aws

API Reference

AWS Wickr

API Version 2024-02-01

AWS Wickr: API Reference

Table of Contents

Welcome

Welcome to the *AWS Wickr API Reference*.

The AWS Wickr application programming interface (API) is designed for administrators to perform key tasks, such as creating and managing AWS Wickr, networks, users, security groups, bots and more. This guide provides detailed information about the AWS Wickr API, including operations, types, inputs and outputs, and error codes. You can use an AWS SDK, the AWS Command Line Interface (AWS CLI, or the REST API to make API calls for AWS Wickr.

Using AWS SDK

The SDK clients authenticate your requests by using access keys that you provide. For more information, see [Authentication and access using AWS SDKs and tools](#) in the *AWS SDKs and Tools Reference Guide*.

Using AWS CLI

Use your access keys with the AWS CLI to make API calls. For more information about setting up the AWS CLI, see [Getting started with the AWS CLI](#) in the *AWS Command Line Interface User Guide for Version 2*.

Using REST APIs

If you use REST to make API calls, you must authenticate your request by providing a signature. AWS Wickr supports Signature Version 4. For more information, see [AWS Signature Version 4 for API requests](#) in the *AWS Identity and Access Management User Guide*.

Access and permissions to the APIs can be controlled by AWS Identity and Access Management. The managed policy [AWSWickrFullAccess](#) grants full administrative permission to the AWS Wickr service APIs. For more information on restricting access to specific operations, see [Identity and access management for AWS Wickr](#) in the *AWS Wickr Administration Guide*.

Types of Errors:

The AWS Wickr APIs provide an HTTP interface. HTTP defines ranges of HTTP Status Codes for different types of error responses.

1. Client errors are indicated by HTTP Status Code class of 4xx
2. Service errors are indicated by HTTP Status Code class of 5xx

In this reference guide, the documentation for each API has an Errors section that includes a brief discussion about HTTP status codes. We recommend looking there as part of your investigation when you get an error.

This document was last published on December 23, 2025.

Actions

The following actions are supported:

- BatchCreateUser

- BatchDeleteUser

- BatchLookupUserUname

- BatchReinviteUser

- BatchResetDevicesForUser

- BatchToggleUserSuspendStatus

- CreateBot

- CreateDataRetentionBot

- CreateDataRetentionBotChallenge

- CreateNetwork

- CreateSecurityGroup

- DeleteBot

- DeleteDataRetentionBot

- DeleteNetwork

- DeleteSecurityGroup

- GetBot

- GetBotsCount

- GetDataRetentionBot

- GetGuestUserHistoryCount

- GetNetwork

- GetNetworkSettings

- GetOidcInfo

- GetSecurityGroup

- GetUser

- GetUsersCount

- ListBlockedGuestUsers

- ListBots

- ListDevicesForUser

- ListGuestUsers

- ListNetworks

- ListSecurityGroups

- ListSecurityGroupUsers

- ListUsers

- RegisterOidcConfig

- RegisterOidcConfigTest

- UpdateBot

- UpdateDataRetention

- UpdateGuestUser

- UpdateNetwork

- UpdateNetworkSettings

- UpdateSecurityGroup

- UpdateUser

BatchCreateUser

Creates multiple users in a specified Wickr network. This operation allows you to provision multiple user accounts simultaneously, optionally specifying security groups, and validation requirements for each user.

> **ⓘ Note**
>
> `codeValidation`, `inviteCode`, and `inviteCodeTtl` are restricted to networks under preview only.

Request Syntax

```
POST /networks/networkId/users HTTP/1.1
X-Client-Token: clientToken
Content-type: application/json

{
   "users": [
      {
         "codeValidation": boolean,
         "firstName": "string",
         "inviteCode": "string",
         "inviteCodeTtl": number,
         "lastName": "string",
         "securityGroupIds": [ "string" ],
         "username": "string"
      }
   ]
}
```

URI Request Parameters

The request uses the following URI parameters.

clientToken

A unique identifier for this request to ensure idempotency. If you retry a request with the same client token, the service will return the same response without creating duplicate users.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9-_:]+`

networkId

The ID of the Wickr network where users will be created.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

users

A list of user objects containing the details for each user to be created, including username, name, security groups, and optional invite codes. Maximum 50 users per batch request.

Type: Array of BatchCreateUserRequestItem objects

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "failed": [
      {
         "field": "string",
         "reason": "string",
         "userId": "string"
      }
   ],
   "message": "string",
   "successful": [
```

```
        {
            "cell": "string",
            "challengeFailures": number,
            "codeValidation": boolean,
            "countryCode": "string",
            "firstName": "string",
            "inviteCode": "string",
            "isAdmin": boolean,
            "isInviteExpired": boolean,
            "isUser": boolean,
            "lastName": "string",
            "otpEnabled": boolean,
            "scimId": "string",
            "securityGroups": [ "string" ],
            "status": number,
            "suspended": boolean,
            "type": "string",
            "uname": "string",
            "userId": "string",
            "username": "string"
        }
    ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

failed

A list of user creation attempts that failed, including error details explaining why each user could not be created.

Type: Array of BatchUserErrorResponseItem objects

message

A message indicating the overall result of the batch operation.

Type: String

Pattern: [\S\s]*

successful

A list of user objects that were successfully created, including their assigned user IDs and invite codes.

Type: Array of User objects

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

BatchDeleteUser

Deletes multiple users from a specified Wickr network. This operation permanently removes user accounts and their associated data from the network.

Request Syntax

```
POST /networks/networkId/users/batch-delete HTTP/1.1
X-Client-Token: clientToken
Content-type: application/json

{
    "userIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

clientToken

A unique identifier for this request to ensure idempotency. If you retry a request with the same client token, the service will return the same response without attempting to delete users again.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9-_:]+`

networkId

The ID of the Wickr network from which users will be deleted.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

userIds

A list of user IDs identifying the users to be deleted from the network. Maximum 50 users per batch request.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: [0-9]+

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "failed": [
      {
         "field": "string",
         "reason": "string",
         "userId": "string"
      }
   ],
   "message": "string",
   "successful": [
      {
         "userId": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

failed

A list of user deletion attempts that failed, including error details explaining why each user could not be deleted.

Type: Array of [BatchUserErrorResponseItem](#) objects

message

A message indicating the overall result of the batch deletion operation.

Type: String

Pattern: [\S\s]*

successful

A list of user IDs that were successfully deleted from the network.

Type: Array of [BatchUserSuccessResponseItem](#) objects

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError](#)

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

BatchLookupUserUname

Looks up multiple user usernames from their unique username hashes (unames). This operation allows you to retrieve the email addresses associated with a list of username hashes.

Request Syntax

```
POST /networks/networkId/users/uname-lookup HTTP/1.1
X-Client-Token: clientToken
Content-type: application/json

{
    "unames": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

clientToken

A unique identifier for this request to ensure idempotency.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9-_:]+`

networkId

The ID of the Wickr network where the users will be looked up.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

unames

A list of username hashes (unames) to look up. Each uname is a unique identifier for a user's username. Maximum 50 unames per batch request.

Type: Array of strings

Pattern: [\S\s]*

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "failed": [
      {
         "field": "string",
         "reason": "string",
         "uname": "string"
      }
   ],
   "message": "string",
   "successful": [
      {
         "uname": "string",
         "username": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

failed

A list of username hash lookup attempts that failed, including error details explaining why each lookup failed.

Type: Array of BatchUnameErrorResponseItem objects

message

A message indicating the overall result of the batch lookup operation.

