignar con el atributo de la aplicación. Por ejemplo, es posible que desee asignar el atributo de la aplicación **Username** al atributo del usuario **email** de IAM Identity Center. Para ver la lista de los atributos de usuario permitidos en IAM Identity Center, consulte la tabla que encontrará en [Asignaciones de atributos entre Centro de identidades de IAM y directorio de proveedores de identidades externos](#).
8. En la tercera columna de la tabla, seleccione el formato adecuado del atributo en el menú.
9. Seleccione Save changes (Guardar cambios).

# Cuenta de AWS acceso

AWS IAM Identity Center está integrado con AWS Organizations, lo que le permite gestionar de forma centralizada los permisos de varias cuentas Cuentas de AWS sin necesidad de configurar cada una de sus cuentas de forma manual. Puede definir los permisos y asignarlos a los usuarios de la fuerza laboral para controlar su acceso a determinados recursos Cuentas de AWS mediante una [instancia organizativa](#) de IAM Identity Center. [Las instancias de cuentas](#) del IAM Identity Center no admiten el acceso a las cuentas.

## Cuenta de AWS tipos

Existen dos tipos de Cuentas de AWS entradas AWS Organizations:

- Cuenta de administración: la Cuenta de AWS que se utiliza para crear la organización.
- Cuentas de miembros: el resto Cuentas de AWS que pertenecen a una organización.

Para obtener más información sobre Cuenta de AWS los tipos, consulte [AWS Organizations Terminología y conceptos](#) en la Guía del AWS Organizations usuario.

También puede optar por registrar una cuenta de miembro como administrador delegado de IAM Identity Center. Los usuarios de esta cuenta pueden realizar la mayoría de las tareas administrativas de IAM Identity Center. Para obtener más información, consulte [Administración delegada](#).

La siguiente tabla indica si los usuarios de la cuenta pueden realizar la tarea administrativa de IAM Identity Center para cada tipo de tarea y cuenta.

| Tareas administrativas de IAM Identity Center                     | Cuenta miembro                                                                            | Cuenta de administrador delegado                                                          | Cuenta de administración                                                                    |
|-------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Lectura de usuarios o grupos (leer el grupo en sí y sus miembros) | <br>Sí | <br>Sí | <br>Sí |

| Tareas administrativas de IAM Identity Center                                | Cuenta miembro                                                                            | Cuenta de administrador delegado                                                          | Cuenta de administración                                                                    |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Cómo agregar, editar o eliminar usuarios o grupos                            | <br>No   | <br>Sí   | <br>Sí   |
| Cómo habilitar o deshabilitar el acceso de usuarios                          | <br>No   | <br>Sí   | <br>Sí   |
| Cómo habilitar, deshabilitar o administrar los atributos entrantes           | <br>No   | <br>Sí   | <br>Sí   |
| Cambio o administración de las fuentes de identidad                          | <br>No | <br>Sí | <br>Sí |
| Creación, edición o eliminación de aplicaciones administradas por el cliente | <br>No | <br>Sí | <br>Sí |
| Cree, edite o elimine aplicaciones AWS gestionadas                           | <br>Sí | <br>Sí | <br>Sí |



| Tareas administrativas de IAM Identity Center                                            | Cuenta miembro                                                                            | Cuenta de administrador delegado                                                          | Cuenta de administración                                                                    |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| Configuración de MFA                                                                     | <br>No   | <br>Sí   | <br>Sí   |
| Administración de conjuntos de permisos no aprovisionados en la cuenta de administración | <br>No   | <br>Sí   | <br>Sí   |
| Administración de conjuntos de permisos aprovisionados en la cuenta de administración    | <br>No   | <br>No   | <br>Sí   |
| Activar IAM Identity Center                                                              | <br>No | <br>No | <br>Sí |
| Eliminación de la configuración de IAM Identity Center                                   | <br>No | <br>No | <br>Sí |
| Cómo habilitar o deshabilitar el acceso de los usuarios en la cuenta de administración   | <br>No | <br>No | <br>Sí |

| Tareas administrativas de IAM Identity Center                            | Cuenta miembro                                                                          | Cuenta de administrador delegado                                                        | Cuenta de administración                                                                  |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| Registro o cancelación de una cuenta miembro como administrador delegado | <br>No | <br>No | <br>Sí |

## Asignación Cuenta de AWS de acceso

Puede usar los conjuntos de permisos para simplificar la forma en que asigna el acceso a los usuarios, grupos y Cuentas de AWS de su organización. Los conjuntos de permisos se guardan en IAM Identity Center y definen el nivel de acceso que tienen los usuarios y grupos en una cuenta de AWS. Puede crear un único conjunto de permisos y asignarlo a varias Cuentas de AWS de su organización. También puede asignar varios conjuntos de permisos al mismo usuario.

Para obtener más información sobre los conjuntos de permisos, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

### Note

También puede asignar a sus usuarios acceso de inicio de sesión único a las aplicaciones. Para obtener información, consulte [Acceso de aplicaciones](#).

## La experiencia del usuario final

El portal de AWS acceso proporciona a los usuarios del IAM Identity Center un acceso de inicio de sesión único a todas sus aplicaciones Cuentas de AWS y aplicaciones asignadas a través de un portal web. El portal de AWS acceso es diferente del [AWS Management Console](#), que es un conjunto de consolas de servicio para administrar los recursos. AWS

Al crear un conjunto de permisos, el nombre que especifique para el conjunto de permisos aparece en el portal de AWS acceso como un rol disponible. Los usuarios inician sesión en el portal de AWS acceso, eligen un rol y Cuenta de AWS, a continuación, eligen el rol. Tras elegir el rol, pueden

acceder a los AWS servicios mediante el uso de las credenciales temporales AWS Management Console o recuperar las credenciales temporales para acceder a AWS los servicios mediante programación.

Para abrir AWS Management Console o recuperar las credenciales temporales y acceder a ellas AWS mediante programación, los usuarios siguen estos pasos:

1. Los usuarios abren una ventana del navegador y utilizan la URL de inicio de sesión que usted proporciona para ir al AWS portal de acceso.
2. Con sus credenciales de directorio, inician sesión en el portal de AWS acceso.
3. Tras la autenticación, en la página del portal de AWS acceso, eligen la pestaña Cuentas para ver la lista Cuentas de AWS a la que tienen acceso.
4. A continuación, los usuarios eligen la Cuenta de AWS que quieren usar.
5. Debajo del nombre de la Cuenta de AWS, todos los conjuntos de permisos a los que estén asignados los usuarios aparecen como roles disponibles. Por ejemplo, si asignó un usuario `john_stiles` al conjunto de `PowerUser` permisos, el rol se mostrará en el portal de AWS acceso como `PowerUser/john_stiles`. Los usuarios que tienen asignados varios conjuntos de permisos eligen el rol de que quieren utilizar. Los usuarios pueden elegir su rol para acceder a AWS Management Console.
6. Además del rol, los usuarios del portal de AWS acceso pueden recuperar credenciales temporales para el acceso mediante línea de comandos o mediante programación seleccionando las teclas de acceso.

Para step-by-step obtener información que puede proporcionar a los usuarios de su plantilla, consulte [Uso del portal de AWS acceso](#) y [Obtención de las credenciales de usuario de IAM Identity Center para la AWS CLI o AWS SDKs](#).

## Aplicación y limitación del acceso

Al habilitar IAM Identity Center, este crea un rol vinculado a un servicio. También puede utilizar las políticas de control de servicios (SCPs).

## Delegación y aplicación del acceso

Un rol vinculado a un servicio es un tipo de rol de IAM que está vinculado directamente a un servicio. AWS Tras activar el Centro de identidad de IAM, el Centro de identidades de IAM puede crear un rol vinculado a un servicio en cada uno de los componentes de la organización. Cuenta de AWS Esta

función proporciona permisos predefinidos que permiten al Centro de Identidad de IAM delegar y hacer cumplir qué usuarios tienen acceso de inicio de sesión único a determinados miembros de su organización. Cuentas de AWS Organizations Para utilizar esta característica, debe asignar a uno o más usuarios el acceso a una cuenta. Para obtener más información, consulte [Entender los roles vinculados a servicios en IAM Identity Center](#) y [Uso de roles vinculados a servicios para IAM Identity Center](#).

## Límite de acceso al almacén de identidades desde las cuentas de los miembros

En el caso del servicio de almacén de identidades utilizado por IAM Identity Center, los usuarios que tienen acceso a una cuenta de miembro pueden utilizar acciones de la API que requieren permisos de lectura. Las cuentas de los miembros tienen acceso a las acciones de lectura en los espacios de nombres sso-directory e identitystore. Para obtener más información, consulte [Acciones, recursos y claves de condición del AWS IAM Identity Center directorio](#) y [Acciones, recursos y claves de condición de AWS Identity Store](#) en la Referencia de autorización de servicios.

Para evitar que los usuarios de las cuentas de los miembros utilicen las operaciones de la API en el almacén de identidades, puede [asociar una política de control de servicio \(SCP\)](#). Un SCP es un tipo de política de organización que puede utilizar para administrar permisos en su organización. El siguiente ejemplo de SCP impide que los usuarios de las cuentas de los miembros accedan a cualquier operación de la API del almacén de identidades.

```
{
  "Sid": "ExplicitlyBlockIdentityStoreAccess",
  "Effect": "Deny",
  "Action": ["identitystore:*", "sso-directory:*"],
  "Resource": "*"
}
```

### Note

Limitar el acceso de las cuentas de los miembros puede afectar a la funcionalidad de las aplicaciones habilitadas para IAM Identity Center.

Para obtener más información, consulte [las políticas de control de servicios \(SCPs\)](#) en la Guía del AWS Organizations usuario.

# Administración delegada

La administración delegada proporciona una forma cómoda para que los usuarios asignados a una cuenta miembro registrada realicen la mayoría de las tareas administrativas de IAM Identity Center. Al activar el Centro de Identidad de IAM, su instancia del Centro de Identidad de IAM se crea en la cuenta de administración de forma AWS Organizations predeterminada. Se diseñó originalmente de esta manera para que IAM Identity Center pudiera aprovisionar, desaprovisionar y actualizar las características en todas las cuentas de los miembros de su organización. Aunque su instancia del IAM Identity Center debe residir siempre en la cuenta de administración, puede delegar la administración del Centro de Identidad de IAM a una cuenta de miembro en AWS Organizations, lo que amplía la capacidad de administrar el Centro de Identidad de IAM desde fuera de la cuenta de administración.

Habilitar la administración delegada proporciona los siguientes beneficios:

- Minimiza la cantidad de personas que necesitan acceder a la cuenta de administración para ayudar a mitigar los problemas de seguridad
- Permite a determinados administradores asignar usuarios y grupos a las aplicaciones y a las cuentas de los miembros de su organización

Para obtener más información sobre cómo funciona el Centro de Identidad de IAM, consulte [AWS Organizations Cuenta de AWS acceso](#). Para obtener información adicional y revisar un ejemplo de escenario empresarial que muestre cómo configurar la administración delegada, consulte [Getting started with IAM Identity Center delegated administration](#) en el blog de seguridad de AWS .

## Temas

- [Prácticas recomendadas](#)
- [Requisitos previos](#)
- [Registro de una cuenta miembro](#)
- [Anulación del registro de una cuenta miembro](#)
- [Consulte qué cuenta miembro se ha registrado como administrador delegado](#)

## Prácticas recomendadas

Estas son algunas prácticas recomendadas antes de configurar la administración delegada.

- Otorgue el mínimo privilegio a la cuenta de administración: dado que la cuenta de administración es una cuenta con muchos privilegios y para cumplir con el principio de privilegios mínimos, le recomendamos encarecidamente que restrinja el acceso a la cuenta de administración al menor número posible de personas. La característica de administrador delegado tiene por objeto minimizar el número de personas que necesitan acceder a la cuenta de administración.
- Cree conjuntos de permisos para usarlos únicamente en la cuenta de administración: esto facilita la administración de conjuntos de permisos diseñados específicamente para los usuarios que acceden a su cuenta de administración y ayuda a diferenciarlos de los conjuntos de permisos administrados por su cuenta de administrador delegado.
- Tenga en cuenta su ubicación de Active Directory: si piensa utilizar Active Directory como fuente de identidad de IAM Identity Center, localice el directorio en la cuenta del miembro en la que haya activado la característica de administrador delegado de IAM Identity Center. Si decide cambiar la fuente de identidad de IAM Identity Center de cualquier otra fuente a Active Directory, o cambiarla de Active Directory a cualquier otra fuente, el directorio debe residir en (ser propiedad de) la cuenta de miembro administrador delegado de IAM Identity Center, si existe alguna; de lo contrario, debe estar en la cuenta de administración.
- Cree asignaciones de usuarios únicamente en la cuenta de administración: el administrador delegado no puede modificar los conjuntos de permisos aprovisionados en la cuenta de administración. Sin embargo, los administradores delegados pueden añadir, editar y eliminar grupos y asignaciones de grupo.

## Requisitos previos

Antes de poder registrar una cuenta como administrador delegado, primero debe configurar el siguiente entorno implementado:

- AWS Organizations debe estar habilitado y configurado con al menos una cuenta de miembro además de su cuenta de administración predeterminada.
- Si su fuente de identidad está configurada en Active Directory, la característica [Centro de identidades de IAM y sincronización de AD configurable](#) debe estar habilitada.

## Registro de una cuenta miembro

Para configurar una administración delegada, primero debe registrar una cuenta miembro en su organización como administrador delegado. Los usuarios de la cuenta de ese miembro que tengan permisos suficientes tendrán acceso administrativo a IAM Identity Center. Una vez que la cuenta

miembro se registra correctamente para la administración delegada, se denomina una cuenta de administrador delegado. Para obtener más información sobre las tareas que puede realizar la cuenta de administrador delegado, consulte [Cuenta de AWS tipos](#).

IAM Identity Center solo permite registrar una cuenta miembro como administrador delegado a la vez. Solo puede registrar una cuenta de miembro si ha iniciado sesión con las credenciales de la cuenta de administración.

Utilice el siguiente procedimiento para conceder acceso administrativo al Centro de identidad de IAM registrando una cuenta de miembro específica en su AWS organización como administrador delegado.

 Important

Esta operación delega el acceso administrativo de IAM Identity Center a los usuarios administradores de esta cuenta miembro. Todos los usuarios que dispongan de permisos suficientes para acceder a esta cuenta de administrador delegado pueden realizar todas las tareas administrativas de IAM Identity Center desde la cuenta, excepto:

- Habilitación de IAM Identity Center
- Eliminación de las configuraciones de IAM Identity Center
- Administración de conjuntos de permisos aprovisionados en la cuenta de administración
- Registro o cancelación del registro de otras cuentas de miembros como administradores delegados
- Habilitación o deshabilitación del acceso de usuarios en la cuenta de administración

El administrador delegado puede editar la pertenencia al grupo.

## Registro de una cuenta miembro

1. Inicie sesión AWS Management Console con las credenciales de su cuenta de administración. AWS Organizations Se requieren las credenciales de la cuenta de administración para ejecutar la [RegisterDelegatedAdministratorAPI](#).
2. Seleccione la región en la que está activado IAM Identity Center y, a continuación, abra [la consola de IAM Identity Center](#).
3. Elija Configuración y, a continuación, seleccione la pestaña Administración.

4. En la sección Administrador delegado, elija Registro de cuenta.
5. En la página Registrar un administrador delegado, selecciona el Cuenta de AWS que deseas registrar y, a continuación, selecciona Registrar cuenta.

## Anulación del registro de una cuenta miembro

Solo puede cancelar el registro de una cuenta de miembro si ha iniciado sesión con las credenciales de la cuenta de administración.

Utilice el siguiente procedimiento para eliminar el acceso administrativo al Centro de identidad de IAM anulando el registro de una cuenta de miembro de su AWS organización que anteriormente había sido designada como administrador delegado.

### Important

Al anular el registro de una cuenta, se elimina de forma efectiva la posibilidad de que todos los usuarios administradores administren IAM Identity Center desde esa cuenta. Como resultado, ya no pueden administrar las identidades de IAM Identity Center, la gestión del acceso, la autenticación o el acceso a las aplicaciones desde esta cuenta. Esta operación no afectará a ningún permiso o asignación configurados en el Centro de Identidad de IAM y, por lo tanto, no afectará a los usuarios finales, ya que seguirán teniendo acceso a sus aplicaciones y Cuentas de AWS desde el portal de acceso. AWS

## Anulación del registro de una cuenta miembro

1. Inicie sesión AWS Management Console con las credenciales de su cuenta de administración. AWS Organizations Se requieren las credenciales de la cuenta de administración para ejecutar la [DeregisterDelegatedAdministratorAPI](#).
2. Seleccione la región en la que está activado IAM Identity Center y, a continuación, abra [la consola de IAM Identity Center](#).
3. Elija Configuración y, a continuación, seleccione la pestaña Administración.
4. En la sección Administrador delegado, elija Anular el registro de cuenta.
5. En el cuadro de diálogo Anular el registro de cuenta, revise las implicaciones de seguridad y, a continuación, escriba el nombre de la cuenta miembro para confirmar que lo entiende.
6. Elija Anular el registro de la cuenta.



## Consulte qué cuenta miembro se ha registrado como administrador delegado

Utilice el siguiente procedimiento para averiguar qué cuenta de miembro de su cuenta se AWS Organizations ha configurado como administrador delegado del Centro de Identidad de IAM.

Cómo ver su cuenta de miembro registrado

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la sección Detalles, busque el nombre de la cuenta registrada en Administrador delegado. También puede encontrar esta información seleccionando la pestaña Administración y consultándola en la sección Administrador delegado.

## Acceso elevado temporal para Cuentas de AWS

Todo acceso al suyo Cuenta de AWS implica algún nivel de privilegio. Las operaciones delicadas, como cambiar la configuración de un recurso de alto valor, por ejemplo, un entorno de producción, requieren un tratamiento especial debido al alcance y al impacto potencial. El acceso elevado temporal (también conocido como just-in-time acceso) es una forma de solicitar, aprobar y realizar un seguimiento del uso de un permiso para realizar una tarea específica durante un tiempo específico. El acceso elevado temporal complementa otras formas de control de acceso, como los conjuntos de permisos y la autenticación multifactorial.

AWS IAM Identity Center proporciona las siguientes opciones para la administración temporal del acceso elevado en diferentes entornos empresariales y técnicos:

- Soluciones compatibles gestionadas por el proveedor: AWS ha validado las integraciones de IAM Identity Center con las [ofertas de algunos socios](#) y evaluado sus capacidades en relación con un [conjunto común de requisitos de los clientes](#). Elija la solución que mejor se adapte a su situación y siga las instrucciones del proveedor para habilitar esta funcionalidad con IAM Identity Center.
- Autogestionado y autosuficiente: esta opción proporciona un punto de partida si está interesado en un acceso elevado temporal a uno AWS solo y puede implementar, personalizar y mantener la capacidad usted mismo. Para obtener más información, consulte [Temporary elevated access management \(TEAM\)](#).

## Socios AWS de seguridad validados para un acceso elevado temporal

AWS Los socios de seguridad utilizan diferentes enfoques para abordar un [conjunto común de requisitos de acceso elevado temporal](#). Le recomendamos que revise detenidamente las soluciones de cada socio para que pueda elegir la que mejor se adapte a sus necesidades y preferencias, incluidos su negocio, la arquitectura de su entorno de nube y su presupuesto.

### Note

Para la recuperación ante desastres, le recomendamos que [configure el acceso de emergencia a la AWS Management Console](#) antes de que se produzca una interrupción.

AWS Identity ha validado las capacidades y la integración con IAM Identity Center para las siguientes just-in-time ofertas de AWS Security Partners:

- [CyberArk Secure Cloud Access](#)— Como parte de elloCyberArk Identity Security Platform, esta oferta proporciona un acceso elevado bajo demanda AWS y entornos multinube. Las aprobaciones se gestionan mediante la integración con el ITSM o con las herramientas. ChatOps Todas las sesiones se pueden grabar para su auditoría y cumplimiento.
- [Tenable \(previously Ermetic\)](#)— La Tenable plataforma incluye el aprovisionamiento de un acceso just-in-time privilegiado para las operaciones administrativas en AWS entornos multinube. Los registros de sesión de todos los entornos de nube, incluidos los registros de acceso de AWS CloudTrail , están disponibles en una única interfaz para su análisis y auditoría. La capacidad se integra con herramientas empresariales y para desarrolladores, como Slack y Microsoft Teams.
- [OktaSolicitudes de acceso](#): parte del gobierno de la Okta identidad, le permite [configurar un flujo de trabajo de solicitudes de just-in-time acceso utilizando Okta](#) como proveedor de identidad externo (IdP) de IAM Identity Center y sus conjuntos de permisos de IAM Identity Center.

Esta lista se actualizará a medida que se AWS validen las capacidades de otras soluciones de socios y la integración de estas soluciones con el IAM Identity Center. Los socios pueden nominar sus soluciones a través de la competencia de seguridad de la Red de AWS Socios (APN). Para obtener más información, consulte Socios con competencias en [AWS seguridad](#).

 Note

Si utiliza políticas basadas en recursos, Amazon Elastic Kubernetes Service (Amazon EKS AWS Key Management Service ) o ([Hacer referencia a conjuntos de permisos en políticas de recursos, mapas de configuración de Amazon EKS Cluster y políticas AWS KMS clave](#))AWS KMS, consulte antes de elegir la solución. just-in-time

## Se evaluaron las capacidades de acceso elevado temporal para su validación por parte de los socios AWS

AWS Identity ha comprobado que las capacidades de acceso elevado temporal que ofrecen y las [solicitudes de Okta acceso responden a](#) los siguientes requisitos comunes de los clientes: [CyberArk Secure Cloud AccessTenable](#)

- Los usuarios pueden solicitar el acceso a un conjunto de permisos durante un período de tiempo especificado por el usuario, especificando la AWS cuenta, el conjunto de permisos, el período de tiempo y el motivo.
- Los usuarios pueden recibir el estado de aprobación de su solicitud.
- Los usuarios no pueden invocar una sesión con un alcance determinado, a menos que haya una solicitud aprobada con el mismo alcance e invoque la sesión durante el período de tiempo aprobado.
- Hay una forma de especificar quién puede aprobar las solicitudes.
- Los aprobadores no pueden aprobar sus propias solicitudes.
- Los aprobadores tienen una lista de solicitudes pendientes, aprobadas y rechazadas, y pueden exportarla para los auditores.
- Los aprobadores pueden aprobar y rechazar las solicitudes pendientes.
- Los aprobadores pueden agregar una nota en la que explique su decisión.
- Los aprobadores pueden revocar una solicitud aprobada, lo que impide el uso futuro del acceso elevado.

 Note

Si un usuario ha iniciado sesión con acceso elevado cuando se revoca una solicitud aprobada, el usuario perderá el acceso inmediatamente. Para obtener más información

acerca de las sesiones de autenticación, consulte [Autenticación mediante el IAM Identity Center](#).

- Las acciones y aprobaciones de los usuarios están disponibles para su auditoría.

## Acceso mediante inicio de sesión único a Cuentas de AWS

Puede asignar permisos a los usuarios de su directorio conectado a la cuenta de administración o a las cuentas de los miembros de su organización en AWS Organizations función de las funciones [laborales más comunes](#). También puede utilizar permisos personalizados para satisfacer sus requisitos de seguridad específicos. Por ejemplo, puede conceder a los administradores de bases de datos permisos amplios a Amazon RDS en las cuentas de desarrollo pero limitar sus permisos en las cuentas de producción. IAM Identity Center configura todos los permisos de usuario necesarios en sus cuentas de Cuentas de AWS de forma automática.

### Note

Puede que tengas que conceder permisos a los usuarios o grupos para operar en la cuenta AWS Organizations de administración. Como se trata de una cuenta con muchos privilegios, las restricciones de seguridad adicionales requieren que tengas la política de [IAMFullacceso](#) o permisos equivalentes antes de poder configurarla. Estas restricciones de seguridad adicionales no son obligatorias para ninguna de las cuentas de los miembros de su AWS organización.

### Temas

- [Asigne el acceso de usuario o grupo a Cuentas de AWS](#)
- [Eliminación del acceso de usuarios y grupos a una Cuenta de AWS](#)
- [Revocar las sesiones de roles de IAM activas creadas por conjuntos de permisos](#)
- [Delegue quién puede asignar el acceso de inicio de sesión único a los usuarios y grupos de la cuenta de administración](#)

## Asigne el acceso de usuario o grupo a Cuentas de AWS

Utilice el siguiente procedimiento para asignar el acceso de inicio de sesión único a usuarios y grupos del directorio conectado y para utilizar conjuntos de permisos para determinar su nivel de acceso.

Para comprobar el acceso existente de usuarios y grupos, consulte [Ver y cambiar un conjunto de permisos](#).

### Note

Para simplificar la administración de los permisos de acceso, se recomienda asignar el acceso directamente a grupos en lugar de a usuarios individuales. Con los grupos puede conceder o denegar permisos para grupos de usuarios en lugar de asignar esos permisos a cada individuo. Si un usuario se va a otra organización, basta con cambiarlo a un grupo diferente y automáticamente recibirá los permisos necesarios para la nueva organización.

Para asignar el acceso de usuario o grupo a Cuentas de AWS

1. Abra la [consola de IAM Identity Center](#)

### Note

Antes de continuar con el paso siguiente, compruebe que la consola de IAM Identity Center utiliza alguna de las regiones donde se encuentra su directorio AWS Managed Microsoft AD .

2. En el panel de navegación, en Permisos para varias cuentas, elija Cuentas de AWS.
3. En la página de Cuentas de AWS, se muestra una lista de su organización en forma de árbol. Seleccione la casilla de verificación situada junto a la casilla Cuenta de AWS a la que desee asignar el acceso. Si desea configurar el acceso administrativo para IAM Identity Center, seleccione la casilla de verificación situada junto a la cuenta de administración.

### Note

Puedes seleccionar hasta 10 Cuentas de AWS a la vez por conjunto de permisos al asignar el acceso de inicio de sesión único a usuarios y grupos. Para asignar más de

10 Cuentas de AWS al mismo conjunto de usuarios y grupos, repita este procedimiento según sea necesario para las cuentas adicionales. Cuando se le solicite, seleccione los mismos usuarios, grupos y conjunto de permisos.

4. Seleccione Asignar usuarios o grupos.
5. Para el paso 1: seleccionar usuarios y grupos, en la página Asignar usuarios y grupos a **AWS-account-name** «», haga lo siguiente:
  1. En la pestaña Usuarios, seleccione uno o más usuarios a los que desee conceder el acceso de inicio de sesión único.

Para filtrar los resultados, escriba el nombre del usuario que desea en el cuadro de búsqueda.
  2. En la pestaña Grupos, seleccione uno o más grupos a los que desee conceder el acceso de inicio de sesión único.

Para filtrar los resultados, escriba el nombre del grupo que desea en el cuadro de búsqueda.
  3. Para mostrar los usuarios y grupos que ha seleccionado, elija el triángulo lateral situado junto a Usuarios y grupos seleccionados.
  4. Tras confirmar que se haya seleccionado los usuarios y grupos correctos, seleccione Siguiente.
6. Para el paso 2: seleccionar conjuntos de permisos, en la página Asignar conjuntos de permisos a **AWS-account-name** «», haga lo siguiente:
  1. Seleccione uno o varios conjuntos de permisos. Si es necesario, puede crear y seleccionar nuevos conjuntos de permisos.
    - Para seleccionar uno o más conjuntos de permisos existentes, en Conjuntos de permisos, seleccione los conjuntos de permisos que desee aplicar a los usuarios y grupos que seleccionó en el paso anterior.
    - Para crear uno o más conjuntos de permisos nuevos, elija Crear conjunto de permisos y siga los pasos que se indican en [Crea un conjunto de permisos..](#) Tras crear los conjuntos de permisos que desea aplicar, en la consola de IAM Identity Center, vuelva a las Cuentas de AWS y siga las instrucciones hasta llegar al paso 2: seleccionar conjuntos de permisos. Cuando llegue a este paso, seleccione los nuevos conjuntos de permisos que ha creado y continúe con el siguiente paso de este procedimiento.
  2. Tras confirmar que se haya seleccionado los conjuntos de permisos correctos, seleccione Siguiente.

7. Para el paso 3: Revisar y enviar, en la página Revisar y enviar las tareas a **AWS-account-name** «», haga lo siguiente:
  1. Revise los usuarios, grupos y los conjuntos de permisos seleccionados.
  2. Tras confirmar que se haya seleccionado los usuarios, grupos y los conjuntos de permisos correctos, seleccione Enviar.

### Consideraciones

- El proceso de asignación de usuarios y grupos puede tardar unos minutos en completarse. Es importante que deje esta página abierta hasta que se complete el proceso correctamente.

#### Note

Puede que tengas que conceder permisos a los usuarios o grupos para operar en la cuenta AWS Organizations de administración. Como se trata de una cuenta con muchos privilegios, las restricciones de seguridad adicionales requieren que tengas la política de [IAMFullacceso](#) o permisos equivalentes antes de poder configurarla. Estas restricciones de seguridad adicionales no son obligatorias para ninguna de las cuentas de los miembros de su AWS organización.

8. Si se aplica alguna de las siguientes condiciones, siga los pasos que se indican en [Solicitar MFA a los usuarios](#) para habilitar la MFA en IAM Identity Center:

- Está utilizando el directorio predeterminado del Identity Center como origen e de identidad.
- Utiliza un AWS Managed Microsoft AD directorio o un directorio autoadministrado en Active Directory como fuente de identidad y no usa RADIUS AWS Directory Service MFA con.

#### Note

Si utiliza un proveedor de identidad externo, tenga en cuenta que el IdP externo, no el IAM Identity Center, administra la configuración de MFA. No se admite el uso de MFA en IAM Identity Center para uso externo. IdPs

Al configurar el acceso a la cuenta para el usuario administrativo, del IAM Identity Center crea el rol de IAM correspondiente. Esta función, que está controlada por el Centro de Identidad de IAM,

se crea en el lugar correspondiente Cuenta de AWS y las políticas especificadas en el conjunto de permisos se adjuntan a la función.

Como alternativa, puede utilizar [AWS CloudFormation](#) para crear y asignar conjuntos de permisos y asignar usuarios a esos conjuntos de permisos. A continuación, los usuarios pueden [iniciar sesión en el portal de acceso de AWS](#) o utilizar los comandos de la [AWS Command Line Interface \(AWS CLI\)](#).

## Eliminación del acceso de usuarios y grupos a una Cuenta de AWS

Utilice este procedimiento para eliminar el acceso de inicio de sesión único a uno o varios usuarios y grupos del directorio conectado. Cuenta de AWS También puede utilizar la [delete-account-assignment](#) AWS CLI.

### Note

Cuando necesite desaproveccionar usuarios o grupos del Centro de Identidad de IAM, primero debe [eliminar cualquier asignación de conjuntos de permisos](#) de sus usuarios y grupos antes de eliminarlos.

Para eliminar el acceso de usuarios y grupos a un Cuenta de AWS

1. Abra la [consola de IAM Identity Center](#).
2. En el panel de navegación, en Permisos para varias cuentas, elija Cuentas de AWS.
3. En la página Cuentas de AWS, aparece una lista de su organización en forma de árbol. Seleccione el nombre del grupo Cuenta de AWS que contiene los usuarios y grupos a los que desea eliminar el acceso de inicio de sesión único.
4. En la página de información general de Cuenta de AWS, en Usuarios y grupos asignados, seleccione el nombre de uno o más usuarios o grupos y elija Eliminar el acceso.
5. En el cuadro de diálogo Eliminar el acceso, confirme que los nombres de los usuarios o grupos son correctos y elija Eliminar el acceso.

## Revocar las sesiones de roles de IAM activas creadas por conjuntos de permisos

El siguiente es un procedimiento general para revocar una sesión de conjunto de permisos activa para un usuario del IAM Identity Center. El procedimiento parte del supuesto de que se desea



eliminar todos los accesos de un usuario cuyas credenciales estén comprometidas o de un usuario fraudulento que se encuentre en el sistema. El requisito previo es haber seguido las instrucciones que figuran en [Prepárese para revocar una sesión de rol de IAM activa creada por un conjunto de permisos](#). Suponemos que la política de denegación de todo está presente en una política de control de servicio (SCP).

 Note

AWS recomienda crear una automatización para gestionar todos los pasos, excepto las operaciones que solo se realizan en la consola.

1. Obtenga el ID de la persona cuyo acceso debe revocar. Puede usar el almacén de identidades APIs para buscar al usuario por su nombre de usuario.
2. Actualice la política de denegación para agregar el ID de usuario del paso 1 de su política de control de servicio (SCP). Tras completar este paso, el usuario objetivo pierde el acceso y no puede realizar acciones con ninguna de las funciones a las que afecte la política.
3. Elimine todas las asignaciones de conjuntos de permisos para el usuario. Si el acceso se asigna mediante la pertenencia a un grupo, elimine al usuario de todos los grupos y de todas las asignaciones directas de conjuntos de permisos. Este paso impide que el usuario asuma roles de IAM adicionales. Si un usuario tiene una sesión activa en el portal de AWS acceso y usted lo desactiva, podrá seguir asumiendo nuevas funciones hasta que le quite el acceso.
4. Si usa un proveedor de identidades (IdP) o Microsoft Active Directory como fuente de identidad, deshabilite al usuario en la fuente de identidad. La desactivación del usuario impide la creación de sesiones adicionales en el portal de acceso AWS . Utilice su IdP o la documentación de la API de Microsoft Active Directory para obtener información sobre cómo automatizar este paso. Si utiliza el directorio del IAM Identity Center como fuente de identidad, no desactive todavía el acceso de los usuarios. Inhabilitará el acceso de usuarios en el paso 6.
5. En la consola del IAM Identity Center, busque al usuario y elimine su sesión activa.
  - a. Seleccione Usuarios.
  - b. Elija el usuario cuya sesión activa desea eliminar.
  - c. En la página de detalles del usuario, elija la pestaña Sesiones activas.
  - d. Seleccione las casillas de verificación situadas junto a las identidades que desea eliminar y elija Eliminar sesión.

Tras eliminar una sesión de usuario, el usuario perderá inmediatamente el acceso al portal de AWS acceso. Obtenga información sobre la [duración de la sesión](#).

6. En la consola del IAM Identity Center, deshabilite el acceso de los usuarios.
  - a. Seleccione Usuarios.
  - b. Seleccione el usuario cuyo acceso desea desactivar.
  - c. En la página de detalles del usuario, expanda Información general y pulse el botón Desactivar el acceso del usuario para evitar que el usuario vuelva a iniciar sesión.
7. Deje en vigor la política de denegación durante al menos 12 horas. De lo contrario, el usuario con una sesión de rol de IAM activa habrá restablecido las acciones con el rol de IAM. Si espera 12 horas, las sesiones activas caducan y el usuario no podrá volver a acceder al rol de IAM.

 Important

Si deshabilita el acceso de un usuario antes de detener la sesión de usuario (completó el paso 6 sin completar el paso 5), ya no podrá detener la sesión del usuario a través de la consola del IAM Identity Center. Si deshabilita inadvertidamente el acceso de los usuarios antes de detenerla, puede volver a habilitar al usuario, detener su sesión y, a continuación, volver a deshabilitar su acceso.

[Ahora puede cambiar las credenciales del usuario si su contraseña está comprometida y restaurar sus asignaciones.](#)

## Delegue quién puede asignar el acceso de inicio de sesión único a los usuarios y grupos de la cuenta de administración

La concesión de acceso de inicio de sesión único a la cuenta de administración utilizando la consola de IAM Identity Center es una acción que requiere privilegios. De forma predeterminada, solo un Usuario raíz de la cuenta de AWS usuario que tenga asociadas las políticas IAMFullAccess AWS administradas AWSSSOMasterAccountAdministratory las políticas administradas puede asignar el acceso de inicio de sesión único a la cuenta de administración. Las IAMFullAccesspolíticas AWSSSOMasterAccountAdministratory gestionan el acceso mediante inicio de sesión único a la cuenta de administración de una organización. AWS Organizations

Como alternativa, puede utilizarlas AWS CLI para crear conjuntos de permisos, adjuntar políticas y asignarlos. A continuación se enumeran los comandos de cada paso:

- Para crear un conjunto de permisos: [create-permission-set](#)
- Para adjuntarlo AWS Managed Policy a un conjunto de permisos: [attach-managed-policy-to-permission-set](#)
- [Para adjuntar una política gestionada por el cliente a un conjunto de permisos: - attach-customer-managed-policy to-permission-set](#)
- Para asignar un conjunto de permisos a un director: [create-account-assignment](#)

Siga los pasos que se describen a continuación para delegar permisos para administrar el acceso de inicio de sesión único a los usuarios y grupos en su directorio.

Para otorgar permisos para administrar el acceso de inicio de sesión único a los usuarios y grupos del directorio

1. Inicie sesión en la consola de IAM Identity Center como usuario raíz de la cuenta de administración o con otro usuario que tenga permisos de administrador en la cuenta de administración.
2. Siga los pasos que se indican en [Crea un conjunto de permisos](#). para crear un conjunto de permisos y, a continuación, haga lo siguiente:
  1. En la página Crear un conjunto de permisos nuevo, active la casilla Crear un conjunto de permisos personalizado y, a continuación, elija Siguiente: Detalles.
  2. En la página Crear un nuevo conjunto de permisos, especifique un nombre para el conjunto de permisos personalizado y, si lo desea, una descripción. Si es necesario, modifique la duración de la sesión y especifique una URL de estado de retransmisión.

 Note

Para la URL del estado de retransmisión, debe especificar una URL que esté en la AWS Management Console. Por ejemplo:

**<https://console.aws.amazon.com/ec2/>**

Para obtener más información, consulte [Configure el estado de la retransmisión para acceder rápidamente a AWS Management Console](#).

3. En ¿Qué políticas desea incluir en su conjunto de permisos?, active la casilla Adjuntar políticas administradas de AWS .
  4. En la lista de políticas de IAM, elija tanto la política como AWSSSOMasterAccountAdministratorla IAMFullAccess AWS gestionada. Estas políticas conceden permisos a todos los usuarios a los que se les asigne acceso a este conjunto de permisos en el futuro.
  5. Elija Siguiente: etiquetas.
  6. En Añadir etiquetas (opcional), especifique los valores de clave y valor (opcional) y, a continuación, seleccione Siguiente: revisar. Para obtener más información acerca de las etiquetas, consulte [Recursos de etiquetado AWS IAM Identity Center](#).
  7. Revise las selecciones y, a continuación, elija Crear.
3. Siga los pasos que se indican en [Asigne el acceso de usuario o grupo a Cuentas de AWS](#) para asignar los usuarios y grupos adecuados al conjunto de permisos que acaba de crear.
  4. Informe a los usuarios asignados de que, cuando inicien sesión en el portal de acceso AWS y seleccionen la pestaña Cuentas, deberán elegir el nombre de característica adecuado para autenticarse con los permisos que usted acaba de delegar.

## Administre Cuentas de AWS con conjuntos de permisos

Un conjunto de permisos es una plantilla que usted crea y mantiene, y que define un conjunto de una o más [políticas de IAM](#). Los conjuntos de permisos simplifican la asignación del Cuenta de AWS acceso a los usuarios y grupos de su organización. Por ejemplo, puede crear un conjunto de permisos de administrador de base de datos que incluya políticas para administrar los servicios de AWS RDS, DynamoDB y Aurora, y usar ese conjunto de permisos único para conceder acceso a una lista de objetivos Cuentas de AWS de su organización a los administradores de [AWS bases de datos](#).

El Centro de identidad de IAM asigna el acceso a un usuario o grupo de uno o más con conjuntos de permisos. Cuentas de AWS Cuando asigna un conjunto de permisos, IAM Identity Center crea los roles de IAM controlados por IAM Identity Center correspondientes en cada cuenta y adjunta a esos roles las políticas especificadas en el conjunto de permisos. El Centro de identidad de IAM administra la función y permite que los usuarios autorizados que haya definido asuman la función mediante el portal de usuarios de IAM Identity Center o la CLI AWS . A medida que modifica el conjunto de permisos, IAM Identity Center garantiza que las políticas y los roles de IAM correspondientes se actualicen en consecuencia.

Puede agregar [políticas administradas por AWS](#), [políticas administradas por los clientes](#), políticas insertadas y [políticas administradas por AWS para las funciones de trabajo](#) a sus conjuntos de permisos. También puede asignar una política administrada por AWS o una política administrada por el cliente como [límite de permisos](#).

Para crear un conjunto de permisos, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

## Creación de un conjunto de permisos que aplique los permisos de privilegio mínimo

Para seguir la práctica recomendada de aplicar permisos con privilegios mínimos, después de crear un conjunto de permisos administrativos, cree un conjunto de permisos más restrictivo y asígnelo a uno o más usuarios. Los conjuntos de permisos creados en el procedimiento anterior proporcionan un punto de partida para evaluar la cantidad de acceso a los recursos que necesitan los usuarios. Para cambiar a los permisos con privilegios mínimos, puede ejecutar IAM Access Analyzer para supervisar a los directores con políticas gestionadas. AWS Después de saber qué permisos utilizan, puede escribir una política personalizada o generar una política con solo los permisos necesarios para su equipo.

Con IAM Identity Center, puede asignar varios conjuntos de permisos al mismo usuario. A su usuario administrativo también se le deben asignar conjuntos de permisos adicionales y más restrictivos. De esta forma, pueden acceder a usted solo Cuenta de AWS con los permisos necesarios, en lugar de utilizar siempre sus permisos administrativos.

Por ejemplo, si es desarrollador, después de crear su usuario administrativo en IAM Identity Center, puede crear un nuevo conjunto de permisos que conceda permisos de `PowerUserAccess` y, a continuación, asignarse ese conjunto de permisos a usted. A diferencia del conjunto de permisos administrativos, que utiliza permisos de `AdministratorAccess`, el conjunto de permisos de `PowerUserAccess` no permite la administración de usuarios de IAM y grupos. Al iniciar sesión en el AWS portal de acceso para acceder a su AWS cuenta, puede `PowerUserAccess` elegir no `AdministratorAccess` realizar las tareas de desarrollo en la cuenta.

Tenga en cuenta las siguientes consideraciones:

- Para empezar rápidamente a crear un conjunto de permisos más restrictivo, utilice un conjunto de permisos predefinido en lugar de uno personalizado.

Con un conjunto de permisos predefinido, que utiliza [permisos predefinidos](#), puede elegir una única política AWS gestionada de una lista de políticas disponibles. Cada política otorga un nivel específico de acceso a AWS los servicios y recursos o permisos para una función laboral común. Para obtener información sobre cada una de estas políticas, consulte [Políticas administradas de AWS para funciones de trabajo](#).

- Puede configurar la duración de la sesión de un conjunto de permisos para controlar el tiempo que un usuario permanece registrado en una Cuenta de AWS.

Cuando los usuarios se federan Cuenta de AWS y utilizan la consola de AWS gestión o la interfaz de línea de AWS comandos (AWS CLI), IAM Identity Center utiliza la configuración de duración de la sesión del conjunto de permisos para controlar la duración de la sesión. De forma predeterminada, el valor de Duración de la sesión, que determina el tiempo que un usuario puede iniciar sesión Cuenta de AWS antes de AWS cerrar la sesión del usuario, se establece en una hora. Puede especificar un valor máximo de 12 horas. Para obtener más información, consulte [Definir la duración de la sesión para Cuentas de AWS](#).