Type: String

Pattern: [\S\s]*

successful

A list of successfully resolved username hashes with their corresponding email addresses.

Type: Array of BatchUnameSuccessResponseItem objects

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

BatchReinviteUser

Resends invitation codes to multiple users who have pending invitations in a Wickr network. This operation is useful when users haven't accepted their initial invitations or when invitations have expired.

Request Syntax

```
PATCH /networks/networkId/users/re-invite HTTP/1.1
X-Client-Token: clientToken
Content-type: application/json

{
    "userIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

clientToken

A unique identifier for this request to ensure idempotency.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9-_:]+`

networkId

The ID of the Wickr network where users will be reinvited.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

userIds

A list of user IDs identifying the users to be reinvited to the network. Maximum 50 users per batch request.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: [0-9]+

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "failed": [
      {
         "field": "string",
         "reason": "string",
         "userId": "string"
      }
   ],
   "message": "string",
   "successful": [
      {
         "userId": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

failed

A list of reinvitation attempts that failed, including error details explaining why each user could not be reinvited.

Type: Array of BatchUserErrorResponseItem objects

message

A message indicating the overall result of the batch reinvitation operation.

Type: String

Pattern: [\S\s]*

successful

A list of user IDs that were successfully reinvited.

Type: Array of BatchUserSuccessResponseItem objects

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

BatchResetDevicesForUser

Resets multiple devices for a specific user in a Wickr network. This operation forces the selected devices to log out and requires users to re-authenticate, which is useful for security purposes or when devices need to be revoked.

Request Syntax

```
PATCH /networks/networkId/users/userId/devices HTTP/1.1
X-Client-Token: clientToken
Content-type: application/json

{
   "appIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

clientToken

A unique identifier for this request to ensure idempotency.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9-_:]+`

networkId

The ID of the Wickr network containing the user whose devices will be reset.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

userId

The ID of the user whose devices will be reset.

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: `[0-9]+`

Required: Yes

Request Body

The request accepts the following data in JSON format.

appIds

A list of application IDs identifying the specific devices to be reset for the user. Maximum 50 devices per batch request.

Type: Array of strings

Pattern: `[\S\s]*`

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "failed": [
      {
         "appId": "string",
         "field": "string",
         "reason": "string"
      }
   ],
   "message": "string",
   "successful": [
      {
         "appId": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

failed

A list of device reset attempts that failed, including error details explaining why each device could not be reset.

Type: Array of BatchDeviceErrorResponseItem objects

message

A message indicating the overall result of the batch device reset operation.

Type: String

Pattern: `[\S\s]*`

successful

A list of application IDs that were successfully reset.

Type: Array of BatchDeviceSuccessResponseItem objects

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

BatchToggleUserSuspendStatus

Suspends or unsuspends multiple users in a Wickr network. Suspended users cannot access the network until they are unsuspended. This operation is useful for temporarily restricting access without deleting user accounts.

Request Syntax

```
PATCH /networks/networkId/users/toggleSuspend?suspend=suspend HTTP/1.1
X-Client-Token: clientToken
Content-type: application/json

{
    "userIds": [ "string" ]
}
```

URI Request Parameters

The request uses the following URI parameters.

clientToken

A unique identifier for this request to ensure idempotency.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9-_:]+`

networkId

The ID of the Wickr network where users will be suspended or unsuspended.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

suspend

A boolean value indicating whether to suspend (true) or unsuspend (false) the specified users.

Required: Yes

Request Body

The request accepts the following data in JSON format.

userIds

A list of user IDs identifying the users whose suspend status will be toggled. Maximum 50 users per batch request.

Type: Array of strings

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: [0-9]+

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "failed": [
      {
         "field": "string",
         "reason": "string",
         "userId": "string"
      }
   ],
   "message": "string",
   "successful": [
      {
         "userId": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

failed

> A list of suspend status toggle attempts that failed, including error details explaining why each user's status could not be changed.
>
> Type: Array of BatchUserErrorResponseItem objects

message

> A message indicating the overall result of the batch suspend status toggle operation.
>
> Type: String
>
> Pattern: [\S\s]*

successful

> A list of user IDs whose suspend status was successfully toggled.
>
> Type: Array of BatchUserSuccessResponseItem objects

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

> The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.
>
> **message**
>
> > A detailed message explaining what was wrong with the request and how to correct it.
>
> HTTP Status Code: 400

ForbiddenError

> Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

> A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError](#)

> One or more fields in the request failed validation. This error provides detailed information
> about which fields were invalid and why, allowing you to correct the request and retry.

reasons

> A list of validation error details, where each item identifies a specific field that failed
> validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the
following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateBot

Creates a new bot in a specified Wickr network. Bots are automated accounts that can send and receive messages, enabling integration with external systems and automation of tasks.

Request Syntax

```
POST /networks/networkId/bots HTTP/1.1
Content-type: application/json

{
   "challenge": "string",
   "displayName": "string",
   "groupId": "string",
   "username": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network where the bot will be created.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request accepts the following data in JSON format.

challenge

The password for the bot account.

Type: String

Pattern: [\S\s]*

Required: Yes

groupId

The ID of the security group to which the bot will be assigned.

Type: String

Pattern: [\S\s]*

Required: Yes

username

The username for the bot. This must be unique within the network and follow the network's naming conventions.

Type: String

Pattern: [\S\s]*

Required: Yes

displayName

The display name for the bot that will be visible to users in the network.

Type: String

Pattern: [\S\s]*

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "botId": "string",
    "displayName": "string",
    "groupId": "string",
```

```
    "message": "string",
    "networkId": "string",
    "username": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

botId

    The unique identifier assigned to the newly created bot.

    Type: String

    Length Constraints: Minimum length of 1. Maximum length of 10.

    Pattern: [0-9]+

displayName

    The display name of the newly created bot.

    Type: String

    Pattern: [\S\s]*

groupId

    The ID of the security group to which the bot was assigned.

    Type: String

    Pattern: [\S\s]*

message

    A message indicating the result of the bot creation operation.

    Type: String

    Pattern: [\S\s]*

networkId

The ID of the network where the bot was created.

Type: String

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

username

The username of the newly created bot.

Type: String

Pattern: `[\S\s]*`

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateDataRetentionBot

Creates a data retention bot in a Wickr network. Data retention bots are specialized bots that handle message archiving and compliance by capturing and storing messages for regulatory or organizational requirements.

Request Syntax

```
POST /networks/networkId/data-retention-bots HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network where the data retention bot will be created.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "message": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

message

A message indicating that the data retention bot was successfully provisioned.

Type: String

Pattern: `[\S\s]*`

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateDataRetentionBotChallenge

Creates a new challenge password for the data retention bot. This password is used for authentication when the bot connects to the network.

Request Syntax

```
POST /networks/networkId/data-retention-bots/challenge HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network containing the data retention bot.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "challenge": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

challenge

The newly generated challenge password for the data retention bot.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

> A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

> A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

> A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

> A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

> A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateNetwork

Creates a new Wickr network with specified access level and configuration. This operation provisions a new communication network for your organization.

Request Syntax

```
POST /networks HTTP/1.1
Content-type: application/json

{
   "accessLevel": "string",
   "enablePremiumFreeTrial": boolean,
   "encryptionKeyArn": "string",
   "networkName": "string"
}
```

URI Request Parameters

The request does not use any URI parameters.

Request Body

The request accepts the following data in JSON format.

accessLevel

The access level for the network. Valid values are STANDARD or PREMIUM, which determine the features and capabilities available to network members.

Type: String

Valid Values: STANDARD | PREMIUM

Required: Yes

networkName

The name for the new network. Must be between 1 and 20 characters.

Type: String

Pattern: [\S\s]*

Required: Yes

enablePremiumFreeTrial

Specifies whether to enable a premium free trial for the network. It is optional and has a default value as false. When set to true, the network starts with premium features for a limited trial period.

Type: Boolean

Required: No

encryptionKeyArn

The ARN of the AWS KMS customer managed key to use for encrypting sensitive data in the network.

Type: String

Pattern: `[\S\s]*`

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "encryptionKeyArn": "string",
    "networkId": "string",
    "networkName": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

encryptionKeyArn

The ARN of the KMS key being used to encrypt sensitive data in the network.

Type: String

Pattern: `[\S\s]*`

networkId

The unique identifier assigned to the newly created network.

Type: String

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

networkName

The name of the newly created network.

Type: String

Pattern: `[\S\s]*`

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

> A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

> A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

> A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

> A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

> A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError](#)

> One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

> A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

CreateSecurityGroup

Creates a new security group in a Wickr network. Security groups allow you to organize users and control their permissions, features, and security settings.

Request Syntax

```
POST /networks/networkId/security-groups HTTP/1.1
X-Client-Token: clientToken
Content-type: application/json

{
    "name": "string",
    "securityGroupSettings": {
        "enableGuestFederation": boolean,
        "enableRestrictedGlobalFederation": boolean,
        "federationMode": number,
        "globalFederation": boolean,
        "lockoutThreshold": number,
        "permittedNetworks": [ "string" ],
        "permittedWickrAwsNetworks": [
            {
                "networkId": "string",
                "region": "string"
            }
        ],
        "permittedWickrEnterpriseNetworks": [
            {
                "domain": "string",
                "networkId": "string"
            }
        ]
    }
}
```

URI Request Parameters

The request uses the following URI parameters.

clientToken

A unique identifier for this request to ensure idempotency.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9-_:]+`

networkId

The ID of the Wickr network where the security group will be created.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

name

The name for the new security group.

Type: String

Pattern: `[\S\s]*`

Required: Yes

securityGroupSettings

The configuration settings for the security group, including permissions, federation settings, and feature controls.

Type: SecurityGroupSettingsRequest object

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "securityGroup": {
```

```
      "activeDirectoryGuid": "string",
      "activeMembers": number,
      "botMembers": number,
      "id": "string",
      "isDefault": boolean,
      "modified": number,
      "name": "string",
      "securityGroupSettings": {
         "alwaysReauthenticate": boolean,
         "atakPackageValues": [ "string" ],
         "calling": {
            "canStart11Call": boolean,
            "canVideoCall": boolean,
            "forceTcpCall": boolean
         },
         "checkForUpdates": boolean,
         "enableAtak": boolean,
         "enableCrashReports": boolean,
         "enableFileDownload": boolean,
         "enableGuestFederation": boolean,
         "enableNotificationPreview": boolean,
         "enableOpenAccessOption": boolean,
         "enableRestrictedGlobalFederation": boolean,
         "federationMode": number,
         "filesEnabled": boolean,
         "forceDeviceLockout": number,
         "forceOpenAccess": boolean,
         "forceReadReceipts": boolean,
         "globalFederation": boolean,
         "isAtoEnabled": boolean,
         "isLinkPreviewEnabled": boolean,
         "locationAllowMaps": boolean,
         "locationEnabled": boolean,
         "lockoutThreshold": number,
         "maxAutoDownloadSize": number,
         "maxBor": number,
         "maxTtl": number,
         "messageForwardingEnabled": boolean,
         "passwordRequirements": {
            "lowercase": number,
            "minLength": number,
            "numbers": number,
            "symbols": number,
            "uppercase": number
```

```
        },
        "permittedNetworks": [ "string" ],
        "permittedWickrAwsNetworks": [
          {
            "networkId": "string",
            "region": "string"
          }
        ],
        "permittedWickrEnterpriseNetworks": [
          {
            "domain": "string",
            "networkId": "string"
          }
        ],
        "presenceEnabled": boolean,
        "quickResponses": [ "string" ],
        "showMasterRecoveryKey": boolean,
        "shredder": {
          "canProcessManually": boolean,
          "intensity": number
        },
        "ssoMaxIdleMinutes": number
      }
    }
  }
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

securityGroup

The details of the newly created security group, including its ID, name, and settings.

Type: SecurityGroup object

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

[ResourceNotFoundError](#)

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

[UnauthorizedError](#)

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError](#)

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)

- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteBot

Deletes a bot from a specified Wickr network. This operation permanently removes the bot account and its associated data from the network.

Request Syntax

```
DELETE /networks/networkId/bots/botId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

botId

> The unique identifier of the bot to be deleted.
>
> Length Constraints: Minimum length of 1. Maximum length of 10.
>
> Pattern: [0-9]+
>
> Required: Yes

networkId

> The ID of the Wickr network from which the bot will be deleted.
>
> Length Constraints: Fixed length of 8.
>
> Pattern: [0-9]{8}
>
> Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
    "message": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

message

A message indicating the result of the bot deletion operation.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do
not meet the API requirements, such as invalid field values, missing required parameters, or
improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user
does not have the necessary permissions to perform the requested operation, even though they
are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteDataRetentionBot

Deletes the data retention bot from a Wickr network. This operation permanently removes the bot and all its associated data from the database.

Request Syntax

```
DELETE /networks/networkId/data-retention-bots HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network from which the data retention bot will be deleted.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "message": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

message

A message indicating that the data retention bot and all associated data were successfully deleted.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the
following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteNetwork

Deletes a Wickr network and all its associated resources, including users, bots, security groups, and settings. This operation is permanent and cannot be undone.

Request Syntax

```
DELETE /networks/networkId HTTP/1.1
X-Client-Token: clientToken
```

URI Request Parameters

The request uses the following URI parameters.

clientToken

A unique identifier for this request to ensure idempotency. If you retry a request with the same client token, the service will return the same response without attempting to delete the network again.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9-_:]+`

networkId

The ID of the Wickr network to delete.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
    "message": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

message

A message indicating that the network deletion has been initiated successfully.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

> A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError](#)

> One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.
>
> **reasons**
>
> > A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.
>
> HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

DeleteSecurityGroup

Deletes a security group from a Wickr network. This operation cannot be performed on the default security group.

Request Syntax

```
DELETE /networks/networkId/security-groups/groupId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

groupId

The unique identifier of the security group to delete.

Pattern: `[\S\s]*`

Required: Yes

networkId

The ID of the Wickr network from which the security group will be deleted.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json
```

```
{
    "groupId": "string",
    "message": "string",
    "networkId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

groupId

The ID of the security group that was deleted.

Type: String

Pattern: [\S\s]*

message

A message indicating the result of the security group deletion operation.

Type: String

Pattern: [\S\s]*

networkId

The ID of the network from which the security group was deleted.

Type: String

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetBot

Retrieves detailed information about a specific bot in a Wickr network, including its status, group membership, and authentication details.