- También puede configurar la duración de la sesión del portal de AWS acceso para controlar el tiempo que un usuario de la fuerza laboral permanece conectado al portal.

De forma predeterminada, el valor de Duración máxima de la sesión, que determina el tiempo que un usuario de Workforce puede iniciar sesión en el portal de AWS acceso antes de tener que volver a autenticarse, es de ocho horas. Puede especificar un valor máximo de 90 días. Para obtener más información, consulte [Configure la duración de la sesión del portal de acceso AWS y de las aplicaciones integradas del IAM Identity Center](#).

- Cuando inicie sesión en el portal de AWS acceso, elija el rol que proporciona los permisos con privilegios mínimos.

Cada conjunto de permisos que cree y asigne a su usuario aparece como un rol disponible en el AWS portal de acceso. Cuando inicie sesión en el portal en calidad de ese usuario, elija el rol que corresponda al conjunto de permisos más restrictivo que pueda usar para realizar tareas en la cuenta, en lugar de AdministratorAccess.

- Puede agregar otros usuarios a IAM Identity Center y asignar conjuntos de permisos nuevos o existentes a esos usuarios.

Para obtener información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

## Temas

- [Permisos predefinidos para las políticas administradas de AWS](#)
- [Permisos personalizados para las políticas AWS administradas y administradas por los clientes](#)
- [Creación, administración y eliminación de conjuntos de permisos](#)
- [Configure las propiedades del conjunto de permisos](#)

## Permisos predefinidos para las políticas administradas de AWS

Puede crear un conjunto de permisos predefinido con políticas AWS administradas.

Cuando crea un conjunto de permisos con permisos predefinidos, elige una política de una lista de políticas AWS administradas. Dentro de las políticas disponibles, puede elegir entre políticas de permisos comunes y políticas de funciones de trabajo.

### Políticas de permisos comunes

Elija de una lista de políticas AWS administradas que le permitan acceder a los recursos en su totalidad Cuenta de AWS. Puede agregar una de las siguientes políticas:

- AdministratorAccess
- PowerUserAccess
- ReadOnlyAccess
- ViewOnlyAccess

### Políticas de funciones de trabajo

Elija de una lista de políticas AWS administradas que le permitan acceder a sus recursos Cuenta de AWS que puedan ser relevantes para un puesto en su organización. Puede agregar una de las siguientes políticas:

- Billing
- DataScientist
- DatabaseAdministrator
- NetworkAdministrator
- SecurityAudit
- SupportUser
- SystemAdministrator

Para obtener una descripción detallada de las políticas de permisos y las políticas de funciones de trabajo comunes disponibles, consulte [políticas administradas de AWS para las funciones de trabajo](#) en la Guía del usuario de AWS Identity and Access Management .

Para obtener instrucciones acerca de cómo crear un conjunto de permisos, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

## Permisos personalizados para las políticas AWS administradas y administradas por los clientes

Puede crear un conjunto de permisos con permisos personalizados y combinar cualquiera de las políticas AWS administradas y administradas por los clientes que tenga en AWS Identity and Access Management (IAM) con las políticas integradas. También puede incluir el límite de permisos al establecer el máximo de permisos posibles que otras políticas pueden conceder a los usuarios de su conjunto de permisos.

Para obtener instrucciones acerca de cómo crear un conjunto de permisos, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

Tipos de políticas que puede adjuntar a su conjunto de permisos

### Temas

- [Políticas insertadas](#)
- [AWS políticas gestionadas](#)
- [Políticas administradas por el cliente](#)
- [Límites de permisos](#)

## Políticas insertadas

Puede adjuntar una política insertada a un conjunto de permisos. Una política insertada es un bloque de texto con el formato de una política de IAM que se añade directamente al conjunto de permisos. Al crear un conjunto de permisos nuevo, puede pegar una política o generar una nueva con la herramienta de creación de políticas de la consola de IAM Identity Center. También puede crear políticas de IAM con el [generador de políticas de AWS](#).

Al implementar un conjunto de permisos con una política integrada, el Centro de Identidad de IAM crea una política de IAM en la que Cuentas de AWS se asigna el conjunto de permisos. IAM Identity



Center crea la política al asignar el conjunto de permisos definido en la cuenta. A continuación, la política se adjunta a la función de IAM Cuenta de AWS que asuma su usuario.

Cuando crea una política en línea y asigna su conjunto de permisos, IAM Identity Center configura las políticas propias por usted. Cuentas de AWS Al crear su conjunto de permisos [Políticas administradas por el cliente](#), debe crear las políticas usted Cuentas de AWS mismo antes de asignar el conjunto de permisos.

## AWS políticas gestionadas

Puede adjuntar políticas AWS administradas a su conjunto de permisos. AWS las políticas gestionadas son políticas de IAM que AWS mantiene. Por el contrario, [Políticas administradas por el cliente](#) son las políticas de IAM de su cuenta las que usted crea y mantiene. AWS las políticas gestionadas abordan los casos de uso más comunes con privilegios mínimos en su Cuenta de AWS. Puede asignar una política AWS gestionada como permisos para la función que crea IAM Identity Center o como [límite de permisos](#).

AWS mantiene [políticas AWS gestionadas para las funciones laborales](#) que asignan permisos de acceso a sus recursos específicos para cada trabajo. AWS Puede agregar una política de función de trabajo si decide utilizar permisos predefinidos con su conjunto de permisos. Al elegir permisos personalizados, puede agregar más de una política de función de trabajo.

Cuenta de AWS También contiene una gran cantidad de políticas de IAM AWS gestionadas para aplicaciones específicas Servicios de AWS y combinaciones de ellas. Servicios de AWS Al crear un conjunto de permisos con permisos personalizados, puede elegir entre muchas políticas AWS gestionadas adicionales para asignarlas a su conjunto de permisos.

AWS rellena cada una de ellas Cuenta de AWS con políticas AWS administradas. Para implementar un conjunto de permisos con políticas AWS administradas, no necesita crear primero una política en su Cuentas de AWS. Al crear su conjunto de permisos [Políticas administradas por el cliente](#), debe crear las políticas usted Cuentas de AWS mismo antes de asignar el conjunto de permisos.

Para obtener más información sobre las políticas AWS administradas, consulte las [políticas AWS administradas](#) en la Guía del usuario de IAM.

## Políticas administradas por el cliente

Puede adjuntar políticas administradas por el cliente a su conjunto de permisos. Las políticas administradas por el cliente son políticas de IAM de su cuenta que usted crea y mantiene. Por

el contrario, [AWS políticas gestionadas](#) son las políticas de IAM de su cuenta las que se AWS mantienen. Puede asignar una política gestionada por el cliente como permisos para la función que crea IAM Identity Center o como límite de [permisos](#).

Al crear un conjunto de permisos con una política gestionada por el cliente, debe crear una política de IAM con el mismo nombre y la misma ruta en cada Cuenta de AWS lugar donde IAM Identity Center asigne el conjunto de permisos. Si va a especificar una ruta personalizada, asegúrese de especificar la misma ruta en cada una de Cuenta de AWS. Para obtener más información, consulte [Nombres fáciles de recordar y rutas](#) en la Guía del usuario de IAM. IAM Identity Center adjunta la política de IAM al rol de IAM que crea en su Cuenta de AWS. Como práctica recomendada, aplique los mismos permisos a la política en cada cuenta a la que asigne el conjunto de permisos. Para obtener más información, consulte [Utilice las políticas de IAM en los conjuntos de permisos](#).

#### Note

Cuando se adjunta una política gestionada por el cliente a un conjunto de permisos, el nombre de la política no distingue entre mayúsculas y minúsculas.

Para obtener más información, consulte [Políticas administradas por el cliente](#) en la Guía del usuario de IAM.

## Límites de permisos

Puede adjuntar un límite de permisos a su conjunto de permisos. Un límite de permisos es una política de IAM AWS gestionada o gestionada por el cliente que establece los permisos máximos que una política basada en la identidad puede conceder a un responsable de IAM. Cuando aplica un límite de permisos, su [Políticas insertadas](#), [Políticas administradas por el cliente](#) y [AWS políticas gestionadas](#) no pueden conceder ningún permiso que exceda los permisos que concede su límite de permisos. Un límite de permisos no concede ningún permiso, sino que hace que IAM ignore todos los permisos que exceden límite.

Al crear un conjunto de permisos con una política administrada por el cliente como límite de permisos, debe crear una política de IAM con el mismo nombre en cada Cuenta de AWS donde IAM Identity Center asigne el conjunto de permisos. IAM Identity Center adjunta la política de IAM como límite de permisos al rol de IAM que usted crea en su Cuenta de AWS .

Para obtener más información, consulte [Límites de permisos para las entidades de IAM](#) en la Guía del usuario de IAM.

## Creación, administración y eliminación de conjuntos de permisos

Los conjuntos de permisos definen el nivel de acceso que tienen los usuarios y grupos en una Cuenta de AWS. Los conjuntos de permisos se almacenan en IAM Identity Center y se pueden aprovisionar a una o varias Cuentas de AWS. Puedes asignar más de un conjunto de permisos a un usuario. Para obtener más información acerca de los conjuntos de permisos y cómo se usan en IAM Identity Center, consulte [Administre Cuentas de AWS con conjuntos de permisos](#).

### Note

Puede buscar y ordenar los conjuntos de permisos por nombre en la consola del IAM Identity Center.

Tenga en cuenta las siguientes consideraciones al crear conjuntos de permisos:

- Instancia de organización

Para usar conjuntos de permisos, necesitará usar una instancia de organización del IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

- Comience con un conjunto de permisos predefinido

Con un conjunto de permisos predefinido, que utiliza [permisos predefinidos](#), puede elegir una única política AWS gestionada de una lista de políticas disponibles. Cada política otorga un nivel específico de acceso a AWS los servicios y recursos o permisos para una función laboral común. Para obtener información sobre cada una de estas políticas, consulte [Políticas administradas de AWS para funciones de trabajo](#). Una vez recopilados los datos de uso, puede refinar el conjunto de permisos para que sea más restrictivo.

- Limite la duración de las sesiones de administración a periodos de trabajo razonables

Cuando los usuarios se federan en su Cuenta de AWS AWS Management Console o utilizan la interfaz de línea de AWS comandos (AWS CLI), IAM Identity Center utiliza la configuración de duración de la sesión del conjunto de permisos para controlar la duración de la sesión. Cuando la sesión del usuario alcance la duración de la sesión, se cerrará la sesión de la consola y se le pedirá que vuelva a iniciar sesión. Como práctica recomendada de seguridad, es aconsejable que no defina una duración de la sesión mayor de la que necesita para realizar el rol. De forma predeterminada, el valor de Duración de la sesión es de una hora. Puede especificar un valor

máximo de 12 horas. Para obtener más información, consulte [Definir la duración de la sesión para Cuentas de AWS](#).

- Limite la duración de las sesiones en el portal de usuarios de la plantilla

Los usuarios de la plantilla utilizan las sesiones del portal para elegir los roles y acceder a las aplicaciones. De forma predeterminada, el valor de Duración máxima de la sesión, que determina el tiempo que un usuario de la fuerza laboral puede iniciar sesión en el portal de AWS acceso antes de tener que volver a autenticarse, es de ocho horas. Puede especificar un valor máximo de 90 días. Para obtener más información, consulte [Configure la duración de la sesión del portal de acceso AWS y de las aplicaciones integradas del IAM Identity Center](#).

- Utilice el rol que proporcione permisos con privilegios mínimos

Cada conjunto de permisos que cree y asigne a su usuario aparece como un rol disponible en el portal de AWS acceso. Cuando inicie sesión en el portal en calidad de ese usuario, elija el rol que corresponda al conjunto de permisos más restrictivo que pueda usar para realizar tareas en la cuenta, en lugar de AdministratorAccess. Pruebe sus conjuntos de permisos para comprobar que proporcionan el acceso necesario antes de enviar la invitación al usuario.

#### Note

También puede utilizar [AWS CloudFormation](#) para crear y asignar conjuntos de permisos y asignar usuarios a esos conjuntos de permisos.

## Temas

- [Crea un conjunto de permisos.](#)
- [Ver y cambiar un conjunto de permisos](#)
- [Delegue la administración del conjunto de permisos](#)
- [Utilice las políticas de IAM en los conjuntos de permisos](#)
- [Elimine los conjuntos de permisos del Centro de identidades de IAM](#)
- [Eliminación de conjuntos de permisos de IAM Identity Center](#)

## Crea un conjunto de permisos.

Utilice este procedimiento para crear un conjunto de permisos predefinido que utilice una única política administrada o un conjunto de permisos personalizado de AWS que utilice hasta 10 políticas de AWS administradas o administradas por el cliente y una política integrada. Puede solicitar un ajuste en el número máximo de 10 políticas en la [consola Service Quotas](#) para IAM. Puede crear un conjunto de permisos en la consola de IAM Identity Center.

### Note

Para usar los conjuntos de permisos, necesitará usar una instancia organizativa del IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

### Creación de un conjunto de permisos

1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija Crear conjunto de permisos.
4. En la página Seleccione el tipo de conjunto de permisos, en Tipo de conjunto de permisos, seleccione un tipo.
5. Elija una o más políticas que desee usar para el conjunto de permisos, en característica del tipo de conjunto de permisos:
  - Conjunto de permisos predefinido
    1. En Política para el conjunto de permisos predefinido, seleccione una de las políticas de característica de trabajo o de permisos comunes de IAM de la lista y, a continuación, elija Siguiente. Con el fin de obtener más información, consulte las [políticas administradas por AWS](#) o las [políticas características de trabajo administradas por AWS](#) en la Guía del usuario de AWS Identity and Access Management IAM.
  - 2. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.
- Conjunto de permisos personalizado
  1. Elija Siguiente.

2. En la página Especificar políticas y límite de permisos, elija los tipos de políticas de IAM que desee aplicar a su nuevo conjunto de permisos. De forma predeterminada, puede añadir cualquier combinación de hasta 10 políticas administradas de AWS y políticas administradas por el cliente a su conjunto de permisos. Esta cuota la establece IAM. Para aprovechar esta cuota, solicite un aumento de la cuota de IAM en las políticas administradas asociadas a un rol de IAM en la consola de Service Quotas para cada Cuenta de AWS en la que desee asignar el conjunto de permisos.
- Amplíe las políticas AWS gestionadas para añadir políticas de IAM que creen AWS y mantengan. Para obtener más información, consulte [AWS políticas gestionadas](#).
  - a. Busque y elija las políticas administradas de AWS que desee aplicar a sus usuarios en el conjunto de permisos.
  - b. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.
- Amplíe las políticas administradas por el cliente para añadir políticas de IAM que usted cree y mantiene. Para obtener más información, consulte [Políticas administradas por el cliente](#).
  - a. Elija Adjuntar políticas e introduzca el nombre de la política que desee añadir a su conjunto de permisos. En cada cuenta a la que desee asignar el conjunto de permisos, cree una política con el nombre que ingresó. Como práctica recomendada, asigne los mismos permisos a la política en cada cuenta.
  - b. Seleccione Adjuntar más para añadir otra política.
  - c. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.
- Amplíe Política integrada para agregar un texto de política personalizado con formato JSON. Las políticas integradas no se corresponden con los recursos de IAM existentes. Para crear una política en línea, introduce un lenguaje de política personalizado en el formulario proporcionado. IAM Identity Center añade la política a los recursos de IAM que crea en las cuentas de sus miembros. Para obtener más información, consulte [Políticas insertadas](#).

- a. Agregue las acciones y los recursos que desee en el editor interactivo a su política integrada. Se pueden agregar declaraciones adicionales con Agregar nueva declaración.
    - b. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.
  - Amplíe el límite de permisos para añadir una AWS política de IAM gestionada o gestionada por el cliente como máximo de permisos que pueden asignar las demás políticas del conjunto de permisos. Para obtener más información, consulte [Límites de permisos](#).
    - a. Elija Utilizar un límite de permisos para controlar los permisos máximos.
    - b. Elija una política administrada por AWS para establecer una política de IAM que AWS cree y mantenga como sus límites de permisos. Elija políticas administradas por el cliente para establecer una política de IAM que usted cree y mantenga como sus límites de permisos.
    - c. Si desea añadir otro tipo de política, elija su contenedor y haga su selección. Seleccione Siguiente cuando haya elegido todas las políticas que quiera aplicar. Vaya al paso 6 para completar la página Detalles sobre cómo especificar el conjunto de permisos.
6. En la página Especificar detalles de conjunto de permisos, haga lo siguiente:
1. En Nombre del conjunto de permisos, escriba un nombre para identificar este conjunto de permisos en IAM Identity Center. El nombre que especifique para este conjunto de permisos aparece en el portal de AWS acceso como un rol disponible. Los usuarios inician sesión en el portal de AWS acceso, eligen un rol y Cuenta de AWS, a continuación, eligen el rol.

 Note

Los nombres de los conjuntos de permisos deben ser únicos en su instancia de IAM Identity Center.

2. (Opcional) También puede introducir una descripción. La descripción solo aparece en la consola del IAM Identity Center, no en el portal de AWS acceso.

3. (Opcional) Especifique el valor de la duración de la sesión. Este valor determina el tiempo que un usuario puede iniciar sesión antes de que la consola cierre su sesión. Para obtener más información, consulte [Definir la duración de la sesión para Cuentas de AWS](#).
4. (Opcional) Especifique el valor del estado de retransmisión. Este valor se utiliza en el proceso de federación para redirigir a los usuarios dentro de la cuenta. Para obtener más información, consulte [Configure el estado de la retransmisión para acceder rápidamente a AWS Management Console](#).

 Note

La URL del estado de retransmisión debe estar dentro de la AWS Management Console. Por ejemplo:

**`https://console.aws.amazon.com/ec2/`**

5. Expanda Etiquetas (opcional), elija Añadir etiqueta, y especifique los valores de Clave y valor (opcional).

Para obtener más información acerca de las etiquetas, consulte [Recursos de etiquetado AWS IAM Identity Center](#).

6. Elija Siguiente.
7. En la página Revisar y crear, revise las selecciones que ha realizado y, a continuación, elija Crear.
8. De forma predeterminada, al crear un conjunto de permisos, el conjunto de permisos no se aprovisiona (se usa en ninguno Cuentas de AWS). Para aprovisionar un conjunto de permisos en una Cuenta de AWS, debe asignar el acceso al Centro de Identidad de IAM a los usuarios y grupos de la cuenta y, a continuación, aplicar el conjunto de permisos a esos usuarios y grupos. Para obtener más información, consulte [Asigne el acceso de usuario o grupo a Cuentas de AWS](#).

## Ver y cambiar un conjunto de permisos

Puede utilizar conjuntos de permisos para conceder a los usuarios acceso a Cuentas de AWS. Puede ver y cambiar un conjunto de permisos con la AWS IAM Identity Center consola. Puede buscar y ordenar los conjuntos de permisos por nombre en la consola del IAM Identity Center. Para obtener más información acerca de los conjuntos de permisos y cómo se usan en IAM Identity Center, consulte [the section called “Conjuntos de permisos”](#).



No se requieren conjuntos de permisos para administrar el acceso de los usuarios a las aplicaciones.

 Note

Para usar conjuntos de permisos, necesitará usar una instancia organizativa del IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

Vea las asignaciones de conjuntos de permisos

Utilice este procedimiento para ver el conjunto de permisos aplicado en la AWS IAM Identity Center consola.

All Cuentas de AWS where a permission set is provisioned

Para ver todas las asignaciones de un conjunto de permisos, utilice el procedimiento siguiente:

1. Inicie sesión en AWS Management Console y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En Permisos para varias cuentas, elija Conjuntos de permisos.
3. En la página Conjuntos de permisos, seleccione el conjunto de permisos que desee ver.
4. Una vez en la página de conjuntos de permisos seleccionados, en la pestaña Cuentas, podrá ver las cuentas en las que se utiliza el conjunto de permisos. Puede seleccionar la cuenta para ver cómo se aprovisiona el conjunto de permisos en la cuenta. Puede [eliminar](#), editar y adjuntar políticas al conjunto de permisos.

All permission sets for an Cuenta de AWS

Para ver todas las asignaciones de un conjunto de permisos, utilice el siguiente procedimiento:

1. Inicie sesión en AWS Management Console y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En Permisos para varias cuentas, elija Cuentas de AWS. Seleccione la cuenta para la que desea ver los conjuntos de permisos aprovisionados.
3. Una vez en la Cuenta de AWS página seleccionada, en la pestaña Conjuntos de permisos, podrá ver los distintos conjuntos de permisos asignados al seleccionado Cuenta de AWS.

Puede seleccionar el hipervínculo del conjunto de permisos para obtener más información sobre el conjunto de permisos.

## All applied permission sets to users and groups

Para ver todos los conjuntos de permisos asignados a los usuarios o grupos, utilice el siguiente procedimiento:

1. Inicie sesión en AWS Management Console y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. Seleccione Usuarios o Grupos en el panel de control para ver los usuarios o grupos del IAM Identity Center.
  - a. Una vez en la página de usuarios, seleccione el usuario al que desee ver los conjuntos de permisos aplicados. A continuación, seleccione la Cuentas de AWS pestaña y la sección situada Cuenta de AWS debajo de la sección de acceso a la AWS cuenta. Podrás ver los conjuntos de permisos aplicados y Cuenta de AWS para el usuario seleccionado.
  - b. Una vez en la página Grupos, seleccione el grupo en el que desee ver los conjuntos de permisos aplicados. A continuación, seleccione la Cuentas de AWS pestaña y la sección situada Cuenta de AWS debajo de la sección de Cuenta de AWS acceso. Podrá ver los conjuntos de permisos aplicados y Cuenta de AWS para el grupo seleccionado.

## Cambiar un conjunto de permisos

Utilice este procedimiento para cambiar un [conjunto de permisos](#) con la consola de IAM Identity Center. Puede añadir o eliminar conjuntos de permisos de usuarios o grupos.

1. Inicie sesión en AWS Management Console y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En Permisos para varias cuentas, elija Cuentas de AWS.
3. En la página Cuenta de AWS, aparece una lista de su organización en forma de árbol. Seleccione el nombre de la Cuenta de AWS de la que desea cambiar el conjunto de permisos.
4. En la página Descripción general de la Cuenta de AWS, en Usuarios y grupos asignados, seleccione el nombre de usuario o el nombre del grupo del conjunto de permisos que desee cambiar. A continuación, elija Cambiar conjuntos de permisos.

5. Realice los cambios que desee en el conjunto de permisos y, a continuación, seleccione Guardar cambios.
6. Vaya a la pestaña Conjuntos de permisos, seleccione el conjunto de permisos modificado recientemente y elija Actualizar.
7. En la página Actualizar permisos, seleccione Actualizar.

## Delegue la administración del conjunto de permisos

El Centro de Identidad de IAM le permite delegar la administración de los conjuntos de permisos y las asignaciones en las cuentas mediante la creación de [políticas de IAM](#) que hacen referencia a los [nombres de recursos de Amazon \(ARNs\) de los recursos](#) del Centro de Identidad de IAM. Por ejemplo, puede crear políticas que permitan a distintos administradores administrar las asignaciones en cuentas específicas para conjuntos de permisos con etiquetas específicas.

### Note

Para usar conjuntos de permisos, necesitará usar una instancia organizativa del IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

Puede utilizar uno de los siguientes métodos para crear este tipo de políticas.

- (Recomendado) Cree [conjuntos de permisos](#) en IAM Identity Center, cada uno con una política diferente, y asigne los conjuntos de permisos a distintos usuarios o grupos. Esto le permite administrar permisos administrativos de los usuarios que inician sesión en el [origen de identidad de IAM Identity Center](#) que haya elegido.
- Cree políticas personalizadas en IAM y, a continuación, adjúntelas a los roles de IAM que asuman sus administradores. Para obtener información sobre las características, consulte [roles de IAM](#) para obtener los permisos administrativos que se les han asignado en IAM Identity Center.

### Important

Los recursos del IAM Identity Center ARNs distinguen mayúsculas de minúsculas.

A continuación, se muestra el caso adecuado para hacer referencia al conjunto de permisos y los tipos de recursos de la cuenta de IAM Identity Center.

| Tipos de recursos | ARN                                                                     | Claves de contexto         |
|-------------------|-------------------------------------------------------------------------|----------------------------|
| PermissionSet     | arn:\${Partition}:sso::permissionSet/\${InstanceId}/\${PermissionSetId} | aws:ResourceTag/\${TagKey} |
| Cuenta            | arn:\${Partition}:sso::account/\${AccountId}                            | No aplicable               |

## Utilice las políticas de IAM en los conjuntos de permisos

En [Crea un conjunto de permisos](#), aprendió a añadir políticas, incluidas las políticas administradas por el cliente y los límites de permisos, a un conjunto de permisos. Al añadir políticas y permisos administrados por el cliente a un conjunto de permisos, IAM Identity Center no crea ninguna política en Cuentas de AWS. En su lugar, debe crear esas políticas por adelantado en cada cuenta a la que desee asignar su conjunto de permisos y hacerlas coincidir con las especificaciones de nombre y ruta de su conjunto de permisos. Cuando asignas un conjunto de permisos a un Cuenta de AWS miembro de tu organización, el Centro de Identidad de IAM crea un [rol AWS Identity and Access Management \(IAM\)](#) y asocia tus políticas de [IAM](#) a ese rol.

### Consideraciones

- Para usar conjuntos de permisos, necesitará usar una instancia organizativa del IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).
- Antes de asignar el conjunto de permisos a las políticas de IAM, debe preparar su cuenta de miembro. El nombre de una política de IAM de su cuenta de miembro debe coincidir con el nombre de la política de su cuenta de administración. IAM Identity Center no puede asignar el conjunto de permisos si la política no existe en su cuenta de miembro.

 Note

Cuando se adjunta una política gestionada por el cliente a un conjunto de permisos, el nombre de la política no distingue entre mayúsculas y minúsculas.

- Los permisos que otorga la política no tienen por qué coincidir exactamente entre las cuentas.

### Asignar una política de IAM a un conjunto de permisos

1. Cree una política de IAM en cada uno de los Cuentas de AWS lugares a los que desee asignar el conjunto de permisos.
2. Asignar permisos a la política de IAM. Puede asignar diferentes permisos en diferentes cuentas. Para disfrutar de una experiencia coherente, configure y mantenga permisos idénticos en cada política. Puedes usar recursos de automatización, por ejemplo, AWS CloudFormation StackSets para crear copias de una política de IAM con el mismo nombre y permisos en cada cuenta de miembro. Para obtener más información al respecto CloudFormation StackSets, consulte [Cómo trabajar con ella AWS CloudFormation StackSets](#) en la guía del AWS CloudFormation usuario.
3. Cree un conjunto de permisos en su cuenta de administración y añada su política de IAM a las políticas administradas por el cliente o al límite de permisos. Para obtener más información sobre cómo crear un conjunto de permisos, consulte [Crea un conjunto de permisos](#).
4. Añada cualquier política integrada, política administrada por AWS o política de IAM adicional que haya preparado.
5. Cree y asigne su conjunto de permisos.

### Elimine los conjuntos de permisos del Centro de identidades de IAM

Puede eliminar un conjunto de permisos de los usuarios y grupos del IAM Identity Center en la consola del IAM Identity Center. También puede eliminar un conjunto de permisos de un. Cuenta de AWS Para obtener más información acerca de los conjuntos de permisos y cómo se usan en IAM Identity Center, consulte [Administre Cuentas de AWS con conjuntos de permisos](#).

**Note**

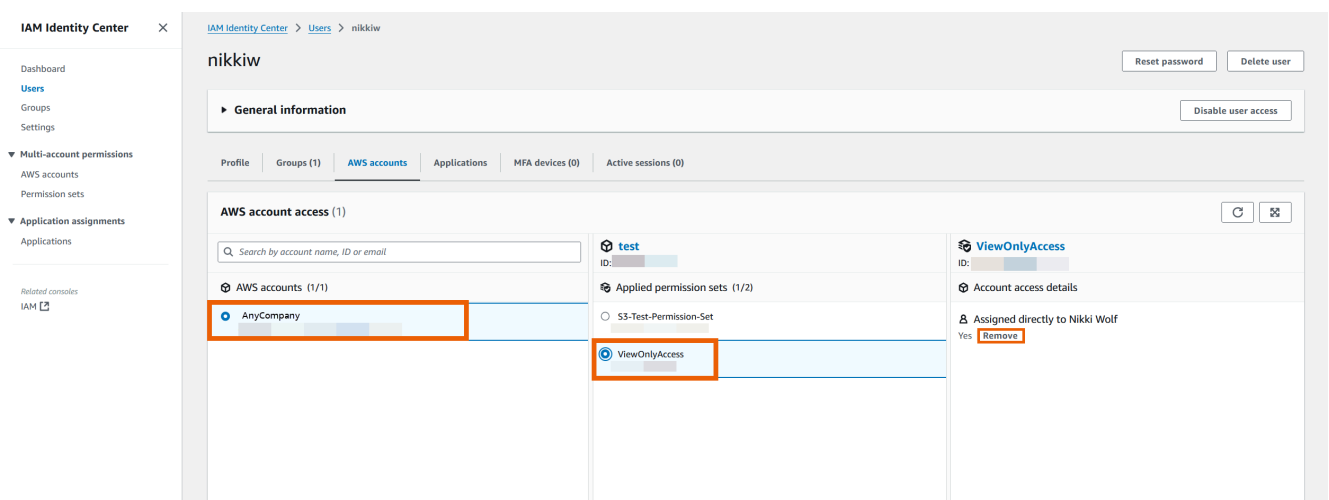
Para usar conjuntos de permisos, necesitará usar una instancia organizativa del IAM Identity Center. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).

## Remove permission set from a user

### Eliminar un conjunto de permisos de un usuario

Utilice este procedimiento para eliminar un conjunto de permisos de un usuario con la consola de IAM Identity Center.

1. Inicie sesión en AWS Management Console y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En el Centro de identidades de IAM, seleccione Usuarios.
3. Seleccione el nombre de usuario del que desee eliminar un conjunto de permisos.
4. En la página de detalles del usuario, seleccione la Cuentas de AWS pestaña. En Cuenta de AWS acceso, selecciona tu Cuenta de AWS.
5. En el panel derecho, aparecen los permisos aplicados al usuario seleccionado. Seleccione el conjunto de permisos que desee eliminar. En Detalles de acceso a la cuenta, selecciona Eliminar.
6. Aparece un cuadro de diálogo que le pregunta si desea eliminar este conjunto de permisos. Seleccione Eliminar.

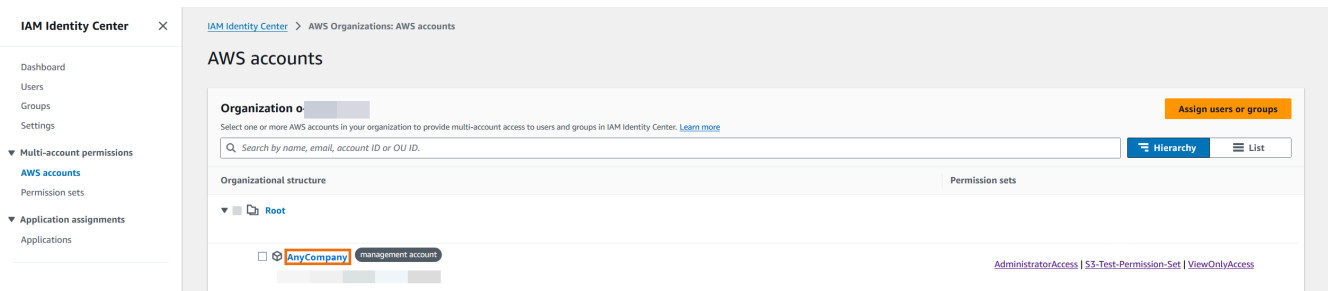


## Remove permission set from a group

### Eliminar un conjunto de permisos de un grupo

Utilice este procedimiento para eliminar un conjunto de permisos de un grupo con la consola de IAM Identity Center.

1. Inicie sesión en AWS Management Console y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En Permisos para varias cuentas, selecciona Cuentas de AWS. Selecciona el enlace a tu cuenta de administración.



3. En la pestaña Usuarios y grupos asignados, seleccione el grupo del que desee eliminar el conjunto de permisos y, a continuación, seleccione Cambiar conjunto de permisos.
4. En la página Cambiar conjuntos de permisos, borra el conjunto de permisos que desees eliminar y, a continuación, selecciona Guardar cambios.

## Remove permission set from an Cuenta de AWS

Utilice este procedimiento para eliminar un conjunto de permisos de la consola Cuenta de AWS de IAM Identity Center.

1. Inicie sesión en AWS Management Console y abra la AWS IAM Identity Center consola en <https://console.aws.amazon.com/singlesignon/>.
2. En Permisos para varias cuentas, selecciona Cuentas de AWS. Seleccione el nombre Cuenta de AWS del que desea eliminar el conjunto de permisos.
3. En la página de descripción general del Cuenta de AWS, seleccione la pestaña Conjuntos de permisos. Seleccione el conjunto de permisos que desee eliminar. A continuación, selecciona Eliminar.

4. En el cuadro de diálogo Eliminar conjunto de permisos, confirme que se ha seleccionado el conjunto de permisos correcto, escriba **Delete** para confirmar la eliminación y, a continuación, seleccione Eliminar acceso.

## Eliminación de conjuntos de permisos de IAM Identity Center

Antes de poder eliminar un conjunto de permisos del Centro de identidades de IAM, debe [eliminarlo](#) de todos los Cuentas de AWS que utilizan el conjunto de permisos. Para comprobar el acceso existente de usuarios y grupos, consulte [Ver y cambiar un conjunto de permisos](#).

### Consideraciones

- Para usar conjuntos de permisos, necesitará usar una instancia organizativa del Centro de identidades de IAM. Para obtener más información, consulte [Instancias de organización y cuenta de IAM Identity Center](#).
- Si desea revocar una sesión de conjunto de permisos activa, consulte [Revocar las sesiones de roles de IAM activas creadas por conjuntos de permisos](#).
- Debe eliminar los conjuntos de permisos y las asignaciones de aplicaciones de los usuarios o grupos que desee eliminar antes de eliminarlos. De lo contrario, tendrá conjuntos de permisos y aplicaciones sin asignar y sin usar en el Centro de identidades de IAM.

Utilice el siguiente procedimiento para eliminar uno o más conjuntos de permisos para que ningún miembro de la organización pueda utilizarlos. Cuenta de AWS

#### Important

Todos los usuarios y grupos a los que se haya asignado este conjunto de permisos, independientemente de quién lo utilice, ya no podrán iniciar sesión. Cuenta de AWS Para comprobar el acceso existente de usuarios y grupos, consulte [Ver y cambiar un conjunto de permisos](#).

Para eliminar un conjunto de permisos de un Cuenta de AWS

1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Seleccione el conjunto de permisos que desea eliminar y, a continuación, elija Eliminar.



4. En el cuadro de diálogo Eliminar conjunto de permisos, escriba el nombre del conjunto de permisos para confirmar la eliminación y, a continuación, seleccione Eliminar. El nombre distingue entre mayúsculas y minúsculas.

## Configure las propiedades del conjunto de permisos

En el IAM Identity Center, los administradores pueden realizar las siguientes tareas de configuración y administración para controlar el acceso de los usuarios y la duración de la sesión.

| Tarea                                                                                                                                                      | Más información                                                                                           |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|
| Los administradores pueden establecer la duración máxima de las sesiones de usuario al acceder a AWS los recursos a través del Centro de identidad de IAM. | <a href="#">Definir la duración de la sesión para Cuentas de AWS</a>                                      |
| Los administradores pueden personalizar la página de destino que ven los usuarios tras autenticarse correctamente a través del IAM Identity Center.        | <a href="#">Configure el estado de la retransmisión para acceder rápidamente a AWS Management Console</a> |
| Asegúrese de que los usuarios ya no tengan acceso a AWS los recursos cuando se revoquen sus permisos.                                                      | <a href="#">Utilice una política de denegación para revocar los permisos de los usuarios activos</a>      |

### Definir la duración de la sesión para Cuentas de AWS

Para cada [conjunto de permisos](#), puede especificar una duración de la sesión para controlar el tiempo durante el cual un usuario puede iniciar sesión en una cuenta de Cuenta de AWS. Cuando transcurra el tiempo especificado, AWS cierra la sesión del usuario.

Al crear un nuevo conjunto de permisos, la duración de la sesión se establece de forma predeterminada en una hora (en segundos). La duración mínima de la sesión es de una hora y se puede establecer en un máximo de 12 horas. IAM Identity Center crea automáticamente roles de IAM en cada cuenta asignada para cada conjunto de permisos y las configura con una duración máxima de sesión de 12 horas.

Cuando los usuarios se federan en su Cuenta de AWS consola o cuando se utiliza el AWS Command Line Interface (AWS CLI), el Centro de Identidad de IAM utiliza la configuración de duración de la sesión del conjunto de permisos para controlar la duración de la sesión. De forma predeterminada, los roles de IAM generados por IAM Identity Center para los conjuntos de permisos solo los pueden asumir los usuarios de IAM Identity Center, lo que garantiza que se cumpla la duración de sesión especificada en el conjunto de permisos de IAM Identity Center.

 Important

Como práctica recomendada de seguridad, es aconsejable que no defina una duración de la sesión mayor de la que necesita para realizar el rol.

Una vez que se ha creado un conjunto de permisos, puede actualizarlo para aplicar una nueva duración de la sesión. Utilice el siguiente procedimiento para modificar la duración de la sesión para un conjunto de permisos.

Para definir la duración de la sesión

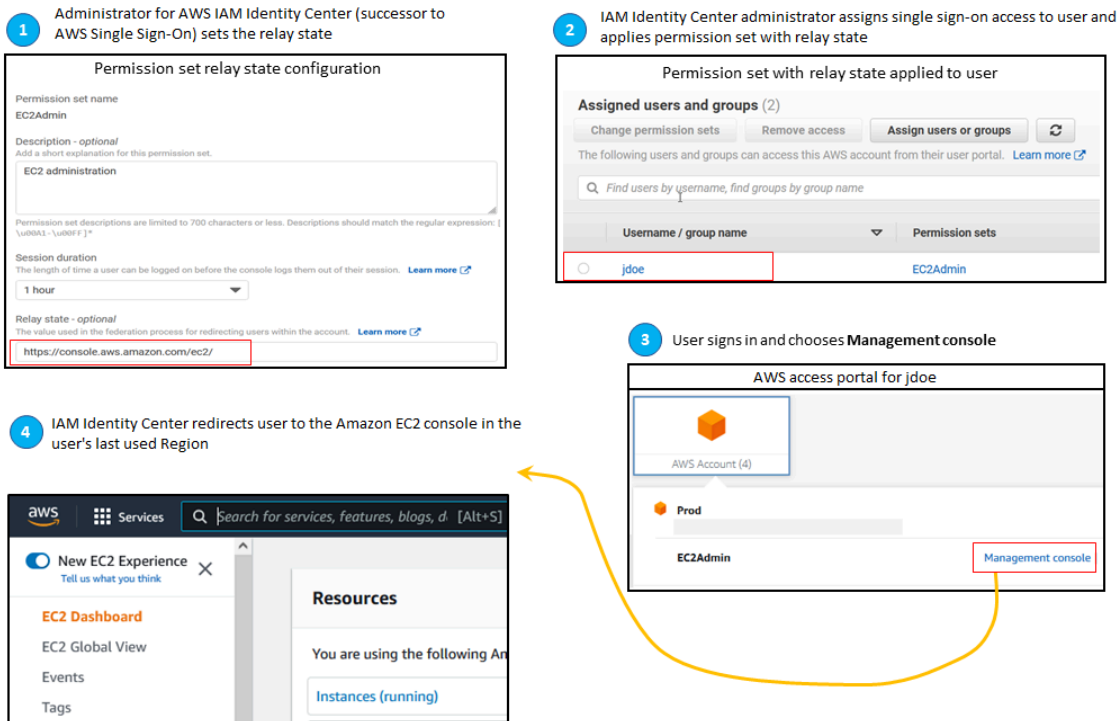
1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija el nombre del conjunto de permisos para el que desea cambiar la duración de la sesión.
4. En la página de detalles del conjunto de permisos, a la derecha del encabezado de la sección Configuración general, elija Editar.
5. En la página Editar la configuración general del conjunto de permisos, elija un nuevo valor para la duración de la sesión.
6. Si el conjunto de permisos está aprovisionado en alguna Cuentas de AWS, los nombres de las cuentas aparecen en Para volver Cuentas de AWS a aprovisionarse automáticamente. Una vez actualizado el valor de duración de la sesión del conjunto de permisos, se vuelve a aprovisionar a todas las personas Cuentas de AWS que utilizan el conjunto de permisos. Esto significa que el nuevo valor de esta configuración se aplica a todas las Cuentas de AWS que usen el conjunto de permisos.
7. Seleccione Save changes (Guardar cambios).
8. En la parte superior de la página de Cuentas de AWS, aparece una notificación.

- Si el conjunto de permisos está aprovisionado en una o varias Cuentas de AWS, la notificación confirma que las Cuentas de AWS se han reaprovisionado correctamente y que el conjunto de permisos actualizado se ha aplicado a las cuentas.
- Si el conjunto de permisos no está aprovisionado en una Cuenta de AWS, la notificación confirma que se actualizó la configuración del conjunto de permisos.

## Configure el estado de la retransmisión para acceder rápidamente a AWS Management Console

De forma predeterminada, cuando un usuario inicia sesión en el portal de AWS acceso, elige una cuenta y, a continuación, elige el rol que AWS crea a partir del conjunto de permisos asignado, el Centro de Identidad de IAM redirige el navegador del usuario al. AWS Management Console Puede cambiar este comportamiento si configura el estado de retransmisión en la URL de una consola diferente.

La configuración del estado de la retransmisión permite proporcionar al usuario un acceso rápido a la consola más adecuada para su rol. Por ejemplo, puede establecer el estado de retransmisión en la URL de la EC2 consola de Amazon (**<https://console.aws.amazon.com/ec2/>**) para redirigir al usuario a esa consola cuando elija el rol de EC2 administrador de Amazon. Durante el redireccionamiento a la URL predeterminada o a la URL del estado de retransmisión, el Centro de Identidad de IAM dirige el navegador del usuario al punto final de la consola en el último lugar Región de AWS utilizado por el usuario. Por ejemplo, si un usuario finalizó su última sesión de consola en la región de Europa (Estocolmo) (eu-north-1), se redirige al usuario a la consola de EC2 Amazon de esa región.



Para configurar IAM Identity Center para que redirija al usuario a una consola en una Región de AWS específica, incluya la especificación de la región como parte de la URL. Por ejemplo, para redirigir al usuario a la EC2 consola de Amazon en la región EE.UU. Este (Ohio) (us-east-2), especifique la URL de la consola de EC2 Amazon en esa región (). **https://us-east-2.console.aws.amazon.com/ec2/** Si ha habilitado IAM Identity Center en la región Oeste de EE. UU. (Oregón) (us-west-2) y desea dirigir al usuario a esa región, especifique **https://us-west-2.console.aws.amazon.com**.

## Configurar el estado de la retransmisión

Utilice el siguiente procedimiento para configurar la URL del estado de retransmisión de un conjunto de permisos.