Request Syntax

```
GET /networks/networkId/bots/botId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

botId

The unique identifier of the bot to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: `[0-9]+`

Required: Yes

networkId

The ID of the Wickr network containing the bot.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
    "botId": "string",
    "displayName": "string",
    "groupId": "string",
    "hasChallenge": boolean,
    "lastLogin": "string",
    "pubkey": "string",
    "status": number,
    "suspended": boolean,
    "uname": "string",
    "username": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

botId

The unique identifier of the bot.

Type: String

Pattern: [\S\s]*

displayName

The display name of the bot that is visible to users.

Type: String

Pattern: [\S\s]*

groupId

The ID of the security group to which the bot belongs.

Type: String

Pattern: [\S\s]*

hasChallenge

Indicates whether the bot has a password set.

Type: Boolean

lastLogin

The timestamp of the bot's last login.

Type: String

Pattern: [\S\s]*

pubkey

The public key of the bot used for encryption.

Type: String

Pattern: [\S\s]*

status

The current status of the bot (1 for pending, 2 for active).

Type: Integer

suspended

Indicates whether the bot is currently suspended.

Type: Boolean

uname

The unique username hash identifier for the bot.

Type: String

Pattern: [\S\s]*

username

The username of the bot.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

> A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

> A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

> A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

> A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetBotsCount

Retrieves the count of bots in a Wickr network, categorized by their status (pending, active, and total).

Request Syntax

```
GET /networks/networkId/bots/count HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network for which to retrieve bot counts.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "active": number,
    "pending": number,
    "total": number
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

active

The number of bots with active status.

Type: Integer

pending

The number of bots with pending status (invited but not yet activated).

Type: Integer

total

The total number of bots in the network (active and pending).

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetDataRetentionBot

Retrieves information about the data retention bot in a Wickr network, including its status and whether the data retention service is enabled.

Request Syntax

```
GET /networks/networkId/data-retention-bots HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network containing the data retention bot.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "botExists": boolean,
   "botName": "string",
   "isBotActive": boolean,
   "isDataRetentionBotRegistered": boolean,
   "isDataRetentionServiceEnabled": boolean,
   "isPubkeyMsgAcked": boolean
```

```
    }
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

botExists

Indicates whether a data retention bot exists in the network.

Type: Boolean

botName

The name of the data retention bot.

Type: String

Pattern: [\S\s]*

isBotActive

Indicates whether the data retention bot is active and operational.

Type: Boolean

isDataRetentionBotRegistered

Indicates whether the data retention bot has been registered with the network.

Type: Boolean

isDataRetentionServiceEnabled

Indicates whether the data retention service is enabled for the network.

Type: Boolean

isPubkeyMsgAcked

Indicates whether the public key message has been acknowledged by the bot.

Type: Boolean

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

> The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.
>
> **message**
>
>> A detailed message explaining what was wrong with the request and how to correct it.
>
> HTTP Status Code: 400

ForbiddenError

> Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.
>
> **message**
>
>> A message explaining why access was denied and what permissions are required.
>
> HTTP Status Code: 403

InternalServerError

> An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.
>
> **message**
>
>> A message describing the internal server error that occurred.
>
> HTTP Status Code: 500

RateLimitError

> The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

> A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

> A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

> A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

> A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetGuestUserHistoryCount

Retrieves historical guest user count data for a Wickr network, showing the number of guest users per billing period over the past 90 days.

Request Syntax

```
GET /networks/networkId/guest-users/count HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network for which to retrieve guest user history.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "history": [
      {
         "count": "string",
         "month": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

history

A list of historical guest user counts, organized by month and billing period.

Type: Array of GuestUserHistoryCount objects

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

> A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

> A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

> A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

> A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

> A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetNetwork

Retrieves detailed information about a specific Wickr network, including its configuration, access level, and status.

Request Syntax

```
GET /networks/networkId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network to retrieve.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "accessLevel": "string",
   "awsAccountId": "string",
   "encryptionKeyArn": "string",
   "freeTrialExpiration": "string",
   "migrationState": number,
   "networkArn": "string",
   "networkId": "string",
   "networkName": "string",
```

```
    "standing": number
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

accessLevel

The access level of the network (STANDARD or PREMIUM), which determines available features and capabilities.

Type: String

Valid Values: STANDARD | PREMIUM

awsAccountId

The AWS account ID that owns the network.

Type: String

Pattern: [\S\s]*

networkArn

The Amazon Resource Name (ARN) of the network.

Type: String

Pattern: [\S\s]*

networkId

The unique identifier of the network.

Type: String

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

networkName

The name of the network.

Type: String

Pattern: [\S\s]*

encryptionKeyArn

The ARN of the AWS KMS customer managed key used for encrypting sensitive data in the network.

Type: String

Pattern: [\S\s]*

freeTrialExpiration

The expiration date and time for the network's free trial period, if applicable.

Type: String

Pattern: [\S\s]*

migrationState

The SSO redirect URI migration state, managed by the SSO redirect migration wizard. Values: 0 (not started), 1 (in progress), or 2 (completed).

Type: Integer

standing

The current standing or status of the network.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

[UnauthorizedError]

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError]

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2]
- [AWS SDK for .NET]
- [AWS SDK for C++]
- [AWS SDK for Go v2]
- [AWS SDK for Java V2]
- [AWS SDK for JavaScript V3]
- [AWS SDK for Kotlin]

- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetNetworkSettings

Retrieves all network-level settings for a Wickr network, including client metrics, data retention, and other configuration options.

Request Syntax

```
GET /networks/networkId/settings HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network whose settings will be retrieved.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "settings": [
      {
         "optionName": "string",
         "type": "string",
         "value": "string"
      }
```

```
    ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

settings

A list of network settings, where each setting includes a name, value, and type.

Type: Array of Setting objects

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetOidcInfo

Retrieves the OpenID Connect (OIDC) configuration for a Wickr network, including SSO settings and optional token information if access token parameters are provided.

Request Syntax

```
GET /networks/networkId/oidc?
certificate=certificate&clientId=clientId&clientSecret=clientSecret&code=code&codeVerifier=code
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

certificate

The CA certificate for secure communication with the OIDC provider (optional).

Pattern: [\S\s]*

clientId

The OAuth client ID for retrieving access tokens (optional).

Pattern: [\S\s]*

clientSecret

The OAuth client secret for retrieving access tokens (optional).

Pattern: [\S\s]*

code

The authorization code for retrieving access tokens (optional).

Pattern: [\S\s]*

codeVerifier

The PKCE code verifier for enhanced security in the OAuth flow (optional).

Pattern: [\S\s]*

grantType

The OAuth grant type for retrieving access tokens (optional).

Pattern: `[\S\s]*`

networkId

The ID of the Wickr network whose OIDC configuration will be retrieved.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

redirectUri

The redirect URI for the OAuth flow (optional).

Pattern: `[\S\s]*`

url

The URL for the OIDC provider (optional).

Pattern: `[\S\s]*`

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "openidConnectInfo": {
      "applicationId": number,
      "applicationName": "string",
      "caCertificate": "string",
      "clientId": "string",
      "clientSecret": "string",
      "companyId": "string",
```

```
      "customUsername": "string",
      "extraAuthParams": "string",
      "issuer": "string",
      "redirectUrl": "string",
      "scopes": "string",
      "secret": "string",
      "ssoTokenBufferMinutes": number,
      "userId": "string"
   },
   "tokenInfo": {
      "accessToken": "string",
      "codeChallenge": "string",
      "codeVerifier": "string",
      "expiresIn": number,
      "idToken": "string",
      "refreshToken": "string",
      "tokenType": "string"
   }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

openidConnectInfo

The OpenID Connect configuration information for the network, including issuer, client ID, scopes, and other SSO settings.

Type: OidcConfigInfo object

tokenInfo

OAuth token information including access token, refresh token, and expiration details (only present if token parameters were provided in the request).

Type: OidcTokenInfo object

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetSecurityGroup

Retrieves detailed information about a specific security group in a Wickr network, including its settings, member counts, and configuration.

Request Syntax

```
GET /networks/networkId/security-groups/groupId HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

groupId

The unique identifier of the security group to retrieve.

Pattern: `[\S\s]*`

Required: Yes

networkId

The ID of the Wickr network containing the security group.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "securityGroup": {
```

```
      "activeDirectoryGuid": "string",
      "activeMembers": number,
      "botMembers": number,
      "id": "string",
      "isDefault": boolean,
      "modified": number,
      "name": "string",
      "securityGroupSettings": {
         "alwaysReauthenticate": boolean,
         "atakPackageValues": [ "string" ],
         "calling": {
            "canStart11Call": boolean,
            "canVideoCall": boolean,
            "forceTcpCall": boolean
         },
         "checkForUpdates": boolean,
         "enableAtak": boolean,
         "enableCrashReports": boolean,
         "enableFileDownload": boolean,
         "enableGuestFederation": boolean,
         "enableNotificationPreview": boolean,
         "enableOpenAccessOption": boolean,
         "enableRestrictedGlobalFederation": boolean,
         "federationMode": number,
         "filesEnabled": boolean,
         "forceDeviceLockout": number,
         "forceOpenAccess": boolean,
         "forceReadReceipts": boolean,
         "globalFederation": boolean,
         "isAtoEnabled": boolean,
         "isLinkPreviewEnabled": boolean,
         "locationAllowMaps": boolean,
         "locationEnabled": boolean,
         "lockoutThreshold": number,
         "maxAutoDownloadSize": number,
         "maxBor": number,
         "maxTtl": number,
         "messageForwardingEnabled": boolean,
         "passwordRequirements": {
            "lowercase": number,
            "minLength": number,
            "numbers": number,
            "symbols": number,
            "uppercase": number
```

```
        },
        "permittedNetworks": [ "string" ],
        "permittedWickrAwsNetworks": [
            {
                "networkId": "string",
                "region": "string"
            }
        ],
        "permittedWickrEnterpriseNetworks": [
            {
                "domain": "string",
                "networkId": "string"
            }
        ],
        "presenceEnabled": boolean,
        "quickResponses": [ "string" ],
        "showMasterRecoveryKey": boolean,
        "shredder": {
            "canProcessManually": boolean,
            "intensity": number
        },
        "ssoMaxIdleMinutes": number
    }
}
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

securityGroup

The detailed information about the security group, including all its settings and member counts.

Type: SecurityGroup object

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- [AWS SDK for Java V2](#)

- [AWS SDK for JavaScript V3](#)

- [AWS SDK for Kotlin](#)

- [AWS SDK for PHP V3](#)

- [AWS SDK for Python](#)

- [AWS SDK for Ruby V3](#)

GetUser

Retrieves detailed information about a specific user in a Wickr network, including their profile, status, and activity history.

Request Syntax

```
GET /networks/networkId/users/userId?endTime=endTime&startTime=startTime HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

endTime

The end time for filtering the user's last activity. Only activity before this timestamp will be considered. Time is specified in epoch seconds.

networkId

The ID of the Wickr network containing the user.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

startTime

The start time for filtering the user's last activity. Only activity after this timestamp will be considered. Time is specified in epoch seconds.

userId

The unique identifier of the user to retrieve.

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: `[0-9]+`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "firstName": "string",
   "isAdmin": boolean,
   "lastActivity": number,
   "lastLogin": number,
   "lastName": "string",
   "securityGroupIds": [ "string" ],
   "status": number,
   "suspended": boolean,
   "userId": "string",
   "username": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

userId

The unique identifier of the user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: [0-9]+

firstName

The first name of the user.

Type: String

Pattern: [\S\s]*

isAdmin

Indicates whether the user has administrator privileges in the network.

Type: Boolean

lastActivity

The timestamp of the user's last activity in the network, specified in epoch seconds.

Type: Integer

lastLogin

The timestamp of the user's last login to the network, specified in epoch seconds.

Type: Integer

lastName

The last name of the user.

Type: String

Pattern: [\S\s]*

securityGroupIds

A list of security group IDs to which the user belongs.

Type: Array of strings

Pattern: [\S]+

status

The current status of the user (1 for pending, 2 for active).

Type: Integer

suspended

Indicates whether the user is currently suspended.

Type: Boolean

username

The email address or username of the user.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time.
Wait a moment and retry the request. Consider implementing exponential backoff in your
application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a
network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error
occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information
about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed
validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

GetUsersCount

Retrieves the count of users in a Wickr network, categorized by their status (pending, active, rejected) and showing how many users can still be added.

Request Syntax

```
GET /networks/networkId/users/count HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network for which to retrieve user counts.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "active": number,
   "pending": number,
   "rejected": number,
   "remaining": number,
   "total": number
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

active

The number of users with active status in the network.

Type: Integer

pending

The number of users with pending status (invited but not yet accepted).

Type: Integer

rejected

The number of users who have rejected network invitations.

Type: Integer

remaining

The number of additional users that can be added to the network while maintaining premium free trial eligibility.

Type: Integer

total

The total number of users in the network (active and pending combined).

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin

- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

ListBlockedGuestUsers

Retrieves a paginated list of guest users who have been blocked from a Wickr network. You can filter and sort the results.

Request Syntax

```
GET /networks/networkId/guest-users/blocklist?
admin=admin&maxResults=maxResults&nextToken=nextToken&sortDirection=sortDirection&sortFields=so
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

admin

Filter results to only include blocked guest users that were blocked by this administrator.

Pattern: [\S\s]*

maxResults

The maximum number of blocked guest users to return in a single page. Valid range is 1-100. Default is 10.

networkId

The ID of the Wickr network from which to list blocked guest users.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

nextToken

The token for retrieving the next page of results. This is returned from a previous request when there are more results available.

Pattern: [\S\s]*

sortDirection

The direction to sort results. Valid values are 'ASC' (ascending) or 'DESC' (descending). Default is 'DESC'.

Valid Values: ASC | DESC

sortFields

The field to sort blocked guest users by. Accepted values include 'username', 'admin', and 'modified'.

Pattern: [\S\s]*

username

Filter results to only include blocked guest users with usernames matching this value.

Pattern: [\S\s]*

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "blocklist": [
      {
         "admin": "string",
         "modified": "string",
         "username": "string",
         "usernameHash": "string"
      }
   ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

blocklist

   A list of blocked guest user objects within the current page.

   Type: Array of BlockedGuestUser objects

nextToken

   The token to use for retrieving the next page of results. If this is not present, there are no more
   results.

   Type: String

   Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

   The request was invalid or malformed. This error occurs when the request parameters do
   not meet the API requirements, such as invalid field values, missing required parameters, or
   improperly formatted data.

   message

      A detailed message explaining what was wrong with the request and how to correct it.

   HTTP Status Code: 400

ForbiddenError

   Access to the requested resource is forbidden. This error occurs when the authenticated user
   does not have the necessary permissions to perform the requested operation, even though they
   are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListBots

Retrieves a paginated list of bots in a specified Wickr network. You can filter and sort the results based on various criteria.

Request Syntax

```
GET /networks/networkId/bots?
displayName=displayName&groupId=groupId&maxResults=maxResults&nextToken=nextToken&sortDirection
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

displayName

> Filter results to only include bots with display names matching this value.

> Pattern: `[\S\s]*`

groupId

> Filter results to only include bots belonging to this security group.

> Pattern: `[\S\s]*`

maxResults

> The maximum number of bots to return in a single page. Valid range is 1-100. Default is 10.

networkId

> The ID of the Wickr network from which to list bots.

> Length Constraints: Fixed length of 8.