1. Abra la [consola de IAM Identity Center](#)
2. En Permisos para varias cuentas, elija Conjunto de permisos.
3. Elija el nombre del conjunto de permisos para el que desea configurar la nueva URL de estado de retransmisión.
4. En la página de detalles del conjunto de permisos, a la derecha del encabezado de la sección Configuración general, elija Editar.

5. En la página Editar la configuración general del conjunto de permisos, en Estado de retransmisión, escriba la URL de la consola para cualquiera de los AWS servicios. Por ejemplo:

**`https://console.aws.amazon.com/ec2/`**

 Note

La URL del estado de retransmisión debe estar dentro de la AWS Management Console.

6. Si el conjunto de permisos está aprovisionado en alguna Cuentas de AWS, los nombres de las cuentas aparecen en Cuentas de AWS Para volver a aprovisionarse automáticamente. Una vez actualizada la URL del estado de retransmisión del conjunto de permisos, se vuelve a aprovisionar a todas las personas Cuentas de AWS que utilizan el conjunto de permisos. Esto significa que el nuevo valor de esta configuración se aplica a todos los Cuentas de AWS que usen el conjunto de permisos.
7. Seleccione Save changes (Guardar cambios).
8. En la parte superior de la página de organización de AWS , aparece una notificación.
  - Si el conjunto de permisos está aprovisionado en una o varias Cuentas de AWS, la notificación confirma que las Cuentas de AWS se han reaprovisionado correctamente y que el conjunto de permisos actualizado se ha aplicado a las cuentas.
  - Si el conjunto de permisos no está aprovisionado en una Cuenta de AWS, la notificación confirma que se actualizó la configuración del conjunto de permisos.

 Note

Puedes automatizar este proceso mediante la AWS API, un AWS SDK o el AWS Command Line Interface(AWS CLI). Para obtener más información, consulte:

- Las acciones CreatePermissionSet o UpdatePermissionSet de la referencia de la [API de IAM Identity Center](#)
- Los comandos create-permission-set o update-permission-set de la sección [sso-admin](#) de la Referencia de comandos de AWS CLI .

## Utilice una política de denegación para revocar los permisos de los usuarios activos

Es posible que tengas que revocar el acceso de un usuario del Centro de Identidad de IAM Cuentas de AWS mientras esté utilizando activamente un conjunto de permisos. Puede quitarle la posibilidad de usar sus sesiones de rol de IAM activas al implementar una política de denegación para un usuario no especificado con antelación y, cuando sea necesario, puede actualizar la política de denegación para especificar el usuario cuyo acceso deseas bloquear. En este tema, se explica cómo crear una política de denegación y las consideraciones sobre cómo implementar la política.

Prepárese para revocar una sesión de rol de IAM activa creada por un conjunto de permisos

Puede impedir que el usuario tome medidas con un rol de IAM que esté utilizando activamente al aplicar una política de denegación de acceso a un usuario específico mediante el uso de una política de control de servicios. También puede impedir que un usuario utilice cualquier conjunto de permisos hasta que cambie su contraseña, lo que evita que un usuario malintencionado o haga un uso indebido de credenciales robadas. Si necesita denegar el acceso de forma generalizada e impedir que un usuario vuelva a entrar en un conjunto de permisos o acceda a otros conjuntos de permisos, también puede eliminar todos los accesos de los usuarios, detener la sesión activa del portal de acceso AWS e inhabilitar el inicio de sesión del usuario. Consulte [Revocar las sesiones de roles de IAM activas creadas por conjuntos de permisos](#) para obtener información sobre cómo usar la política de denegación junto con acciones adicionales para una revocación de acceso más amplia.

### Política de denegación

Puede utilizar una política de denegación con una condición que coincida con el `UserID` del usuario en el almacén de identidades del IAM Identity Center para evitar que un rol de IAM que el usuario esté utilizando activamente lleve a cabo nuevas acciones. El uso de esta política evita que otros usuarios puedan estar utilizando el mismo conjunto de permisos al implementar la política de denegación. Esta política utiliza el marcador de posición de ID de usuario, *Add user ID here*, para `identitystore:userId` que deberá actualizarlo con el ID de usuario al que desee revocar el acceso.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "*"
      ],

```

```
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "identitystore:userId": "Add user ID here"
      }
    }
  }
]
```

Aunque puede usar otra clave de condición, por ejemplo, “aws:userId”, “identitystore:userId” es cierto que se trata de un valor único a nivel mundial que está asociado a una persona. El uso de “aws:userId” en esta condición puede verse afectado por la forma en que se sincronizan los atributos del usuario con respecto a la fuente de identidades y puede cambiar si el nombre de usuario o la dirección de correo electrónico del usuario cambian.

En la consola del IAM Identity Center, puede buscar el `identitystore:userId` de un usuario. Para ello, vaya a Usuarios, busque el usuario por su nombre, amplíe la sección de información general y copie el ID. También es conveniente detener la sesión del portal de AWS acceso de un usuario e inhabilitar su acceso de inicio de sesión en la misma sección mientras busca el seudónimo. Para automatizar el proceso de creación de una política de denegación, obtenga el seudónimo del usuario consultando el almacén de identidades. APIs

### Implementación de la política de denegación

Puedes usar un seudónimo que no sea válido, por ejemplo *Add user ID here*, para implementar la política de denegación con antelación mediante una política de control de servicios (SCP) que adjuntes a Cuentas de AWS los usuarios a la que puedan tener acceso. Este es el enfoque recomendado por su facilidad y velocidad de impacto. Cuando revoque el acceso de un usuario con la política de denegación, editará la política para reemplazar el marcador de posición de ID de usuario por el ID de la persona cuyo acceso deseas revocar. Esto impide que el usuario realice alguna acción con los permisos establecidos en todas las cuentas que asocie al SCP. Bloquea las acciones del usuario incluso si utiliza su sesión activa en el portal de acceso AWS para navegar a diferentes cuentas y asumir funciones diferentes. Con el acceso del usuario totalmente bloqueado por el SCP, puede deshabilitar su capacidad de iniciar sesión, revocar sus asignaciones y detener su sesión en el portal de AWS acceso si es necesario.

Como alternativa al uso SCPs, también puede incluir la política de denegación en la política integrada de conjuntos de permisos y en las políticas administradas por el cliente que utilizan los conjuntos de permisos a los que el usuario puede acceder.

Si debe revocar el acceso a más de una persona, puede utilizar una lista de valores en el bloque de condiciones, como:

```
"Condition": {
  "StringEquals": {
    "identitystore:userId": [" user1 userId", "user2 userId"...]
  }
}
```

### Important

Independientemente del método o los métodos que utilice, debe tomar cualquier otra medida correctiva y mantener el ID del usuario en la política durante al menos 12 horas. Transcurrido ese tiempo, todas las funciones que el usuario haya asumido caducarán y, a continuación, podrá eliminar su ID de la política de denegación.

## Hacer referencia a conjuntos de permisos en políticas de recursos, mapas de configuración de Amazon EKS Cluster y políticas AWS KMS clave

Al asignar un conjunto de permisos a una AWS cuenta, el Centro de Identidad de IAM crea un rol con un nombre que comienza por. `AWSReservedSSO_`

El nombre completo y el nombre de recurso de Amazon (ARN) del rol utilizan el siguiente formato:

| Nombre                                                                             | ARN                                                                                                                                                                            |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>AWSReservedSSO_ <i>permission-set-name</i><br/><i>e-unique-suffix</i></code> | <code>arn:aws:iam:: <i>aws-account-ID</i>:role/aws-reserved/sso.amazonaws.com/ <i>aws-region</i> /AWSReservedSSO_ <i>permission-set-name</i><br/><i>e-unique-suffix</i></code> |

Si su fuente de identidad en el Centro de identidad de IAM está alojada en us-east-1, no *aws-region* existe en el ARN. El nombre completo y el (ARN) del rol utilizan el siguiente formato:



| Nombre                                                   | ARN                                                                                                                                       |
|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| AWSReservedSSO_ <i>permission-set-name_unique-suffix</i> | arn:aws:iam:: <i>aws-account-ID</i> :role/<br>aws-reserved/sso.amazonaws.com/<br>AWSReservedSSO_ <i>permission-set-name_unique-suffix</i> |

Por ejemplo, si crea un conjunto de permisos que concede acceso a la AWS cuenta a los administradores de bases de datos, se crea el rol correspondiente con el siguiente nombre y ARN:

| Nombre                                                | ARN                                                                                                                                   |
|-------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| AWSReservedSSO_DatabaseAdministrator_1234567890abcdef | arn:aws:iam::111122223333:role/<br>aws-reserved/sso.amazonaws.com/<br>eu-west-2/AWSReservedSSO_DatabaseAdministrator_1234567890abcdef |

Si elimina todas las asignaciones a este conjunto de permisos de la AWS cuenta, también se eliminará el rol correspondiente que creó IAM Identity Center. Si más adelante realiza una nueva asignación al mismo conjunto de permisos, IAM Identity Center crea un nuevo rol para el conjunto de permisos. El nombre y el ARN del nuevo rol incluyen un sufijo diferente y único. En este ejemplo, el sufijo único es abcdef0123456789.

| Nombre                                                        | ARN                                                                                                                                           |
|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| AWSReservedSSO_DatabaseAdministrator_ <b>abcdef0123456789</b> | arn:aws:iam::111122223333:role/<br>aws-reserved/sso.amazonaws.com/<br>eu-west-2/AWSReservedSSO_DatabaseAdministrator_ <b>abcdef0123456789</b> |

El cambio de sufijo en el nuevo nombre y ARN del rol provocará que cualquier política que haga referencia al nombre y al ARN originales lo out-of-date sea, lo que interrumpirá el acceso de las

personas que usen el conjunto de permisos correspondiente. Por ejemplo, un cambio en el ARN del rol interrumpirá el acceso de los usuarios del conjunto de permisos si se hace referencia al ARN original en las siguientes configuraciones:

- En el fichero `aws-auth ConfigMap` para los clústeres de Amazon Elastic Kubernetes Service (Amazon EKS) cuando utiliza el `aws-auth ConfigMap` para el acceso al clúster.
- En una política basada en recursos para una clave (). AWS Key Management Service AWS KMS. Esta política también se denomina política de claves.

#### Note

Le recomendamos que utilice las [entradas de acceso de Amazon EKS](#) para gestionar el acceso a sus clústeres de Amazon EKS. Esto le permite usar los permisos de IAM para administrar los principales que tienen acceso a un clúster de Amazon EKS. Al utilizar las entradas de acceso de Amazon EKS, puede utilizar una entidad principal de IAM con permisos de Amazon EKS para recuperar el acceso a un clúster sin necesidad de ponerse en contacto con Soporte.

Si bien puede actualizar las políticas basadas en recursos de la mayoría de AWS los servicios para que hagan referencia a un nuevo ARN para un rol que corresponda a un conjunto de permisos, debe tener un rol de respaldo que cree en IAM para Amazon EKS si AWS KMS el ARN cambia. En el caso de Amazon EKS, el rol de IAM de respaldo debe existir en `aws-auth ConfigMap`. Para ello AWS KMS, debe estar en sus políticas clave. Si no tienes un rol de IAM alternativo con permisos para actualizar la política `aws-auth ConfigMap` o la política AWS KMS clave, ponte en contacto con nosotros Soporte para recuperar el acceso a esos recursos.

## Recomendaciones para evitar interrupciones en el acceso

Para evitar interrupciones en el acceso debido a cambios en el ARN de un rol que corresponde a un conjunto de permisos, le recomendamos que haga lo siguiente.

- Mantenga al menos una asignación de conjunto de permisos.

Mantenga esta asignación en las AWS cuentas que contienen las funciones a las que hace referencia en Amazon EKS, en las políticas clave o en AWS KMS las políticas basadas en recursos para otras. `aws-auth ConfigMap` Servicios de AWS

Por ejemplo, si crea un conjunto de EKSAccess permisos y hace referencia al ARN de rol correspondiente desde la AWS cuenta111122223333, asigna permanentemente un grupo administrativo al conjunto de permisos de esa cuenta. Como la asignación es permanente, IAM Identity Center no eliminará el rol correspondiente, lo que elimina el riesgo de cambiar el nombre. El grupo administrativo siempre tendrá acceso sin correr el riesgo de que se incrementen los privilegios.

- Para los clústeres de Amazon EKS que utilizan **aws-auth ConfigMap** e AWS KMS incluyen un rol creado en IAM.

Si hace referencia al rol ARNs para los conjuntos de permisos de un **aws-auth ConfigMap** clúster de Amazon EKS o a las políticas clave para AWS KMS las claves, le recomendamos que también incluya al menos un rol que cree en IAM. El rol debe permitirle acceder al clúster de Amazon EKS o administrar la política AWS KMS clave. El conjunto de permisos debe poder asumir este rol. De esta forma, si el ARN del rol de un conjunto de permisos cambia, puede actualizar la referencia al ARN en la **aws-auth ConfigMap** política clave o. AWS KMS En la siguiente sección, se proporciona un ejemplo de cómo se puede crear una política de confianza para un rol creado en IAM. El rol solo lo puede asumir un conjunto de permisos de AdministratorAccess.

## Ejemplo de políticas de confianza personalizadas

A continuación se muestra un ejemplo de una política de confianza personalizada que proporciona un conjunto de permisos de AdministratorAccess con acceso a un rol creado en IAM. Entre los elementos clave de esta base, se incluyen los siguientes:

- El elemento principal de esta política de confianza especifica el principal de la AWS cuenta. En esta política, los directores de la AWS cuenta 111122223333 con **sts:AssumeRole** permisos pueden asumir la función creada en IAM.
- El **Condition** element de esta política de confianza especifica requisitos adicionales para las entidades principales que pueden asumir el rol creado en IAM. En esta política, el conjunto de permisos con el siguiente rol ARN puede asumir el rol.

```
arn:aws:iam::111122223333:role/aws-reserved/sso.amazonaws.com/eu-west-2/
AWSReservedSSO_AdministratorAccess_*
```

 Note

El elemento `Condition` incluye el operador de condiciones `ArnLike` y utiliza un comodín al final del ARN del rol de permisos, en lugar de un sufijo único. Esto significa que la política permite que el conjunto de permisos asuma el rol creado en IAM incluso si el ARN del rol del conjunto de permisos cambia.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::111122223333:root"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws:iam::111122223333:role/aws-reserved/
sso.amazonaws.com/eu-west-2/AWSReservedSSO_AdministratorAccess_*"
        }
      }
    }
  ]
}
```

La inclusión de un rol que cree en IAM en dicha política le proporcionará acceso de emergencia a sus clústeres de Amazon EKS u otros AWS recursos si un conjunto de permisos o todas las asignaciones al conjunto de permisos se eliminan y se vuelven a crear accidentalmente. AWS KMS keys

## Control de acceso basado en atributos

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. Puede utilizar el Centro de Identidad de IAM para gestionar el acceso a sus AWS recursos a través de varios Cuentas de AWS atributos de usuario que procedan de cualquier fuente de identidad del Centro de Identidad de IAM. En AWS, estos atributos se

denominan etiquetas. El uso de los atributos de usuario como etiquetas le AWS ayuda a simplificar el proceso de creación de permisos detallados AWS y garantiza que sus empleados solo tengan acceso a AWS los recursos con las etiquetas correspondientes.

Por ejemplo, puede asignar a los desarrolladores Bob y Sally, que pertenecen a 2 equipos diferentes, el mismo conjunto de permisos en IAM Identity Center y, a continuación, seleccionar el atributo del nombre del equipo para controlar el acceso. Cuando Bob y Sally inician sesión en su Cuentas de AWS, el Centro de Identidad de IAM envía el atributo del nombre del equipo en la AWS sesión para que Bob y Sally solo puedan acceder a los recursos AWS del proyecto si el atributo del nombre del equipo coincide con la etiqueta del nombre del equipo del recurso del proyecto. Si Bob se pasa al equipo de Sally en el futuro, puede modificar su acceso simplemente actualizando el atributo de nombre de su equipo en el directorio corporativo. La próxima vez que Bob inicie sesión, tendrá acceso automáticamente a los recursos del proyecto de su nuevo equipo sin necesidad de actualizar los permisos de AWS.

Este enfoque también ayuda a reducir el número de permisos distintos que hay que crear y gestionar en IAM Identity Center, ya que los usuarios asociados a los mismos conjuntos de permisos ahora pueden tener permisos únicos en característica de sus atributos. Puede utilizar estos atributos de usuario en los conjuntos de permisos y las políticas basadas en recursos del Centro de Identidad de IAM para implementar el ABAC en los recursos y simplificar la gestión de permisos a gran escala AWS.

## Ventajas

Las siguientes son ventajas adicionales del uso de ABAC en IAM Identity Center.

- ABAC requiere menos conjuntos de permisos: dado que no tiene que crear diferentes políticas para diferentes roles de trabajo, debe crear menos conjuntos de permisos. Esto reduce la complejidad de la administración de permisos.
- Con ABAC, los equipos pueden cambiar y crecer rápidamente: los permisos para los nuevos recursos se conceden automáticamente en característica de los atributos cuando los recursos se etiquetan adecuadamente al crearlos.
- Utilice los atributos de los empleados de su directorio corporativo con ABAC: puede utilizar los atributos de los empleados existentes de cualquier fuente de identidad configurada en IAM Identity Center para tomar decisiones de control de acceso en AWS.
- AWS CloudTrail Controle quién accede a los recursos: los administradores de seguridad pueden determinar fácilmente la identidad de una sesión al revisar los atributos del usuario para realizar un seguimiento de la actividad de los usuarios. AWS

Para obtener información acerca de cómo configurar ABAC mediante la consola de IAM Identity Center, consulte [Atributos para controlar el acceso](#). Para obtener información sobre cómo habilitar y configurar ABAC mediante el Centro de identidad de IAM APIs, consulte [CreateInstanceAccessControlAttributeConfiguration](#) la Guía de referencia de la API del Centro de identidades de IAM.

## Temas

- [Lista de comprobación: configurar ABAC mediante el IAM Identity Center AWS](#)
- [Atributos para controlar el acceso](#)

## Lista de comprobación: configurar ABAC mediante el IAM Identity Center AWS

Esta lista de comprobación incluye las tareas de configuración necesarias para preparar los recursos de AWS y configurar IAM Identity Center para el acceso a ABAC. Completar las tareas en esta lista de verificación en orden. Cuando un enlace de referencia lo lleve a un tema, vuelva a ese tema para poder continuar con el resto de las tareas de esta lista de verificación.

| Paso | Tarea                                                                                                                                                                                                                                                                                                                                  | Referencia                                                 |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------|
| 1    | Revise cómo añadir etiquetas a todos sus recursos.<br>AWS Para implementar ABAC en IAM Identity Center, primero tendrá que añadir etiquetas a todos los recursos de AWS en los que desee implementar ABAC.                                                                                                                             | • <a href="#">Etiquetar recursos AWS</a>                   |
| 2    | Revise cómo configurar su origen de identidad en IAM Identity Center con las identidades y los atributos de usuario asociados en su almacén de identidades.<br>El Centro de Identidad de IAM le permite utilizar los atributos de usuario de cualquier fuente de identidad del Centro de Identidad de IAM compatible para ABAC in. AWS | • <a href="#">Administración de su fuente de identidad</a> |
| 3    | En función de los siguientes criterios, determine qué atributos desea utilizar para tomar decisiones de control de acceso AWS y envíelos al IAM Identity Center.                                                                                                                                                                       | • <a href="#">Introducción</a>                             |

| Paso | Tarea                                                                                                                                                                                                                                                                                                                                                                                                    | Referencia                                                                                                                                                                                                                                                                                                                                                              |
|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | <ul style="list-style-type: none"> <li>Si utiliza un proveedor de identidades (IdP) externo, decida si desea utilizar los atributos transferidos desde el IdP o seleccionar los atributos de IAM Identity Center.</li> </ul>                                                                                                                                                                             | <ul style="list-style-type: none"> <li><a href="#">Elección de los atributos al utilizar un proveedor de identidades externo como fuente de identidad</a></li> </ul>                                                                                                                                                                                                    |
|      | <ul style="list-style-type: none"> <li>Si elige que su IdP envíe atributos, configure su IdP para que transmita los atributos en las aserciones de SAML. Consulte las secciones <code>Optional</code> del tutorial correspondiente a su IdP específico.</li> </ul>                                                                                                                                       | <ul style="list-style-type: none"> <li><a href="#">Tutoriales de fuentes de identidad de IAM Identity Center</a></li> </ul>                                                                                                                                                                                                                                             |
|      | <ul style="list-style-type: none"> <li>Si utiliza un IdP como fuente de identidad y elige seleccionar atributos en IAM Identity Center, averigüe cómo configurar el SCIM para que los valores de los atributos procedan de su IdP. Si no puede utilizar SCIM con su IdP, añada los usuarios y sus atributos mediante la página de usuario de la consola de IAM Identity Center.</li> </ul>               | <ul style="list-style-type: none"> <li><a href="#">Aprovisionamiento de un proveedor de identidad externo al IAM Identity Center mediante SCIM</a></li> <li><a href="#">Atributos de proveedor de identidad externos compatibles</a></li> </ul>                                                                                                                         |
|      | <ul style="list-style-type: none"> <li>Si utiliza Active Directory o IAM Identity Center como fuente de identidad, o si utiliza un IdP y elige seleccionar atributos en IAM Identity Center, revise los atributos disponibles que puede configurar. A continuación, vaya inmediatamente al paso 4 para empezar a configurar los atributos de ABAC mediante la consola de IAM Identity Center.</li> </ul> | <ul style="list-style-type: none"> <li><a href="#">Elección de los atributos al utilizar IAM Identity Center como fuente de identidad</a></li> <li><a href="#">Elección de los atributos al utilizar AWS Managed Microsoft AD como origen de identidad</a></li> <li><a href="#">Mapeos predeterminados entre Centro de identidades de IAM y Microsoft AD</a></li> </ul> |

| Paso | Tarea                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | Referencia                                                                                                                              |
|------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 4    | <p>Seleccione los atributos que desee utilizar para ABAC en la página Atributos para el control de acceso de la consola de IAM Identity Center. En esta página, puede seleccionar los atributos para el control de acceso desde el origen de identidad que configuró en el paso 2. Una vez que sus identidades y sus atributos estén en el Centro de Identidad de IAM, debe crear pares clave-valor (mapeos) que se le transferirán Cuentas de AWS para que los utilice en las decisiones de control de acceso.</p>                     | <ul style="list-style-type: none"> <li>• <a href="#">Habilitación y configuración de atributos para el control de acceso</a></li> </ul> |
| 5    | <p>Cree políticas de permisos personalizadas dentro de su conjunto de permisos y utilice los atributos de control de acceso para crear reglas ABAC, de modo que los usuarios solo puedan acceder a los recursos con etiquetas coincidentes. Los atributos de usuario que configuró en el paso 4 se utilizan como etiquetas en AWS para tomar decisiones sobre el control de acceso. Puede hacer referencia a los atributos de control de acceso en la política de permisos mediante la condición <code>aws:PrincipalTag/key</code>.</p> | <ul style="list-style-type: none"> <li>• <a href="#">Crear políticas de permisos para ABAC en IAM Identity Center</a></li> </ul>        |
| 6    | <p>En sus archivos Cuentas de AWS, asigne los usuarios a los conjuntos de permisos que creó en el paso 5. De este modo, se garantiza que, cuando se federen en sus cuentas y accedan a AWS los recursos, solo obtengan acceso en función de las etiquetas coincidentes.</p>                                                                                                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• <a href="#">Asigne el acceso de usuario o grupo a Cuentas de AWS</a></li> </ul>                |

Tras completar estos pasos, los usuarios que se federen en un único inicio Cuenta de AWS de sesión tendrán acceso a sus AWS recursos en función de los atributos coincidentes.

## Atributos para controlar el acceso

Atributos para el control de acceso es el nombre de la página de la consola de IAM Identity Center en la que se seleccionan los atributos de usuario que se quieren utilizar en las políticas para controlar



el acceso a los recursos. Puedes asignar usuarios a las cargas de trabajo en AWS función de los atributos existentes en la fuente de identidad de los usuarios.

Por ejemplo, suponga que desea asignar acceso a los buckets de S3 en característica de los nombres de los departamentos. En la página Atributos para el control de acceso, seleccione el atributo de usuario Departamento para su uso con el control de acceso basado en atributos (ABAC). En el conjunto de permisos de IAM Identity Center, escriba una política que conceda acceso a los usuarios solo cuando el atributo Departamento coincida con la etiqueta de departamento que asignó a sus buckets de S3. IAM Identity Center transfiere el atributo de departamento del usuario a la cuenta a la que se accede. A continuación, el atributo se utiliza para determinar el acceso en característica de la política. Para obtener más información acerca de Pitr, consulte [Control de acceso basado en atributos](#).

## Introducción

La forma de empezar a configurar los atributos para el control de acceso depende del origen de identidad que utilice. Independientemente del origen de identidad que elija, una vez seleccionados los atributos, tendrá que crear o editar las políticas de conjuntos de permisos. Estas políticas deben permitir que las identidades de los usuarios accedan a los recursos de AWS .

### Elección de los atributos al utilizar IAM Identity Center como fuente de identidad

Al configurar IAM Identity Center como fuente de identidad, primero se añaden los usuarios y se configuran sus atributos. A continuación, vaya a la página Atributos para el control de acceso y seleccione los atributos que desee utilizar en las políticas. Por último, navegue hasta la página Cuentas de AWS para crear o editar conjuntos de permisos para usar los atributos de ABAC.

### Elección de los atributos al utilizar AWS Managed Microsoft AD como origen de identidad

Al configurar el Centro de identidades de IAM AWS Managed Microsoft AD como fuente de identidad, primero se asigna un conjunto de atributos de Active Directory a los atributos de usuario del Centro de identidades de IAM. A continuación, vaya a la página de atributos para el control de acceso. A continuación, elija los atributos que desee utilizar en la configuración de ABAC en característica del conjunto existente de atributos de SSO mapeados desde Active Directory. Por último, cree reglas de ABAC utilizando los atributos de control de acceso de los conjuntos de permisos para permitir que las identidades de los usuarios accedan a los recursos de AWS . Para obtener una lista de las asignaciones predeterminadas de los atributos de usuario del Centro de identidades de IAM a los atributos de usuario de su directorio, consulte. AWS Managed Microsoft AD [Mapeos predeterminados entre Centro de identidades de IAM y Microsoft AD](#)

## Elección de los atributos al utilizar un proveedor de identidades externo como fuente de identidad

Al configurar IAM Identity Center con un proveedor de identidades (IdP) externo como origen de identidad, hay 2 formas de utilizar los atributos de ABAC.

- Puede configurar su IdP para que envíe los atributos mediante aserciones de SAML. En este caso, IAM Identity Center transfiere el nombre y el valor del atributo desde el IdP para la evaluación de la política.

### Note

Los atributos de las aserciones de SAML no estarán visibles en la página Atributos para el control de acceso. Deberá conocer estos atributos con antelación y añadirlos a las reglas de control de acceso al crear políticas. Si decide confiar en los atributos externos IdPs, estos atributos siempre se transferirán cuando los usuarios se federen en ellos. Cuentas de AWS En situaciones en las que los mismos atributos llegan a IAM Identity Center a través de SAML y SCIM, el valor de los atributos de SAML prevalece en las decisiones de control de acceso.

- Puede configurar los atributos que utilizará en la página Atributos para el control de acceso de la consola de IAM Identity Center. Los valores de atributos que elija aquí sustituyen a los valores de cualquier atributo coincidente que provenga de un IdP a través de una afirmación. Dependiendo de si utiliza o no SCIM, tenga en cuenta lo siguiente:
  - Si utiliza SCIM, el IdP sincroniza automáticamente los valores de los atributos en IAM Identity Center. Es posible que los atributos adicionales necesarios para el control de acceso no estén presentes en la lista de atributos del SCIM. En ese caso, considere la posibilidad de colaborar con el administrador de TI de su IdP para enviar dichos atributos a IAM Identity Center mediante aserciones de SAML con el prefijo requerido `https://aws.amazon.com/SAML/Attributes/AccessControl:`. Para obtener información sobre cómo configurar los atributos de usuario para el control de acceso en su IdP para enviarlos mediante aserciones de SAML, consulte el [Tutoriales de fuentes de identidad de IAM Identity Center](#) de su IdP.
  - Si no utiliza SCIM, debe añadir los usuarios manualmente y establecer sus atributos como si utilizara IAM Identity Center como origen de identidad. A continuación, vaya a la página Atributos para el control de acceso y seleccione los atributos que desee utilizar en las políticas.

Para obtener una lista completa de los atributos de usuario compatibles entre los atributos de usuario del Centro de Identidad de IAM y los atributos de usuario del externo IdPs, consulte. [Atributos de proveedores de identidad externos compatibles](#)

Para comenzar a utilizar ABAC en IAM Identity Center, consulte los temas siguientes.

#### Temas

- [Habilitación y configuración de atributos para el control de acceso](#)
- [Crear políticas de permisos para ABAC en IAM Identity Center](#)

## Habilitación y configuración de atributos para el control de acceso

[Para utilizar el control de acceso basado en atributos \(ABAC\), primero debe activarlo en la página de configuración de la consola de IAM Identity Center o en la API del IAM Identity Center.](#)

Independientemente de la fuente de identidad, siempre puede configurar los atributos de usuario desde el almacén de identidades para usarlos en ABAC. En la consola, puede hacerlo accediendo a la pestaña Atributos para el control de acceso de la página de configuración. Si utilizas un proveedor de identidad (IdP) externo como fuente de identidad, también tienes la opción de recibir atributos del IdP externo en las aserciones de SAML. En este caso, debe configurar el IdP externo para enviar los atributos deseados. Si un atributo de una afirmación de SAML también se define como atributo ABAC en el Centro de Identidad de IAM, el Centro de Identidad de IAM enviará el valor desde su almacén de identidades como etiqueta de sesión al iniciar [sesión](#) en un. Cuenta de AWS

#### Note

No puede ver los atributos configurados y enviados por un IdP externo desde la página Atributos para el control de acceso de la consola de IAM Identity Center. Si transfiere atributos de control de acceso en las aserciones de SAML desde su IdP externo, esos atributos se envían directamente a la Cuenta de AWS cuando los usuarios se federan. Los atributos no estarán disponibles en IAM Identity Center para su mapeo.

#### Temas

- [Activar atributos para el control de acceso](#)
- [Seleccione sus atributos para controlar el acceso](#)
- [Desactivar atributos para el control de acceso](#)

## Activar atributos para el control de acceso

Utilice el siguiente procedimiento para activar la característica de control de los atributos de acceso (ABAC) mediante la consola de IAM Identity Center.

### Note

Si ya tiene conjuntos de permisos y planea habilitar ABAC en su instancia de IAM Identity Center, las restricciones de seguridad adicionales requieren que primero tenga la política `iam:UpdateAssumeRolePolicy`. Estas restricciones de seguridad adicionales no son obligatorias si no ha creado ningún conjunto de permisos en su cuenta.

## Cómo activar atributos para el control de acceso

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, busque el cuadro de información Atributos para el control de acceso y, a continuación, elija Activar. Continúe con el siguiente procedimiento para configurarlo.

## Seleccione sus atributos para controlar el acceso

Utilice el siguiente procedimiento para configurar atributos para la configuración de ABAC.

## Selección de los atributos mediante la consola de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Atributos para el control de acceso y, a continuación, elija Administrar atributos.
4. En la página Atributos para el control de acceso, seleccione Añadir atributo e introduzca los detalles de clave y valor. Aquí es donde mapeará el atributo que proviene de su fuente de identidad a un atributo que IAM Identity Center pasa como etiqueta de sesión.

| Key ⓘ       | Value (optional) ⓘ                          | Remove |
|-------------|---------------------------------------------|--------|
| Department  | <code>\${path:enterprise.department}</code> | ✕      |
| CostCenter  | <code>\${path:enterprise.costCenter}</code> | ✕      |
| Add new key | Add new value                               |        |

La clave representa el nombre que se le da al atributo para su uso en las políticas. Puede ser cualquier nombre arbitrario, pero debe especificar ese nombre exacto en las políticas que cree para el control de acceso. Por ejemplo, supongamos que utiliza Okta (un IdP externo) como fuente de identidad y necesita transferir los datos del centro de costos de su organización como etiquetas de sesión. En Key, debe introducir un nombre que coincida de forma similar, como el nombre de su clave. CostCenter Es importante tener en cuenta que, sea cual sea el nombre que elija aquí, también debe tener el mismo nombre en su [Clave de condición de aws:PrincipalTag](#) (es decir, "ec2:ResourceTag/CostCenter": "\${aws:PrincipalTag/CostCenter}").

#### ⓘ Note

Use un atributo de un solo valor para su clave (por ejemplo, **Manager**). Por ejemplo, IAM Identity Center no admite atributos con varios valores para ABAC (por ejemplo, **Manager, IT Systems**).

El valor representa el contenido del atributo que proviene del origen de la identidad configurada. Aquí puede introducir cualquier valor de la tabla de fuentes de identidad correspondiente que aparece en [Asignaciones de atributos entre Centro de identidades de IAM y directorio de proveedores de identidades externos](#). Por ejemplo, utilizando el contexto proporcionado en el ejemplo mencionado anteriormente, revisaría la lista de atributos de IdP admitidos y determinaría que la coincidencia más cercana con un atributo compatible sería `${path:enterprise.costCenter}` y, a continuación, lo introduciría en el campo Valor. Consulta la captura de pantalla proporcionada arriba como referencia. Tenga en cuenta que no puede usar valores de atributos de IdP externos fuera de esta lista para ABAC a menos que utilice la opción de pasar los atributos a través de la aserción SAML.

5. Seleccione Save changes (Guardar cambios).

Ahora que ha configurado el mapeo de sus atributos de control de acceso, debe completar el proceso de configuración de ABAC. Para ello, cree sus reglas ABAC y agréguelas a sus conjuntos de permisos (políticas and/or basadas en recursos). Esto es necesario para poder conceder a las identidades de los usuarios el acceso a los recursos de AWS . Para obtener más información, consulte [Crear políticas de permisos para ABAC en IAM Identity Center](#).

### Desactivar atributos para el control de acceso

Utilice el siguiente procedimiento para deshabilitar la característica ABAC y eliminar todas las asignaciones de atributos que se hayan configurado.

A fin de desactivar atributos para el control de acceso, siga estos pasos:

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. En la página de configuración, seleccione la pestaña Atributos para el control de acceso y, a continuación, elija Administrar atributos.
4. En la página Administrar atributos para el control de acceso, selecciona Desactivar.
5. En la ventana de diálogo Desactivar los atributos para el control de acceso, revise la información y, cuando esté listo, introdúzcala y **DISABLE**, a continuación, seleccione Confirmar.

#### Important

Este paso elimina todos los atributos y detiene el uso de los atributos para el control de acceso al federarse, Cuentas de AWS independientemente de si hay algún atributo presente en las aserciones de SAML de un proveedor de fuentes de identidad externo.

## Crear políticas de permisos para ABAC en IAM Identity Center

Puede crear políticas de permisos que determinen quién puede acceder a sus recursos de AWS en característica de los valores de atributos configurados. Cuando habilita ABAC y especifica atributos, IAM Identity Center transfiere los valores de atributo del usuario autenticado a IAM para utilizarlos en la evaluación de políticas.

Clave de condición de aws:PrincipalTag

Puede utilizar los atributos de control de acceso en sus conjuntos de permisos mediante la clave de condición aws:PrincipalTag para crear reglas de control de acceso. Por ejemplo, en la

siguiente política, puede etiquetar todos los recursos de su organización con sus centros de costes respectivos. También puede utilizar un único conjunto de permisos que conceda a los desarrolladores acceso a los recursos de sus centros de costos. Ahora, cuando los desarrolladores se federan en la cuenta mediante el inicio de sesión único y su atributo de centro de costos, solo tienen acceso a los recursos de sus respectivos centros. A medida que el equipo vaya añadiendo más desarrolladores y recursos a su proyecto, solo tendrás que etiquetar los recursos con el centro de costos correcto. A continuación, se transfiere la información del centro de costes en la AWS sesión cuando los desarrolladores se federan en Cuentas de AWS ella. Por tanto, a medida que la organización agrega nuevos recursos y desarrolladores al centro de costos, los desarrolladores pueden administrar los recursos alineados con sus centros sin necesidad de actualizar los permisos.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "ec2:ResourceTag/CostCenter": "${aws:PrincipalTag/CostCenter}"
        }
      }
    }
  ]
}
```

Para obtener más información, consulte [aws:PrincipalTagy EC2: Iniciar o detener instancias en función de las etiquetas principales y de recursos coincidentes](#) en la Guía del usuario de IAM.

Si las políticas contienen atributos no válidos en sus condiciones, la condición de la política fallará y se denegará el acceso. Para obtener más información, consulte [Error: “Se ha producido un error inesperado” cuando un usuario intenta iniciar sesión con un proveedor de identidad externo](#).

## Reparar el proveedor de identidad de IAM

Al añadir un acceso de inicio de sesión único a un Cuenta de AWS, el Centro de Identidad de IAM crea un proveedor de identidades de IAM en cada uno de ellos. Cuenta de AWS Un proveedor de identidad de IAM le ayuda a proteger su Cuenta de AWS , ya que no tiene que distribuir ni integrar credenciales de seguridad a largo plazo, como por ejemplo, claves de acceso, en su aplicación.

Si elimina o modifica su proveedor de identidades, debe volver a aplicar manualmente las asignaciones de usuarios y grupos. Al volver a aplicar las asignaciones de usuarios y grupos, se vuelve a crear el proveedor de identidades. Para obtener más información, consulte:

- [Cuenta de AWS acceso](#)
- [Acceso de aplicaciones](#)

## Entender los roles vinculados a servicios en IAM Identity Center

[Roles vinculados a servicios](#) son permisos predefinidos que permiten a IAM Identity Center delegar e implementar qué usuarios tienen acceso de inicio de sesión único a determinadas Cuentas de AWS de su organización en AWS Organizations. El servicio habilita esta funcionalidad al proporcionar un rol vinculado al servicio en cada uno de los miembros de su organización. Cuenta de AWS Luego, el servicio permite que otros AWS servicios, como IAM Identity Center, aprovechen esas funciones para realizar tareas relacionadas con el servicio. Para obtener más información, consulte [AWS Organizations y los roles vinculados a servicios](#).

Al activar IAM Identity Center, este crea un rol vinculado al servicio en todas las cuentas de la organización en AWS Organizations. IAM Identity Center también crea el mismo rol vinculado a servicios en todas las cuentas que se añaden posteriormente a su organización. Este rol permite a IAM Identity Center acceder a los recursos de cada cuenta en su nombre. Para obtener más información, consulte [Cuenta de AWS acceso](#).

Las funciones vinculadas al servicio que se crean en cada una de ellas reciben un nombre. Cuenta de AWS `AWSServiceRoleForSSO` Para obtener más información, consulte [Uso de roles vinculados a servicios para IAM Identity Center](#).



 Notas

- Si has iniciado sesión en la cuenta de AWS Organizations administración, esta utilizará tu rol en el que hayas iniciado sesión actualmente y no el rol vinculado al servicio. De este modo se evita la escalada de privilegios.
- Cuando el IAM Identity Center realiza cualquier operación de IAM en la cuenta de AWS Organizations administración, todas las operaciones se realizan con las credenciales del director de IAM. Esto permite que los inicios de sesión CloudTrail proporcionen visibilidad de quién realizó todos los cambios de privilegios en la cuenta de administración.

# Diseño de resiliencia y comportamiento regional

El servicio IAM Identity Center está totalmente gestionado y utiliza AWS servicios duraderos y de alta disponibilidad, como Amazon S3 y Amazon EC2. Para garantizar la disponibilidad en caso de que se interrumpa la zona de disponibilidad, IAM Identity Center opera en varias zonas de disponibilidad.

Habilita el Centro de Identidad de IAM en su cuenta AWS Organizations de administración. Esto es necesario para que IAM Identity Center pueda aprovisionar, desaproveccionar y actualizar los roles de todas sus Cuentas de AWS. Al activar el Centro de Identidad de IAM, se despliega en el Región de AWS que está seleccionado actualmente. Si desea realizar la implementación en una Región de AWS específica, cambie la selección de región antes de activar IAM Identity Center.

## Note

IAM Identity Center controla el acceso a sus conjuntos de permisos y aplicaciones únicamente desde su región principal. Le recomendamos que tenga en cuenta los riesgos asociados al control de acceso cuando IAM Identity Center opere en una sola región.

Si bien IAM Identity Center determina el acceso desde la región en la que se habilita el servicio, las Cuentas de AWS son globales. Esto significa que, una vez que los usuarios inicien sesión en el Centro de Identidad de IAM, podrán operar en cualquier región al acceder a Cuentas de AWS través del Centro de Identidad de IAM. Sin embargo, la mayoría de las aplicaciones AWS administradas, como Amazon SageMaker AI, deben instalarse en la misma región que el IAM Identity Center para que los usuarios se autenticuen y asignen el acceso a estas aplicaciones. Para obtener información sobre las restricciones regionales al utilizar una aplicación con IAM Identity Center, consulte la documentación de la aplicación.

También puede utilizar IAM Identity Center para autenticar y autorizar el acceso a las aplicaciones basadas en SAML a las que se puede acceder a través de una URL pública, independientemente de la plataforma o la nube en la que se haya creado la aplicación.

No recomendamos utilizar [Instancias de cuenta de IAM Identity Center](#) como medio para implementar la resiliencia, ya que se crea un segundo punto de control aislado que no está conectado a la instancia de organización.

## Diseñado para la disponibilidad

En la siguiente tabla, se muestra la disponibilidad para la que se ha diseñado el IAM Identity Center. Estos valores no representan un acuerdo de nivel de servicio ni una garantía, sino que proporcionan información sobre los objetivos de diseño. Los porcentajes de disponibilidad hacen referencia al acceso a los datos o las funciones y no a la durabilidad (por ejemplo, la retención de datos a largo plazo).

| Componente de servicio                        | Objetivo de diseño de disponibilidad |
|-----------------------------------------------|--------------------------------------|
| Plano de datos (incluido el inicio de sesión) | 99.95%                               |
| Plano de control                              | 99.90%                               |

## Configure el acceso de emergencia al AWS Management Console

El IAM Identity Center se creó a partir de una AWS infraestructura de alta disponibilidad y utiliza una arquitectura de zonas de disponibilidad para eliminar los puntos únicos de error. Para disponer de un nivel de protección adicional en el improbable caso de que se produzca una avería o se produjera una Región de AWS avería en el centro de identidad de IAM, le recomendamos que configure una configuración que pueda utilizar para proporcionar acceso temporal al AWS Management Console

AWS le permite:

- [Conecte su IdP de terceros a IAM Identity Center.](#)
- Conecte su IdP de terceros a una persona Cuentas de AWS mediante la federación basada en [SAML 2.0](#).

Si utiliza IAM Identity Center, puede utilizar estas funciones para crear la configuración de acceso de emergencia que se describe en las siguientes secciones. Esta configuración le permite utilizar el IAM Identity Center como mecanismo de acceso. Cuenta de AWS Si el Centro de Identidad de IAM se interrumpe, los usuarios de sus operaciones de emergencia pueden iniciar sesión en el AWS Management Console mediante la federación directa con las mismas credenciales que utilizan para acceder a sus cuentas. Esta configuración funciona cuando IAM Identity Center no está disponible, pero el plano de datos de IAM y su proveedor de identidades (IdP) externo están disponibles.

 Important

Le recomendamos que implemente esta configuración antes de que se produzca una interrupción, ya que no podrá crearla si también se interrumpe su acceso para crear los roles de IAM requeridos. Pruebe esta configuración periódicamente para asegurarse de que su equipo sepa qué hacer en caso de que se interrumpa IAM Identity Center.

## Temas

- [Resumen de la configuración del acceso de emergencia](#)
- [Cómo diseñar sus roles de operaciones críticas](#)
- [Cómo planificar su modelo de acceso](#)
- [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#)
- [Cómo crear la configuración de acceso de emergencia](#)
- [Tareas de preparación de emergencias](#)
- [Proceso de conmutación por error de emergencia](#)
- [Volver a las operaciones normales](#)
- [Configuración única de una aplicación de federación de IAM directa en Okta](#)

## Resumen de la configuración del acceso de emergencia

Complete las tareas siguientes para configurar el acceso de emergencia:

1. [Cree una cuenta de operaciones de emergencia en su organización en AWS Organizations](#). Esta cuenta pasará a ser su cuenta de operaciones de emergencia.
2. Conecte el IdP a la cuenta de operaciones de emergencia mediante la [federación basada en SAML 2.0](#).
3. En la cuenta de operaciones de emergencia, [cree un rol para la federación de proveedores de identidades de terceros](#). Además, cree un rol de operaciones de emergencia en cada una de sus cuentas de carga de trabajo, con los permisos necesarios.
4. [Delegue el acceso a sus cuentas de carga de trabajo para el rol de IAM](#) que creó en la cuenta de operaciones de emergencia. Para autorizar el acceso a su cuenta de operaciones de emergencia, cree un grupo de operaciones de emergencia en su IdP, sin miembros.

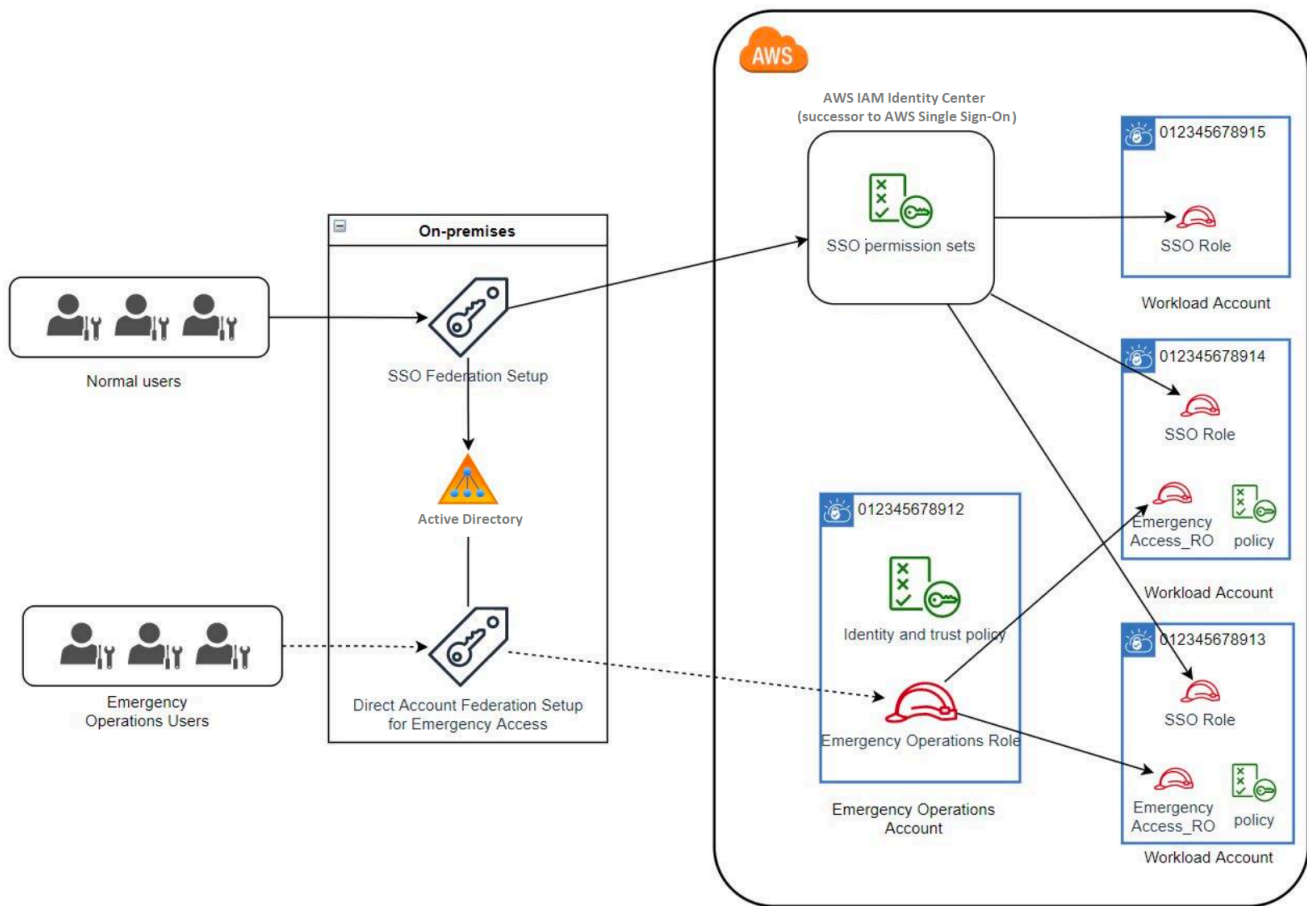
5. Permita que el grupo de operaciones de emergencia de su IdP utilice el rol de operaciones de emergencia creando una regla en su IdP que [permita el acceso federado de SAML 2.0 a la AWS Management Console](#).

Durante las operaciones normales, nadie tiene acceso a la cuenta de operaciones de emergencia porque el grupo de operaciones de emergencia de su IdP no tiene miembros. En caso de que se produzca una interrupción en IAM Identity Center, utilice su IdP para añadir usuarios de confianza al grupo de operaciones de emergencia de su IdP. A continuación, estos usuarios pueden iniciar sesión en su IdP, acceder a la AWS Management Console cuenta de operaciones de emergencia y asumir la función de operaciones de emergencia en la cuenta de operaciones de emergencia. A partir de ahí, estos usuarios pueden [cambiar de rol](#) al de acceso de emergencia en sus cuentas de carga de trabajo, donde tienen que realizar tareas operativas.

## Cómo diseñar sus roles de operaciones críticas

Con este diseño, se configura una cuenta única Cuenta de AWS en la que se federa a través de IAM, de modo que los usuarios puedan asumir funciones operativas fundamentales. Las funciones de operaciones críticas tienen una política de confianza que permite a los usuarios asumir el rol correspondiente en sus cuentas de carga de trabajo. Los roles de las cuentas de carga de trabajo proporcionan los permisos que los usuarios necesitan para realizar tareas esenciales.

En el diagrama siguiente se proporciona información general del diseño.



## Cómo planificar su modelo de acceso

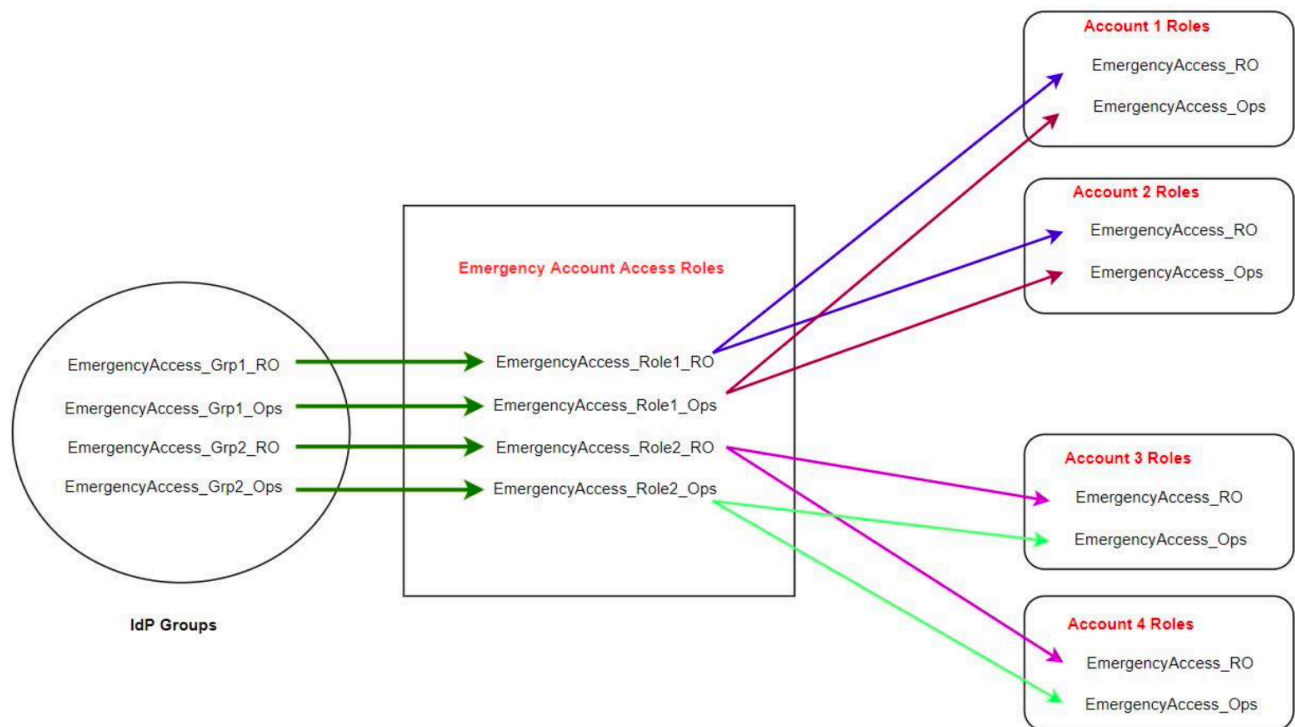
Antes de configurar el acceso de emergencia, cree un plan sobre cómo funcionará el modelo de acceso. Utilice el siguiente proceso para crear este plan:

1. Identifique los Cuentas de AWS lugares en los que el acceso de emergencia de los operadores es esencial durante una interrupción en el IAM Identity Center. Por ejemplo, es probable que sus cuentas de producción sean esenciales, pero es posible que sus cuentas de desarrollo y prueba no lo sean.
2. Para ese conjunto de cuentas, identifique los roles críticos específicos que necesita en sus cuentas. En todas estas cuentas, defina de manera coherente lo que pueden hacer los roles. Esto simplifica el trabajo en su cuenta de acceso de emergencia, en la que puede crear roles multicuentas. Le recomendamos que comience con 2 roles distintos en estas cuentas: de solo lectura (RO) y de operaciones (Ops). Si es necesario, puede crear más roles y asignarlos a un grupo distinto de usuarios de acceso de emergencia en su configuración.

- Identifique y cree grupos de acceso de emergencia en su IdP. Los miembros del grupo son los usuarios a los que está delegando el acceso a los roles de acceso de emergencia.
- Defina qué roles pueden asumir estos grupos en la cuenta de acceso de emergencia. Para ello, defina reglas en su IdP que generen notificaciones que enumeren los roles a los que puede acceder el grupo. Estos grupos pueden entonces asumir sus roles de solo lectura o de operaciones en la cuenta de acceso de emergencia. A partir de esos roles, pueden asumir los roles correspondientes en sus cuentas de carga de trabajo.

## Cómo diseñar una asignación de roles, cuentas y grupos de emergencia

En el siguiente diagrama, se muestra cómo asignar los grupos de acceso de emergencia a los roles de la cuenta de acceso de emergencia. El diagrama también muestra las relaciones de confianza entre roles que permiten que los roles de las cuentas de acceso de emergencia accedan a los roles correspondientes de las cuentas de carga de trabajo. Recomendamos que el diseño de su plan de emergencia utilice estas asignaciones como punto de partida.



## Cómo crear la configuración de acceso de emergencia

Utilice la siguiente tabla de asignación para crear su configuración de acceso de emergencia. Esta tabla refleja un plan que incluye 2 roles en las cuentas de carga de trabajo: de solo lectura (RO) y de operaciones (Ops), con las correspondientes políticas de confianza y permisos. Las políticas de confianza permiten que los roles de las cuentas de acceso de emergencia accedan a los roles de las cuentas de carga de trabajo individuales. Los roles individuales de la cuenta de carga de trabajo también tienen políticas de permisos sobre lo que el rol puede hacer en la cuenta. Las políticas de permisos pueden ser [políticas administradas por AWS](#) o [políticas administradas por el cliente](#).

| Cuenta                         | Roles a crear                                                                                                                              | Política de confianza         | Política de permisos                                     |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|----------------------------------------------------------|
| Cuenta 1                       | Emergency<br>Access_RO                                                                                                                     | Emergency<br>Access_Role1_RO  | arn:aws:iam::aws:policy/ReadOnlyAccess                   |
| Cuenta 1                       | Emergency<br>Access_Ops                                                                                                                    | Emergency<br>Access_Role1_Ops | arn:aws:iam::aws:policy/job-function/SystemAdministrator |
| Cuenta 2                       | Emergency<br>Access_RO                                                                                                                     | Emergency<br>Access_Role2_RO  | arn:aws:iam::aws:policy/ReadOnlyAccess                   |
| Cuenta 2                       | Emergency<br>Access_Ops                                                                                                                    | Emergency<br>Access_Role2_Ops | arn:aws:iam::aws:policy/job-function/SystemAdministrator |
| Cuenta de acceso de emergencia | Emergency<br>Access_Role1_RO<br><br>Emergency<br>Access_Role1_Ops<br><br>Emergency<br>Access_Role2_RO<br><br>Emergency<br>Access_Role2_Ops | IdP                           | AssumeRole para el recurso de rol en la cuenta           |



En este plan de asignación, la cuenta de acceso de emergencia contiene 2 roles de solo lectura y 2 roles de operaciones. Estos roles confían en su IdP para autenticar y autorizar a los grupos seleccionados a acceder a los roles pasando los nombres de los roles en aserciones. En las cuentas 1 y 2 de carga de trabajo hay los correspondientes roles de solo lectura y operaciones. Para la cuenta de carga de trabajo 1, el rol `EmergencyAccess_R0` confía en el rol `EmergencyAccess_Role1_R0` que reside en la cuenta de acceso de emergencia. En la tabla se especifican patrones de confianza similares entre los roles de solo lectura y operaciones de la cuenta de carga de trabajo y los correspondientes roles de acceso de emergencia.

## Tareas de preparación de emergencias

Para preparar la configuración de acceso de emergencia, recomendamos que realice las siguientes tareas antes de que se produzca una emergencia.

1. Configure una aplicación de federación de IAM directa en su IdP. Para obtener más información, consulte [Configuración única de una aplicación de federación de IAM directa en Okta](#).
2. Cree una conexión de IdP en la cuenta de acceso de emergencia a la que se pueda acceder durante el evento.
3. Cree roles de acceso de emergencia en las cuentas de acceso de emergencia tal y como se describe en la tabla de asignación anterior.
4. Cree roles de operaciones temporales con políticas de confianza y permisos en cada una de las cuentas de carga de trabajo.
5. Cree grupos de operaciones temporales en su IdP. Los nombres de los grupos dependerán de los nombres de los roles de operaciones temporales.
6. Pruebe la federación de IAM directa.
7. Deshabilite la aplicación de federación de IdP en su IdP para evitar su uso regular.

## Proceso de conmutación por error de emergencia

Si una instancia del IAM Identity Center no está disponible y decide que debe proporcionar acceso de emergencia a la consola de AWS administración, le recomendamos el siguiente proceso de conmutación por error.

1. El administrador del IdP habilita la aplicación de federación de IAM directa en su IdP.
2. Los usuarios solicitan el acceso al grupo de operaciones temporal a través del mecanismo que ya tiene, como una solicitud por correo electrónico, un canal de Slack u otra forma de comunicación.

3. Los usuarios que añada a sus grupos de acceso de emergencia inician sesión en el IdP, seleccionan la cuenta de acceso de emergencia y los usuarios eligen un rol para usarlo en la cuenta de acceso de emergencia. A partir de estos roles, pueden asumir roles en las cuentas de carga de trabajo correspondientes que tienen una confianza cruzada con el rol de cuenta de emergencia.

## Volver a las operaciones normales

Consulte el [Panel de estado de AWS](#) para confirmar cuándo se restablece el estado del servicio de IAM Identity Center. Para volver a las operaciones normales, siga estos pasos:

1. Cuando el icono de estado del servicio de IAM Identity Center indique que el servicio está en buen estado, inicie sesión en IAM Identity Center.
2. Si puede iniciar sesión correctamente en IAM Identity Center, comuníquese a los usuarios con acceso de emergencia que IAM Identity Center está disponible. Indique a estos usuarios que cierren sesión y usen el portal de AWS acceso para volver a iniciar sesión en el IAM Identity Center.
3. Una vez que todos los usuarios con acceso de emergencia cierren la sesión, deshabilite en el IdP la aplicación de federación de IdP. Le recomendamos que realice esta tarea después del horario de trabajo.
4. Elimine todos los usuarios del grupo de acceso de emergencia del IdP.

Su infraestructura de roles de acceso de emergencia sigue funcionando como un plan de acceso alternativo, pero ahora está deshabilitada.

## Configuración única de una aplicación de federación de IAM directa en Okta

1. Inicie sesión en su Okta cuenta como usuario con permisos administrativos.
2. En la Okta En la Consola de administración, en Aplicaciones, selecciona Aplicaciones.
3. Seleccione Explorar el catálogo de aplicaciones. Busque y elija Federación de cuentas de AWS . Seleccione Agregar integración.
4. [Para configurar la federación de IAM directa, sigue AWS los pasos de Cómo configurar SAML 2.0 para la federación de AWS cuentas.](#)

- En la pestaña Opciones de inicio de sesión, seleccione SAML 2.0 e introduzca los ajustes de Filtro de grupo y Patrón de valores de rol. El nombre del grupo para el directorio de usuarios depende del filtro que configure.

|                    |                                                                                                     |
|--------------------|-----------------------------------------------------------------------------------------------------|
| Group Filter       | <code>^aws\#\S+\#(?{{role}})[\w\-\+]\#(?{{accountid}}\d+)\\$</code>                                 |
| Role Value Pattern | <code>arn:aws:iam::\${accountid}:saml-provider/Okta,arn:aws:iam::\${accountid}:role/\${role}</code> |

En la figura anterior, la variable `role` corresponde al rol de operaciones de emergencia en su cuenta de acceso de emergencia. Por ejemplo, si crea el `EmergencyAccess_Role1_R0` rol (tal y como se describe en la tabla de mapeo) en Cuenta de AWS 123456789012 y si los ajustes del filtro de grupo están configurados tal como se muestra en la figura anterior, el nombre de su grupo debería serlo. `aws#EmergencyAccess_Role1_R0#123456789012`

- En el directorio (por ejemplo, el directorio de Active Directory), cree el grupo de acceso de emergencia y especifique un nombre para el directorio (por ejemplo, `aws#EmergencyAccess_Role1_R0#123456789012`). Asigne sus usuarios a este grupo mediante el mecanismo de aprovisionamiento existente.
- En la cuenta de acceso de emergencia, [configure una política de confianza personalizada](#) que proporcione los permisos necesarios para que se asuma el rol de acceso de emergencia durante una interrupción. A continuación, se muestra un ejemplo de una política de confianza personalizada asociada al rol `EmergencyAccess_Role1_R0`. Para ver un ejemplo, consulte la cuenta de emergencia en el diagrama en [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Federated": "arn:aws:iam::123456789012:saml-provider/Okta"
      },
      "Action": [
        "sts:AssumeRoleWithSAML",
        "sts:SetSourceIdentity",
        "sts:TagSession"
      ]
    }
  ],
}
```

```

        "Condition":{
            "StringEquals":{
                "SAML:aud":"https://~/.signin.aws.amazon.com/saml"
            }
        }
    }
}
]
}

```

8. A continuación se muestra un ejemplo de una declaración de una política de permisos asociada al rol `EmergencyAccess_Role1_R0`. Para ver un ejemplo, consulte la cuenta de emergencia en el diagrama en [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#).

```

{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Action":"sts:AssumeRole",
      "Resource":[
        "arn:aws:iam::<account 1>:role/EmergencyAccess_R0",
        "arn:aws:iam::<account 2>:role/EmergencyAccess_R0"
      ]
    }
  ]
}

```

9. En las cuentas de carga de trabajo, configure una política de confianza personalizada. A continuación se muestra un ejemplo de declaración de una política de confianza asociada al rol `EmergencyAccess_R0`. En este ejemplo, la cuenta `123456789012` es la cuenta de acceso de emergencia. Para ver un ejemplo, consulte la cuenta de carga de trabajo en el diagrama en [Cómo diseñar una asignación de roles, cuentas y grupos de emergencia](#).

```

{
  "Version": "2012-10-17",
  "Statement":[
    {
      "Effect":"Allow",
      "Principal":{
        "AWS":"arn:aws:iam::123456789012:root"
      },
      "Action":"sts:AssumeRole"
    }
  ]
}

```

```
}  
]  
}
```

 **Note**

La mayoría de IdPs permiten mantener desactivada la integración de una aplicación hasta que sea necesaria. Le recomendamos que mantenga la aplicación de federación de IAM directa desactivada en su IdP hasta que sea necesaria para el acceso de emergencia.

# Seguridad en AWS IAM Identity Center

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted AWS y usted. El [modelo de responsabilidad compartida](#) la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura. Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los [programas de conformidad de AWS](#). Para obtener más información sobre los programas de conformidad aplicables AWS IAM Identity Center, consulte los [AWS servicios incluidos en el ámbito de aplicación por programa de conformidad](#).
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. También eres responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza IAM Identity Center. En los siguientes temas se le mostrará cómo configurar IAM Identity Center para cumplir con sus objetivos de seguridad y conformidad. También aprenderá a utilizar otros AWS servicios que le ayudan a supervisar y proteger los recursos del IAM Identity Center.

## Temas

- [Administración de identidades y accesos para IAM Identity Center](#)
- [Consola de IAM Identity Center y autorización de la API](#)
- [AWS STS condicionan las claves de contexto del IAM Identity Center](#)
- [Registro y supervisión en IAM Identity Center](#)
- [Validación de la conformidad en IAM Identity Center](#)
- [Resiliencia en IAM Identity Center](#)
- [Seguridad de la infraestructura en IAM Identity Center](#)

# Administración de identidades y accesos para IAM Identity Center

El acceso al Centro de Identidad de IAM requiere credenciales que AWS pueda utilizar para autenticar sus solicitudes. Esas credenciales deben tener permisos para acceder a AWS los recursos, como una aplicación AWS gestionada.

La autenticación del portal de AWS acceso está controlada por el directorio que haya conectado al IAM Identity Center. Sin embargo, la autorización de los Cuentas de AWS que están disponibles para los usuarios desde el portal de AWS acceso viene determinada por dos factores:

1. A quién se le ha asignado el acceso a ellas Cuentas de AWS en la consola del IAM Identity Center. Para obtener más información, consulte [Acceso mediante inicio de sesión único a Cuentas de AWS](#).
2. Qué nivel de permisos se ha concedido a los usuarios en la consola de IAM Identity Center para permitirles el acceso adecuado a esas Cuentas de AWS. Para obtener más información, consulte [Creación, administración y eliminación de conjuntos de permisos](#).

En las siguientes secciones se explica cómo, como administrador, puede controlar el acceso a la consola del IAM Identity Center o delegar el acceso administrativo a day-to-day las tareas desde la consola del IAM Identity Center.

- [Autenticación](#)
- [Control de acceso](#)

## Autenticación

Aprenda a acceder AWS mediante las identidades de [IAM](#).

## Control de acceso

Aunque tenga credenciales válidas para autenticar las solicitudes, si no tiene permisos, no podrá crear recursos de IAM Identity Center ni acceder a estos. Por ejemplo, debe tener permisos para crear un directorio conectado de IAM Identity Center.

En las secciones siguientes se describe cómo administrar los permisos de IAM Identity Center. Recomendamos que lea primero la información general.

- [Información general sobre la administración de permisos de acceso para los recursos de IAM Identity Center](#)
- [Ejemplos de políticas basadas en identidades para IAM Identity Center](#)
- [Uso de roles vinculados a servicios para IAM Identity Center](#)

## Información general sobre la administración de permisos de acceso para los recursos de IAM Identity Center

Cada AWS recurso es propiedad de un Cuenta de AWS, y los permisos para crear o acceder a los recursos se rigen por políticas de permisos. Para proporcionar acceso, un administrador de cuentas puede agregar permisos a las identidades de IAM (es decir, usuarios, grupos y roles). Algunos servicios (por ejemplo, AWS Lambda) también admiten añadir permisos a recursos.

### Note

Un administrador de cuentas (o usuario administrador) es un usuario que tiene privilegios de administrador. Para obtener más información, consulte [Prácticas recomendadas de IAM](#) en la Guía del usuario de IAM.

### Temas

- [Recursos y operaciones de IAM Identity Center](#)
- [Titularidad de los recursos](#)
- [Administración del acceso a los recursos](#)
- [Especificación de elementos de política: acciones, efectos, recursos y entidades principales](#)
- [Especificación de las condiciones de una política](#)

## Recursos y operaciones de IAM Identity Center

En IAM Identity Center, los recursos principales son instancias de aplicación, perfiles y conjuntos de permisos.



## Titularidad de los recursos

El propietario de un recurso es Cuenta de AWS quien creó un recurso. Es decir, el propietario Cuenta de AWS del recurso es la entidad principal (la cuenta, un usuario o un rol de IAM) que autentica la solicitud que crea el recurso. Los siguientes ejemplos ilustran cómo funciona:

- Si Usuario raíz de la cuenta de AWS crea un recurso del Centro de identidad de IAM, como una instancia de aplicación o un conjunto de permisos, usted Cuenta de AWS es el propietario de ese recurso.
- Si crea un usuario en su AWS cuenta y le concede permisos para crear los recursos del IAM Identity Center, el usuario podrá crear los recursos del IAM Identity Center. Sin embargo, su AWS cuenta, a la que pertenece el usuario, es propietaria de los recursos.
- Si crea un rol de IAM en su AWS cuenta con permisos para crear recursos del Centro de Identidad de IAM, cualquier persona que pueda asumir el rol podrá crear recursos del Centro de Identidad de IAM. Su Cuenta de AWS, a la que pertenece el rol, será la propietaria de los recursos de IAM Identity Center.

## Administración del acceso a los recursos

Una política de permisos describe quién tiene acceso a qué. En la siguiente sección se explican las opciones disponibles para crear políticas de permisos.

### Note

En esta sección se explica el uso de IAM en el contexto de IAM Identity Center. No se proporciona información detallada sobre el servicio de IAM. Para ver la documentación completa de IAM, consulte [What is IAM?](#) (¿Qué es IAM?) en la Guía del usuario de IAM. Para obtener más información sobre la sintaxis y descripciones de las políticas de IAM, consulte [AWS Referencia de políticas de IAM](#) en la Guía del usuario de IAM.

Las políticas que se asocian a una identidad de IAM se denominan políticas basadas en la identidad (políticas de IAM). Las políticas que se asocian a un recurso se denominan "políticas basadas en recursos". IAM Identity Center solo admite políticas basadas en identidades (políticas de IAM).

### Temas

- [Políticas basadas en identidades \(políticas de IAM\)](#)

- [Políticas basadas en recursos](#)

## Políticas basadas en identidades (políticas de IAM)

Puede agregar permisos a identidades de IAM. Por ejemplo, puede hacer lo siguiente:

- Adjunta una política de permisos a un usuario o grupo de tu cuenta Cuenta de AWS: el administrador de la cuenta puede utilizar una política de permisos asociada a un usuario concreto para conceder permisos a ese usuario para añadir un recurso del IAM Identity Center, como una nueva aplicación.
- Adjuntar una política de permisos a un rol (conceder permisos para cuentas cruzadas): puede adjuntar una política de permisos basada en identidades a un rol de IAM para conceder permisos para cuentas cruzadas.

Para obtener más información sobre el uso de IAM para delegar permisos, consulte [Access management](#) (Administración de accesos) en la Guía del usuario de IAM.

La siguiente política de permisos concede permisos a un usuario para ejecutar todas las acciones que empiezan por List. Estas acciones muestran información sobre un recurso de IAM Identity Center, como una instancia de la aplicación o un conjunto de permisos. Tenga en cuenta que el carácter comodín (\*) en el elemento Resource indica que las acciones están permitidas para todos los recursos de IAM Identity Center propiedad de la cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sso:List*",
      "Resource": "*"
    }
  ]
}
```

Para obtener más información acerca del uso de políticas basadas en identidades con IAM Identity Center, consulte [Ejemplos de políticas basadas en identidades para IAM Identity Center](#). Para obtener más información acerca de los usuarios, los grupos, los roles y los permisos, consulte [Identidades \(usuarios, grupos y roles\)](#) en la Guía del usuario de IAM.

## Políticas basadas en recursos

Otros servicios, como Amazon S3, también admiten políticas de permisos basadas en recursos. Por ejemplo, puede asociar una política a un bucket de S3 para administrar los permisos de acceso a dicho bucket. IAM Identity Center no admite políticas basadas en recursos.

## Especificación de elementos de política: acciones, efectos, recursos y entidades principales

Para cada recurso de IAM Identity Center (consulte [Recursos y operaciones de IAM Identity Center](#)), el servicio define un conjunto de operaciones de la API. Para conceder permisos para estas operaciones de la API, IAM Identity Center define un conjunto de acciones que usted puede especificar en una política. Tenga en cuenta que la realización de una operación de la API puede requerir permisos para más de una acción.

A continuación, se indican los elementos básicos de la política:

- **Recurso:** en una política, se usa un nombre de recurso de Amazon (ARN) para identificar el recurso al que se aplica la política.
- **Acción:** utilice palabras clave de acción para identificar las operaciones del recurso que desea permitir o denegar. Por ejemplo, el permiso `sso:DescribePermissionsPolicies` permite al usuario ejecutar la operación `DescribePermissionsPolicies` de IAM Identity Center.
- **Efecto:** especifique el efecto que se producirá cuando el usuario solicite la acción específica; puede ser permitir o denegar. Si no concede acceso de forma explícita (permitir) a un recurso, el acceso se deniega implícitamente. También puede denegar explícitamente el acceso a un recurso para asegurarse de que un usuario no pueda obtener acceso a él, aunque otra política le conceda acceso.
- **Entidad principal:** en las políticas basadas en identidades (políticas de IAM), el usuario al que se asocia esta política es la entidad principal implícita. Para las políticas basadas en recursos, debe especificar el usuario, la cuenta, el servicio u otra entidad que desee que reciba permisos (se aplica solo a las políticas basadas en recursos). IAM Identity Center no admite políticas basadas en recursos.

Para obtener más información acerca de la sintaxis y las descripciones de las políticas del IAM, consulte [Referencia de políticas de AWS IAM](#) en la Guía del usuario de IAM.

## Especificación de las condiciones de una política

Al conceder permisos, puede utilizar el lenguaje de la política de acceso para especificar las condiciones que se deben cumplir para que se aplique una política. Por ejemplo, es posible que desee que solo se aplique una política después de una fecha específica. Para obtener más información sobre cómo especificar condiciones en un lenguaje de política, consulte [Condition](#) en la Guía del usuario de IAM.

Para expresar condiciones, se usan claves de condición predefinidas. No hay claves de condición específicas para IAM Identity Center. Sin embargo, hay claves de AWS condición que puede utilizar según convenga. Para obtener una lista completa de AWS las claves, consulte las [claves de condición globales disponibles](#) en la Guía del usuario de IAM.

## Ejemplos de políticas basadas en identidades para IAM Identity Center

En este tema se proporcionan ejemplos de políticas de IAM que puede crear para conceder permisos a los usuarios y roles para administrar IAM Identity Center.

### Important

Le recomendamos que primero consulte los temas de introducción en los que se explican los conceptos básicos y las opciones disponibles para administrar el acceso a sus recursos de IAM Identity Center. Para obtener más información, consulte [Información general sobre la administración de permisos de acceso para los recursos de IAM Identity Center](#).

En las secciones de este tema se explica lo siguiente:

- [Ejemplos de políticas personalizadas](#)
- [Permisos necesarios para usar la consola de IAM Identity Center](#)

## Ejemplos de políticas personalizadas

En esta sección se proporcionan ejemplos de casos de uso habituales que requieren una política de IAM personalizada. Estas políticas de ejemplo son políticas basadas en la identidad, que no especifican el elemento de la entidad principal. Esto se debe a que, con una política basada en identidades, no se especifica la entidad principal que obtiene el permiso. En su lugar, usted adjunta la política a la entidad principal. Cuando se adjunta una política de permisos basada en la identidad a un rol de IAM, la entidad principal identificada en la política de confianza del rol obtiene los permisos.

Puede crear políticas basadas en la identidad en IAM y adjuntarlas a usuarios, grupos y roles. and/or También puede aplicar estas políticas a los usuarios de IAM Identity Center al crear un conjunto de permisos en IAM Identity Center.

 Note

Utilice estos ejemplos cuando cree políticas para su entorno y asegúrese de realizar pruebas tanto en casos positivos (“acceso concedido”) como negativos (“acceso denegado”) antes de implementar estas políticas en su entorno de producción. Para obtener más información sobre cómo probar las políticas de IAM, consulte [Probar las políticas de IAM con el simulador de política de IAM](#) en la Guía del usuario de IAM.

## Temas

- [Ejemplo 1: permitir que un usuario visualice IAM Identity Center](#)
- [Ejemplo 2: Permitir que un usuario gestione los permisos Cuentas de AWS en el Centro de identidades de IAM](#)
- [Ejemplo 3: permitir a un usuario administrar aplicaciones en IAM Identity Center](#)
- [Ejemplo 4: permitir a un usuario administrar usuarios y grupos en el directorio de Identity Center](#)

### Ejemplo 1: permitir que un usuario visualice IAM Identity Center

La siguiente política de permisos concede permisos de solo lectura a un usuario para que pueda visualizar todos los ajustes y la información del directorio configurados en IAM Identity Center.

 Note

Esta política se proporciona únicamente con fines ilustrativos. En un entorno de producción, le recomendamos que utilice la política ViewOnlyAccess AWS gestionada del Centro de identidades de IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
```

```

    "Action": [
      "ds:DescribeDirectories",
      "ds:DescribeTrusts",
      "iam:ListPolicies",
      "organizations:DescribeOrganization",
      "organizations:DescribeAccount",
      "organizations:ListParents",
      "organizations:ListChildren",
      "organizations:ListAccounts",
      "organizations:ListRoots",
      "organizations:ListAccountsForParent",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListOrganizationalUnitsForParent",
      "sso:ListManagedPoliciesInPermissionSet",
      "sso:ListPermissionSetsProvisionedToAccount",
      "sso:ListAccountAssignments",
      "sso:ListAccountsForProvisionedPermissionSet",
      "sso:ListPermissionSets",
      "sso:DescribePermissionSet",
      "sso:GetInlinePolicyForPermissionSet",
      "sso-directory:DescribeDirectory",
      "sso-directory:SearchUsers",
      "sso-directory:SearchGroups"
    ],
    "Resource": "*"
  }
]
}

```

**Ejemplo 2:** Permitir que un usuario gestione los permisos Cuentas de AWS en el Centro de identidades de IAM

La siguiente política de permisos permite a un usuario crear, administrar y desplegar conjuntos de permisos para sus Cuentas de AWS.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:AttachManagedPolicyToPermissionSet",
        "sso:CreateAccountAssignment",

```

```

        "sso:CreatePermissionSet",
        "sso:DeleteAccountAssignment",
        "sso:DeleteInlinePolicyFromPermissionSet",
        "sso:DeletePermissionSet",
        "sso:DetachManagedPolicyFromPermissionSet",
        "sso:ProvisionPermissionSet",
        "sso:PutInlinePolicyToPermissionSet",
        "sso:UpdatePermissionSet"
    ],
    "Resource": "*"
},
{
    "Sid": "IAMListPermissions",
    "Effect": "Allow",
    "Action": [
        "iam:ListRoles",
        "iam:ListPolicies"
    ],
    "Resource": "*"
},
{
    "Sid": "AccessToSSOProvisionedRoles",
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription"
    ],
    "Resource": "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
},
{
    "Effect": "Allow",
    "Action": [
        "iam:GetSAMLProvider"
    ],
    "Resource": "arn:aws:iam::*:saml-provider/AWSSSO_*_DO_NOT_DELETE"
}

```

```
}
]
}
```

### Note

Los permisos adicionales que figuran en "Sid": "AccessToSSOProvisionedRoles" las secciones y son necesarios únicamente para que el usuario pueda crear asignaciones en la cuenta AWS Organizations de administración. "Sid": "IAMListPermissions" En algunos casos, es posible que también deba agregar iam:UpdateSAMLProvider a estas secciones.

## Ejemplo 3: permitir a un usuario administrar aplicaciones en IAM Identity Center

La siguiente política de permisos concede permisos para que los usuarios visualicen y configuren aplicaciones en IAM Identity Center, incluidas las aplicaciones SaaS preintegradas del catálogo de IAM Identity Center.

### Note

La operación sso:AssociateProfile utilizada en el siguiente ejemplo de política es necesaria para administrar las asignaciones de usuarios y grupos a las aplicaciones. También permite al usuario asignar usuarios y grupos Cuentas de AWS mediante los conjuntos de permisos existentes. Si un usuario debe gestionar el Cuenta de AWS acceso desde el Centro de identidades de IAM y necesita los permisos necesarios para gestionar los conjuntos de permisos, consulte [Ejemplo 2: Permitir que un usuario gestione los permisos Cuentas de AWS en el Centro de identidades de IAM](#).

Desde octubre de 2020, muchas de estas operaciones solo están disponibles a través de la consola AWS . Este ejemplo de política incluye acciones de "lectura", como enumerar, obtener y buscar, que, en este caso, son relevantes para que la consola funcione sin errores.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```



```

    "Action": [
        "sso:AssociateProfile",
        "sso:CreateApplicationInstance",
        "sso:ImportApplicationInstanceServiceProviderMetadata",
        "sso>DeleteApplicationInstance",
        "sso>DeleteProfile",
        "sso:DisassociateProfile",
        "sso:GetApplicationTemplate",
        "sso:UpdateApplicationInstanceServiceProviderConfiguration",
        "sso:UpdateApplicationInstanceDisplayData",
        "sso>DeleteManagedApplicationInstance",
        "sso:UpdateApplicationInstanceStatus",
        "sso:GetManagedApplicationInstance",
        "sso:UpdateManagedApplicationInstanceStatus",
        "sso:CreateManagedApplicationInstance",
        "sso:UpdateApplicationInstanceSecurityConfiguration",
        "sso:UpdateApplicationInstanceResponseConfiguration",
        "sso:GetApplicationInstance",
        "sso:CreateApplicationInstanceCertificate",
        "sso:UpdateApplicationInstanceResponseSchemaConfiguration",
        "sso:UpdateApplicationInstanceActiveCertificate",
        "sso>DeleteApplicationInstanceCertificate",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationTemplates",
        "sso:ListApplications",
        "sso:ListApplicationInstances",
        "sso:ListDirectoryAssociations",
        "sso:ListProfiles",
        "sso:ListProfileAssociations",
        "sso:ListInstances",
        "sso:GetProfile",
        "sso:GetSSOStatus",
        "sso:GetSsoConfiguration",
        "sso-directory:DescribeDirectory",
        "sso-directory:DescribeUsers",
        "sso-directory:ListMembersInGroup",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers"
    ],
    "Resource": "*"
}

```

## Ejemplo 4: permitir a un usuario administrar usuarios y grupos en el directorio de Identity Center

La siguiente política de permisos concede permisos para permitir que un usuario pueda crear, visualizar, modificar y eliminar usuarios y grupos en IAM Identity Center.

En algunos casos, las modificaciones directas de los usuarios y grupos de IAM Identity Center están restringidas. Por ejemplo, cuando se selecciona Active Directory o un proveedor de identidades externo con el aprovisionamiento automático activado como fuente de identidad.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso-directory:ListGroupsWithUser",
        "sso-directory:DisableUser",
        "sso-directory:EnableUser",
        "sso-directory:SearchGroups",
        "sso-directory>DeleteGroup",
        "sso-directory:AddMemberToGroup",
        "sso-directory:DescribeDirectory",
        "sso-directory:UpdateUser",
        "sso-directory:ListMembersInGroup",
        "sso-directory:CreateUser",
        "sso-directory:DescribeGroups",
        "sso-directory:SearchUsers",
        "sso:ListDirectoryAssociations",
        "sso-directory:RemoveMemberFromGroup",
        "sso-directory>DeleteUser",
        "sso-directory:DescribeUsers",
        "sso-directory:UpdateGroup",
        "sso-directory:CreateGroup"
      ],
      "Resource": "*"
    }
  ]
}
```

## Permisos necesarios para usar la consola de IAM Identity Center

Para que un usuario pueda trabajar con la consola de IAM Identity Center sin errores, necesita permisos adicionales. Si se ha creado una política de IAM más restrictiva que los permisos

mínimos requeridos, la consola no funcionará como es debido para los usuarios con esa política. El siguiente ejemplo muestra el conjunto de permisos que podrían ser necesarios para garantizar un funcionamiento sin errores en la consola de IAM Identity Center.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "sso:DescribeAccountAssignmentCreationStatus",
        "sso:DescribeAccountAssignmentDeletionStatus",
        "sso:DescribePermissionSet",
        "sso:DescribePermissionSetProvisioningStatus",
        "sso:DescribePermissionsPolicies",
        "sso:DescribeRegisteredRegions",
        "sso:GetApplicationInstance",
        "sso:GetApplicationTemplate",
        "sso:GetInlinePolicyForPermissionSet",
        "sso:GetManagedApplicationInstance",
        "sso:GetMfaDeviceManagementForDirectory",
        "sso:GetPermissionSet",
        "sso:GetPermissionsPolicy",
        "sso:GetProfile",
        "sso:GetSharedSsoConfiguration",
        "sso:GetSsoConfiguration",
        "sso:GetSSOStatus",
        "sso:GetTrust",
        "sso:ListAccountAssignmentCreationStatus",
        "sso:ListAccountAssignmentDeletionStatus",
        "sso:ListAccountAssignments",
        "sso:ListAccountsForProvisionedPermissionSet",
        "sso:ListApplicationInstanceCertificates",
        "sso:ListApplicationInstances",
        "sso:ListApplications",
        "sso:ListApplicationTemplates",
        "sso:ListDirectoryAssociations",
        "sso:ListInstances",
        "sso:ListManagedPoliciesInPermissionSet",
        "sso:ListPermissionSetProvisioningStatus",
        "sso:ListPermissionSets",
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:ListProfileAssociations",
```