> Pattern: `[0-9]{8}`

> Required: Yes

nextToken

> The token for retrieving the next page of results. This is returned from a previous request when there are more results available.

Pattern: [\S\s]*

sortDirection

The direction to sort results. Valid values are 'ASC' (ascending) or 'DESC' (descending). Default is 'DESC'.

Valid Values: ASC | DESC

sortFields

The fields to sort bots by. Multiple fields can be specified by separating them with '+'. Accepted values include 'username', 'firstName', 'displayName', 'status', and 'groupId'.

Pattern: [\S\s]*

status

Filter results to only include bots with this status (1 for pending, 2 for active).

username

Filter results to only include bots with usernames matching this value.

Pattern: [\S\s]*

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "bots": [
      {
         "botId": "string",
         "displayName": "string",
         "groupId": "string",
         "hasChallenge": boolean,
         "lastLogin": "string",
         "pubkey": "string",
```

```
            "status": number,
            "suspended": boolean,
            "uname": "string",
            "username": "string"
        }
    ],
    "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

bots

>   A list of bot objects matching the specified filters and within the current page.

>   Type: Array of Bot objects

nextToken

>   The token to use for retrieving the next page of results. If this is not present, there are no more results.

>   Type: String

>   Pattern: `[\S\s]*`

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

>   The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

>   **message**

>>   A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListDevicesForUser

Retrieves a paginated list of devices associated with a specific user in a Wickr network. This operation returns information about all devices where the user has logged into Wickr.

Request Syntax

```
GET /networks/networkId/users/userId/devices?
maxResults=maxResults&nextToken=nextToken&sortDirection=sortDirection&sortFields=sortFields
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

maxResults

   The maximum number of devices to return in a single page. Valid range is 1-100. Default is 10.

networkId

   The ID of the Wickr network containing the user.

   Length Constraints: Fixed length of 8.

   Pattern: `[0-9]{8}`

   Required: Yes

nextToken

   The token for retrieving the next page of results. This is returned from a previous request when there are more results available.

   Pattern: `[\S\s]*`

sortDirection

   The direction to sort results. Valid values are 'ASC' (ascending) or 'DESC' (descending). Default is 'DESC'.

   Valid Values: ASC | DESC

sortFields

The fields to sort devices by. Multiple fields can be specified by separating them with '+'. Accepted values include 'lastlogin', 'type', 'suspend', and 'created'.

Pattern: `[\S\s]*`

userId

The unique identifier of the user whose devices will be listed.

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: `[0-9]+`

Required: Yes

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "devices": [
      {
         "appId": "string",
         "created": "string",
         "lastLogin": "string",
         "statusText": "string",
         "suspend": boolean,
         "type": "string"
      }
   ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

devices

A list of device objects associated with the user within the current page.

Type: Array of BasicDeviceObject objects

nextToken

The token to use for retrieving the next page of results. If this is not present, there are no more results.

Type: String

Pattern: `[\S\s]*`

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError](#)

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

ListGuestUsers

Retrieves a paginated list of guest users who have communicated with your Wickr network. Guest users are external users from federated networks who can communicate with network members.

Request Syntax

```
GET /networks/networkId/guest-users?
billingPeriod=billingPeriod&maxResults=maxResults&nextToken=nextToken&sortDirection=sortDirecti
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

billingPeriod

Filter results to only include guest users from this billing period (e.g., '2024-01').

Pattern: `[\S\s]*`

maxResults

The maximum number of guest users to return in a single page. Valid range is 1-100. Default is 10.

networkId

The ID of the Wickr network from which to list guest users.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

nextToken

The token for retrieving the next page of results. This is returned from a previous request when there are more results available.

Pattern: `[\S\s]*`

sortDirection

The direction to sort results. Valid values are 'ASC' (ascending) or 'DESC' (descending). Default is 'DESC'.

Valid Values: ASC | DESC

sortFields

The field to sort guest users by. Accepted values include 'username' and 'billingPeriod'.

Pattern: [\S\s]*

username

Filter results to only include guest users with usernames matching this value.

Pattern: [\S\s]*

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "guestlist": [
      {
         "billingPeriod": "string",
         "username": "string",
         "usernameHash": "string"
      }
   ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

guestlist

A list of guest user objects within the current page.

Type: Array of GuestUser objects

nextToken

The token to use for retrieving the next page of results. If this is not present, there are no more results.

Type: String

Pattern: `[\S\s]*`

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListNetworks

Retrieves a paginated list of all Wickr networks associated with your AWS account. You can sort the results by network ID or name.

Request Syntax

```
GET /networks?
maxResults=maxResults&nextToken=nextToken&sortDirection=sortDirection&sortFields=sortFields
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

maxResults

The maximum number of networks to return in a single page. Valid range is 1-100. Default is 10.

nextToken

The token for retrieving the next page of results. This is returned from a previous request when there are more results available.

Pattern: [\S\s]*

sortDirection

The direction to sort results. Valid values are 'ASC' (ascending) or 'DESC' (descending). Default is 'DESC'.

Valid Values: ASC | DESC

sortFields

The field to sort networks by. Accepted values are 'networkId' and 'networkName'. Default is 'networkId'.

Pattern: [\S\s]*

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "networks": [
      {
         "accessLevel": "string",
         "awsAccountId": "string",
         "encryptionKeyArn": "string",
         "freeTrialExpiration": "string",
         "migrationState": number,
         "networkArn": "string",
         "networkId": "string",
         "networkName": "string",
         "standing": number
      }
   ],
   "nextToken": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

networks

   A list of network objects for the AWS account.

   Type: Array of Network objects

nextToken

   The token to use for retrieving the next page of results. If this is not present, there are no more results.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++

- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

ListSecurityGroups

Retrieves a paginated list of security groups in a specified Wickr network. You can sort the results by various criteria.

Request Syntax

```
GET /networks/networkId/security-groups?
maxResults=maxResults&nextToken=nextToken&sortDirection=sortDirection&sortFields=sortFields
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

maxResults

The maximum number of security groups to return in a single page. Valid range is 1-100. Default is 10.

networkId

The ID of the Wickr network from which to list security groups.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

nextToken

The token for retrieving the next page of results. This is returned from a previous request when there are more results available.

Pattern: `[\S\s]*`

sortDirection

The direction to sort results. Valid values are 'ASC' (ascending) or 'DESC' (descending). Default is 'DESC'.

Valid Values: ASC | DESC

sortFields

The field to sort security groups by. Accepted values include 'id' and 'name'.

Pattern: [\S\s]*

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json


{
   "nextToken": "string",
   "securityGroups": [
      {
         "activeDirectoryGuid": "string",
         "activeMembers": number,
         "botMembers": number,
         "id": "string",
         "isDefault": boolean,
         "modified": number,
         "name": "string",
         "securityGroupSettings": {
            "alwaysReauthenticate": boolean,
            "atakPackageValues": [ "string" ],
            "calling": {
               "canStart11Call": boolean,
               "canVideoCall": boolean,
               "forceTcpCall": boolean
            },
            "checkForUpdates": boolean,
            "enableAtak": boolean,
            "enableCrashReports": boolean,
            "enableFileDownload": boolean,
            "enableGuestFederation": boolean,
            "enableNotificationPreview": boolean,
            "enableOpenAccessOption": boolean,
            "enableRestrictedGlobalFederation": boolean,
            "federationMode": number,
```

```
            "filesEnabled": boolean,
            "forceDeviceLockout": number,
            "forceOpenAccess": boolean,
            "forceReadReceipts": boolean,
            "globalFederation": boolean,
            "isAtoEnabled": boolean,
            "isLinkPreviewEnabled": boolean,
            "locationAllowMaps": boolean,
            "locationEnabled": boolean,
            "lockoutThreshold": number,
            "maxAutoDownloadSize": number,
            "maxBor": number,
            "maxTtl": number,
            "messageForwardingEnabled": boolean,
            "passwordRequirements": {
                "lowercase": number,
                "minLength": number,
                "numbers": number,
                "symbols": number,
                "uppercase": number
            },
            "permittedNetworks": [ "string" ],
            "permittedWickrAwsNetworks": [
                {
                    "networkId": "string",
                    "region": "string"
                }
            ],
            "permittedWickrEnterpriseNetworks": [
                {
                    "domain": "string",
                    "networkId": "string"
                }
            ],
            "presenceEnabled": boolean,
            "quickResponses": [ "string" ],
            "showMasterRecoveryKey": boolean,
            "shredder": {
                "canProcessManually": boolean,
                "intensity": number
            },
            "ssoMaxIdleMinutes": number
        }
    }
```

```
    ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The token to use for retrieving the next page of results. If this is not present, there are no more results.