```
        "sso:ListProfiles",
        "sso:ListTagsForResource",
        "sso-directory:DescribeDirectory",
        "sso-directory:DescribeGroups",
        "sso-directory:DescribeUsers",
        "sso-directory:ListGroupsForUser",
        "sso-directory:ListMembersInGroup",
        "sso-directory:SearchGroups",
        "sso-directory:SearchUsers"
    ],
    "Resource": "*"
}
]
```

## AWS políticas gestionadas para el Centro de Identidad de IAM

Cómo [crear políticas de IAM administradas por el cliente](#) que proporcionen a su equipo solo los permisos necesarios. Para empezar rápidamente, puede utilizar las políticas AWS gestionadas. Estas políticas cubren casos de uso comunes y están disponibles en su Cuenta de AWS. Para obtener más información sobre las políticas administradas de AWS, consulte [Políticas administradas de AWS](#) en la Guía del usuario de IAM.

AWS los servicios mantienen y AWS actualizan las políticas administradas. No puede cambiar los permisos en las políticas AWS gestionadas. En ocasiones, los servicios agregan permisos adicionales a una política administrada de AWS para admitir características nuevas. Este tipo de actualización afecta a todas las identidades (usuarios, grupos y roles) donde se asocia la política. Es más probable que los servicios actualicen una política gestionada por AWS cuando se lanza una nueva característica o cuando se ponen a disposición nuevas operaciones. Los servicios no eliminan los permisos de una política AWS administrada, por lo que las actualizaciones de la política no afectarán a los permisos existentes.

Además, AWS admite políticas administradas para funciones laborales que abarcan varios servicios. Por ejemplo, la política ReadOnlyAccess AWS gestionada proporciona acceso de solo lectura a todos los AWS servicios y recursos. Cuando un servicio lanza una nueva función, AWS agrega permisos de solo lectura para nuevas operaciones y recursos. Para obtener una lista y descripciones de las políticas de funciones de trabajo, consulte [Políticas administradas de AWS para funciones de trabajo](#) en la Guía del usuario de IAM.

Las nuevas acciones que permiten enumerar y eliminar las sesiones de los usuarios están disponibles en el nuevo espacio de nombres de `identitystore-auth`. Los permisos adicionales para las acciones de este espacio de nombres se actualizarán en esta página. Al crear sus políticas de IAM personalizadas, evite utilizar \* después de `identitystore-auth`, ya que esto se aplica a todas las acciones que existan en el espacio de nombres ahora o en el futuro.

## AWS política gestionada: AWSSSOMaster AccountAdministrator

La política `AWSSSOMasterAccountAdministrator` proporciona a las entidades principales las acciones administrativas necesarias. La política está destinada a los directores que desempeñan la función de AWS IAM Identity Center administradores. Con el tiempo, la lista de acciones proporcionada se actualizará para adaptarla a la funcionalidad actual de IAM Identity Center y a las acciones que se requieren como administrador.

Puede adjuntar la política `AWSSSOMasterAccountAdministrator` a las identidades de IAM. Cuando adjuntas la `AWSSSOMasterAccountAdministrator` política a una identidad, concedes AWS IAM Identity Center permisos administrativos. Los directores que cuenten con esta política pueden acceder al Centro de Identidad de IAM desde la cuenta de AWS Organizations administración y desde todas las cuentas de los miembros. Esta entidad principal puede administrar por completo todas las operaciones de IAM Identity Center, incluida la posibilidad de crear una instancia de IAM Identity Center, los usuarios, los conjuntos de permisos y las asignaciones. El director también puede instanciar esas asignaciones en todas las cuentas de los miembros de la AWS organización y establecer conexiones entre los directorios AWS Directory Service gestionados y el IAM Identity Center. A medida que se publiquen nuevas características administrativas, el administrador de la cuenta recibirá estos permisos automáticamente.

### Agrupaciones de permisos

Esta política se agrupa en instrucciones basadas en el conjunto de permisos proporcionados.

- `AWSSSOMasterAccountAdministrator`: permite a IAM Identity Center [transferir el rol de servicio](#) designado como `AWSServiceRoleforSSO` a IAM Identity Center, para que más adelante pueda asumir el rol y realizar acciones en su nombre. Esto es necesario cuando la persona o la aplicación intenta habilitar IAM Identity Center. Para obtener más información, consulte [Cuenta de AWS acceso](#).
- `AWSSSOMemberAccountAdministrator`— Permite a IAM Identity Center realizar acciones de administrador de cuentas en un entorno de varias cuentas. AWS Para obtener más información, consulte [AWS política gestionada: AWSSSOMember AccountAdministrator](#).

- **AWSSSOManageDelegatedAdministrator**: permite a IAM Identity Center registrar y anular el registro de un administrador delegado para su organización.

Para ver los permisos de esta política, consulte la Referencia de políticas

[AWSSSOMasterAccountAdministrator](#) AWS gestionadas.

### Información adicional acerca de esta política

Cuando el Centro de Identidad de IAM se activa por primera vez, el servicio del Centro de Identidad de IAM crea un [rol vinculado al servicio](#) en la cuenta de AWS Organizations administración (anteriormente, cuenta maestra) para que el Centro de Identidad de IAM pueda administrar los recursos de su cuenta. Las acciones necesarias son `iam:CreateServiceLinkedRole` y `iam:PassRole`, que se muestran en los siguientes fragmentos.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AWSSSOCreateSLR",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:AWSServiceName" : "sso.amazonaws.com"
        }
      }
    },
    {
      "Sid" : "AWSSSOMasterAccountAdministrator",
      "Effect" : "Allow",
      "Action" : "iam:PassRole",
      "Resource" : "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/AWSServiceRoleForSSO",
      "Condition" : {
        "StringLike" : {
          "iam:PassedToService" : "sso.amazonaws.com"
        }
      }
    }
  ],
  {
```

```

    "Sid" : "AWSSSOMemberAccountAdministrator",
    "Effect" : "Allow",
    "Action" : [
        "ds:DescribeTrusts",
        "ds:UnauthorizeApplication",
        "ds:DescribeDirectories",
        "ds:AuthorizeApplication",
        "iam:ListPolicies",
        "organizations:EnableAWSServiceAccess",
        "organizations:ListRoots",
        "organizations:ListAccounts",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeOrganization",
        "organizations:ListChildren",
        "organizations:DescribeAccount",
        "organizations:ListParents",
        "organizations:ListDelegatedAdministrators",
        "sso:*",
        "sso-directory:*",
        "identitystore:*",
        "identitystore-auth:*",
        "ds:CreateAlias",
        "access-analyzer:ValidatePolicy",
        "signin:CreateTrustedIdentityPropagationApplicationForConsole",
        "signin:ListTrustedIdentityPropagationApplicationsForConsole"
    ],
    "Resource" : "*"
},
{
    "Sid" : "AWSSSOManageDelegatedAdministrator",
    "Effect" : "Allow",
    "Action" : [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
    ],
    "Resource" : "*",
    "Condition" : {
        "StringEquals" : {
            "organizations:ServicePrincipal" : "sso.amazonaws.com"
        }
    }
},
{

```

```
    "Sid": "AllowDeleteSyncProfile",
    "Effect": "Allow",
    "Action": [
        "identity-sync:DeleteSyncProfile"
    ],
    "Resource": [
        "arn:aws:identity-sync:*:*:profile/*"
    ]
  }
]
```

## AWS política gestionada: AWSSSOMember AccountAdministrator

La política `AWSSSOMemberAccountAdministrator` proporciona a las entidades principales las acciones administrativas necesarias. La política está destinada a las entidades principales que desempeñan el rol de un administrador de IAM Identity Center. Con el tiempo, la lista de acciones proporcionada se actualizará para adaptarla a la funcionalidad actual de IAM Identity Center y a las acciones que se requieren como administrador.

Puede adjuntar la política `AWSSSOMemberAccountAdministrator` a las identidades de IAM. Cuando adjuntas la `AWSSSOMemberAccountAdministrator` política a una identidad, concedes AWS IAM Identity Center permisos administrativos. Los directores que cuenten con esta política pueden acceder al Centro de Identidad de IAM desde la cuenta de AWS Organizations administración y desde todas las cuentas de los miembros. Esta entidad principal puede administrar por completo todas las operaciones de IAM Identity Center, incluida la capacidad de crear usuarios, conjuntos de permisos y asignaciones. El director también puede instanciar esas asignaciones en todas las cuentas de los miembros de la AWS organización y establecer conexiones entre los directorios AWS Directory Service gestionados y el IAM Identity Center. A medida que se publiquen nuevas características administrativas, el administrador de la cuenta recibe estos permisos automáticamente.

Para ver los permisos de esta política, consulte la Referencia de políticas [AWSSSOMemberAccountAdministrator](#) [AWS](#) gestionadas.

### Información adicional acerca de esta política

Los administradores de IAM Identity Center administran a los usuarios, los grupos y las contraseñas en su almacén de directorios de Identity Center (sso-directory). El rol de administrador de la cuenta incluye permisos para las siguientes acciones:



- "sso:\*"
- "sso-directory:\*"

Los administradores del centro de identidad de IAM necesitan permisos limitados para realizar las siguientes AWS Directory Service acciones para realizar las tareas diarias.

- "ds:DescribeTrusts"
- "ds:UnauthorizeApplication"
- "ds:DescribeDirectories"
- "ds:AuthorizeApplication"
- "ds:CreateAlias"

Estos permisos permiten a los administradores de IAM Identity Center identificar los directorios existentes y administrar aplicaciones para que puedan configurarse para su uso con IAM Identity Center. Para obtener más información acerca de cada una de estas acciones, consulte [Permisos de la API de AWS Directory Service : referencia acerca de las acciones, los recursos y las condiciones](#).

IAM Identity Center utiliza las políticas de IAM para conceder permisos a los usuarios de IAM Identity Center. Los administradores de IAM Identity Center crean conjuntos de permisos y les adjuntan políticas. El administrador de IAM Identity Center debe tener los permisos para enumerar las políticas existentes, de modo que pueda elegir qué políticas usar con el conjunto de permisos que está creando o actualizando. Para establecer permisos seguros y funcionales, el administrador de IAM Identity Center debe tener permisos para ejecutar la validación de la política de IAM Access Analyzer.

- "iam:ListPolicies"
- "access-analyzer:ValidatePolicy"

Los administradores del centro de identidad de IAM necesitan un acceso limitado a las siguientes AWS Organizations acciones para realizar las tareas diarias:

- "organizations:EnableAWSServiceAccess"
- "organizations:ListRoots"
- "organizations:ListAccounts"
- "organizations:ListOrganizationalUnitsForParent"

- "organizations:ListAccountsForParent"
- "organizations:DescribeOrganization"
- "organizations:ListChildren"
- "organizations:DescribeAccount"
- "organizations:ListParents"
- "organizations:ListDelegatedAdministrators"
- "organizations:RegisterDelegatedAdministrator"
- "organizations:DeregisterDelegatedAdministrator"

Estos permisos permiten a los administradores de IAM Identity Center trabajar con los recursos de la organización (cuentas) para realizar tareas administrativas básicas de IAM Identity Center, como las siguientes:

- Identificación de la cuenta de administración que pertenece a la organización
- Identificación de las cuentas de los miembros que pertenecen a la organización
- Habilitar el acceso AWS al servicio para las cuentas
- Configuración y administración de un administrador delegado

Para obtener más información acerca de cómo hacer uso de un administrador delegado con IAM Identity Center, consulte [Administración delegada](#). Para obtener más información sobre cómo se utilizan estos permisos AWS Organizations, consulte [Uso AWS Organizations con otros AWS servicios](#).

## AWS política gestionada: AWSSSODirectory administrador

Puede adjuntar la política AWSSSODirectoryAdministrator a las identidades de IAM.

Esta política concede permisos administrativos a los usuarios y grupos de IAM Identity Center. Las entidades principales que cuentan con esta política adjunta pueden realizar cualquier actualización a los usuarios y grupos de IAM Identity Center.

Para ver los permisos de esta política, consulte [AWSSSODirectoryAdministrator](#) en AWS Managed Policy Reference.

## AWS política gestionada: AWSSSOREad únicamente

Puede adjuntar la política AWSSSOREadOnly a las identidades de IAM.

Esta política otorga permisos de solo lectura que permiten a los usuarios ver información en IAM Identity Center. Las entidades principales que cuentan con esta política adjunta no pueden ver los usuarios y grupos de IAM Identity Center directamente. Las entidades principales que cuentan con esta política adjunta no pueden realizar ninguna actualización en IAM Identity Center. Por ejemplo, las entidades principales que cuentan con estos permisos pueden visualizar los ajustes de IAM Identity Center, pero no pueden cambiar ninguno de los valores de la configuración.

Para ver los permisos de esta política, consulte [AWSSSORedSolo](#) en la referencia de políticas AWS gestionadas.

### AWS política gestionada: AWSSSODirectory ReadOnly

Puede adjuntar la política AWSSSODirectoryReadOnly a las identidades de IAM.

Esta política concede permisos de solo lectura que permiten a los usuarios ver los usuarios y grupos en IAM Identity Center. Las entidades principales que cuentan con esta política adjunta no pueden ver las asignaciones, los conjuntos de permisos, las aplicaciones ni los ajustes de IAM Identity Center. Las entidades principales que cuentan con esta política adjunta no pueden realizar ninguna actualización en IAM Identity Center. Por ejemplo, las entidades principales que cuentan con estos permisos pueden ver los usuarios de IAM Identity Center, pero no pueden cambiar ningún atributo de usuario ni asignar dispositivos de MFA.

Para ver los permisos de esta política, consulte la Referencia [AWSSSODirectoryReadOnly](#) de políticas AWS gestionadas.

### AWS política gestionada: AWSIdentity SyncFullAccess

Puede adjuntar la política AWSIdentitySyncFullAccess a las identidades de IAM.

Las entidades principales que cuentan con esta política adjunta tienen permisos de acceso total para crear y eliminar perfiles de sincronización, asociar o actualizar un perfil de sincronización con un destino de sincronización, crear, enumerar y eliminar filtros de sincronización, e iniciar o detener la sincronización.

#### Detalles del permiso

Para ver los permisos de esta política, consulte la Referencia [AWSIdentitySyncFullAccess](#) de políticas AWS gestionadas.

### AWS política gestionada: AWSIdentity SyncReadOnlyAccess

Puede adjuntar la política AWSIdentitySyncReadOnlyAccess a las identidades de IAM.

Esta política concede permisos de solo lectura que permiten a los usuarios ver información sobre el perfil de sincronización de identidades, los filtros y la configuración de destino. Las entidades principales que cuentan con esta política adjunta no pueden actualizar la configuración de sincronización. Por ejemplo, las entidades principales que cuentan con estos permisos pueden visualizar los ajustes de sincronización de identidades, pero no pueden cambiar ninguno de los valores del perfil o del filtro.

Para ver los permisos de esta política, consulte la Referencia [AWSIdentitySyncReadOnlyAccess](#) de políticas AWS gestionadas.

## AWS política gestionada: AWSSSOService RolePolicy

No puede adjuntar la política AWSSSOServiceRolePolicy a las identidades de IAM.

Esta política está asociada a una función vinculada al servicio que permite a IAM Identity Center delegar y hacer cumplir qué usuarios tienen acceso de inicio de sesión único a una entrada específica. Cuentas de AWS Organizations Al habilitar la IAM, se crea una función vinculada al servicio en todos los ámbitos de la organización. Cuentas de AWS IAM Identity Center también crea el mismo rol vinculado a servicios en todas las cuentas que se añaden posteriormente a su organización. Este rol permite a IAM Identity Center acceder a los recursos de cada cuenta en su nombre. Los roles vinculados al servicio que se crean en cada uno de ellos reciben un nombre. Cuenta de AWS AWSServiceRoleForSSO Para obtener más información, consulte [Uso de roles vinculados a servicios para IAM Identity Center](#).

## AWS política gestionada: AWSIAMIdentity CenterAllowListForIdentityContext

Al asumir un rol con el contexto de identidad del Centro de Identidad de IAM, AWS Security Token Service (AWS STS) asocia automáticamente la AWSIAMIdentityCenterAllowListForIdentityContext política al rol.

Esta política proporciona la lista de acciones que se permiten cuando se utiliza la propagación de identidades de confianza con roles que se asumen con el contexto de identidad de IAM Identity Center. Se bloquearán todas las demás acciones que se invoquen en este contexto. El contexto de identidad se transmite como ProvidedContext.

Para ver los permisos de esta política, consulte la Referencia de políticas [AWSIAMIdentityCenterAllowListForIdentityContext](#) AWS gestionadas.

## IAM Identity Center actualiza las políticas AWS gestionadas

En la siguiente tabla se describen las actualizaciones de las políticas AWS gestionadas del Centro de Identidad de IAM desde que este servicio comenzó a realizar el seguimiento de estos cambios. Para obtener alertas automáticas sobre los cambios que se produzcan en esta página, suscríbase al canal RSS en la página de historial de documentos de IAM Identity Center.

| Cambio                                                          | Descripción                                                                                                                                                                                                                                                           | Fecha                    |
|-----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| <a href="#">AWSSSOServiceRolePolicy</a>                         | Esta política ahora incluye permisos para <code>llamaridentity-sync:DeleteSyncProfile</code> .                                                                                                                                                                        | 11 de febrero de 2025    |
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye las <code>qapps:ListQAppSessionData</code> <code>qapps:ExportQAppSessionData</code> acciones necesarias para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 2 de octubre de 2024     |
| <a href="#">AWSSSOMasterAccountAdministrator</a>                | El Centro de Identidad de IAM ha añadido una nueva acción para conceder <code>DeleteSyncProfile</code> permisos que le permitan utilizar esta política para eliminar los perfiles de sincronización. Esta acción está asociada a la <code>DeleteInstance</code> API.  | 26 de septiembre de 2024 |
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye la <code>s3:ListCallerAccess</code>                                                                                                                                                                                                       | 4 de septiembre de 2024  |

| Cambio                                                          | Descripción                                                                                                                                                                                                                                                                                 | Fecha               |
|-----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                                                 | sGrants acción para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones.                                                                                                                                            |                     |
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye lasaoss :APIAccessAll , es:ESHttpHead es:ESHttpPost es:ESHttpGet es:ESHttpPatch es:ESHttpDelete , y es:ESHttpPut las acciones para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 12 de julio de 2024 |

| Cambio                                                          | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Fecha               |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye las opciones <code>qapps:PredictQApp</code> , <code>qapps:ImportDocument</code> , <code>qapps:AssociateLibraryItemReview</code> <code>qapps:DisassociateLibraryItemReview</code> <code>qapps:GetQAppSession</code> <code>qapps:UpdateQAppSession</code> <code>qapps:GetQAppSessionMetadata</code> <code>qapps:UpdateQAppSessionMetadata</code> , y <code>qapps:TagResource</code> las acciones para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 27 de junio de 2024 |

| Cambio                                                          | Descripción                                                                                                                                                                                                                                                                  | Fecha              |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye las acciones elasticmapreduce:AddJobFlowSteps ,elasticmapreduce:DescribeCluster ,elasticmapreduce:CancelSteps ,elasticmapreduce:DescribeStep y elasticmapreduce:ListSteps para respaldar la propagación de identidades confiables en Amazon EMR. | 17 de mayo de 2024 |



| Cambio                                                                 | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Fecha               |
|------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | Esta política ahora incluye las <code>qapps:CreateQApp</code> , <code>qapps:PredictProblemStatementFromConversation</code> , <code>qapps:PredictQAppFromProblemStatement</code> , <code>qapps:CopyQApp</code> , <code>qapps:GetQApp</code> , <code>qapps:ListQApps</code> , <code>qapps:UpdateQApp</code> , <code>qapps&gt;DeleteQApp</code> , <code>qapps:AssociateQAppWithUser</code> , <code>qapps:DissociateQAppFromUser</code> , <code>qapps:ImportDocumentToQAppSession</code> , <code>qapps:CreateLibraryItem</code> , <code>qapps:GetLibraryItem</code> , <code>qapps:UpdateLibraryItem</code> , <code>qapps:CreateLibraryItemReview</code> , <code>qapps:ListLibraryItems</code> , <code>qapps:CreateSubscriptionToken</code> , <code>qapps:StartQAppSession</code> , y <code>qapps:StopQAppSession</code> las acciones para respaldar las sesiones de consola con | 30 de abril de 2024 |

| Cambio                                                  | Descripción                                                                                                                                                                                                                                                                                                                              | Fecha               |
|---------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
|                                                         | identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones.                                                                                                                                                                                                                                                   |                     |
| <a href="#"><u>AWSSSOMasterAccountAdministrator</u></a> | Esta política ahora incluye las <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> acciones necesarias para respaldar <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 26 de abril de 2024 |
| <a href="#"><u>AWSSSOMemberAccountAdministrator</u></a> | Esta política ahora incluye las <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> acciones necesarias para respaldar <code>signin:CreateTrustedIdentityPropagationApplicationForConsole</code> las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 26 de abril de 2024 |

| Cambio                                                          | Descripción                                                                                                                                                                                                                                      | Fecha               |
|-----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AWSSSOReadSolo</a>                                  | Esta política ahora incluye la <code>signin:ListTrustedIdentityPropagationApplicationsForConsole</code> acción para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 26 de abril de 2024 |
| <a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a> | Esta política ahora incluye la <code>qbusiness:PutFeedback</code> acción para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones.                                       | 26 de abril de 2024 |

| Cambio                                                                 | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Fecha               |
|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | Esta política ahora incluye las opciones <code>q:StartConversation</code> , <code>q:SendMessage</code> , <code>q:ListConversations</code> , <code>q:GetConversation</code> , <code>q:StartTroubleshootingAnalysis</code> , <code>q:GetTroubleshootingResults</code> , <code>q:StartTroubleshootingResolutionExplanation</code> , y <code>q:UpdateTroubleshootingCommandResult</code> las acciones para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 24 de abril de 2024 |
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | Esta política ahora incluye la <code>sts:SetContext</code> acción para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones.                                                                                                                                                                                                                                                                                                                                 | 19 de abril de 2024 |

| Cambio                                                                 | Descripción                                                                                                                                                                                                                                                                                                                                                                    | Fecha                   |
|------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | Esta política ahora incluye las <code>qbusiness:Chat</code> , <code>qbusiness:ChatSync</code> , <code>qbusiness:ListConversations</code> , <code>qbusiness:ListMessages</code> , y <code>qbusiness&gt;DeleteConversation</code> las acciones para respaldar las sesiones de consola con identidad mejorada para las aplicaciones AWS administradas que admiten estas sesiones. | 11 de abril de 2024     |
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | La política ahora incluye las acciones <code>s3:GetAccessGrantsInstanceForPrefix</code> y <code>s3:GetDataAccess</code> .                                                                                                                                                                                                                                                      | 26 de noviembre de 2023 |
| <a href="#"><u>AWSIAMIdentityCenterAllowListForIdentityContext</u></a> | Esta política proporciona la lista de acciones que se permiten cuando se utiliza la propagación de identidades de confianza con roles que se asumen con el contexto de identidad de IAM Identity Center.                                                                                                                                                                       | 15 de noviembre de 2023 |
| <a href="#"><u>AWSSSODirectoryReadOnly</u></a>                         | Ahora esta política incluye el nuevo espacio de nombres de <code>identitystore-auth</code> con nuevos permisos que permiten a los usuarios enumerar y obtener sesiones.                                                                                                                                                                                                        | 21 de febrero de 2023   |

| Cambio                                           | Descripción                                                                                                                                                                              | Fecha                 |
|--------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">AWSSSOServiceRolePolicy</a>          | Ahora esta política permite realizar la acción <a href="#">UpdateSAMLProvider</a> en la cuenta de administración.                                                                        | 20 de octubre de 2022 |
| <a href="#">AWSSSOMasterAccountAdministrator</a> | Ahora esta política incluye el nuevo espacio de nombres de <code>identitystore-auth</code> con nuevos permisos que permiten al administrador enumerar y eliminar sesiones de un usuario. | 20 de octubre de 2022 |
| <a href="#">AWSSSOMemberAccountAdministrator</a> | Ahora esta política incluye el nuevo espacio de nombres de <code>identitystore-auth</code> con nuevos permisos que permiten al administrador enumerar y eliminar sesiones de un usuario. | 20 de octubre de 2022 |
| <a href="#">AWSSSODirectoryAdministrator</a>     | Ahora esta política incluye el nuevo espacio de nombres de <code>identitystore-auth</code> con nuevos permisos que permiten al administrador enumerar y eliminar sesiones de un usuario. | 20 de octubre de 2022 |

| Cambio                                                  | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                 | Fecha                |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <a href="#"><u>AWSSSOMasterAccountAdministrator</u></a> | Esta política ahora incluye nuevos permisos para realizar llamadas <a href="#"><u>ListDelegatedAdministrators</u></a> . AWS Organizations Ahora esta política también incluye un subconjunto de permisos de <code>AWSSSOManageDelegatedAdministrator</code> que incluye permisos para realizar llamadas a <a href="#"><u>RegisterDelegatedAdministrator</u></a> y <a href="#"><u>DeregisterDelegatedAdministrator</u></a> . | 16 de agosto de 2022 |
| <a href="#"><u>AWSSSOMemberAccountAdministrator</u></a> | Esta política ahora incluye nuevos permisos para llamar <a href="#"><u>ListDelegatedAdministrators</u></a> AWS Organizations. Ahora esta política también incluye un subconjunto de permisos de <code>AWSSSOManageDelegatedAdministrator</code> que incluye permisos para realizar llamadas a <a href="#"><u>RegisterDelegatedAdministrator</u></a> y <a href="#"><u>DeregisterDelegatedAdministrator</u></a> .             | 16 de agosto de 2022 |

| Cambio                                                                                                                                 | Descripción                                                                                                                                                                                    | Fecha                |
|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------|
| <a href="#">AWSSSOReadSolo</a>                                                                                                         | Esta política ahora incluye nuevos permisos para llamar <a href="#">ListDelegatedAdministrators</a> en AWS Organizations.                                                                      | 11 de agosto de 2022 |
| <a href="#">AWSSSOServiceRolePolicy</a>                                                                                                | Ahora esta política incluye nuevos permisos para realizar llamadas a <a href="#">DeleteRolePermissionsBoundary</a> en <a href="#">PutRolePermissionsBoundary</a> .                             | 14 de julio de 2022  |
| <a href="#">AWSSSOServiceRolePolicy</a>                                                                                                | Ahora esta política incluye nuevos permisos para realizar llamadas a <a href="#">ListAWSServiceAccessForOrganization</a> and <a href="#">ListDelegatedAdministrators</a> en AWS Organizations. | 11 de mayo de 2022   |
| <a href="#">AWSSSOMasterAccountAdministrator</a><br><a href="#">AWSSSOMemberAccountAdministrator</a><br><a href="#">AWSSSOReadSolo</a> | Agregue permisos de IAM Access Analyzer para permitir a una entidad principal utilizar las verificaciones de políticas para la validación.                                                     | 28 de abril de 2022  |



| Cambio                                                  | Descripción                                                                                                                                                                                                                                                                                                                                            | Fecha               |
|---------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#"><u>AWSSSOMasterAccountAdministrator</u></a> | <p>Ahora esta política permite todas las acciones del servicio Almacén de identidades de IAM Identity Center.</p> <p>Para obtener información acerca de las acciones disponibles en el servicio de almacén de identidades de IAM, consulte <a href="#"><u>Referencia de la API del servicio Almacén de identidades de IAM Identity Center</u></a>.</p> | 29 de marzo de 2022 |
| <a href="#"><u>AWSSSOMemberAccountAdministrator</u></a> | Ahora esta política permite todas las acciones del servicio Almacén de identidades de IAM Identity Center.                                                                                                                                                                                                                                             | 29 de marzo de 2022 |
| <a href="#"><u>AWSSSODirectoryAdministrator</u></a>     | Ahora esta política permite todas las acciones del servicio Almacén de identidades de IAM Identity Center.                                                                                                                                                                                                                                             | 29 de marzo de 2022 |
| <a href="#"><u>AWSSSODirectoryReadOnly</u></a>          | Ahora esta política concede acceso a las acciones de lectura del servicio Almacén de identidades de IAM Identity Center. Este acceso es necesario para recuperar la información de los usuarios y los grupos del servicio Almacén de identidades de IAM Identity Center.                                                                               | 29 de marzo de 2022 |

| Cambio                                                               | Descripción                                                                                                                                          | Fecha               |
|----------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">AWSIdentitySyncFullAccess</a>                            | Esta política permite obtener acceso completo a permisos de sincronización de identidades.                                                           | 3 de marzo de 2022  |
| <a href="#">AWSIdentitySyncReadOnlyAccess</a>                        | Esta política concede permisos de solo lectura que permiten a una entidad principal visualizar la configuración de la sincronización de identidades. | 3 de marzo de 2022  |
| <a href="#">AWSSSORReadSolo</a>                                      | Esta política concede permisos de solo lectura que permiten a una entidad principal visualizar los ajustes de configuración de IAM Identity Center.  | 4 de agosto de 2021 |
| IAM Identity Center comenzó a realizar el seguimiento de los cambios | IAM Identity Center comenzó a realizar un seguimiento de los cambios en las políticas AWS gestionadas.                                               | 4 de agosto de 2021 |

## Uso de roles vinculados a servicios para IAM Identity Center

AWS IAM Identity Center utiliza funciones AWS Identity and Access Management vinculadas al [servicio](#) (IAM). Un rol vinculado a servicios es un tipo único de rol de IAM que está vinculado directamente a IAM Identity Center. Está predefinido por el Centro de Identidad de IAM e incluye todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre. Para obtener más información, consulte [Entender los roles vinculados a servicios en IAM Identity Center](#).

Un rol vinculado a servicios simplifica la configuración de IAM Identity Center porque ya no tendrá que agregar manualmente los permisos necesarios. IAM Identity Center define los permisos de su rol vinculado a servicios y, a menos que esté definido de otra manera, solo IAM Identity Center puede

asumir su rol. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda asociar a ninguna otra entidad de IAM.

Para obtener información acerca de otros servicios que admiten roles vinculados a servicios, consulte [Servicios de AWS que funcionan con IAM](#) y busque los servicios que muestran Yes (Sí) en la columna Service Linked Role (Rol vinculado a servicios). Elija una opción Sí con un enlace para ver la documentación acerca del rol vinculado a servicios en cuestión.

## Permisos de roles vinculados a servicios para IAM Identity Center

El Centro de identidad de IAM utiliza la función vinculada al servicio denominada `AWSServiceRoleForSSO` para conceder permisos al Centro de identidad de IAM para gestionar los AWS recursos, incluidas las funciones de IAM, las políticas y el IdP de SAML en su nombre.

La función de `AWSService RoleFor SSO` vinculada al servicio confía en los siguientes servicios para que la asuman:

- IAM Identity Center (prefijo de servicio: `sso`)

La política de permisos de los roles `AWSSSOService RolePolicy` vinculados a un servicio permite al Centro de Identidad de IAM completar lo siguiente en los roles de la ruta `«/aws-reserved/sso.amazonaws.com/»` y con el prefijo de nombre `«SSO_»`: `AWSReserved`

- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam>DeleteRolePermissionsBoundary`
- `iam>DeleteRolePolicy`
- `iam:DetachRolePolicy`
- `iam:GetRole`
- `iam:ListRolePolicies`
- `iam:PutRolePolicy`
- `iam:PutRolePermissionsBoundary`
- `iam:ListAttachedRolePolicies`

La política de permisos de funciones AWSSSOService RolePolicy vinculadas al servicio permite a IAM Identity Center completar lo siguiente en los proveedores de SAML con el prefijo «\_»: AWSSSO

- `iam:CreateSAMLProvider`
- `iam:GetSAMLProvider`
- `iam:UpdateSAMLProvider`
- `iam>DeleteSAMLProvider`

La política de permisos de roles AWSSSOService RolePolicy vinculados al servicio permite al Centro de Identidad de IAM completar lo siguiente en todas las organizaciones:

- `organizations:DescribeAccount`
- `organizations:DescribeOrganization`
- `organizations:ListAccounts`
- `organizations:ListAWSServiceAccessForOrganization`
- `organizations:ListDelegatedAdministrators`

La política de permisos de funciones AWSSSOService RolePolicy vinculadas al servicio permite a IAM Identity Center realizar las siguientes tareas en todas las funciones de IAM (\*):

- `iam:listRoles`

La política de permisos de roles AWSSSOService RolePolicy vinculados al servicio permite al Centro de Identidad de IAM completar lo siguiente en «arn:aws:iam: \*:»: role/aws-service-role/ssso.amazonaws.com/AWSServiceRoleForSSO

- `iam:GetServiceLinkedRoleDeletionStatus`
- `iam>DeleteServiceLinkedRole`

La política de permisos de roles AWSSSOService RolePolicy vinculados al servicio permite al Centro de Identidad de IAM completar lo siguiente en «arn:aws:identity-sync: \*:\*:profile/\*»:

- `identity-sync>DeleteSyncProfile`

Para obtener más información [IAM Identity Center actualiza las políticas AWS gestionadas](#) sobre AWSSSOService RolePolicy las actualizaciones de la política de permisos de roles vinculados al servicio, consulte.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "IAMRoleProvisioningActions",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam>DeleteRolePermissionsBoundary",
        "iam:PutRolePermissionsBoundary",
        "iam:PutRolePolicy",
        "iam:UpdateRole",
        "iam:UpdateRoleDescription",
        "iam:UpdateAssumeRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
      ],
      "Condition": {
        "StringNotEquals": {
          "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
        }
      }
    },
    {
      "Sid": "IAMRoleReadActions",
      "Effect": "Allow",
      "Action": [
        "iam:GetRole",
        "iam:ListRoles"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "IAMRoleCleanupActions",
      "Effect": "Allow",

```

```

    "Action":[
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:ListRolePolicies",
        "iam:ListAttachedRolePolicies"
    ],
    "Resource":[
        "arn:aws:iam::*:role/aws-reserved/sso.amazonaws.com/*"
    ]
},
{
    "Sid":"IAMSLRCleanupActions",
    "Effect":"Allow",
    "Action":[
        "iam:DeleteServiceLinkedRole",
        "iam:GetServiceLinkedRoleDeletionStatus",
        "iam:DeleteRole",
        "iam:GetRole"
    ],
    "Resource":[
        "arn:aws:iam::*:role/aws-service-role/sso.amazonaws.com/
AWSServiceRoleForSSO"
    ]
},
{
    "Sid": "IAMSAMLProviderCreationAction",
    "Effect": "Allow",
    "Action": [
        "iam:CreateSAMLProvider"
    ],
    "Resource": [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ],
    "Condition": {
        "StringNotEquals": {
            "aws:PrincipalOrgMasterAccountId": "${aws:PrincipalAccount}"
        }
    }
},
{
    "Sid": "IAMSAMLProviderUpdateAction",
    "Effect": "Allow",
    "Action": [

```

```

        "iam:UpdateSAMLProvider"
    ],
    "Resource": [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ]
},
{
    "Sid": "IAMSAMLProviderCleanupActions",
    "Effect": "Allow",
    "Action": [
        "iam:DeleteSAMLProvider",
        "iam:GetSAMLProvider"
    ],
    "Resource": [
        "arn:aws:iam::*:saml-provider/AWSSSO_*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowUnauthAppForDirectory",
    "Effect": "Allow",
    "Action": [
        "ds:UnauthorizeApplication"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowDescribeForDirectory",
    "Effect": "Allow",
    "Action": [

```

```

        "ds:DescribeDirectories",
        "ds:DescribeTrusts"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowDescribeAndListOperationsOnIdentitySource",
    "Effect": "Allow",
    "Action": [
        "identitystore:DescribeUser",
        "identitystore:DescribeGroup",
        "identitystore:ListGroups",
        "identitystore:ListUsers"
    ],
    "Resource": [
        "*"
    ]
},
{
    "Sid": "AllowDeleteSyncProfile",
    "Effect": "Allow",
    "Action": [
        "identity-sync:DeleteSyncProfile"
    ],
    "Resource": [
        "arn:aws:identity-sync*:*:profile/*"
    ]
}
]
}

```

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte [Permisos de roles vinculados a servicios](#) en la Guía del usuario de IAM.

## Creación de un rol vinculado a servicios para IAM Identity Center

No necesita crear manualmente un rol vinculado a servicios. Una vez activado, IAM Identity Center crea un rol vinculado al servicio en todas las cuentas de la organización en Organizations. AWS IAM Identity Center también crea el mismo rol vinculado a servicios en todas las cuentas que se añaden



posteriormente a su organización. Este rol permite a IAM Identity Center acceder a los recursos de cada cuenta en su nombre.

#### Notas

- Si ha iniciado sesión en la cuenta de AWS Organizations administración, esta utilizará su función con la que ha iniciado sesión actualmente y no la función vinculada al servicio. De este modo se evita la escalada de privilegios.
- Cuando el IAM Identity Center realiza cualquier operación de IAM en la cuenta de AWS Organizations administración, todas las operaciones se realizan con las credenciales del director de IAM. Esto permite que los inicios de sesión CloudTrail proporcionen visibilidad de quién realizó todos los cambios de privilegios en la cuenta de administración.

#### Important

Si utilizaba el servicio IAM Identity Center antes del 7 de diciembre de 2017, cuando comenzó a admitir funciones vinculadas al servicio, IAM Identity Center creó la función de `AWSService RoleFor SSO` en su cuenta. Para obtener más información, consulte [Un nuevo rol ha aparecido en mi cuenta de IAM](#).

Si elimina este rol vinculado a un servicio y necesita crearlo de nuevo, puede seguir el mismo proceso para volver a crear el rol en su cuenta.

## Edición de un rol vinculado a servicios para IAM Identity Center

El Centro de Identidad de IAM no le permite editar la función de SSO vinculada al servicio. `AWSService RoleFor` Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte [Editar un rol vinculado a servicios](#) en la Guía del usuario de IAM.

## Eliminación de un rol vinculado a servicios para IAM Identity Center

No es necesario eliminar manualmente la función de SSO. `AWSService RoleFor` Cuando Cuenta de AWS se elimina un elemento de una AWS organización, el Centro de Identidad de IAM limpia automáticamente los recursos y elimina el rol vinculado al servicio. Cuenta de AWS

También puede utilizar la consola de IAM, la CLI de IAM o la API de IAM para eliminar manualmente el rol vinculado a servicios. Para ello, primero debe limpiar manualmente los recursos del rol vinculado al servicio para poder eliminarlo después manualmente.

 Note

Si el servicio IAM Identity Center está utilizando el rol cuando intenta eliminar los recursos, la eliminación podría producir un error. En tal caso, espere unos minutos e intente de nuevo la operación.

Para eliminar los recursos del Centro de Identidad de IAM utilizados por el SSO AWSService RoleFor

1. [Eliminación del acceso de usuarios y grupos a una Cuenta de AWS](#) para todos los usuarios y grupos que tengan acceso a la Cuenta de AWS.
2. [Elimine los conjuntos de permisos del Centro de identidades de IAM](#) que ha asociado con la Cuenta de AWS.

Para eliminar manualmente el rol vinculado a servicios mediante IAM

Utilice la consola de IAM, la CLI de IAM o la API de IAM para eliminar la función vinculada al servicio de AWSService RoleFor SSO. Para obtener más información, consulte [Eliminación de un rol vinculado a servicios](#) en la Guía del usuario de IAM.

## Consola de IAM Identity Center y autorización de la API

La consola de IAM Identity Center existente APIs admite la doble autorización, lo que le permite seguir utilizando las operaciones de la API existentes cuando haya más nuevas disponibles. APIs Si ya tiene instancias de IAM Identity Center que se hayan creado antes del 15 de noviembre de 2023 y el 15 de octubre de 2020, puede utilizar las siguientes tablas para determinar qué operaciones de la API se asignan ahora a las operaciones de la API más recientes que se publicaron después de esas fechas.

### Temas

- [Acciones de la API después de noviembre de 2023](#)
- [Acciones de la API después de octubre de 2020](#)

## Acciones de la API después de noviembre de 2023

Las instancias de IAM Identity Center que se crearon antes del 15 de noviembre de 2023 aceptan las acciones de la API antiguas y nuevas, siempre que no se deniegue explícitamente ninguna de ellas. Las instancias creadas después del 15 de noviembre de 2023 utilizan las [acciones de la API más recientes](#) a efectos de la autorización en la consola de IAM Identity Center.

| Nombre de operación de la consola utilizado antes del 15 de noviembre de 2023 | Acción de la API utilizada después del 15 de noviembre de 2023 |
|-------------------------------------------------------------------------------|----------------------------------------------------------------|
| AssociateProfile                                                              | CreateApplicationAssignment                                    |
| CreateManagedApplicationInstance   CreateApplicationInstance                  | CreateApplication                                              |
| CreateManagedApplicationInstance                                              | PutApplicationAuthenticationMethod                             |
| DeleteApplicationInstance   DeleteManagedApplicationInstance                  | DeleteApplication                                              |
| DeleteSSO                                                                     | DeleteInstance                                                 |
| DisassociateProfile                                                           | DeleteApplicationAssignment                                    |
| GetApplicationTemplate                                                        | DescribeApplicationProvider                                    |
| GetManagedApplicationInstance                                                 | DescribeApplication                                            |
| GetSharedSsoConfiguration                                                     | DescribeInstance                                               |
| ListApplicationInstances                                                      | ListApplications                                               |
| ListApplicationTemplates                                                      | ListApplicationProviders                                       |
| ListDirectoryAssociations                                                     | DescribeInstance                                               |
| ListProfileAssociations                                                       | ListApplicationAssignments                                     |

| Nombre de operación de la consola utilizado antes del 15 de noviembre de 2023                                   | Acción de la API utilizada después del 15 de noviembre de 2023 |
|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------|
| UpdateApplicationInstanceDisplayData   UpdateApplicationInstanceStatus   UpdateManagedApplicationInstanceStatus | UpdateApplication                                              |

## Acciones de la API después de octubre de 2020

Las instancias de IAM Identity Center que se crearon antes del 15 de octubre de 2020 aceptan las acciones de la API antiguas y nuevas, siempre que no se deniegue explícitamente ninguna de ellas. Las instancias creadas después del 15 de octubre de 2020 utilizan las [acciones de la API más recientes](#) a efectos de la autorización en la consola de IAM Identity Center.

| Operation name                         | API actions used before October 15, 2020 | API actions used after October 15, 2020 |
|----------------------------------------|------------------------------------------|-----------------------------------------|
| AssociateProfile                       | AssociateProfile                         | CreateAccountAssignment                 |
| AttachManagedPolicy                    | PutPermissionsPolicy                     | AttachManagedPolicyToPermissionSet      |
| CreatePermissionSet                    | CreatePermissionSet                      | CreatePermissionSet                     |
| DeleteApplicationInstanceForAWSAccount | DeleteApplicationInstance   DeleteTrust  | DeleteAccountAssignment                 |
| DeleteApplicationProfileForAwsAccount  | DeleteProfile                            | DeleteAccountAssignment                 |
| DeletePermissionsPolicy                | DeletePermissionsPolicy                  | DeleteInlinePolicyFromPermissionSet     |
| DeletePermissionSet                    | DeletePermissionSet                      | DeletePermissionSet                     |
| DescribePermissionsPolicies            | DescribePermissionsPolicies              | ListManagedPoliciesInPermissionSet      |

| Operation name                                   | API actions used before October 15, 2020           | API actions used after October 15, 2020 |
|--------------------------------------------------|----------------------------------------------------|-----------------------------------------|
| DetachManagedPolicy                              | DeletePermissionsPolicy                            | DetachManagedPolicyFromPermissionSet    |
| DisassociateProfile                              | DisassociateProfile                                | DeleteAccountAssignment                 |
| GetApplicationInstanceForAWSAccount              | GetApplicationInstance                             | ListAccountAssignments                  |
| GetAWSAccountProfileStatus                       | GetProfile                                         | ListPermissionSetsProvisionedToAccount  |
| GetPermissionSet                                 | GetPermissionSet                                   | DescribePermissionSet                   |
| GetPermissionsPolicy                             | GetPermissionsPolicy                               | GetInlinePolicyForPermissionSet         |
| ListAccountsWithProvisionedPermissionSet         | ListApplicationInstances   GetApplicationInstance  | ListAccountsForProvisionedPermissionSet |
| ListAWSAccountProfiles                           | ListProfiles   GetProfile                          | ListPermissionSetsProvisionedToAccount  |
| ListPermissionSets                               | ListPermissionSets                                 | ListPermissionSets                      |
| ListProfileAssociations                          | ListProfileAssociations                            | ListAccountAssignments                  |
| ProvisionApplicationInstanceForAWSAccount        | GetApplicationInstance   CreateApplicationInstance | CreateAccountAssignment                 |
| ProvisionApplicationProfileForAWSAccountInstance | GetProfile   CreateProfile   UpdateProfile         | CreateAccountAssignment                 |
| ProvisionSAMLProvider                            | GetTrust   CreateTrust   UpdateTrust               | CreateAccountAssignment                 |
| PutPermissionsPolicy                             | PutPermissionsPolicy                               | PutInlinePolicyToPermissionSet          |

| Operation name      | API actions used before October 15, 2020 | API actions used after October 15, 2020 |
|---------------------|------------------------------------------|-----------------------------------------|
| UpdatePermissionSet | UpdatePermissionSet                      | UpdatePermissionSet                     |

## AWS STS condicionan las claves de contexto del IAM Identity Center

Cuando un [director](#) hace una [solicitud](#) AWS, AWS recopila la información de la solicitud en un contexto de solicitud, que se utiliza para evaluar y autorizar la solicitud. Puede utilizar el elemento `Condition` de una política JSON para comparar las claves de la solicitud de contexto con los valores de claves que especifique en su política. La información de la solicitud proviene de diferentes orígenes, que abarcan la entidad principal que realiza la solicitud, el recurso con el que se realiza la solicitud y los metadatos sobre la solicitud en sí. Las claves de condición específicas del servicio se definen para su uso con un servicio individual. AWS

El IAM Identity Center incluye un proveedor de AWS STS contexto que permite a las aplicaciones AWS gestionadas y a las aplicaciones de terceros añadir valores a las claves de condición definidas por el IAM Identity Center. Estas claves se incluyen en los [roles de IAM](#). Los valores clave se establecen cuando una aplicación pasa un token a. AWS STS La aplicación obtiene el token al que pasa de una AWS STS de las siguientes maneras:

- Durante la autenticación con el IAM Identity Center.
- Tras el intercambio del token con un [emisor de token de confianza](#) para propagar la identidad de forma fiable. En este caso, la aplicación obtiene un token de un emisor de token de confianza y lo cambia por un token del IAM Identity Center.

Estas claves suelen ser utilizadas por aplicaciones que se integran con la propagación de identidades de confianza. En algunos casos, cuando hay valores clave, puede utilizarlas en las políticas de IAM que cree para permitir o denegar permisos.

Por ejemplo, es posible que desee proporcionar acceso condicional a un recurso en función del valor de `UserId`. Este valor indica qué usuario del IAM Identity Center utiliza el rol. El ejemplo es similar al uso de `SourceId`. Sin embargo, a diferencia de `SourceId`, el valor de `UserId` representa un usuario específico y verificado del almacén de identidades. Este valor está presente en el token que

la aplicación obtiene y al que, a continuación, pasa. AWS STS No es una cadena de uso general que pueda contener valores arbitrarios.

## Temas

- [almacén de identidades: UserId](#)
- [almacén de identidades: IdentityStoreArn](#)
- [centro de identidad: ApplicationArn](#)
- [centro de identidad: CredentialId](#)
- [centro de identidad: InstanceArn](#)

## almacén de identidades: UserId

Esta clave de contexto es `UserId` del usuario del IAM Identity Center, que es el sujeto de la afirmación de contexto emitida por el IAM Identity Center. La afirmación de contexto se pasa a. AWS STS Puede utilizar esta clave para comparar el `UserId` del usuario del IAM Identity Center en nombre del que se realiza la solicitud con el identificador del usuario que se especifique en la política.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud después de establecer una afirmación de contexto emitida por el Centro de Identidad de IAM, cuando se asume una función mediante cualquier AWS STS `assume-role` comando de la operación AWS CLI o AWS STS `AssumeRole` de la API.
- [Tipo de datos: cadena](#)
- Tipo de valor: valor único

## almacén de identidades: IdentityStoreArn

Esta clave de contexto es el ARN del almacén de identidades que está adjunto a la instancia del IAM Identity Center que emitió la afirmación de contexto. También es el almacén de identidades en el que puede buscar los atributos para `identitystore:UserID`. Puede usar esta clave en las políticas para determinar si `identitystore:UserID` proviene de un ARN de almacén de identidades esperado.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud después de establecer una afirmación de contexto emitida por el Centro de Identidad de IAM, cuando se asume una función mediante cualquier AWS STS `assume-role` comando de la operación o de la AWS CLI API. AWS STS `AssumeRole`

- Tipo de datos: [ARN](#), [cadena](#)
- Tipo de valor: valor único

## centro de identidad: ApplicationArn

Esta clave de contexto es el ARN de la aplicación para la que el IAM Identity Center emitió una afirmación de contexto. Puede usar esta clave en las políticas para determinar si `identitycenter:ApplicationArn` proviene de una aplicación esperada. El uso de esta clave puede ayudar a evitar que una aplicación inesperada acceda a un rol de IAM.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud de una operación de AWS STS `AssumeRole` API. El contexto de la solicitud incluye una afirmación de contexto emitida por el IAM Identity Center.
- Tipo de datos: [ARN](#), [cadena](#)
- Tipo de valor: valor único

## centro de identidad: CredentialId

Esta clave de contexto es un identificador aleatorio para la credencial de rol con identidad mejorada y se utiliza únicamente para el registro. Como este valor clave es impredecible, le recomendamos que no lo utilice para afirmaciones de contexto en políticas.

- Disponibilidad: esta clave se incluye en el contexto de la solicitud de una operación de AWS STS `AssumeRole` API. El contexto de la solicitud incluye una afirmación de contexto emitida por el IAM Identity Center.
- Tipo de datos: [cadena](#)
- Tipo de valor: valor único

## centro de identidad: InstanceArn

Esta clave de contexto es el ARN de la instancia de IAM Identity Center que emitió la afirmación de contexto para `identitystore:UserID`. Puede utilizar esta clave para determinar si `identitystore:UserID` y la afirmación de contexto provienen de un ARN de instancia de IAM Identity Center esperado.



- Disponibilidad: esta clave se incluye en el contexto de la solicitud de una operación de AWS STS AssumeRole API. El contexto de la solicitud incluye una afirmación de contexto emitida por el IAM Identity Center.
- Tipo de datos: [ARN](#), [cadena](#)
- Tipo de valor: valor único

## Registro y supervisión en IAM Identity Center

Una práctica recomendada es supervisar su organización para asegurarse de que los cambios se registren. La supervisión le ayuda a garantizar que puede investigar cualquier cambio inesperado y revertir los cambios no deseados. Actualmente, IAM Identity Center admite dos AWS servicios que le ayudan a supervisar su organización y la actividad que se lleva a cabo en ella: AWS CloudTrail Amazon EventBridge.

### Temas

- [Registrar las llamadas a la API de IAM Identity Center con AWS CloudTrail](#)
- [Registro de llamadas a la API del IAM Identity Center SCIM con AWS CloudTrail](#)
- [Connect los componentes de la aplicación con Amazon EventBridge](#)
- [Registrar errores de sincronización de AD configurables](#)

## Registrar las llamadas a la API de IAM Identity Center con AWS CloudTrail

AWS IAM Identity Center está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio en el Centro de Identidad de IAM. CloudTrail captura las llamadas a la API del Centro de Identidad de IAM como eventos. Las llamadas capturadas incluyen las llamadas realizadas desde la consola de IAM Identity Center y las llamadas de código a las operaciones de la API de IAM Identity Center. Si crea una [ruta](#), puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos del IAM Identity Center. Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos. Con la información recopilada por CloudTrail, puede determinar la solicitud que se realizó al Centro de Identidad de IAM, la dirección IP desde la que se realizó la solicitud, quién la hizo, cuándo se realizó y detalles adicionales.

Para obtener más información CloudTrail, consulte la [Guía del AWS CloudTrail usuario](#).

En la siguiente tabla se resumen los CloudTrail eventos del IAM Identity Center, sus fuentes de CloudTrail eventos y sus coincidencias. APIs Consulte las [referencias de la API del IAM Identity Center](#) para obtener más información sobre. APIs

 Note

Hay un grupo adicional de CloudTrail eventos, denominado inicio de sesión, que se AWS emite al iniciar sesión AWS como usuario del IAM Identity Center. Estos eventos no tienen un público coincidente y APIs, por lo tanto, no aparecen en las referencias de la API.

| CloudTrail eventos                           | Público APIs                                 | Descripción                                                                                                                                                                                                                   | CloudTrail fuentes de eventos                            |
|----------------------------------------------|----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|
| <a href="#">Centro de identidades de IAM</a> | <a href="#">Centro de identidades de IAM</a> | El Centro de Identidad de IAM APIs permite la gestión de conjuntos de permisos, aplicaciones, emisores de tokens de confianza, asignaciones de cuentas y aplicaciones, instancias del Centro de Identidad de IAM y etiquetas. | sso.amazonaws.com                                        |
| <a href="#">Almacén de identidades</a>       | <a href="#">Tienda de identidades</a>        | El almacén de identidades APIs permite gestionar el ciclo de vida de los usuarios y grupos de su fuerza laboral, así como de las membresías de los grupos de usuarios. Además, admiten la                                     | sso-directory.amazonaws.com, identitystore.amazonaws.com |

| CloudTrail eventos                   | Público APIs                         | Descripción                                                                                                                                                                 | CloudTrail fuentes de eventos               |
|--------------------------------------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|
|                                      |                                      | administración de los dispositivos MFA de los usuarios.                                                                                                                     |                                             |
| <a href="#">OIDC</a>                 | <a href="#">OIDC</a>                 | El OIDC APIs admite la propagación confiable de identidad y el inicio de sesión y los kits de herramientas IDE como AWS CLI usuario del IAM Identity Center ya autenticado. | sso.amazonaws.com , sso-oauth.amazonaws.com |
| <a href="#">AWS portal de acceso</a> | <a href="#">AWS portal de acceso</a> | El portal de AWS acceso APIs admite las operaciones del portal de AWS acceso y los usuarios obtienen las credenciales de las cuentas a través del AWS CLI.                  | sso.amazonaws.com                           |

| CloudTrail eventos                    | Público APIs           | Descripción                                                                                                                                                                                                                                            | CloudTrail fuentes de eventos    |
|---------------------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| <a href="#">Tienda de identidades</a> | <a href="#">SCIM</a>   | El SCIM APIs admite el aprovisionamiento de usuarios, grupos y membresías a grupos a través del protocolo SCIM. Para obtener más información, consulte <a href="#">Registro de llamadas a la API del IAM Identity Center SCIM con AWS CloudTrail</a> . | identitystore-scim.amazonaws.com |
| <a href="#">AWS Sign-In</a>           | No hay una API pública | AWS Emite CloudTrail eventos de inicio de sesión para la autenticación de los usuarios y los flujos de federación al IAM Identity Center.                                                                                                              | signin.amazonaws.com             |

## Temas

- [CloudTrail casos de uso del IAM Identity Center](#)
- [La información del centro de identidad de IAM se encuentra en CloudTrail](#)

## CloudTrail casos de uso del IAM Identity Center

Los CloudTrail eventos que emite el Centro de Identidad de IAM pueden ser valiosos para una variedad de casos de uso. Las organizaciones pueden usar estos registros de eventos para monitorear y auditar el acceso de los usuarios y la actividad en su AWS entorno. Esto puede ayudar a los casos de uso relacionados con el cumplimiento, ya que los registros recopilan detalles sobre quién accede a qué recursos y cuándo. También puedes usar los CloudTrail datos para investigar incidentes, lo que permite a los equipos analizar las acciones de los usuarios y rastrear los

comportamientos sospechosos. Además, el historial de eventos puede respaldar las iniciativas de solución de problemas, ya que proporciona visibilidad de los cambios realizados en los permisos y las configuraciones de los usuarios a lo largo del tiempo.

En las siguientes secciones se describen los casos de uso fundamentales que sirven de base a sus flujos de trabajo, como la auditoría, la investigación de incidentes y la solución de problemas.

## Identificación del usuario y la sesión en los eventos iniciados por los usuarios del IAM Identity Center CloudTrail

El Centro de Identidad de IAM emite dos CloudTrail campos que le permiten identificar al usuario del Centro de Identidad de IAM detrás de los CloudTrail eventos, como iniciar sesión en el Centro de Identidad de IAM o usar el portal de AWS acceso AWS CLI, incluida la administración de los dispositivos de MFA:

- `userId`— El identificador de usuario único e inmutable del almacén de identidades de una instancia del IAM Identity Center.
- `identityStoreArn`— El nombre de recurso de Amazon (ARN) del almacén de identidades que contiene al usuario.

Los `identityStoreArn` campos `userId` y se muestran en el `onBehalfOf` elemento anidado dentro del `userIdentity` elemento, como se muestra en el siguiente ejemplo. En este ejemplo, se muestran estos dos campos en un evento en el que el `userIdentity` tipo es "IdentityCenterUser". También puede incluir estos campos en los eventos de los usuarios autenticados del IAM Identity Center en los que el `userIdentity` tipo sea "Unknown". Sus flujos de trabajo deben aceptar ambos valores de tipo.

```
"userIdentity":{
  "type":"IdentityCenterUser",
  "accountId":"111122223333",
  "onBehalfOf": {
    "userId": "544894e8-80c1-707f-60e3-3ba6510dfac1",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "90e292de-5eb8-446e-9602-90f7c45044f7"
}
```

 Note

Le recomendamos que utilice `userId` y `identityStoreArn` para identificar al usuario responsable de los CloudTrail eventos del IAM Identity Center. Evite utilizar los campos `userName` o `principalId` debajo del `userIdentity` elemento cuando realice un seguimiento de las acciones de un usuario del Centro de Identidad de IAM que inicie sesión y utilice el portal de AWS acceso. Si sus flujos de trabajo, como la auditoría o la respuesta a incidentes, dependen de tener acceso al `username`, tiene dos opciones:

- Recupere el nombre de usuario del directorio del Centro de Identidad de IAM como se explica en [El CloudTrail nombre de usuario en los eventos de inicio de sesión](#).
- Obtenga el `UserName` que el Centro de Identidad de IAM emite en el `additionalEventData` elemento Iniciar sesión. Esta opción no requiere acceso al directorio del Centro de identidades de IAM. Para obtener más información, consulte [El CloudTrail nombre de usuario en los eventos de inicio de sesión](#).

Para recuperar los detalles de un usuario, incluido el `username` campo, consulte el almacén de identidades con el ID de usuario y el ID del almacén de identidades como parámetros. Puede realizar esta acción mediante la solicitud de [DescribeUser](#) API o mediante la CLI. El siguiente es un ejemplo de comando CLI. Puede omitir el `region` parámetro si la instancia del centro de identidad de IAM se encuentra en la región predeterminada de la CLI.

```
aws identitystore describe-user \  
--identity-store-id d-1234567890 \  
--user-id 544894e8-80c1-707f-60e3-3ba6510dfac1 \  
--region your-region-id
```

Para determinar el valor del identificador del almacén de identidades para el comando CLI del ejemplo anterior, puede extraer el identificador del almacén de identidades del `identityStoreArn` valor. En el ARN de ejemplo `arn:aws:identitystore::111122223333:identitystore/d-1234567890`, el ID del almacén de identidades es `d-1234567890`. Como alternativa, puede localizar el ID del almacén de identidades accediendo a la pestaña Identity Store de la sección Configuración de la consola del IAM Identity Center.

Si va a automatizar la búsqueda de usuarios en el directorio del Centro de Identidad de IAM, le recomendamos que calcule la frecuencia de las búsquedas de usuarios y que tenga en cuenta el límite máximo del [Centro de Identidad de IAM en la API de Identity Store](#). El almacenamiento

en caché de los atributos de usuario recuperados puede ayudarle a mantenerse dentro del límite máximo.

El `credentialId` valor se establece en el ID de la sesión del usuario del Centro de Identidad de IAM utilizada para solicitar la acción. Puede utilizar este valor para identificar CloudTrail los eventos iniciados dentro de la misma sesión de usuario autenticada del IAM Identity Center, excepto los eventos de inicio de sesión.

 Note

El [AuthWorkflowID](#) campo emitido en los eventos de inicio de sesión permite rastrear todos los CloudTrail eventos asociados a una secuencia de inicio de sesión antes del comienzo de una sesión de usuario del IAM Identity Center.

Correlacionar los usuarios entre el Centro de Identidad de IAM y los directorios externos

El Centro de identidades de IAM proporciona dos atributos de usuario que puede utilizar para correlacionar un usuario de su directorio con el mismo usuario de un directorio externo (por ejemplo, Microsoft Active Directory y). Okta Universal Directory

- `externalId`— El identificador externo de un usuario del Centro de identidades de IAM. Se recomienda asignar este identificador a un identificador de usuario inmutable en el directorio externo. Tenga en cuenta que el Centro de identidades de IAM no emite este valor en. CloudTrail
- `username`— Un valor proporcionado por el cliente con el que los usuarios suelen iniciar sesión. El valor puede cambiar (por ejemplo, con una actualización de SCIM). Tenga en cuenta que cuando la fuente de identidad es AWS Directory Service, el nombre de usuario que emite IAM Identity Center CloudTrail coincide con el nombre de usuario que introduce para autenticarse. No es necesario que el nombre de usuario coincida exactamente con el nombre de usuario del directorio del Centro de identidades de IAM.

Si tiene acceso a los CloudTrail eventos pero no al directorio del Centro de Identidad de IAM, puede utilizar el nombre de usuario que aparece debajo del `additionalEventData` elemento al iniciar sesión. Para obtener más información sobre el nombre de usuario en `additionalEventData`, consulte. [El CloudTrail nombre de usuario en los eventos de inicio de sesión](#)

La asignación de estos dos atributos de usuario a los atributos de usuario correspondientes en un directorio externo se define en el Centro de identidades de IAM cuando la fuente de identidad es la AWS Directory Service. Para obtener más información, consulte [Asignaciones de atributos entre Centro de identidades de IAM y directorio de proveedores de identidades externos](#) IdPs Externos que proporcionan a los usuarios SCIM su propio mapeo. Incluso si utiliza el directorio del Centro de Identidad de IAM como fuente de identidad, puede utilizar el `externalId` atributo para hacer una referencia cruzada de los principios de seguridad con su directorio externo.

En la siguiente sección se explica cómo buscar a un usuario del Centro de Identidad de IAM teniendo en cuenta el nombre y del usuario. `username externalId`

Visualización de un usuario del Centro de Identidad de IAM por nombre de usuario e ID externo

Para recuperar los atributos de usuario del directorio del Centro de Identidad de IAM para un nombre de usuario conocido, solicite primero el correspondiente `userId` mediante la solicitud de [GetUserId](#) API y, a continuación, emita una solicitud de [DescribeUser](#) API, como se muestra en el ejemplo anterior. En el siguiente ejemplo, se muestra cómo se puede recuperar un nombre `userId` de usuario específico del almacén de identidades. Puede omitir el `region` parámetro si su instancia del centro de identidad de IAM se encuentra en la región predeterminada con la CLI.

```
aws identitystore get-user-id \
  --identity-store d-9876543210 \
  --alternate-identifier '{
    "UniqueAttribute": {
      "AttributePath": "username",
      "AttributeValue": "anyuser@example.com"
    }
  }' \
  --region your-region-id
```

Del mismo modo, puede utilizar el mismo mecanismo si conoce el. `externalId` Actualiza la ruta del atributo del ejemplo anterior con el `externalId` valor y el valor del atributo con la información específica `externalId` que estás buscando.

Visualización del identificador seguro (SID) de un usuario en Microsoft Active Directory (AD) y ExternalID

En algunos casos, el IAM Identity Center emite el SID de un usuario en el `principalId` campo de los CloudTrail eventos, como los que emiten el portal de AWS acceso y el APIs OIDC. Estos casos se están eliminando gradualmente. Recomendamos que sus flujos de trabajo utilicen el atributo AD



objectguid cuando necesite un identificador de usuario único de AD. Puede encontrar este valor en el externalId atributo del directorio del Centro de identidad de IAM. Sin embargo, si sus flujos de trabajo requieren el uso de SID, recupere el valor de AD, ya que no está disponible en el Centro de identidades de IAM. APIs

[Correlacionar los usuarios entre el Centro de Identidad de IAM y los directorios externos](#) explica cómo utilizar los username campos externalId y para correlacionar un usuario del Centro de Identidad de IAM con un usuario coincidente en un directorio externo. De forma predeterminada, el Centro de identidad de IAM externalId se asigna al objectguid atributo de AD y esta asignación es fija. El centro de identidad de IAM ofrece a los administradores la flexibilidad de mapear de username forma diferente a la que se asigna por defecto userprincipalname en AD.

Puede ver estas asignaciones en la consola de IAM Identity Center. Vaya a la pestaña Fuente de identidad de la configuración y seleccione Administrar la sincronización en el menú Acciones. En la sección Administrar la sincronización, selecciona el botón Ver asignaciones de atributos.

Si bien puedes usar cualquier identificador de usuario único de AD disponible en el Centro de Identidad de IAM para buscar un usuario en AD, te recomendamos que lo utilices objectguid en tus consultas, ya que es un identificador inmutable. En el siguiente ejemplo se muestra cómo consultar Microsoft AD con Powershell para recuperar un usuario mediante el objectguid valor del usuario de16809ecc-7225-4c20-ad98-30094aefdbca. Una respuesta correcta a esta consulta incluye el SID del usuario.

```
Install-WindowsFeature -Name RSAT-AD-PowerShell

Get-ADUser `
  -Filter {objectGUID -eq [GUID]::Parse("16809ecc-7225-4c20-ad98-30094aefdbca")} `
  -Properties *
```

## La información del centro de identidad de IAM se encuentra en CloudTrail

CloudTrail está habilitada en su cuenta Cuenta de AWS al crear la cuenta. Cuando se produce una actividad en el Centro de Identidad de IAM, esa actividad se registra en un CloudTrail evento junto con otros eventos de AWS servicio en el historial de eventos. Puede ver, buscar y descargar los eventos recientes en su Cuenta de AWS. Para obtener más información, consulte [Visualización de eventos con el historial de CloudTrail eventos](#).

 Note

Para obtener más información sobre la evolución de la identificación de los usuarios y el seguimiento de las acciones de los usuarios en CloudTrail los eventos, consulte la sección [Cambios importantes en CloudTrail los eventos del IAM Identity Center](#) en el blog AWS de seguridad.

Para obtener un registro continuo de los eventos en su centro de identidad Cuenta de AWS, incluidos los eventos del IAM Identity Center, cree un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3. De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS . La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. Además, puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos. Para obtener más información, consulte los siguientes temas en la Guía del usuario de AWS CloudTrail :

- [Introducción a la creación de registros de seguimiento](#)
- [CloudTrail servicios e integraciones compatibles](#)
- [Configuración de las notificaciones de Amazon SNS para CloudTrail](#)
- [Recibir archivos de CloudTrail registro de varias regiones](#) y [recibir archivos de CloudTrail registro de varias cuentas](#)

Cuando el CloudTrail registro está activado en su cuenta Cuenta de AWS, las llamadas a la API realizadas a las acciones del Centro de Identidad de IAM se registran en los archivos de registro. Los registros del IAM Identity Center se escriben junto con otros registros de AWS servicio en un archivo de registro. CloudTrail determina cuándo crear y escribir en un nuevo archivo en función del período de tiempo y del tamaño del archivo.

CloudTrail eventos para el centro de identidad de IAM compatible APIs

En las siguientes secciones se proporciona información sobre los CloudTrail eventos asociados a lo siguiente APIs que admite el Centro de identidades de IAM:

- [API de IAM Identity Center](#)
- [API de Identity Store](#)

- [API OIDC](#)
- [AWS API del portal de acceso](#)

## CloudTrail eventos de las operaciones de la API de IAM Identity Center

La siguiente lista contiene los CloudTrail eventos que las operaciones públicas del IAM Identity Center emiten con la fuente de `sso.amazonaws.com` eventos. Para obtener más información sobre las operaciones de la API pública del IAM Identity Center, consulte la referencia de la API del [IAM Identity Center](#).

Puede encontrar eventos adicionales en las operaciones de la API CloudTrail de la consola de IAM Identity Center en las que se basa la consola. Para obtener más información sobre estas consolas APIs, consulte la [Referencia de autorización de servicios](#).

- [AttachCustomerManagedPolicyReferenceToPermissionSet](#)
- [AttachManagedPolicyToPermissionSet](#)
- [CreateAccountAssignment](#)
- [CreateApplication](#)
- [CreateApplicationAssignment](#)
- [CreateInstance](#)
- [CreateInstanceAccessControlAttributeConfiguration](#)
- [CreatePermissionSet](#)
- [CreateTrustedTokenIssuer](#)
- [DeleteAccountAssignment](#)
- [DeleteApplication](#)

- [DeleteApplicationAccessScope](#)
- [DeleteApplicationAssignment](#)
- [DeleteApplicationAuthenticationMethod](#)
- [DeleteApplicationGrant](#)
- [DeleteInlinePolicyFromPermissionSet](#)
- [DeleteInstance](#)
- [DeleteInstanceAccessControlAttributeConfiguration](#)
- [DeletePermissionsBoundaryFromPermissionSet](#)
- [DeletePermissionSet](#)
- [DeleteTrustedTokenIssuer](#)
- [DescribeAccountAssignmentCreationStatus](#)
- [DescribeAccountAssignmentDeletionStatus](#)
- [DescribeApplication](#)
- [DescribeApplicationAssignment](#)
- [DescribeApplicationProvider](#)
- [DescribeInstance](#)
-

[DescribeInstanceAccessControlAttributeConfiguration](#)

- [DescribePermissionSet](#)
- [DescribePermissionSetProvisioningStatus](#)
- [DescribeTrustedTokenIssuer](#)
- [DetachCustomerManagedPolicyReferenceFromPermissionSet](#)
- [DetachManagedPolicyFromPermissionSet](#)
- [GetApplicationAccessScope](#)
- [GetApplicationAssignmentConfiguration](#)
- [GetApplicationAuthenticationMethod](#)
- [GetApplicationGrant](#)
- [GetInlinePolicyForPermissionSet](#)
- [GetPermissionsBoundaryForPermissionSet](#)
- [ListAccountAssignmentCreationStatus](#)
- [ListAccountAssignmentDeletionStatus](#)
- [ListAccountAssignments](#)
-

[ListAccountAssignmentsForPrincipal](#)

•

[ListAccountsForProvisionedPermissionSet](#)

•

[ListApplicationAccessScopes](#)

•

[ListApplicationAssignments](#)

•

[ListApplicationAssignmentsForPrincipal](#)

•

[ListApplicationAuthenticationMethods](#)

•

[ListApplicationGrants](#)

•

[ListApplicationProviders](#)

•

[ListApplications](#)

•

[ListCustomerManagedPolicyReferencesInPermissionSet](#)

•

[ListInstances](#)

•

[ListManagedPoliciesInPermissionSet](#)

•

[ListPermissionSetProvisioningStatus](#)

•

[ListPermissionSets](#)

•

[ListPermissionSetsProvisionedToAccount](#)

•

[ListTagsForResource](#)

- [ListTrustedTokenIssuers](#)
- [ProvisionPermissionSet](#)
- [PutApplicationAccessScope](#)
- [PutApplicationAssignmentConfiguration](#)
- [PutApplicationAuthenticationMethod](#)
- [PutApplicationGrant](#)
- [PutInlinePolicyToPermissionSet](#)
- [PutPermissionsBoundaryToPermissionSet](#)
- [TagResource](#)
- [UntagResource](#)
- [UpdateApplication](#)
- [UpdateInstance](#)
- [UpdateInstanceAccessControlAttributeConfiguration](#)
- [UpdatePermissionSet](#)
- [UpdateTrustedTokenIssuer](#)

## CloudTrail eventos de las operaciones de la API de Identity Store

La siguiente lista contiene los CloudTrail eventos que las operaciones públicas del almacén de identidades emiten con la fuente de `identitystore.amazonaws.com` eventos. Para obtener más información sobre las operaciones de la API pública del almacén de identidades, consulte la [referencia de la API del almacén de identidades](#).

Es posible que veas eventos adicionales en las operaciones CloudTrail de la API de la consola de Identity Store con la fuente de `sso-directory.amazonaws.com` eventos. Son APIs compatibles con la consola y el portal de AWS acceso. Si necesitas detectar la aparición de una operación concreta, como añadir un miembro a un grupo, te recomendamos que consideres utilizar tanto las operaciones de API públicas como las de consola. Para obtener más información sobre estas consolas APIs, consulta la [Referencia de autorización de servicios](#).

- [CreateGroup](#)
- [CreateGroupMembership](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteGroupMembership](#)
- [DeleteUser](#)
- [DescribeGroup](#)
- [DescribeGroupMembership](#)
- [DescribeUser](#)
- [GetGroupId](#)
- [GetGroupMembershipId](#)
- [GetUserId](#)
- [IsMemberInGroups](#)
- [ListGroupMemberships](#)
- [ListGroupMembershipsForMember](#)
- [ListGroups](#)
- [ListUsers](#)
- [UpdateGroup](#)
- [UpdateUser](#)



## CloudTrail eventos de las operaciones de la API de OIDC

La siguiente lista contiene los CloudTrail eventos que emiten las operaciones públicas del OIDC. [Para obtener más información sobre las operaciones de la API pública del OIDC, consulte la Referencia de la API del OIDC.](#)

- [CreateToken](#)(fuente del evento) sso.amazonaws.com
- [CreateTokenWithIAM](#)(fuente del evento) sso-oauth.amazonaws.com)

## CloudTrail eventos de las operaciones de la API del portal de AWS acceso

La siguiente lista contiene los CloudTrail eventos que las operaciones de la API del portal de AWS acceso emiten con la fuente del sso.amazonaws.com evento. Las operaciones de API que se indican como no disponibles en la API pública respaldan las operaciones del portal de AWS acceso. El uso de la AWS CLI puede provocar la emisión de CloudTrail eventos tanto de las operaciones de la API del portal de AWS acceso público como de aquellos que no están disponibles en la API pública. Para obtener más información sobre las operaciones de la API del portal de AWS acceso público, consulta la [referencia de la API del portal de AWS acceso](#).

- [Authenticate](#)(No disponible en la API pública. Proporciona el inicio de sesión en el portal de AWS acceso.)
- [Federate](#)(No disponible en la API pública. Proporciona la federación en las aplicaciones.)
- [ListAccountRoles](#)
- [ListAccounts](#)
- [ListApplications](#)(No está disponible en la API pública. Proporciona los recursos asignados a los usuarios para mostrarlos en el portal de AWS acceso.)
- [ListProfilesForApplication](#)(No está disponible en la API pública. Proporciona metadatos de la aplicación para mostrarlos en el portal de AWS acceso.)
- [GetRoleCredentials](#)
- [Logout](#)

## Información de identidad en los eventos del IAM Identity Center CloudTrail

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario raíz o de usuario AWS Identity and Access Management (IAM).
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o fue un usuario federado.
- Si la solicitud la realizó otro AWS servicio.
- Si la solicitud la realizó un usuario del IAM Identity Center. Si es así, los `identityStoreArn` campos `userId` y están disponibles en los CloudTrail eventos para identificar al usuario del Centro de Identidad de IAM que inició la solicitud. Para obtener más información, consulte [Identificación del usuario y la sesión en los eventos iniciados por los usuarios del IAM Identity Center CloudTrail](#).

Para obtener más información, consulte el [elemento `userIdentity` de CloudTrail](#).

#### Note

Actualmente, el Centro de Identidad de IAM no emite CloudTrail eventos para las siguientes acciones:

- El usuario inicia sesión en aplicaciones web AWS gestionadas (por ejemplo, Amazon SageMaker AI Studio) con la API de [OIDC](#). Estas aplicaciones web son un subconjunto de un conjunto más amplio [the section called “AWS aplicaciones gestionadas”](#), que también incluye aplicaciones no web, como Amazon Athena SQL y Amazon S3 Access Grants.
- [Recuperación de los atributos de usuario y grupo mediante aplicaciones AWS administradas con la API Identity Store](#).

## Descripción de CloudTrail los eventos del IAM Identity Center

Un registro de seguimiento es una configuración que permite la entrega de eventos a un bucket de Amazon S3 que especifique. Un evento representa una solicitud única de cualquier fuente e incluye información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail los eventos no son un registro ordenado de las llamadas a la API pública, por lo que no aparecen en ningún orden específico. Obtén información sobre el [contenido de un CloudTrail registro](#) en la Guía del CloudTrail usuario.

El siguiente ejemplo muestra una entrada de CloudTrail registro para un administrador (`samadams@example.com`) que tuvo lugar en la consola del IAM Identity Center:

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAJAIENLMexample",
        "arn": "arn:aws:iam::08966example:user/samadams",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIIJM2K4example",
        "userName": "samadams"
      },
      "eventTime": "2017-11-29T22:39:43Z",
      "eventSource": "sso.amazonaws.com",
      "eventName": "DescribePermissionsPolicies",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "203.0.113.0",
      "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
      "requestParameters": {
        "permissionSetId": "ps-79a0dde74b95ed05"
      },
      "responseElements": null,
      "requestID": "319ac6a1-d556-11e7-a34f-69a333106015",
      "eventID": "a93a952b-13dd-4ae5-a156-d3ad6220b071",
      "readOnly": true,
      "resources": [

      ],
      "eventType": "AwsApiCall",
      "recipientAccountId": "111122223333"
    }
  ]
}
```

El siguiente ejemplo muestra una entrada de CloudTrail registro de una acción del usuario final (bobsmith@example.com) que tuvo lugar en el portal de AWS acceso:

```
{
  "Records": [
    {
      "eventVersion": "1.05",
      "userIdentity": {
```

```

        "type": "Unknown",
        "principalId": "example.com//
S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "111122223333",
        "userName": "bobsmith@example.com",
        "onBehalfOf": {
            "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
            "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        },
        "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
    },
    "eventTime": "2017-11-29T18:48:28Z",
    "eventSource": "sso.amazonaws.com",
    "eventName": "ListApplications",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "de6c0435-ce4b-49c7-9bcc-bc5ed631ce04",
    "eventID": "e6e1f3df-9528-4c6d-a877-6b2b895d1f91",
    "eventType": "AwsApiCall",
    "recipientAccountId": "111122223333"
}
]
}

```

El siguiente ejemplo muestra una entrada de CloudTrail registro para una acción de un usuario final (bobsmith@example.com) que tuvo lugar en el IAM Identity Center OIDC:

```

{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "Unknown",
        "principalId": "example.com//S-1-5-21-1122334455-3652759393-4233131409-1126",
        "accountId": "111122223333",
        "userName": "bobsmith@example.com",
        "onBehalfOf": {
            "userId": "94d00cd8-e9e6-4810-b177-b08e84775435",
            "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
        }
    }
}

```

```

    },
    "credentialId" : "cdee2490-82ed-43b3-96ee-b75fbf0b97a5"
  },
  "eventTime": "2020-06-16T01:31:15Z",
  "eventSource": "sso.amazonaws.com",
  "eventName": "CreateToken",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/62.0.3202.94 Safari/537.36",
  "requestParameters": {
    "clientId": "clientid1234example",
    "clientSecret": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "grantType": "urn:ietf:params:oauth:grant-type:device_code",
    "deviceCode": "devicecode1234example"
  },
  "responseElements": {
    "accessToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "tokenType": "Bearer",
    "expiresIn": 28800,
    "refreshToken": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "idToken": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "eventID": "09a6e1a9-50e5-45c0-9f08-e6ef5089b262",
  "readOnly": false,
  "resources": [
    {
      "accountId": "111122223333",
      "type": "IdentityStoreId",
      "ARN": "d-1234567890"
    }
  ],
  "eventType": "AwsApiCall",
  "recipientAccountId": "111122223333"
}

```

## Explicación de los eventos de inicio de sesión de IAM Identity Center

AWS CloudTrail registra los eventos de inicio de sesión correctos y fallidos para todas las fuentes de identidad del IAM Identity Center. Las identidades de origen de IAM Identity Center y Active Directory (AD Connector y AWS Managed Microsoft AD) incluyen eventos de inicio de sesión adicionales que se capturan cada vez que se le pide a un usuario que resuelva un desafío o factor de credenciales específico, además del estado de esa solicitud de verificación de credenciales en particular. Solo

después de que un usuario haya completado todos los desafíos de credenciales requeridos, el usuario iniciará sesión, lo que provocará que se registre un evento `UserAuthentication`.

En la siguiente tabla se muestran los nombres de los CloudTrail eventos de inicio de sesión del IAM Identity Center, su finalidad y su aplicabilidad a las distintas fuentes de identidad.

| Nombre de evento                    | Propósito del evento                                                                                                                                                                                                                                                                      | Aplicabilidad de la fuente de identidad                                           |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <code>CredentialChallenge</code>    | Se utiliza para notificar que IAM Identity Center ha solicitado al usuario que resuelva un desafío de credenciales específico y puntualiza el <code>CredentialType</code> que se requiere (por ejemplo, <code>PASSWORD</code> o <code>TOTP</code> ).                                      | Usuarios nativos del IAM Identity Center, AD Connector y AWS Managed Microsoft AD |
| <code>CredentialVerification</code> | Se utiliza para notificar que el usuario ha intentado resolver una solicitud de <code>CredentialChallenge</code> específica y precisa si la credencial se ha realizado correctamente o no.                                                                                                | Usuarios nativos del IAM Identity Center, AD Connector y AWS Managed Microsoft AD |
| <code>UserAuthentication</code>     | Se utiliza para notificar que todos los requisitos de autenticación con los que se desafió al usuario se han completado con éxito y que el usuario ha iniciado sesión correctamente. Si los usuarios no completan correctamente los desafíos de credenciales requeridos, no se registrará | Todas las fuentes de identidad                                                    |

| Nombre de evento | Propósito del evento                         | Aplicabilidad de la fuente de identidad |
|------------------|----------------------------------------------|-----------------------------------------|
|                  | ningún evento de <i>UserAuthentication</i> . |                                         |

En la siguiente tabla, se muestran otros campos de datos de eventos útiles incluidos en eventos de inicio de sesión CloudTrail específicos.

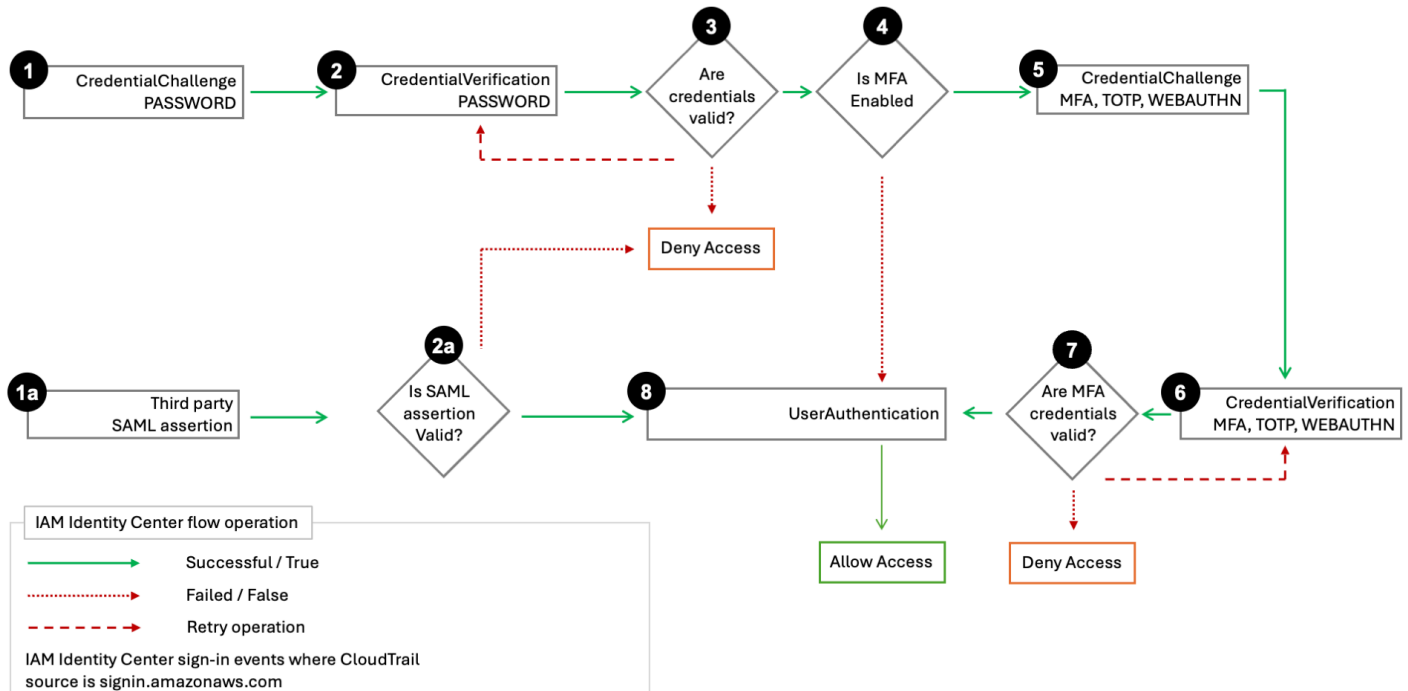
| Campo          | Propósito del evento                                                                                                                                                                                                | Aplicabilidad al evento de inicio de sesión                     | Valores de ejemplo                                                                                                                                               |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AuthWorkflowID | Se utiliza para correlacionar todos los eventos emitidos en una secuencia de inicio de sesión completa. Por cada inicio de sesión de usuario, IAM Identity Center puede emitir varios eventos.                      | CredentialChallenge, CredentialVerification, UserAuthentication | «AuthWorkflowID»: «9de74b32-8362-4a01-a524-de21df59fd83»                                                                                                         |
| CredentialType | Se utiliza para especificar la credencial o el factor que se ha cuestionado. Los eventos de UserAuthentication incluirán todos los valores de CredentialType que se hayan verificado correctamente a lo largo de la | CredentialChallenge, CredentialVerification, UserAuthentication | CredentialType«: «PASSWORD» o «: «PASSWORD, TOTP» (los valores posibles incluyen: PASSWORD, TOTP, WEBAUTHN, CredentialType EXTERNAL_IDP, RESYNC_TOTP, EMAIL_OTP) |

| Campo                    | Propósito del evento                                                                                                                                                   | Aplicabilidad al evento de inicio de sesión | Valores de ejemplo                                       |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------|----------------------------------------------------------|
|                          | secuencia de inicio de sesión del usuario.                                                                                                                             |                                             |                                                          |
| DeviceEnrollmentRequired | Se utiliza para especificar que el usuario debe registrar un dispositivo de MFA durante el inicio de sesión y que el usuario ha completado correctamente la solicitud. | UserAuthentication                          | "«: «verdadero» DeviceEnrollmentRequired                 |
| LoginTo                  | Se utiliza para especificar la ubicación de redireccionamiento tras una secuencia de inicio de sesión correcta.                                                        | UserAuthentication                          | "LoginTo": "https://mydirectory.awsapps.com/start/....." |

## CloudTrail eventos en los flujos de inicio de sesión del IAM Identity Center

El siguiente diagrama describe el flujo de inicio de sesión y los CloudTrail eventos que emite





El diagrama muestra un flujo de inicio de sesión con contraseña y un flujo de inicio de sesión federado.