Type: String

Pattern: [\S\s]*

securityGroups

A list of security group objects in the current page.

Type: Array of SecurityGroup objects

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListSecurityGroupUsers

Retrieves a paginated list of users who belong to a specific security group in a Wickr network.

Request Syntax

```
GET /networks/networkId/security-groups/groupId/users?
maxResults=maxResults&nextToken=nextToken&sortDirection=sortDirection&sortFields=sortFields
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

groupId

The unique identifier of the security group whose users will be listed.

Pattern: [\S\s]*

Required: Yes

maxResults

The maximum number of users to return in a single page. Valid range is 1-100. Default is 10.

networkId

The ID of the Wickr network containing the security group.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

nextToken

The token for retrieving the next page of results. This is returned from a previous request when there are more results available.

Pattern: [\S\s]*

sortDirection

The direction to sort results. Valid values are 'ASC' (ascending) or 'DESC' (descending). Default is 'DESC'.

Valid Values: ASC | DESC

sortFields

The field to sort users by. Multiple fields can be specified by separating them with '+'. Accepted values include 'username', 'firstName', and 'lastName'.

Pattern: [\S\s]*

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "nextToken": "string",
   "users": [
      {
         "cell": "string",
         "challengeFailures": number,
         "codeValidation": boolean,
         "countryCode": "string",
         "firstName": "string",
         "inviteCode": "string",
         "isAdmin": boolean,
         "isInviteExpired": boolean,
         "isUser": boolean,
         "lastName": "string",
         "otpEnabled": boolean,
         "scimId": "string",
         "securityGroups": [ "string" ],
         "status": number,
         "suspended": boolean,
```

```
            "type": "string",
            "uname": "string",
            "userId": "string",
            "username": "string"
        }
    ]
 }
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

users

A list of user objects belonging to the security group within the current page.

Type: Array of User objects

nextToken

The token to use for retrieving the next page of results. If this is not present, there are no more results.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

ListUsers

Retrieves a paginated list of users in a specified Wickr network. You can filter and sort the results based on various criteria such as name, status, or security group membership.

Request Syntax

```
GET /networks/networkId/users?
firstName=firstName&groupId=groupId&lastName=lastName&maxResults=maxResults&nextToken=nextToken
 HTTP/1.1
```

URI Request Parameters

The request uses the following URI parameters.

firstName

Filter results to only include users with first names matching this value.

Pattern: [\S\s]*

groupId

Filter results to only include users belonging to this security group.

Pattern: [\S\s]*

lastName

Filter results to only include users with last names matching this value.

Pattern: [\S\s]*

maxResults

The maximum number of users to return in a single page. Valid range is 1-100. Default is 10.

networkId

The ID of the Wickr network from which to list users.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

nextToken

The token for retrieving the next page of results. This is returned from a previous request when there are more results available.

Pattern: [\S\s]*

sortDirection

The direction to sort results. Valid values are 'ASC' (ascending) or 'DESC' (descending). Default is 'DESC'.

Valid Values: ASC | DESC

sortFields

The fields to sort users by. Multiple fields can be specified by separating them with '+'. Accepted values include 'username', 'firstName', 'lastName', 'status', and 'groupId'.

Pattern: [\S\s]*

status

Filter results to only include users with this status (1 for pending, 2 for active).

username

Filter results to only include users with usernames matching this value.

Pattern: [\S\s]*

Request Body

The request does not have a request body.

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "nextToken": "string",
    "users": [
```

```
        {
            "cell": "string",
            "challengeFailures": number,
            "codeValidation": boolean,
            "countryCode": "string",
            "firstName": "string",
            "inviteCode": "string",
            "isAdmin": boolean,
            "isInviteExpired": boolean,
            "isUser": boolean,
            "lastName": "string",
            "otpEnabled": boolean,
            "scimId": "string",
            "securityGroups": [ "string" ],
            "status": number,
            "suspended": boolean,
            "type": "string",
            "uname": "string",
            "userId": "string",
            "username": "string"
        }
    ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

nextToken

The token to use for retrieving the next page of results. If this is not present, there are no more results.

Type: String

Pattern: [\S\s]*

users

A list of user objects matching the specified filters and within the current page.

Type: Array of User objects

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

[BadRequestError](#)

> The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.
>
> **message**
>
> > A detailed message explaining what was wrong with the request and how to correct it.
>
> HTTP Status Code: 400

[ForbiddenError](#)

> Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.
>
> **message**
>
> > A message explaining why access was denied and what permissions are required.
>
> HTTP Status Code: 403

[InternalServerError](#)

> An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.
>
> **message**
>
> > A message describing the internal server error that occurred.
>
> HTTP Status Code: 500

[RateLimitError](#)

> The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

> A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

> A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

> A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

> A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

RegisterOidcConfig

Registers and saves an OpenID Connect (OIDC) configuration for a Wickr network, enabling Single Sign-On (SSO) authentication through an identity provider.

Request Syntax

```
POST /networks/networkId/oidc/save HTTP/1.1
Content-type: application/json

{
   "companyId": "string",
   "customUsername": "string",
   "extraAuthParams": "string",
   "issuer": "string",
   "scopes": "string",
   "secret": "string",
   "ssoTokenBufferMinutes": number,
   "userId": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

networkId

   The ID of the Wickr network for which OIDC will be configured.

   Length Constraints: Fixed length of 8.

   Pattern: [0-9]{8}

   Required: Yes

Request Body

The request accepts the following data in JSON format.

companyId

   Custom identifier your end users will use to sign in with SSO.

Type: String

Pattern: [\S\s]*

Required: Yes

issuer

The issuer URL of the OIDC provider (e.g., 'https://login.example.com').

Type: String

Pattern: [\S\s]*

Required: Yes

scopes

The OAuth scopes to request from the OIDC provider (e.g., 'openid profile email').

Type: String

Pattern: [\S\s]*

Required: Yes

customUsername

A custom field mapping to extract the username from the OIDC token (optional).

> ⓘ **Note**
>
> The customUsername is only required if you use something other than email as the username field.

Type: String

Pattern: [\S\s]*

Required: No

extraAuthParams

Additional authentication parameters to include in the OIDC flow (optional).

Type: String

Pattern: [\S\s]*

Required: No

secret

The client secret for authenticating with the OIDC provider (optional).

Type: String

Pattern: [\S\s]*

Required: No

ssoTokenBufferMinutes

The buffer time in minutes before the SSO token expires to refresh it (optional).