El flujo de inicio de sesión con contraseña, que consta de los pasos 1 a 8, muestra los pasos durante el proceso de inicio de sesión con nombre de usuario y contraseña. El Centro de Identidad de IAM se establece `userIdentity.additionalEventData.CredentialType` en `PASSWORD` «y el Centro de Identidad de IAM sigue el ciclo de cuestionamiento-respuesta a las credenciales y lo vuelve a intentar si es necesario.

El número de pasos depende del tipo de [inicio de sesión y de la presencia de la autenticación multifactor \(MFA\)](#). El proceso inicial da como resultado tres o cinco CloudTrail eventos y `UserAuthentication` finaliza la secuencia para que la autenticación se realice correctamente. Los intentos fallidos de autenticación con contraseña provocan CloudTrail eventos adicionales, ya que el Centro de Identidad de IAM vuelve a emitir la autenticación `CredentialChallenge` normal o, si está habilitada, la autenticación MFA.

El flujo de inicio de sesión con contraseña también cubre el escenario en el que un usuario del Centro de Identidad de IAM recién creado con una llamada a la `CreateUser` API inicia sesión con una contraseña de un solo uso (OTP). El tipo de credencial en este escenario es «». `EMAIL_OTP`

El flujo de inicio de sesión federado, que consta de los pasos 1a, 2a y 8, muestra los pasos principales del proceso de autenticación federada, en los que un [proveedor de identidad proporciona una afirmación de SAML, la valida por el Centro de Identidad de IAM y, si es](#) correcta, se obtiene como resultado. `UserAuthentication` El Centro de identidades de IAM no invoca la secuencia de autenticación MFA interna en los pasos 3 a 7 porque un proveedor de identidad federado externo es responsable de toda la autenticación de credenciales de usuario.

El `CloudTrail` nombre de usuario en los eventos de inicio de sesión

El Centro de Identidad de IAM emite el `UserName` campo situado debajo del `additionalEventData` elemento una vez por cada inicio de sesión correcto de un usuario del Centro de Identidad de IAM. En la siguiente lista se describen los dos eventos de inicio de sesión incluidos y las condiciones en las que pueden producirse. Solo una de las condiciones puede cumplirse cuando un usuario inicia sesión.

- `CredentialChallenge`
  - Cuando `CredentialType` es «PASSWORD»: se aplica a la autenticación por contraseña con AWS Directory Service o Directorio de IAM Identity Center.
  - Cuando `CredentialType` es «EMAIL\_OTP»: solo se aplica Directorio de IAM Identity Center cuando un usuario creado con una llamada a la `CreateUser` API intenta iniciar sesión por primera vez y recibe una contraseña de un solo uso para iniciar sesión con esa contraseña una vez.
- `UserAuthentication`
  - Cuando `CredentialType` es «EXTERNAL\_IDP»: se aplica a la autenticación con un IdP externo.

El valor de `UserName` es el siguiente para que las autenticaciones se realicen correctamente:

- Cuando la fuente de identidad es un IdP externo, el valor es igual al `nameID` valor de la afirmación SAML entrante. Este valor es igual al `UserName` campo de. Directorio de IAM Identity Center
- Cuando la fuente de identidad es un Directorio de IAM Identity Center, el valor emitido es igual al `UserName` campo de este directorio.
- Cuando la fuente de identidad es la AWS Directory Service, el valor emitido es igual al nombre de usuario que el usuario introduce durante la autenticación. Por ejemplo, un usuario que tiene el nombre de usuario `anyuser@company.com` puede autenticarse con

anyuseranyuser@company.com, o ycompany.com/anyuser, en cada caso, el valor introducido se emite CloudTrail respectivamente.

#### Note

Le recomendamos que utilice `userId` y `identityStoreArn` para identificar al usuario responsable de los eventos del IAM Identity Center CloudTrail. Si necesita usar el `userName` campo, le recomendamos que use el que está `userName` debajo del `additionalEventData` elemento y evite usar el `userName` campo debajo del `userIdentity` elemento.

Para obtener información adicional sobre cómo utilizar el `UserName` campo, consulte [Correlacionar los usuarios entre el Centro de Identidad de IAM y los directorios externos](#).

Ejemplos de eventos para escenarios de inicio de sesión en IAM Identity Center

Los siguientes ejemplos muestran la secuencia de CloudTrail eventos esperada para diferentes escenarios de inicio de sesión.

#### Temas

- [Inicio de sesión exitoso al autenticarse solo con contraseña](#)
- [Inicio de sesión correcto al autenticarse con un proveedor de identidad externo](#)
- [Inicio de sesión correcto al autenticarse con una contraseña y una aplicación de autenticación TOTP](#)
- [Inicio de sesión exitoso al autenticarse con una contraseña y se requiere un registro MFA forzado](#)
- [Inicio de sesión fallido al autenticarse solo con una contraseña](#)

#### Inicio de sesión exitoso al autenticarse solo con contraseña

La siguiente secuencia de eventos muestra un ejemplo de un inicio de sesión exitoso solo con contraseña.

#### CredentialChallenge (Contraseña)

```
{  
  "eventVersion": "1.08",
```

```

"userIdentity":{
  "type":"Unknown",
  "principalId":"111122223333",
  "arn":"",
  "accountId":"111122223333",
  "accessKeyId":"",
  "userName":"bobsmith@example.com",
  "onBehalfOf": {
    "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"eventTime":"2020-12-07T20:33:58Z",
"eventSource":"signin.amazonaws.com",
"eventName":"CredentialChallenge",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
  "UserName":"bobsmith@example.com",
  "CredentialType":"PASSWORD"
},
"requestID":"5be44fffb-6946-4f47-acaf-1adebd4afead",
"eventID":"27ea7725-c1fd-4355-bdba-d0e628e0e604",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"serviceEventDetails":{
  "CredentialChallenge":"Success"
}
}

```

## Exitoso CredentialVerification (contraseña)

```

{
  "eventVersion":"1.08",

```

```

"userIdentity":{
  "type":"Unknown",
  "principalId":"111122223333",
  "arn":"",
  "accountId":"111122223333",
  "accessKeyId":"",
  "userName":"bobsmith@example.com",
  "onBehalfOf": {
    "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"eventTime":"2020-12-07T20:34:09Z",
"eventSource":"signin.amazonaws.com",
"eventName":"CredentialVerification",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
  "CredentialType":"PASSWORD"
},
"requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
"eventID":"c49640f6-0c8a-43d3-a6e0-900e3bb188d4",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialVerification":"Success"
}
}

```

### UserAuthentication Correcto (solo contraseña)

```

{
  "eventVersion":"1.08",

```

```

"userIdentity":{
  "type":"Unknown",
  "principalId":"111122223333",
  "arn":"",
  "accountId":"111122223333",
  "accessKeyId":"",
  "userName":"bobsmith@example.com",
  "onBehalfOf": {
    "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"eventTime":"2020-12-07T20:34:09Z",
"eventSource":"signin.amazonaws.com",
"eventName":"UserAuthentication",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"9de74b32-8362-4a01-a524-de21df59fd83",
  "LoginTo":"https://d-1234567890.awsapps.com/start/?
state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
BshlIc50BAA6ftz73M6LsflWDlF0xvi02K3wet946lC30f_iWdilx-
zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvP7Tqzi0LiBLBUSx
east-1",
  "CredentialType":"PASSWORD"
},
"requestID":"f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
"eventID":"e959a95a-2b33-478d-906c-4fe303e8a9f1",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "UserAuthentication":"Success"
}
}

```

## Inicio de sesión correcto al autenticarse con un proveedor de identidad externo

La siguiente secuencia de eventos muestra un ejemplo de un inicio de sesión correcto cuando se autentica mediante el protocolo SAML con un proveedor de identidad externo.

### UserAuthentication Correcto (proveedor de identidad externo)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "111122223333",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-07T20:34:09Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "UserAuthentication",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "9de74b32-8362-4a01-a524-de21df59fd83",
    "LoginTo": "https://d-1234567890.awsapps.com/start/?state=QVlBQmVGMHFiS0wzWlp1SFgrR25BRnFobU5nQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYSBshIic50BAA6ftz73M6LsfLWD1f0xvi02K3wet9461C30f_iWdilx-zv__4pSHf7mcUIs&wdc_csrf_token=srAzW1jK4GPYYoR452ruZ38DxEsDY9x81q1tVRSnno5pUjISvp7Tqzi0LiBLBUSx-east-1",
    "CredentialType": "EXTERNAL_IDP",
    "UserName": "bobsmith@example.com"
  },
  "requestID": "f3cf52ad-fd3d-4889-8c15-f18d1a7c7393",
  "eventID": "e959a95a-2b33-478d-906c-4fe303e8a9f1",
  "readOnly": false,
}
```

```

    "eventType": "AwsServiceEvent",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "111122223333",
    "serviceEventDetails": {
      "UserAuthentication": "Success"
    }
  }
}

```

Inicio de sesión correcto al autenticarse con una contraseña y una aplicación de autenticación TOTP

La siguiente secuencia de eventos captura un ejemplo en el que se requería una autenticación multifactorial durante el inicio de sesión y el usuario inició sesión correctamente con una contraseña y una aplicación de autenticación TOTP.

### CredentialChallenge (Contraseña)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "111122223333",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "userName": "bobsmith@example.com",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-08T20:40:13Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {

```



```

    "AuthWorkflowID": "303486b5-fce1-4d59-ba1d-eb3acb790729",
    "CredentialType": "PASSWORD",
    "UserName": "bobsmith@example.com"
  },
  "requestID": "e454ea66-1027-4d00-9912-09c0589649e1",
  "eventID": "d89cc0b5-a23a-4b88-843a-89329aeaef2e",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}

```

## Exitoso CredentialVerification (contraseña)

```

{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "111122223333",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "userName": "bobsmith@example.com",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId": "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime": "2020-12-08T20:40:20Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
}

```

```

    "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"PASSWORD"
    },
    "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
    "eventID":"4533fd49-6669-4d0b-b272-a0b2139309a8",
    "readOnly":false,
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"111122223333",
    "serviceEventDetails":{
      "CredentialVerification":"Success"
    }
  }
}

```

## CredentialChallenge (TOTP)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "principalId":"111122223333",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "userName":"bobsmith@example.com",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-08T20:40:20Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialChallenge",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,

```

```

    "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
    },
    "requestID":"92c4ac90-0d9b-452d-95d5-728487612f5e",
    "eventID":"29202f08-f240-40cc-b789-c0cea8a27847",
    "readOnly":false,
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"111122223333",
    "serviceEventDetails":{
      "CredentialChallenge":"Success"
    }
  }
}

```

## Exitoso CredentialVerification (TOTP)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "principalId":"111122223333",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "userName":"bobsmith@example.com",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-08T20:40:27Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"CredentialVerification",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,

```

```

    "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "CredentialType":"TOTP"
    },
    "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
    "eventID":"e889ff1d-fcaf-454f-805d-7132cf2362a4",
    "readOnly":false,
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"111122223333",
    "serviceEventDetails":{
      "CredentialVerification":"Success"
    }
  }
}

```

## Exitoso UserAuthentication (contraseña + TOTP)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "principalId":"111122223333",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "userName":"bobsmith@example.com",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
      "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
  },
  "eventTime":"2020-12-08T20:40:27Z",
  "eventSource":"signin.amazonaws.com",
  "eventName":"UserAuthentication",
  "awsRegion":"us-east-1",
  "sourceIPAddress":"203.0.113.0",
  "userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters":null,
  "responseElements":null,

```

```

    "additionalEventData":{
      "AuthWorkflowID":"303486b5-fce1-4d59-ba1d-eb3acb790729",
      "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVLeFhWeDRmZFJmMmxHcWYwdzhZck5RQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11Fir1mCVJ-4Y5UY6RI10UCXvRePCHd6195xvYg1rwo1Pj7B-7UGIGlYUUVe31Nkzd7ihxKn6DMdnFf00108qc3RF
Sx-pjBXKG_jUcvBk_UILdGytV4o1u97h42B-
TA_6uwdmJiw1dcCz_Rv44d_BS0PkulW-5LVJy1oeP1H0FPPMeheyuk5Uy48d5of9-c\u0026wdc_csrf_token
\u003dNMLui44guoVnxRd0qu2tYJIdyyFPX6SDRNTspIScfMM0AgFbho1nvvCaxPTghHbgHCRIXdfffFtzH0sL1ow419Bobn
\u0026organization\u003dd-9067230c03\u0026region\u003dus-east-1",
      "CredentialType":"PASSWORD,TOTP"
    },
    "requestID":"c40a691f-eeb1-4352-b286-5e909f96f318",
    "eventID":"7a8c8725-db2f-488d-a43e-788dc6c73a4a",
    "readOnly":false,
    "eventType":"AwsServiceEvent",
    "managementEvent":true,
    "eventCategory":"Management",
    "recipientAccountId":"111122223333",
    "serviceEventDetails":{
      "UserAuthentication":"Success"
    }
  }
}

```

Inicio de sesión exitoso al autenticarse con una contraseña y se requiere un registro MFA forzado

La siguiente secuencia de eventos captura un ejemplo de un inicio de sesión con contraseña correcto, pero el usuario tenía que registrar correctamente un dispositivo MFA antes de completar su inicio de sesión.

### CredentialChallenge (Contraseña)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "principalId":"111122223333",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "userName":"bobsmith@example.com",
    "onBehalfOf": {
      "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",

```

```

    "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
  },
  "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"eventTime":"2020-12-09T01:24:02Z",
"eventSource":"signin.amazonaws.com",
"eventName":"CredentialChallenge",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
  "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
  "CredentialType":"PASSWORD",
  "UserName":"bobsmith@example.com"
},
"requestID":"321f4b13-42b5-4005-a0f7-826cad26d159",
"eventID":"8c707b0f-e45a-4a9c-bee2-ff68638d2f1b",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
  "CredentialChallenge":"Success"
}
}

```

## Exitoso CredentialVerification (contraseña)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "principalId":"111122223333",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "userName":"bobsmith@example.com",
    "onBehalfOf": {

```

```

        "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
        "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"eventTime":"2020-12-09T01:24:09Z",
"eventSource":"signin.amazonaws.com",
"eventName":"CredentialVerification",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
    "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
    "CredentialType":"PASSWORD"
},
"requestID":"12b57efa-0a92-4479-91a3-5b6641817c21",
"eventID":"783b0c89-7142-4942-8b84-6ee0de1b992e",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
    "CredentialVerification":"Success"
}
}

```

Exitoso UserAuthentication (se requiere contraseña y registro en MFA)

```

{
  "eventVersion":"1.08",
  "userIdentity":{
    "type":"Unknown",
    "principalId":"111122223333",
    "arn":"",
    "accountId":"111122223333",
    "accessKeyId":"",
    "userName":"bobsmith@example.com",
    "onBehalfOf": {

```

```

        "userId": "94d00cd8-e9e6-4810-b177-b08e84725435",
        "identityStoreArn": "arn:aws:identitystore::111122223333:identitystore/
d-1234567890"
    },
    "credentialId" : "8f761cae-883d-4a3d-af67-3abf46488f71"
},
"eventTime":"2020-12-09T01:24:14Z",
"eventSource":"signin.amazonaws.com",
"eventName":"UserAuthentication",
"awsRegion":"us-east-1",
"sourceIPAddress":"203.0.113.0",
"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
"requestParameters":null,
"responseElements":null,
"additionalEventData":{
    "AuthWorkflowID":"76d8a26d-ad9c-41a4-90c3-d607cdd7155c",
    "LoginTo":"https://d-1234567890.awsapps.com/start/?state
\u003dQVlBQmVGQ3VqdHF5aW9CUDdrNXRTVTJUaWNnQUlnQUJBQk5FWVhSaFVHeGhibVZUZEdGMFpWQmhjbUZ0QUFsUVpYS
\u0026auth_code
\u003d11eZ80S_maUsZ7ABETjeQhyWfvIHYz52rgR28sYAKN1oEk2G07czrwzXvE9HL1N2K9De8LyBEV83SFeDQfrWpkwXf
FJyJqkoGrt_w6rm_MpAn0uyrVq8udY_EgU3fh0L3QWvWiquYnDPMYPmmy_qkZgR9rz__BI
\u0026wdc_csrf_token
\u003dJih9U62o5LQDtYLNqCK8a6xj0gJg5BRWq2tbl75y8vAmwZhAqrgrgbxXat2M646UZGp93krw7WYQdHIgi50YI9QSc
\u003dd-9067230c03\u0026region\u003dus-east-1",
    "CredentialType":"PASSWORD",
    "DeviceEnrollmentRequired":"true"
},
"requestID":"74d24604-a365-4237-8c4a-350795494b92",
"eventID":"a15bf257-7f37-46c0-b67c-fea5fa6166be",
"readOnly":false,
"eventType":"AwsServiceEvent",
"managementEvent":true,
"eventCategory":"Management",
"recipientAccountId":"111122223333",
"serviceEventDetails":{
    "UserAuthentication":"Success"
}
}

```



## Inicio de sesión fallido al autenticarse solo con una contraseña

La siguiente secuencia de eventos captura un ejemplo de un inicio de sesión fallido con solo contraseña.

### CredentialChallenge (Contraseña)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "111122223333",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "userName": "bobsmith@example.com",
  },
  "eventTime": "2020-12-08T18:56:15Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialChallenge",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "adbf67c4-8188-4e2b-8527-fe539e328fa7",
    "CredentialType": "PASSWORD",
    "UserName": "bobsmith@example.com"
  },
  "requestID": "f54848ea-b1aa-402f-bf0d-a54561a2ffcc",
  "eventID": "d96f1d6c-dbd9-4a0b-9a45-6a2b66078c78",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "CredentialChallenge": "Success"
  }
}
```

## Error CredentialVerification (contraseña)

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "Unknown",
    "principalId": "111122223333",
    "arn": "",
    "accountId": "111122223333",
    "accessKeyId": "",
    "userName": "bobsmith@example.com",
  },
  "eventTime": "2020-12-08T18:56:21Z",
  "eventSource": "signin.amazonaws.com",
  "eventName": "CredentialVerification",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "203.0.113.0",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.66 Safari/537.36",
  "requestParameters": null,
  "responseElements": null,
  "additionalEventData": {
    "AuthWorkflowID": "adbf67c4-8188-4e2b-8527-fe539e328fa7",
    "CredentialType": "PASSWORD"
  },
  "requestID": "04528c82-a678-4a1f-a56d-ea2c6445a72a",
  "eventID": "9160fe06-fc2a-474f-9b78-000ee067a09d",
  "readOnly": false,
  "eventType": "AwsServiceEvent",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333",
  "serviceEventDetails": {
    "CredentialVerification": "Failure"
  }
}
```

## Registro de llamadas a la API del IAM Identity Center SCIM con AWS CloudTrail

[IAM Identity Center SCIM](#) está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, rol o un. Servicio de AWS CloudTrail captura las llamadas

a la API del SCIM como eventos. Con la información recopilada por CloudTrail, puede determinar la información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. Para obtener más información CloudTrail, consulte la [Guía AWS CloudTrail del usuario](#).

 Note

CloudTrail está activado en tu cuenta Cuenta de AWS al crear la cuenta. Sin embargo, es posible que tengas que rotar tu token de acceso para poder ver los eventos de SCIM si tu token se creó antes de septiembre de 2024.

Para obtener más información, consulte [Rotar un token de acceso](#).

SCIM admite el registro de las siguientes operaciones como eventos en: CloudTrail

- [CreateGroup](#)
- [CreateUser](#)
- [DeleteGroup](#)
- [DeleteUser](#)
- [GetGroup](#)
- [GetSchema](#)
- [GetUser](#)
- [ListGroups](#)
- [ListResourceTypes](#)
- [ListSchemas](#)
- [ListUsers](#)
- [PatchGroup](#)
- [PatchUser](#)
- [PutUser](#)
- [ServiceProviderConfig](#)

## Ejemplos

Los siguientes son algunos ejemplos de CloudTrail eventos.

## Ejemplo 1: Evento de una llamada de CreateUser exitosa.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "WebIdentityUser",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "CreateUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "requestParameters": {
    "httpBody": {
      "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "schemas" : [
        "urn:ietf:params:scim:schemas:core:2.0:User"
      ],
      "name": {
        "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
        "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
      },
      "active": true,
      "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
    "tenantId": "xxxx"
  },
  "responseElements": {
    "meta" : {
      "created" : "Oct 10, 2024, 1:23:45 PM",
      "lastModified" : "Oct 10, 2024, 1:23:45 PM",
      "resourceType" : "User"
    },
    "displayName" : "HIDDEN_DUE_TO_SECURITY_REASONS",
    "schemas" : [
      "urn:ietf:params:scim:schemas:core:2.0:User"
    ],
    "name": {
      "familyName": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "givenName": "HIDDEN_DUE_TO_SECURITY_REASONS"
    },
  },
}
```

```

    "active": true,
    "id" : "c4488478-a0e1-700e-3d75-96c6bb641596",
    "userName": "HIDDEN_DUE_TO_SECURITY_REASONS"
  },
  "requestID": "xxxx",
  "eventID": "xxxx",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "123456789012",
  "eventCategory": "Management",
  "tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
  }
}

```

Ejemplo 2: El evento de PatchGroup generó un mensaje de error de Missing path in PATCH request debido a la falta de una ruta.

```

{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchGroup",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "Missing path in PATCH request",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REMOVE",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ],
    },
    "schemas": [

```

```

        "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
},
"tenantId": "xxxx",
"id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
    "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

Ejemplo 3: El evento de una CreateGroup llamada genera un mensaje de Duplicate GroupDisplayName error, ya que existe el nombre del grupo que se está intentando crear.

```

{
    "eventVersion": "1.10",
    "userIdentity": {
        "type": "Unknown",
        "accountId": "123456789012",
        "accessKeyId": "xxxx"
    },
    "eventTime": "xxxx",
    "eventSource": "identitystore-scim.amazonaws.com",
    "eventName": "CreateGroup",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "xxx.xxx.xxx.xxx",
    "userAgent": "Go-http-client/2.0",
    "errorCode": "ConflictException",
    "errorMessage": "Duplicate GroupDisplayName",
    "requestParameters": {
        "httpBody": {
            "displayName": "HIDDEN_DUE_TO_SECURITY_REASONS"
        },
        "tenantId": "xxxx"
    },
}

```

```
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}
```

Ejemplo 4: El evento de una llamada de PatchUser que genera un mensaje de error de List attribute emails exceeds allowed limit of 1 error. Los usuarios solo pueden tener una dirección de correo electrónico.

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Unknown",
    "accountId": "123456789012",
    "accessKeyId": "xxxx"
  },
  "eventTime": "xxxx",
  "eventSource": "identitystore-scim.amazonaws.com",
  "eventName": "PatchUser",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "xxx.xxx.xxx.xxx",
  "userAgent": "Go-http-client/2.0",
  "errorCode": "ValidationException",
  "errorMessage": "List attribute emails exceeds allowed limit of 1",
  "requestParameters": {
    "httpBody": {
      "operations": [
        {
          "op": "REPLACE",
          "path": "emails",
          "value": "HIDDEN_DUE_TO_SECURITY_REASONS"
        }
      ]
    },
    "schemas": [
      "HIDDEN_DUE_TO_SECURITY_REASONS"
    ]
  }
}
```

```

    ]
  },
  "tenantId": "xxxx",
  "id": "xxxx"
},
"responseElements": null,
"requestID": "xxxx",
"eventID": "xxxx",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "123456789012",
"eventCategory": "Management",
"tlsDetails": {
  "clientProvidedHostHeader": "scim.us-east-1.amazonaws.com"
}
}

```

## Mensajes de error comunes

Los siguientes son los mensajes de error de validación más comunes que puede recibir en CloudTrail los eventos de las llamadas a la API SCIM de IAM Identity Center:

- El correo electrónico con el atributo de la lista supera el límite permitido de 1
- El límite permitido de direcciones de atributos de lista es de 1
- Se detectó un error de validación: el valor de `*name.familyName*` no cumplía la restricción: el miembro debe cumplir el patrón de expresión regular: `[\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r ]+`
- Se detectaron dos errores de validación: el valor de `'name.familyName'` no pudo cumplir la restricción: el miembro debe tener una longitud mayor o igual a 1; el valor de `'name.familyName'` no pudo cumplir la restricción: el miembro debe cumplir el patrón de expresión regular: `[\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r ]+`
- Se detectaron dos errores de validación: el valor de `'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value'` no cumplía la restricción: el miembro debe tener una longitud mayor o igual a 1; el valor en `'urn:ietf:params:scim:schemas:extension:enterprise:2.0:User.manager.value'` no pudo cumplir la restricción: el miembro debe cumplir con la expresión regular patrón: `[\\p{L}\\p{M}\\p{S}\\p{N}\\p{P}\\t\\n\\r ]+`
- JSON no válido de RequestBody
- Formato de filtro no válido



[Para obtener más información sobre cómo solucionar los errores de aprovisionamiento del IAM Identity Center SCIM, consulte este artículo de AWS re:Post.](#)

## Connect los componentes de la aplicación con Amazon EventBridge

Puede integrar IAM Identity Center con [Amazon EventBridge](#) para generar eventos que inicien notificaciones administrativas o invocar flujos de trabajo automatizados en respuesta a acciones específicas del IAM Identity Center registradas en eventos. CloudTrail

Por ejemplo, puede configurar [EventBridge reglas](#) para detectar cuándo un usuario elimina una aplicación o cuándo el Centro de Identidad de IAM crea un grupo nuevo. [Según su caso de uso, puede dirigir estos eventos a un tema de Amazon SNS para notificarlos a los administradores o invocar una automatización adicional mediante Step AWS Lambda Functions u otros EventBridge servicios compatibles.](#)

## Registrar errores de sincronización de AD configurables

Puede activar el registro en sus configuraciones de sincronización configurables de Active Directory (AD) para recibir registros con información sobre los errores que pueden producirse durante el proceso de sincronización. Con estos registros, puede supervisar si hay algún problema con la sincronización de AD configurable y tomar las medidas necesarias. Puede enviar sus registros a un grupo de registros de Amazon CloudWatch Logs, a un depósito de Amazon Simple Storage Service (Amazon S3) o a un Amazon Data Firehose, y se admite la entrega entre cuentas para los depósitos de Amazon S3 y Firehose.

[Para obtener más información sobre las limitaciones, los permisos y los registros vendidos, consulte Habilitar el registro desde. Servicios de AWS](#)

### Note

Se le cobrará el registro. Para obtener más información, consulta [Vended Logs](#) en la página de [CloudWatch precios de Amazon](#).

Para habilitar los registros de errores de sincronización configurables de AD

1. Inicie sesión en la [consola del IAM Identity Center](#).
2. Elija Configuración.

3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar registros.
4. Seleccione Agregar entrega de registros y uno de los siguientes tipos de destino.
  - a. Elige Amazon CloudWatch Logs. A continuación, seleccione o introduzca el grupo de registro de destino.
  - b. Seleccione A Amazon S3. A continuación, elija o introduzca el bucket de destino.
  - c. Seleccione A Firehose. A continuación, seleccione o introduzca el flujo de entrega de destino.
5. Elija Enviar.

## Para deshabilitar los registros de errores de sincronización configurables de AD

1. Inicie sesión en la [consola del IAM Identity Center](#).
2. Elija Configuración.
3. En la página de Configuraciones, elija la pestaña Origen de identidad, elija Acciones y, a continuación, elija Administrar registros.
4. Seleccione Eliminar para el destino que desea eliminar.
5. Elija Enviar.

## Campos de registro de errores de sincronización de AD configurables

Consulte la siguiente lista para ver los posibles campos del registro de errores.

`sync_profile_name`

El nombre del perfil de sincronización.

`error_code`

El código de error que representa el tipo de error que se ha producido.

`error_message`

Un mensaje que contiene información detallada sobre el error que se ha producido.

## sync\_source

La fuente de sincronización es el lugar desde el que se sincronizan las entidades. En el caso del IAM Identity Center, se trata de un Active Directory (AD) gestionado por AWS Directory Service. La fuente de sincronización contiene el dominio y el ARN del directorio afectado.

## sync\_target

El destino de sincronización es el destino en el que se guardan las entidades. En el caso del IAM Identity Center, se trata de un almacén de identidades. El destino de sincronización contiene el ARN del almacén de identidades afectado.

## source\_entity\_id

Un identificador único para la entidad que está causando el error. En el caso del IAM Identity Center, este es el SID de la entidad.

## source\_entity\_type

El tipo de entidad que está causando el error. El valor puede ser USER o GROUP.

## eventTimestamp

La fecha y hora en que se produjo el error.

## Ejemplos de registros de errores de sincronización de AD configurables

### Ejemplo 1: Un registro de errores de una contraseña caducada de un directorio de AD

```
{
  "sync_profile_name": "EXAMPLE-PROFILE-NAME",
  "error" : {
    "error_code": "InvalidDirectoryCredentials",
    "error_message": "The password for your AD directory has expired. Please reset the password to allow Identity Sync to access the directory."
  },
  "sync_source": {
    "arn": "arn:aws:ds:us-east-1:123456789:directory/d-123456",
    "domain": "EXAMPLE.com"
  },
  "eventTimestamp": "1683355579981"
}
```

### Ejemplo 2: Un registro de errores para un usuario con un nombre de usuario que no es único

```
{
  "sync_profile_name": "EXAMPLE-PROFILE-NAME",
  "error" : {
    "error_code": "ConflictError",
    "error_message": "The source entity has a username conflict with the sync
target. Please verify that the source identity has a unique username in the target."
  },
  "sync_source": {
    "arn": "arn:aws:ds:us-east-1:111122223333:directory/d-123456",
    "domain": "EXAMPLE.com"
  },
  "sync_target": {
    "arn": "arn:aws:identitystore::111122223333:identitystore/d-123456"
  },
  "source_entity_id": "SID-1234",
  "source_entity_type": "USER",
  "eventTimestamp": "1683355579981"
}
```

## Validación de la conformidad en IAM Identity Center

Los auditores externos evalúan la seguridad y el cumplimiento de Servicios de AWS dichos programas, por ejemplo AWS IAM Identity Center , como parte de varios programas de AWS cumplimiento.

Para saber si un programa de cumplimiento Servicio de AWS está dentro del ámbito de aplicación de programas de cumplimiento específicos, consulte [Servicios de AWS Alcance por programa](#) de de cumplimiento y elija el programa de cumplimiento que le interese. Para obtener información general, consulte Programas de [AWS cumplimiento > Programas AWS](#) .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte [Descarga de informes en AWS Artifact](#) .

Su responsabilidad de cumplimiento al Servicios de AWS utilizarlos viene determinada por la confidencialidad de sus datos, los objetivos de cumplimiento de su empresa y las leyes y reglamentos aplicables. AWS proporciona los siguientes recursos para ayudar con el cumplimiento:

- [Cumplimiento de seguridad y gobernanza](#): en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.

- [Referencia de servicios válidos de HIPAA](#): muestra una lista con los servicios válidos de HIPAA. No todos Servicios de AWS cumplen con los requisitos de la HIPAA.
- [AWS Recursos de](#) de cumplimiento: esta colección de libros de trabajo y guías puede aplicarse a su industria y ubicación.
- [AWS Guías de cumplimiento para clientes](#): comprenda el modelo de responsabilidad compartida desde la perspectiva del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST), el Consejo de Normas de Seguridad del Sector de Tarjetas de Pago (PCI) y la Organización Internacional de Normalización (ISO)).
- [Evaluación de los recursos con reglas](#) en la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de los recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- [AWS Security Hub](#)— Esto Servicio de AWS proporciona una visión completa del estado de su seguridad interior AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulte la [Referencia de controles de Security Hub](#).
- [Amazon GuardDuty](#): Servicio de AWS detecta posibles amenazas para sus cargas de trabajo Cuentas de AWS, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puede ayudarlo a cumplir con varios requisitos de conformidad, como la PCI DSS, al cumplir con los requisitos de detección de intrusiones exigidos por ciertos marcos de cumplimiento.
- [AWS Audit Manager](#)— Esto le Servicio de AWS ayuda a auditar continuamente su AWS uso para simplificar la gestión del riesgo y el cumplimiento de las normativas y los estándares del sector.

## Estándares de conformidad admitidos

IAM Identity Center ha sido sometido a auditorías para los siguientes estándares y puede utilizarse en soluciones para las que se exija certificación de conformidad.



AWS [ha ampliado su programa de cumplimiento de la Ley de Portabilidad y Responsabilidad de los Seguros de Salud \(HIPAA\) para incluir el Centro de Identidad de IAM como un servicio que cumple con los requisitos de la HIPAA.](#)

AWS ofrece un [documento técnico centrado en la HIPAA](#) para los clientes que desean obtener más información sobre cómo procesar y almacenar la información de salud. Servicios de AWS Para obtener más información, consulte [Conformidad con HIPAA](#).



El Programa de Asesores Registrados de Seguridad de la Información (IRAP) permite a los clientes del Gobierno australiano garantizar que existen controles apropiados, así como determinar el modelo de responsabilidad adecuado para abordar los requisitos del Manual de Seguridad de la Información (ISM) del Gobierno australiano, elaborado por el Centro Australiano de Ciberseguridad (ACSC). Para obtener más información, consulte [Recursos de IRAP](#).



IAM Identity Center dispone de una declaración de conformidad para el estándar de seguridad de datos del sector de tarjetas de pago (PCI DSS) versión 3.2 de nivel de proveedor de servicios 1.

Los clientes que utilizan AWS productos y servicios para almacenar, procesar o transmitir datos de titulares de tarjetas pueden utilizar las siguientes fuentes de identidad en el Centro de Identidad de IAM para gestionar su propia certificación de conformidad con la PCI DSS:

- Active Directory
- Proveedor de identidades externo

La fuente de identidad de IAM Identity Center actualmente no cumple con el estándar PCI DSS.

Para obtener más información sobre PCI DSS, incluida la forma de solicitar una copia del PCI AWS Compliance Package, consulte [PCI](#) DSS nivel 1.



Los informes de control de organizaciones y sistemas (SOC) son informes de análisis independientes de terceros que muestran cómo IAM Identity Center cumple los controles y objetivos clave de conformidad. Estos informes ayudan tanto a sus auditores como a usted a comprender cómo los controles respaldan las operaciones y la conformidad. Existen 3 tipos de informes de SOC:

- AWS Informe SOC 1: [Descargar con Artifact AWS](#)
- AWS SOC 2: Informe de seguridad, disponibilidad y confidencialidad: [descarga con Artifact AWS](#)
- [AWS SOC 3: Informe de seguridad, disponibilidad y confidencialidad](#)

El IAM Identity Center está dentro del ámbito de aplicación de los AWS informes SOC 1, SOC 2 y SOC 3. Para obtener más información, consulte [Conformidad con SOC](#).

## Resiliencia en IAM Identity Center

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre zonas de disponibilidad sin interrupciones. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de centros de datos únicos o múltiples.

[Para obtener más información sobre AWS las regiones y las zonas de disponibilidad, consulte la infraestructura global.AWS](#)

Para obtener más información sobre AWS IAM Identity Center la resiliencia, consulte [Diseño de resiliencia y comportamiento regional](#).

## Seguridad de la infraestructura en IAM Identity Center

Como servicio gestionado, AWS IAM Identity Center está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte [Seguridad AWS en la nube](#). Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte [Protección de infraestructuras en un marco](#) de buena AWS arquitectura basado en el pilar de la seguridad.

Utilice las llamadas a la API AWS publicadas para acceder al IAM Identity Center a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) como DHE (Ephemeral Diffie-Hellman) o ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puedes utilizar [AWS Security Token Service](#) (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.



# Recursos de etiquetado AWS IAM Identity Center

Una etiqueta es una etiqueta de atributo personalizada que se agrega a un AWS recurso para facilitar la identificación, la organización y la búsqueda de los recursos. Cada etiqueta tiene dos partes:

- Una clave de etiqueta (por ejemplo, `CostCenter`, `Environment` o `Project`). Las claves de etiqueta pueden tener 128 caracteres como máximo y distingue entre mayúsculas y minúsculas.
- Un valor de etiqueta (por ejemplo, `111122223333` o `Production`). Los valores de etiqueta pueden tener una longitud de hasta 256 caracteres y, al igual que las claves de etiqueta, distinguen mayúsculas y minúsculas. Puede establecer el valor de una etiqueta como una cadena vacía, pero no puede asignarle un valor nulo. Omitir el valor de etiqueta es lo mismo que utilizar una cadena vacía.

Las etiquetas ayudan a identificar y organizar AWS los recursos. Muchos AWS servicios admiten el etiquetado, por lo que puede asignar la misma etiqueta a los recursos de diferentes servicios para indicar que los recursos están relacionados. Por ejemplo, puede asignar la misma etiqueta a un conjunto de permisos específico en su instancia de IAM Identity Center. Para obtener más información sobre las estrategias de etiquetado, consulte [Etiquetado de AWS recursos](#) en la Referencia general de AWS guía y Prácticas recomendadas de [etiquetado](#).

Además de identificar, organizar y rastrear tus AWS recursos con etiquetas, puedes utilizarlas en las políticas de IAM para controlar quién puede ver tus recursos e interactuar con ellos. Para obtener más información sobre el uso de etiquetas para controlar el acceso, consulte [Controlar el acceso a AWS los recursos mediante etiquetas](#) en la Guía del usuario de IAM. Por ejemplo, puede permitir que un usuario actualice un conjunto de permisos de IAM Identity Center, pero solo si este conjunto tiene una etiqueta de `owner` con un valor del nombre de ese usuario.

Solo puede aplicar etiquetas a conjuntos de permisos. No puede aplicar etiquetas a las funciones correspondientes en las que crea el Centro de Identidad de IAM. Cuentas de AWS Puede utilizar la consola del Centro de Identidad de IAM AWS CLI o el Centro de Identidad de IAM APIs para añadir, editar o eliminar las etiquetas de un conjunto de permisos.

En las siguientes secciones se ofrece más información acerca de las etiquetas para IAM Identity Center.

Temas

- [Restricciones de las etiquetas](#)
- [Administre las etiquetas a través de la consola de IAM Identity Center](#)
- [AWS CLI ejemplos](#)
- [Administre etiquetas mediante el uso de la API de IAM Identity Center](#)

## Restricciones de las etiquetas

Las siguientes restricciones básicas se aplican a las etiquetas en recursos de IAM Identity Center:

- El número máximo de etiquetas que puede asignar a un recurso es 50.
- La longitud máxima de la clave es de 128 caracteres Unicode.
- La longitud máxima del valor es de 256 caracteres Unicode.
- Los caracteres válidos para una clave y un valor de etiqueta son:  
a-z, A-Z, 0-9, espacio y los siguientes caracteres: \_ . : / = + - y @
- Las claves y los valores distinguen entre mayúsculas y minúsculas.
- No utilice `aws :` como prefijo para claves, ya que está reservado para AWS .

## Administre las etiquetas a través de la consola de IAM Identity Center

Puede utilizar la consola de IAM Identity Center para agregar, editar y eliminar etiquetas asociadas a sus conjuntos de instancias o permisos.

Para administrar etiquetas de conjuntos de permisos para una consola de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#)
2. Elija Conjuntos de permisos.
3. Elija el nombre del conjunto de permisos que tiene las etiquetas que desea administrar.
4. En la pestaña Permisos de la sección Etiquetas, realice una de las siguientes acciones y, a continuación, continúe con el paso siguiente:
  - a. Si ya hay etiquetas asignadas a este conjunto de permisos, elija Edite etiquetas.
  - b. Si no hay ninguna etiqueta asignada a este conjunto de permisos, elija Agregar etiquetas.

5. Para cada etiqueta nueva, escriba los valores en las columnas Clave y Valor (opcional). Cuando haya finalizado, elija Save changes (Guardar cambios).

Para eliminar una etiqueta, seleccione la X en la columna Eliminar situada junto a la etiqueta que desea eliminar.

Para administrar de etiquetas para una instancia de IAM Identity Center

1. Abra la [consola de IAM Identity Center](#).
2. Elija Configuración.
3. Elija la pestaña Etiquetas.
4. Para cada etiqueta, escriba los valores en los campos Clave y Valor (opcional). Cuando haya terminado, seleccione el botón Agregar nueva etiqueta.

Para eliminar una etiqueta, seleccione el botón Eliminar junto a la etiqueta que desee eliminar.

## AWS CLI ejemplos

AWS CLI Proporciona comandos que puede usar para administrar las etiquetas que asigna a su conjunto de permisos.

### Asignación de etiquetas

Utilice los siguientes comandos para asignar etiquetas a su conjunto de permisos.

Example Comando **tag-resource** para un conjunto de permisos

Asigne etiquetas a un conjunto de permisos mediante el uso de [tag-resource](#) en el conjunto de comandos de sso:

```
$ aws sso-admin tag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tags Stage=Test
```

Este comando incluye los siguientes parámetros:

- `instance-arn`: el nombre de recurso de Amazon (ARN) de la instancia de IAM Identity Center en la que se ejecutará la operación.

- **resource-arn**: el ARN del recurso con las etiquetas que se van a enumerar.
- **tags**: los pares de clave-valor de las etiquetas.

Para asignar varias etiquetas a la vez, especifíquelas en una lista separada por comas:

```
$ aws sso-admin tag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

## Visualización de etiquetas

Utilice los siguientes comandos para visualizar las etiquetas que ha asignado a su conjunto de permisos.

Example Comando **list-tags-for-resource** para un conjunto de permisos

Visualice las etiquetas que están asignadas a un conjunto de permisos mediante el uso de [list-tags-for-resource](#) en el conjunto de comandos de sso:

```
$ aws sso-admin list-tags-for-resource --resource-arn sso-resource-arn
```

## Eliminación de etiquetas

Utilice los siguientes comandos para eliminar etiquetas de un conjunto de permisos.

Example Comando **untag-resource** para un conjunto de permisos

Elimine etiquetas de un conjunto de permisos mediante el uso de [untag-resource](#) en el conjunto de comandos de sso:

```
$ aws sso-admin untag-resource \  
> --instance-arn sso-instance-arn \  
> --resource-arn sso-resource-arn \  
> --tag-keys Stage CostCenter Owner
```

Para el parámetro **--tag-keys**, especifique una o más claves de etiquetas y no incluya los valores de etiqueta.

## Cómo aplicar etiquetas al crear un conjunto de permisos

Utilice los siguientes comandos para asignar etiquetas al crear un conjunto de permisos.

Example Comando **create-permission-set** con etiquetas

Cuando se crea un conjunto de permisos a través del comando [create-permission-set](#), es posible especificar etiquetas con el parámetro `--tags`:

```
$ aws sso-admin create-permission-set \  
> --instance-arn sso-instance-arn \  
> --name permission=set-name \  
> --tags Stage=Test, CostCenter=80432, Owner=SysEng
```

## Administre etiquetas mediante el uso de la API de IAM Identity Center

Utilice las siguientes acciones de la API para asignar, ver y eliminar etiquetas para un conjunto de permisos o instancia de IAM Identity Center.

- [TagResource](#)
- [ListTagsForResource](#)
- [UntagResource](#)
- [CreatePermissionSet](#)
- [CreateInstance](#)

# Integración de AWS CLI con IAM Identity Center

AWS La integración de la versión 2 de la interfaz de línea de comandos (CLI) con IAM Identity Center simplifica el proceso de inicio de sesión. Los desarrolladores pueden iniciar sesión directamente en el IAM Identity Center AWS CLI con las mismas credenciales de Active Directory o IAM Identity Center que utilizan normalmente para iniciar sesión en el IAM Identity Center y acceder a las cuentas y funciones que se les asignen. Por ejemplo, después de que un administrador configure el Centro de identidades de IAM para que utilice Active Directory para la autenticación, el desarrollador puede iniciar sesión AWS CLI directamente en él con sus credenciales de Active Directory.

AWS La integración de CLI con IAM Identity Center ofrece las siguientes ventajas:

- Las empresas pueden permitir que sus desarrolladores inicien sesión con las credenciales de IAM Identity Center o Active Directory conectando IAM Identity Center a su Active Directory mediante AWS Directory Service.
- Los desarrolladores pueden iniciar sesión desde la CLI para un acceso más rápido.
- Los desarrolladores pueden enumerar las cuentas y los roles a los que tienen acceso asignado y cambiar de una cuenta a otra.
- Los desarrolladores pueden generar y guardar automáticamente perfiles de rol con nombre en su configuración de la CLI y hacer referencia a ellos en la CLI para ejecutar comandos en las cuentas y roles deseados.
- La CLI administra automáticamente las credenciales a corto plazo para que los desarrolladores puedan iniciar y permanecer en la CLI de forma segura y sin interrupciones, y ejecutar scripts de larga duración.

## Cómo integrar AWS CLI con IAM Identity Center

Para utilizar la integración de AWS CLI con IAM Identity Center, descargue, instale y configure la AWS Command Line Interface versión 2. Para ver los pasos detallados sobre cómo descargar e integrar el AWS CLI IAM Identity Center, consulte [Configuración de la AWS CLI para usar IAM Identity Center](#) en la Guía del AWS Command Line Interface usuario.

# Consideraciones para el acceso AWS Management Console privado

Si su organización utiliza la función de acceso AWS Management Console privado, debe tener en cuenta cómo iniciarán sesión sus usuarios en el Centro de identidades de IAM.

Una política de puntos finales de VPC restringe el inicio de sesión en la consola de administración, lo que impide que los usuarios inicien sesión cuando no Cuentas de AWS están autorizados a acceder. Para obtener más información, consulte [Acceso privado a AWS Management Console](#) en la Guía del usuario de AWS Management Console .

Los puntos finales de VPC bloquean el inicio de sesión en el centro de identidad de IAM

Es importante tener en cuenta que el uso de puntos finales de VPC bloqueará el inicio de sesión en el Centro de identidades de IAM. Esto ocurre cuando un usuario ya ha iniciado sesión en la consola de administración a través del punto final de la VPC. Para garantizar que sus usuarios puedan seguir iniciando sesión en el IAM Identity Center, deben utilizar el punto de conexión público para iniciar sesión en AWS en lugar del punto de conexión de VPC.

# Cuotas y límites de IAM Identity Center

En las siguientes tablas se describen las cuotas de IAM Identity Center. Las solicitudes de aumento de cuota deben provenir de una cuenta de administración o de administrador delegado. Para solicitar un aumento de cuota, consulte [Solicitar un aumento de cuota](#).

## Note

Recomendamos utilizar la AWS CLI y APIs administrar el Centro de identidad de IAM si tiene más de 50 000 usuarios, 10 000 grupos o 500 conjuntos de permisos. Para obtener más información acerca de la CLI, consulte [Integración de AWS CLI con IAM Identity Center](#). Para obtener más información APIs, consulte [Bienvenido a la referencia de la API del Centro de Identidad de IAM](#).

## Cuotas de aplicaciones

| Recurso                                                                                  | Cuota predeterminada    | Se puede aumentar |
|------------------------------------------------------------------------------------------|-------------------------|-------------------|
| Tamaño del archivo de los certificados SAML de proveedores de servicios (en formato PEM) | 2 KB                    | No                |
| Límite de aserción de SAML                                                               | 50 000 caracteres       | No                |
| Límite de tamaño de archivo del certificado de IdP cargado en el IAM Identity Center     | 2500 caracteres (UTF-8) | No                |
| Ámbitos de acceso por aplicación                                                         | 25                      | No                |



## Cuenta de AWS cuotas

| Recurso                                                                                            | Cuota predeterminada                                                                                                                                        | Se puede aumentar |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| Número de conjuntos de permisos permitidos en IAM Identity Center                                  | 2000                                                                                                                                                        | Sí                |
| Número de conjuntos de permisos aprovisionados permitidos por Cuenta de AWS                        | 500                                                                                                                                                         | Sí                |
| Número de políticas insertadas por conjunto de permisos                                            | 1                                                                                                                                                           | No                |
| Número de políticas AWS administradas y administradas por el cliente por conjunto de permisos      | 20 <sup>1</sup>                                                                                                                                             | No                |
| Tamaño máximo de la política insertada por conjunto de permisos                                    | 32 768 bytes.<br><br>El tamaño máximo de los caracteres que no son espacios en blanco en la política insertada por conjunto de permisos es de 10 240 bytes. | No                |
| Número de funciones de IAM (conjuntos de permisos) Cuenta de AWS que se pueden actualizar a la vez | 1                                                                                                                                                           | No                |

<sup>1</sup>AWS Identity and Access Management (IAM) establece una cuota de 10 políticas gestionadas por función. Para aprovechar esta cuota, solicite un aumento de la cuota de IAM en las políticas

gestionadas asociadas a una función de IAM en la consola de Service Quotas para cada uno de los Cuentas de AWS lugares en los que desee implementar el conjunto de permisos.

 Note

[Administre Cuentas de AWS con conjuntos de permisos](#) se aprovisionan Cuentas de AWS como funciones de IAM o utilizan las funciones de IAM existentes y, por lo tanto Cuentas de AWS, respetan las cuotas de IAM. Para obtener más información sobre las cuotas asociadas a los roles de IAM, consulte [Cuotas de IAM y STS](#).

## Cuotas de Active Directory

| Recurso                                                                 | Cuota predeterminada | Se puede aumentar |
|-------------------------------------------------------------------------|----------------------|-------------------|
| Número de directorios conectados que se puede tener de forma simultánea | 1                    | No                |

## Cuotas de almacén de identidades de IAM Identity Center

| Recurso                                                                                | Cuota predeterminada | Se puede aumentar |
|----------------------------------------------------------------------------------------|----------------------|-------------------|
| Número de usuarios admitidos en IAM Identity Center                                    | 100000               | Sí                |
| Número de grupos admitidos en IAM Identity Center                                      | 100000               | No                |
| Número de grupos únicos que se pueden utilizar para evaluar los permisos de un usuario | 1 000                | No                |

## Límites de solicitudes de IAM Identity Center

| Recurso                         | Cuota predeterminada                                                                                                                                                                                                                                                                                                           |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Centro de identidad de IAM APIs | APIs Los <a href="#">centros de identidad de IAM</a> tienen un límite colectivo máximo de 20 transacciones por segundo (TPS). Puede abrir un caso de soporte para solicitar un aumento. <a href="#">CreateAccountAssignment</a> Tiene una tasa máxima de 15 llamadas asíncronas pendientes y este límite no se puede aumentar. |
| Tienda de identidades APIs      | <a href="#">Identity Store APIs</a> tiene un límite colectivo máximo de 20 transacciones por segundo (TPS). Puede abrir un caso de soporte para solicitar un aumento.                                                                                                                                                          |
| SCIM APIs                       | Los <a href="#">SCIM APIs</a> tienen un límite colectivo máximo de 20 transacciones por segundo (TPS). Puede abrir un caso de soporte para solicitar un aumento.                                                                                                                                                               |

## Cuotas adicionales

| Recurso                                                                  | Cuota predeterminada | Se puede aumentar |
|--------------------------------------------------------------------------|----------------------|-------------------|
| Número total de Cuentas de AWS aplicaciones que se pueden configurar* ** | 3 000                | Sí                |
| Total de instancias de IAM Identity Center por cuenta                    | 1                    | No                |
| Total de emisores de tokens de confianza                                 | 10                   | No                |

\* Por ejemplo, puede configurar 2750 cuentas y 250 aplicaciones, lo que da como resultado un total de 3000 cuentas y aplicaciones.

\*\* La operación de la [ProvisionPermissionSet](#) API puede aprovisionar un conjunto de permisos mediante la opción ALL\_PROVISIONED\_ACCOUNTS de, como máximo, 3500 Cuentas de AWS. Si necesita aprovisionar un conjunto de permisos de más de 3500 Cuentas de AWS, puede utilizar la operación de ProvisionPermissionSet API con la AWS\_ACCOUNT opción, que aprovisiona el conjunto de permisos en una sola unidad Cuenta de AWS. Puede realizar hasta tres llamadas simultáneas a ProvisionPermissionSet.

# Resolución de problemas de IAM Identity Center

La siguiente información puede ayudarle a solucionar algunos problemas comunes que puede encontrarse a la hora de configurar o utilizar la consola de IAM Identity Center.

## Problemas al crear una instancia de cuenta de IAM Identity Center

Es posible que se apliquen varias restricciones al crear una instancia de cuenta de IAM Identity Center. Si no puede crear una instancia de cuenta a través de la consola del IAM Identity Center o de la experiencia de configuración de una aplicación AWS gestionada compatible, compruebe los siguientes casos de uso:

- Marque otras Regiones de AWS Cuenta de AWS en las que esté intentando crear la instancia de cuenta. Tiene un límite de una instancia de IAM Identity Center por Cuenta de AWS. Para habilitar la aplicación, cambie a la Región de AWS instancia de IAM Identity Center o cambie a una cuenta sin una instancia de IAM Identity Center.
- Si su organización habilitó IAM Identity Center antes del 14 de septiembre de 2023, es posible que su administrador tenga que activar la creación de instancias de cuenta. Trabaje con el administrador para habilitar la creación de instancias de cuenta desde la consola de IAM Identity Center en la cuenta de administración.
- Es posible que el administrador haya creado una política de control de servicio para limitar la creación de instancias de cuenta de IAM Identity Center. Trabaje con el administrador para agregar su cuenta a la lista de permitidos.

## Recibe un error al intentar ver la lista de aplicaciones en la nube que están preconfiguradas para funcionar con IAM Identity Center

El siguiente error se produce cuando tienes una política que lo permite, `sso:ListApplications` pero no otros centros de identidad de IAM. APIs Actualice la política para resolver este error.

El `ListApplications` permiso autoriza varios: APIs

- La API `ListApplications`.
- Una API interna similar a la API `ListApplicationProviders` utilizada en la consola de IAM Identity Center.

Para ayudar a resolver la duplicación, la API interna ahora también autoriza el uso de la acción `ListApplicationProviders`. Para permitir la API pública `ListApplications`, pero denegar la API interna, la política debe incluir una instrucción que deniegue la acción `ListApplicationProviders`:

```
"Statement": [  
  {  
    "Effect": "Deny",  
    "Action": "sso:ListApplicationProviders",  
    "Resource": "*"  
  },  
  {  
    "Effect": "Allow",  
    "Action": "sso:ListApplications",  
    "Resource": "<instanceArn>" // (or "*" for all instances)  
  }  
]
```

Para permitir la API interna, pero denegar `ListApplications`, la política tiene que permitir solo `ListApplicationProviders`. La API `ListApplications` se deniega si no se permite explícitamente.

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Action": "sso:ListApplicationProviders",  
    "Resource": "*"  
  }  
]
```

Cuando se actualicen sus políticas, póngase en contacto con nosotros Soporte para que eliminen esta medida proactiva.

## Problemas relacionados con el contenido de las confirmaciones de SAML creadas por IAM Identity Center

El Centro de Identidad de IAM ofrece una experiencia de depuración basada en la web para las afirmaciones de SAML creadas y enviadas por el Centro de Identidad de IAM, incluidos los atributos de estas afirmaciones, al acceder a Cuentas de AWS las aplicaciones de SAML desde el portal de acceso. AWS Para visualizar los detalles de una confirmación de SAML que genera IAM Identity Center, siga estos pasos:

1. Inicie sesión en el portal de acceso. AWS
2. Mientras está conectado al portal, mantenga pulsada la tecla Mayúscula, elija el mosaico de aplicaciones y suelte la tecla Mayúscula.
3. Revise la información de la página titulada You are now in administrator mode (Ahora está en modo administrador). Para conservar esta información y poder consultarla en el futuro, elija Copy XML (Copiar XML) y pegue el contenido en otro lugar.
4. Seleccione Enviar a <application> para continuar. Esta opción envía la confirmación al proveedor del servicio.

### Note

Es posible que algunas configuraciones de navegadores y sistemas operativos no admitan este procedimiento. Este procedimiento se ha probado en Windows 10 con los navegadores Firefox, Chrome y Edge.

## Algunos usuarios no logran sincronizarse con IAM Identity Center desde un proveedor de SCIM externo

Si su proveedor de identidades (IdP) está configurado para aprovisionar usuarios al IAM Identity Center mediante la sincronización SCIM, es posible que se produzcan errores de sincronización durante el proceso de aprovisionamiento de usuarios. Esto puede indicar que la configuración de usuario de su IdP no es compatible con los requisitos del IAM Identity Center. Cuando esto suceda, el SCIM del IAM Identity Center APIs devolverá mensajes de error que proporcionan información sobre la causa raíz del problema. Puede localizar estos mensajes de error en los registros o en la

interfaz de usuario de su IdP. Como alternativa, puede encontrar información más detallada sobre los errores de aprovisionamiento en los [registros de AWS CloudTrail](#).

Para más información sobre la implementación del SCIM de IAM Identity Center, incluidas las especificaciones de los parámetros y operaciones obligatorios, opcionales y no admitidos para los objetos de usuario, consulte la [Guía para desarrolladores de la implementación del SCIM de IAM Identity Center](#) en la Guía para desarrolladores de SCIM.

Los siguientes motivos son algunos de los más comunes de este error:

1. El objeto de usuario del IdP carece de un nombre (de pila), un apellido o un nombre para mostrar.

Mensaje de error: «Se detectaron 2 errores de validación: el valor at *'name.givenName'* no pudo cumplir la restricción: el miembro debe cumplir con el patrón de expresión regular: `[\\ p {L}\\ p {M}\\ p {N}\\ p {P}\\ t\\ n\\ r] +`; el valor en *'name.givenName'* no pudo cumplir la restricción: el miembro debe tener una longitud mayor o igual a 1»

- Solución: agregue un nombre (de pila), un apellido y un nombre para el objeto de usuario. Además, asegúrese de que las asignaciones de aprovisionamiento de SCIM para los objetos de usuario de su IdP estén configuradas para enviar valores no vacíos a todos estos atributos.
2. Se está enviando al usuario más de un valor para un único atributo (también conocidos como “atributos de valores múltiples”). Por ejemplo, el usuario puede tener un número de teléfono fijo y laboral especificado en el IdP, o varios correos electrónicos o direcciones físicas, y su IdP está configurado para intentar sincronizar varios o todos los valores de ese atributo.

Mensaje de error: «El atributo de la lista *emails* supera el límite permitido de 1»

- Opciones de solución:
  - i. Actualice las asignaciones de aprovisionamiento de SCIM para los objetos de usuario de su IdP para enviar solo un valor único para un atributo determinado. Por ejemplo, configure una asignación que envíe solo el número de teléfono laboral de cada usuario.
  - ii. Si los atributos adicionales se pueden eliminar de forma segura del objeto de usuario del IdP, puede eliminar los valores adicionales y dejar uno o cero valores establecidos para ese atributo del usuario.



- iii. Si el atributo no es necesario para realizar ninguna acción AWS, elimine la asignación de ese atributo de las asignaciones de aprovisionamiento de SCIM para objetos de usuario en su IdP.
3. Su IdP intenta hacer coincidir a los usuarios del objetivo (en este caso, IAM Identity Center) en función de varios atributos. Como se garantiza que los nombres de usuario sean únicos en una instancia determinada de IAM Identity Center, solo tiene que especificar `username` como atributo utilizado para la coincidencia.
- Solución: asegúrese de que la configuración de SCIM de su IdP utilice solo un atributo para coincidir con los usuarios de IAM Identity Center. Por ejemplo, la asignación de `username` o `userPrincipalName` del IdP al atributo `userName` de SCIM para el aprovisionamiento en IAM Identity Center será correcto y suficiente para la mayoría de las implementaciones.

## Error de usuario o grupo duplicado al aprovisionar usuarios o grupos con un proveedor de identidad externo

Si tiene problemas de sincronización del IAM Identity Center al aprovisionar usuarios o grupos en un proveedor de identidades (IdP) externo, podría deberse a que los usuarios o grupos de su IdP externo no tengan valores de atributos únicos. Es posible que aparezca el siguiente mensaje de error en el IdP externo:

Se negó a crear un nuevo recurso duplicado

Este problema se puede producir en el siguiente escenario:

- Escenario 1
  - Está utilizando atributos no únicos personalizados en su IdP externo para los atributos que deben ser únicos en el IAM Identity Center. Los usuarios o grupos existentes del IAM Identity Center no se sincronizan con su IdP.
- Escenario 2
  - Intenta crear usuarios con atributos duplicados para los atributos que deben ser únicos en el IAM Identity Center.
    - Por ejemplo, crea o tiene un usuario existente del IAM Identity Center con los siguientes atributos:
      - Nombre de usuario: Jane Doe
      - Dirección de correo electrónico principal: `jane_doe@example.com`

- A continuación, intente crear otro usuario en su IdP externo con los siguientes atributos:
  - Nombre de usuario: Richard Doe
  - Dirección de correo electrónico principal: jane\_doe@example.com
  - El IdP externo intenta sincronizar y crear el usuario en el IAM Identity Center. Sin embargo, estas acciones fallan porque ambos usuarios tienen valores duplicados para una dirección de correo electrónico principal que debe ser única.

El nombre de usuario, la dirección de correo electrónico principal y el identificador externo deben ser únicos para que los usuarios del IdP externo se sincronicen correctamente con el Centro de identidades de IAM. Del mismo modo, el nombre del grupo debe ser único para que los grupos de IdP externos se sincronicen correctamente con el IAM Identity Center.

La solución consiste en revisar los atributos de la fuente de identidad y asegurarse de que son únicos.

## Los usuarios no pueden iniciar sesión cuando su nombre de usuario está en formato UPN

Es posible que los usuarios no puedan iniciar sesión en el portal de AWS acceso en función del formato que utilizan para introducir su nombre de usuario en la página de inicio de sesión. En su mayor parte, los usuarios pueden iniciar sesión en el portal de usuarios con su nombre de usuario simple, su nombre de inicio de sesión de nivel inferior (DOMAIN\UserName) o su nombre de inicio de sesión UPN (). `UserName@Corp.Example.com` La excepción a esto se produce cuando IAM Identity Center utiliza un directorio conectado que se ha habilitado con MFA y el modo de verificación se ha establecido en Context-aware o en Always-on. En este escenario, los usuarios deben iniciar sesión con su nombre de inicio de sesión de nivel inferior (DOMAIN\). `UserName` Para obtener más información, consulte [Autenticación multifactor para usuarios de Identity Center](#). Para obtener información general sobre los formatos de nombre de usuario que se utilizan para iniciar sesión en Active Directory, consulte [Formatos de nombre de usuario](#) en el sitio web de documentación de Microsoft.

## Al modificar un rol de IAM, aparece el error: “No se puede realizar la operación en el rol protegido”.

Al revisar las funciones de IAM en una cuenta, es posible que veas que los nombres de las funciones comienzan por «SSO\_». AWSReserved Se trata de los roles que el servicio de IAM Identity Center ha creado en la cuenta y provienen de la asignación de un conjunto de permisos a la cuenta. Si se intenta modificar estos roles desde la consola de IAM, se producirá el siguiente error:

```
'Cannot perform the operation on the protected role 'AWSReservedSSO_RoleName_Here' -  
this role is only modifiable by AWS'
```

Estas funciones solo se pueden modificar desde la consola de administración de IAM Identity Center, que se encuentra en la cuenta de administración de AWS Organizations. Una vez modificado, puede transferir los cambios a las cuentas de AWS a las que esté asignado.

## Los usuarios del directorio no pueden restablecer su contraseña

Cuando un usuario del directorio restablece su contraseña mediante la opción ¿Ha olvidado su contraseña? al iniciar sesión en el portal de AWS acceso, su nueva contraseña debe cumplir con la política de contraseñas predeterminada, tal como se describe en [Requisitos de contraseñas para administrar identidades en IAM Identity Center](#)

Si un usuario introduce una contraseña que cumple con la política y, a continuación, recibe el error `We couldn't update your password`, compruebe si AWS CloudTrail se ha registrado el error. Para ello, busque en la consola del historial de eventos o CloudTrail utilice el siguiente filtro:

```
"UpdatePassword"
```

Si el mensaje indica lo siguiente, es posible que deba ponerse en contacto con el servicio de asistencia:

```
"errorCode": "InternalFailure",  
  "errorMessage": "An unknown error occurred"
```

Otra posible causa de este problema está en la convención de nomenclatura que se aplicó al valor del nombre de usuario. Las convenciones de nomenclatura deben seguir patrones específicos, como “surname.givenName”. Sin embargo, algunos nombres de usuario pueden ser bastante largos o

contener caracteres especiales, lo que puede provocar que se eliminen caracteres en la llamada a la API y, por lo tanto, se produzca un error. Puede intentar restablecer la contraseña con un usuario de prueba de la misma manera para comprobar si es así.

Si el problema persiste, póngase en contacto con el [centro de soporte de AWS](#).

## En un conjunto de permisos se hace referencia a mi usuario, pero no puede acceder a las cuentas o aplicaciones asignadas

Este problema se puede producir si utilizas el Sistema de administración de identidades entre dominios (SCIM) para el aprovisionamiento automático con un proveedor de identidad externo. En concreto, cuando se elimina un usuario o el grupo al que pertenecía el usuario y se vuelve a crear con el mismo nombre de usuario (para los usuarios) o nombre (para los grupos) en el proveedor de identidad, se crea un nuevo identificador interno único para el nuevo usuario o grupo en IAM Identity Center. Sin embargo, IAM Identity Center aún conserva una referencia al identificador anterior en su base de datos de permisos, de modo que el nombre del usuario o grupo sigue apareciendo en la interfaz de usuario, pero se produce un error en el acceso. Esto se debe a que el ID de usuario o grupo subyacente al que hace referencia la interfaz de usuario ya no existe.

Para restablecer el acceso de AWS en este caso, puede eliminar el acceso del usuario o grupo anterior de los lugares de la Cuenta de AWS a los que estaba asignado originalmente y, a continuación, volver a asignar el acceso al usuario o grupo. Esto actualiza el conjunto de permisos con el identificador correcto para el nuevo usuario o grupo. Del mismo modo, para restablecer el acceso a la aplicación, puede eliminar el acceso del usuario o grupo de la lista de usuarios asignados a esa aplicación y, a continuación, volver a agregar el usuario o grupo.

También puede comprobar si se AWS CloudTrail ha registrado el error buscando en los CloudTrail registros los eventos de sincronización de SCIM que hagan referencia al nombre del usuario o grupo en cuestión.

## No puedo configurar correctamente mi aplicación del catálogo de aplicaciones

Si ha agregado una aplicación del catálogo de aplicaciones en IAM Identity Center, tenga en cuenta que cada proveedor de servicios proporciona su propia documentación detallada. Puede acceder a esta información desde la pestaña Configuración de la aplicación en la consola de IAM Identity Center.

Si el problema está relacionado con la configuración de la confianza entre la aplicación del proveedor de servicios y IAM Identity Center, consulte el manual de instrucciones para conocer los pasos a seguir para la resolución de problemas.

## Error: “Se ha producido un error inesperado” cuando un usuario intenta iniciar sesión con un proveedor de identidad externo

Este error puede producirse por varios motivos, pero uno de los más comunes es la falta de coincidencia entre la información del usuario incluida en la solicitud de SAML y la información del usuario en IAM Identity Center.

Para que un usuario de IAM Identity Center inicie sesión correctamente al utilizar un IdP externo como fuente de identidad, debe cumplirse lo siguiente:

- El formato de nameID de SAML (configurado en su proveedor de identidad) debe ser “correo electrónico”
- El valor de nameID debe ser una cadena con el formato correcto (RFC2822) (user@domain.com)
- El valor del nameID debe coincidir exactamente con el nombre de usuario de un usuario existente en IAM Identity Center (no importa si la dirección de correo electrónico en IAM Identity Center coincide o no; la coincidencia entrante se basa en el nombre de usuario)
- La implementación de la federación SAML 2.0 en IAM Identity Center solo admite una confirmación en la respuesta de SAML entre el proveedor de identidades y IAM Identity Center. No admite las confirmaciones de SAML cifradas.
- Si los [Atributos para controlar el acceso](#) están habilitados en su cuenta de IAM Identity Center, se aplican las siguientes confirmaciones:
  - El número de atributos asignados en la solicitud de SAML debe ser 50 o inferior.
  - La solicitud de SAML no debe contener atributos con varios valores.
  - La solicitud de SAML no debe contener varios atributos con el mismo nombre.
  - El atributo no debe contener XML estructurado como valor.
  - El formato del nombre debe ser un formato especificado por SAML y no un formato genérico.

### Note

IAM Identity Center no crea usuarios o grupos “justo a tiempo” para nuevos usuarios o grupos mediante la federación SAML. Esto significa que el usuario debe haber sido

creado previamente en IAM Identity Center, ya sea de forma manual o mediante un aprovisionamiento automático, para poder iniciar sesión en IAM Identity Center.

Este error también se puede producir cuando el punto de conexión del Servicio de Consumidor de Aserción (ACS) configurado en su proveedor de identidad no coincide con la URL de ACS proporcionada por su instancia de IAM Identity Center. Asegúrese de que estos 2 valores coincidan exactamente.

Además, puede solucionar aún más los errores de inicio de sesión de un proveedor de identidad externo consultando AWS CloudTrail y filtrando el nombre del evento Login. ExternalId PDirectory

## Error: “No se pudieron habilitar los atributos del control de acceso”

Este error se puede producir si el usuario que habilita ABAC no tiene los permisos de `iam:UpdateAssumeRolePolicy` necesarios para habilitar [Atributos para controlar el acceso](#).

## El mensaje “El navegador no es compatible” aparece cuando intento registrar un dispositivo para MFA

WebAuthn actualmente es compatible con los navegadores web Google Chrome, Mozilla Firefox, Microsoft Edge y Apple Safari, así como con las plataformas Windows 10 y Android. Algunos componentes de la WebAuthn compatibilidad pueden variar, como la compatibilidad con el autenticador de plataforma en los navegadores macOS e iOS. Si los usuarios intentan registrar WebAuthn dispositivos en un navegador o una plataforma no compatibles, verán determinadas opciones que no son compatibles o recibirán un mensaje de error que indica que no se admiten todos los métodos compatibles. En estos casos, consulte [FIDO2: Autenticación web \(WebAuthn\)](#) para obtener más información sobre la compatibilidad entre navegadores y plataformas. Para obtener más información sobre el Centro de identidades WebAuthn de IAM, consulte. [FIDO2 autenticadores](#)

## El grupo “Usuarios de dominio” de Active Directory no se sincroniza correctamente con IAM Identity Center

El grupo de usuarios de dominio de Active Directory es el “grupo principal” predeterminado para los objetos de usuario de AD. IAM Identity Center no puede leer los grupos principales de Active Directory ni sus membresías. Al asignar el acceso a los recursos o aplicaciones de IAM Identity

Center, utilice grupos distintos del grupo de usuarios del dominio (u otros grupos asignados como grupos principales) para que la membresía a los grupos se refleje correctamente en el almacén de identidades de IAM Identity Center.

## Error de credenciales de MFA no válidas

Este error puede producirse cuando un usuario intenta iniciar sesión en el Centro de identidades de IAM con una cuenta de un proveedor de identidad externo (por ejemplo, Okta o Microsoft Entra ID) antes de que su cuenta se aprovisiona por completo al IAM Identity Center mediante el protocolo SCIM. Una vez que la cuenta de usuario se aprovisiona en IAM Identity Center, este problema debería resolverse. Confirme que la cuenta se haya aprovisionado en IAM Identity Center. Si no es así, compruebe los registros de aprovisionamiento en el proveedor de identidades externo.

## El mensaje “Se ha producido un error inesperado” aparece cuando intento registrarme o iniciar sesión con una aplicación de autenticación

Los sistemas de contraseña temporal de un solo uso (TOTP) basados en el tiempo, como los que utiliza IAM Identity Center en combinación con las aplicaciones de autenticación basadas en código, se basan en la sincronización horaria entre el cliente y el servidor. Asegúrese de que el dispositivo en el que está instalada la aplicación de autenticación esté sincronizado correctamente con una fuente horaria fiable o configure manualmente la hora del dispositivo para que coincida con una fuente fiable, como, por ejemplo, NIST (<https://www.time.gov/>) u otras fuentes equivalentes locales o regionales.

## Aparece el mensaje de error “No es usted, somos nosotros” cuando intento iniciar sesión en el IAM Identity Center

Este error indica que hay un problema de configuración con su instancia de IAM Identity Center o con el proveedor de identidades (IdP) externo que IAM Identity Center utiliza como fuente de identidad. Le recomendamos que realice las siguientes acciones:

- Compruebe la configuración de fecha y hora del dispositivo que utiliza para iniciar sesión. Recomendamos que establezca que la fecha y la hora se ajusten automáticamente. Si no está disponible, le recomendamos que sincronice la fecha y la hora con un servidor de protocolo de hora de red (NTP) conocido.

- Compruebe que el certificado de IdP cargado en el IAM Identity Center es el mismo que el que proporcionó su IdP. Para comprobar el certificado desde la consola del IAM Identity Center, vaya a Configuración. En la pestaña Fuente de identidad, elija Acción y, a continuación, Administrar autenticación. Si los certificados del IdP y del IAM Identity Center no coinciden, importe un certificado nuevo al IAM Identity Center.
- Asegúrese de que el formato NameID del archivo de metadatos de su proveedor de identidad sea el siguiente:
  - `urn:oasis:name:tc:SAML:1.1:nameid-format:emailAddress`
- Si utiliza AD Connector de AWS Directory Service como proveedor de identidad, compruebe que las credenciales de la cuenta de servicio son correctas y no han caducado. Consulte [Actualización de las credenciales de su cuenta de servicio de Conector de AD en AWS Directory Service](#) para obtener más información.

## Mis usuarios no reciben correos electrónicos de IAM Identity Center

Todos los correos electrónicos enviados por el servicio de IAM Identity Center procederán de una de estas direcciones: `no-reply@signin.aws` o `no-reply@login.awsapps.com`. Su sistema de correo electrónico se debe configurar de manera que acepte los mensajes con estas direcciones de correo electrónico como remitente y no los trate como correo basura o spam.

## Error: no puedes delete/modify/remove/assign acceder a los conjuntos de permisos aprovisionados en la cuenta de administración

Este mensaje indica que la característica [Administración delegada](#) está habilitada y que la operación que intentó anteriormente solo la puede realizar correctamente una persona con permisos de cuenta de administración en AWS Organizations. Para resolver este problema, inicie sesión como usuario con estos permisos e intente volver a realizar la tarea o asigne esta tarea a alguien que cuente con los permisos correctos. Para obtener más información, consulte [Registro de una cuenta miembro](#).

## Error: no se encontró el token de sesión o no es válido

Este error puede producirse cuando un cliente, como un navegador web AWS Toolkit AWS CLI, o intenta utilizar una sesión revocada o invalidada en el servidor. Para corregir este problema, vuelva



a la aplicación de cliente o al sitio web e inténtelo de nuevo, incluso vuelva a iniciar sesión si se le solicita. A veces, esto puede requerir que también canceles las solicitudes pendientes, como un intento de conexión pendiente desde tu AWS Toolkit IDE.

# Historial del documento

En la siguiente tabla, se describen los cambios importantes de la AWS IAM Identity Center documentación. Actualizamos la documentación con frecuencia para dar respuesta a los comentarios que se nos envía.

- Última actualización importante de la documentación: 23 de septiembre de 2022

| Cambio                                                                   | Descripción                                                                                                                                                                             | Fecha                 |
|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#">Sesiones de consola con identidad mejorada</a>               | Terminología actualizada para las sesiones de consola con identidad mejorada (anteriormente denominadas sesiones con reconocimiento de identidad).                                      | 12 de mayo de 2025    |
| <a href="#">Cómo empezar con la reorganización</a>                       | Se reorganizó el contenido de introducción para mejorar la claridad y la experiencia del usuario.                                                                                       | 6 de mayo de 2025     |
| <a href="#">Sincronización de la API de Centro de identidades de IAM</a> | Ya no puede aprovisionar a los usuarios de Active Directory con IAM Identity Center AD Sync. En su lugar, puede utilizar la sincronización AD Sync configurable de IAM Identity Center. | 17 de abril de 2025   |
| <a href="#">Actualización a sesión autenticada</a>                       | Actualice la duración de las sesiones del IAM Identity Center cuando se elimine la sesión del usuario.                                                                                  | 2 de abril de 2025    |
| <a href="#">Actualizaciones de la política gestionada AWS</a>            | Se han actualizado los permisos de la política                                                                                                                                          | 11 de febrero de 2025 |

|                                                                                      |                                                                                                                        |                          |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|--------------------------|
|                                                                                      | AWSSS0ServiceRolePolicy AWS gestionada.                                                                                |                          |
| <a href="#">Se mejoró el flujo de trabajo de habilitación de IAM Identity Center</a> | Flujo de trabajo actualizado para habilitar las instancias de organización y cuenta de IAM Identity Center.            | 11 de febrero de 2025    |
| <a href="#">Actualizaciones para la activación del Centro de Identidad de IAM</a>    | Contenido y procedimientos actualizados para habilitar las instancias de organización y cuenta de IAM Identity Center. | 10 de octubre de 2024    |
| <a href="#">Actualizaciones de la política AWS gestionada</a>                        | Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.         | 2 de octubre de 2024     |
| <a href="#">Actualizaciones de la política AWS gestionada</a>                        | Se han actualizado los permisos de la política AWSSS0MasterAccountAdministrator AWS gestionada.                        | 26 de septiembre de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a>                        | Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.         | 4 de septiembre de 2024  |
| <a href="#">Actualizaciones de la sección “¿Qué es el IAM Identity Center?” tema</a> | Se actualizó el contenido que describe las ventajas y las capacidades del IAM Identity Center.                         | 19 de agosto de 2024     |

[Actualizaciones de la política  
AWS gestionada](#)

Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

12 de julio de 2024

[Actualizaciones de la política  
AWS gestionada](#)

Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

27 de junio de 2024

[Actualizaciones de la política  
AWS gestionada](#)

Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

17 de mayo de 2024

[Actualizaciones de la política  
AWS gestionada](#)

Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

30 de abril de 2024

[Actualizaciones de la política  
AWS gestionada](#)

Se han actualizado los permisos de la política AWSSSOMasterAccountAdministrator AWS gestionada.

26 de abril de 2024

|                                                               |                                                                                                                |                     |
|---------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|---------------------|
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Se han actualizado los permisos de la política AWSSS0MemberAccountAdministrator AWS gestionada.                | 26 de abril de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Se han actualizado los permisos de la política AWSSS0ReadOnly AWS gestionada.                                  | 26 de abril de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada. | 26 de abril de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada. | 24 de abril de 2024 |
| <a href="#">Actualizaciones de la política AWS gestionada</a> | Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada. | 19 de abril de 2024 |

[Actualizaciones de la política AWS gestionada](#)

Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

11 de abril de 2024

[Actualizaciones de la política AWS gestionada](#)

Se han actualizado los permisos de la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

26 de noviembre de 2023

[Nuevo tema de política AWS gestionada](#)

Se han añadido detalles para la política AWSIAMIdentityCenterAllowListForIdentityContext AWS gestionada.

15 de noviembre de 2023

[Guía de introducción mejorada sobre el uso de IAM Identity Center](#)

Contenido nuevo agregado para empezar a utilizar IAM Identity Center y crear un usuario administrativo

23 de septiembre de 2022

[Usuarios y grupos actualizados en la referencia de la API de Identity Center](#)

Esta actualización incluye referencias a la nueva creación, actualización y eliminación APIs en la Guía de referencia de las API de Identity Center.

31 de agosto de 2022

[AWS Nombre del inicio de sesión único de \(AWS SSO de\) cambiado por IAM Identity Center AWS](#)

AWS presenta. AWS IAM Identity Center IAM Identity Center amplía las capacidades de AWS Identity and Access Management (IAM) para ayudarle a administrar de forma centralizada las cuentas y el acceso a las aplicaciones para los usuarios de personal. Las características de IAM Identity Center incluyen la asignación de aplicaciones, los permisos para varias cuentas y un portal de acceso AWS .

26 de julio de 2022

[Compatibilidad con límites de permisos y política administrada por el cliente en los conjuntos de permisos](#)

Contenido agregado para usar políticas AWS administradas de y administradas por el cliente AWS Identity and Access Management (IAM) con conjuntos de permisos.

14 de julio de 2022

[Compatibilidad con AWS regiones de habilitadas manualmente](#)

Contenido agregado para utilizar IAM Identity Center en regiones habilitadas de forma manual.

15 de junio de 2022

[Actualizaciones para las políticas AWS gestionadas](#)

Se han actualizado los permisos de la política AWSSS0ServiceRolePolicy AWS gestionada.

11 de mayo de 2022

[Compatibilidad con la administración delegada](#)

Contenido agregado para la característica de administración delegada.

11 de mayo de 2022

|                                                                                    |                                                                                                                                                                                   |                         |
|------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#">Actualizaciones de las políticas AWS gestionadas</a>                   | Se actualizaron los permisos para las AWSSSOMasterAccountAdministrator políticas AWSSSOMemberAccountAdministrator administradas y las políticas AWSSSOREadOnly AWS administradas. | 28 de abril de 2022     |
| <a href="#">Compatibilidad con la sincronización con AD configurable</a>           | Contenido agregado para la característica de sincronización con AD configurable.                                                                                                  | 14 de abril de 2022     |
| <a href="#">Nuevo tema sobre políticas AWS administradas</a>                       | Se han añadido detalles para la política AWSSSOMasterAccountAdministrator AWS gestionada.                                                                                         | 4 de agosto de 2021     |
| <a href="#">Actualizaciones para cuotas</a>                                        | Ajustes en las tablas de cuotas.                                                                                                                                                  | 21 de diciembre de 2020 |
| <a href="#">Nuevos ejemplos de políticas</a>                                       | Nuevos ejemplos agregados de políticas administradas por el cliente y actualizaciones a la sección de permisos requeridos.                                                        | 21 de diciembre de 2020 |
| <a href="#">Compatibilidad con el control de acceso basado en atributos (ABAC)</a> | Contenido agregado para la característica ABAC.                                                                                                                                   | 24 de noviembre de 2020 |
| <a href="#">Compatibilidad con inscripción forzosa de MFA</a>                      | Actualizaciones para exigir a los usuarios que inscriban un dispositivo MFA al iniciar sesión.                                                                                    | 23 de noviembre de 2020 |



|                                                                                    |                                                                                                                                            |                         |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|
| <a href="#"><u>Support para WebAuthn</u></a>                                       | Contenido agregado para la nueva característica WebAuthn.                                                                                  | 20 de noviembre de 2020 |
| <a href="#"><u>Compatibilidad con Ping Identity</u></a>                            | Contenido agregado para integrarlo con productos de Ping Identity en calidad de proveedor de identidad externo compatible.                 | 26 de octubre de 2020   |
| <a href="#"><u>Support para OneLogin</u></a>                                       | Contenido agregado para integrarlo con OneLogin en calidad de proveedor de identidad externo compatible.                                   | 31 de julio de 2020     |
| <a href="#"><u>Compatibilidad con Okta</u></a>                                     | Contenido agregado para integrarlo con Okta en calidad de proveedor de identidad externo compatible.                                       | 28 de mayo de 2020      |
| <a href="#"><u>Compatibilidad con proveedor es de identidad externos</u></a>       | Referencias modificadas del directorio a la fuente de identidad y contenido agregado para admitir a los proveedores de identidad externos. | 26 de noviembre de 2019 |
| <a href="#"><u>Nueva configuración de MFA</u></a>                                  | Tema de la verificación en 2 pasos eliminado y nuevo tema de MFA agregado en su lugar.                                                     | 24 de octubre de 2019   |
| <a href="#"><u>Nueva configuración para agregar la verificación en 2 pasos</u></a> | Contenido agregado sobre cómo habilitar la verificación en dos pasos para los usuarios.                                                    | 16 de enero de 2019     |

|                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                                                                    |                       |
|-----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|
| <a href="#"><u>Compatibilidad con la duración de las sesiones de AWS cuentas de</u></a>                         | Contenido agregado sobre cómo definir la duración de la sesión de una AWS cuenta de.                                                                                                                                                                                                                                                                                                               | 30 de octubre de 2018 |
| <a href="#"><u>Nueva opción para usar el directorio de Identity Center</u></a>                                  | Contenido agregado para elegir un directorio de Identity Center o conectarse a un directorio existente en Active Directory.                                                                                                                                                                                                                                                                        | 17 de octubre de 2018 |
| <a href="#"><u>Compatibilidad con el estado de retransmisión y la duración de la sesión en aplicaciones</u></a> | Se ha agregado contenido sobre el estado de retransmisión y la duración de la sesión para las aplicaciones.                                                                                                                                                                                                                                                                                        | 10 de octubre de 2018 |
| <a href="#"><u>Compatibilidad adicional con las nuevas aplicaciones</u></a>                                     | Se agregó 4me, BambooHR, Bonusly, Citrix ShareFile, ClickTime, Convo, Deputy, Deskpro, Dome9, DruvalnSync, Egnyte, Engagedly, Expensify, Freshdesk, IdeaScale, Igloo, Jitbit, Kudos, LiquidFiles, Lucidchart, PurelyHR, Samanage, ScreenSteps, Sli.do, SmartSheet, Syncplicity, TalentLMS, Trello, UserVoice, Zoho, OpsGenie, DigiCert, WeekDone, ProdPad, y UserEcho al catálogo de aplicaciones. | 3 de agosto de 2018   |
| <a href="#"><u>Compatibilidad con el acceso de cuentas múltiples a cuentas de administración</u></a>            | Contenido agregado sobre cómo delegar a los usuarios el acceso de múltiples cuentas a una cuenta de administración.                                                                                                                                                                                                                                                                                | 9 de julio de 2018    |

[Compatibilidad con las nuevas aplicaciones](#)

Se agregó DocuSign, Keeper Security, y SugarCRM al catálogo de aplicaciones.

16 de marzo de 2018

[Obtener credenciales temporales para acceder a la CLI](#)

Información agregada acerca de cómo obtener credenciales temporales para ejecutar AWS CLI comandos de la.

22 de febrero de 2018

[Nueva guía](#)

Esta es la primera versión de la Guía del usuario de IAM Identity Center.

7 de diciembre de 2017

# AWS Glosario

Para obtener la AWS terminología más reciente, consulte el [AWS glosario](#) de la Glosario de AWS Referencia.

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.