Type: Integer

Required: No

userId

Unique identifier provided by your identity provider to authenticate the access request. Also referred to as clientID.

Type: String

Pattern: [\S\s]*

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "applicationId": number,
   "applicationName": "string",
   "caCertificate": "string",
   "clientId": "string",
```

```
        "clientSecret": "string",
        "companyId": "string",
        "customUsername": "string",
        "extraAuthParams": "string",
        "issuer": "string",
        "redirectUrl": "string",
        "scopes": "string",
        "secret": "string",
        "ssoTokenBufferMinutes": number,
        "userId": "string"
    }
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

companyId

Custom identifier your end users will use to sign in with SSO.

Type: String

Pattern: [\S\s]*

issuer

The issuer URL of the OIDC provider.

Type: String

Pattern: [\S\s]*

scopes

The OAuth scopes configured for the application.

Type: String

Pattern: [\S\s]*

applicationId

The unique identifier for the registered OIDC application.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 10.

applicationName

The name of the registered OIDC application.

Type: String

Pattern: [\S\s]*

caCertificate

The CA certificate used for secure communication with the OIDC provider.

Type: String

Pattern: [\S\s]*

clientId

The OAuth client ID assigned to the application.

Type: String

Pattern: [\S\s]*

clientSecret

The OAuth client secret for the application.

Type: String

Pattern: [\S\s]*

customUsername

The custom field mapping used for extracting the username.

Type: String

Pattern: [\S\s]*

extraAuthParams

The additional authentication parameters configured for the OIDC flow.

Type: String

Pattern: [\S\s]*

redirectUrl

The redirect URL configured for the OAuth flow.

Type: String

Pattern: [\S\s]*

secret

The client secret for authenticating with the OIDC provider.

Type: String

Pattern: [\S\s]*

ssoTokenBufferMinutes

The buffer time in minutes before the SSO token expires.

Type: Integer

userId

The claim field being used as the user identifier.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

RegisterOidcConfigTest

Tests an OpenID Connect (OIDC) configuration for a Wickr network by validating the connection to the identity provider and retrieving its supported capabilities.

Request Syntax

```
POST /networks/networkId/oidc/test HTTP/1.1
Content-type: application/json

{
    "certificate": "string",
    "extraAuthParams": "string",
    "issuer": "string",
    "scopes": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network for which the OIDC configuration will be tested.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request accepts the following data in JSON format.

issuer

The issuer URL of the OIDC provider to test.

Type: String

Pattern: [\S\s]*

Required: Yes

scopes

The OAuth scopes to test with the OIDC provider.

Type: String

Pattern: [\S\s]*

Required: Yes

certificate

The CA certificate for secure communication with the OIDC provider (optional).

Type: String

Pattern: [\S\s]*

Required: No

extraAuthParams

Additional authentication parameters to include in the test (optional).

Type: String

Pattern: [\S\s]*

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "authorizationEndpoint": "string",
   "endSessionEndpoint": "string",
   "grantTypesSupported": [ "string" ],
   "issuer": "string",
```

```
      "logoutEndpoint": "string",
      "microsoftMultiRefreshToken": boolean,
      "responseTypesSupported": [ "string" ],
      "revocationEndpoint": "string",
      "scopesSupported": [ "string" ],
      "tokenEndpoint": "string",
      "tokenEndpointAuthMethodsSupported": [ "string" ],
      "userinfoEndpoint": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

authorizationEndpoint

    The authorization endpoint URL discovered from the OIDC provider.

    Type: String

    Pattern: [\S\s]*

endSessionEndpoint

    The end session endpoint URL for logging out users from the OIDC provider.

    Type: String

    Pattern: [\S\s]*

grantTypesSupported

    The OAuth grant types supported by the OIDC provider.

    Type: Array of strings

    Pattern: [\S\s]*

issuer

    The issuer URL confirmed by the OIDC provider.

    Type: String

Pattern: [\S\s]*

logoutEndpoint

The logout endpoint URL for terminating user sessions.

Type: String

Pattern: [\S\s]*

microsoftMultiRefreshToken

Indicates whether the provider supports Microsoft multi-refresh tokens.

Type: Boolean

responseTypesSupported

The OAuth response types supported by the OIDC provider.

Type: Array of strings

Pattern: [\S\s]*

revocationEndpoint

The token revocation endpoint URL for invalidating tokens.

Type: String

Pattern: [\S\s]*

scopesSupported

The OAuth scopes supported by the OIDC provider.

Type: Array of strings

Pattern: [\S\s]*

tokenEndpoint

The token endpoint URL discovered from the OIDC provider.

Type: String

Pattern: [\S\s]*

tokenEndpointAuthMethodsSupported

The authentication methods supported by the token endpoint.

Type: Array of strings

Pattern: [\S\s]*

userinfoEndpoint

The user info endpoint URL discovered from the OIDC provider.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateBot

Updates the properties of an existing bot in a Wickr network. This operation allows you to modify the bot's display name, security group, password, or suspension status.

Request Syntax

```
PATCH /networks/networkId/bots/botId HTTP/1.1
Content-type: application/json

{
   "challenge": "string",
   "displayName": "string",
   "groupId": "string",
   "suspend": boolean
}
```

URI Request Parameters

The request uses the following URI parameters.

botId

   The unique identifier of the bot to update.

   Length Constraints: Minimum length of 1. Maximum length of 10.

   Pattern: [0-9]+

   Required: Yes

networkId

   The ID of the Wickr network containing the bot to update.

   Length Constraints: Fixed length of 8.

   Pattern: [0-9]{8}

   Required: Yes

Request Body

The request accepts the following data in JSON format.

challenge

The new password for the bot account.

Type: String

Pattern: [\S\s]*

Required: No

displayName

The new display name for the bot.

Type: String

Pattern: [\S\s]*

Required: No

groupId

The ID of the new security group to assign the bot to.

Type: String

Pattern: [\S\s]*

Required: No

suspend

Set to true to suspend the bot or false to unsuspend it. Omit this field for standard updates that don't affect suspension status.

Type: Boolean

Required: No

Response Syntax

```
HTTP/1.1 200
```

```
Content-type: application/json

{
    "message": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

message

A message indicating the result of the bot update operation.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

    A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError](#)

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

    A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateDataRetention

Updates the data retention bot settings, allowing you to enable or disable the data retention service, or acknowledge the public key message.

Request Syntax

```
PATCH /networks/networkId/data-retention-bots HTTP/1.1
Content-type: application/json


{
    "actionType": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network containing the data retention bot.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request accepts the following data in JSON format.

actionType

The action to perform. Valid values are 'ENABLE' (to enable the data retention service), 'DISABLE' (to disable the service), or 'PUBKEY_MSG_ACK' (to acknowledge the public key message).

Type: String

Valid Values: ENABLE | DISABLE | PUBKEY_MSG_ACK

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "message": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

message

A message indicating the result of the update operation.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateGuestUser

Updates the block status of a guest user in a Wickr network. This operation allows you to block or unblock a guest user from accessing the network.

Request Syntax

```
PATCH /networks/networkId/guest-users/usernameHash HTTP/1.1
Content-type: application/json

{
    "block": boolean
}
```

URI Request Parameters

The request uses the following URI parameters.

networkId

    The ID of the Wickr network where the guest user's status will be updated.

    Length Constraints: Fixed length of 8.

    Pattern: [0-9]{8}

    Required: Yes

usernameHash

    The username hash (unique identifier) of the guest user to update.

    Pattern: [\S\s]*

    Required: Yes

Request Body

The request accepts the following data in JSON format.

block

    Set to true to block the guest user or false to unblock them.

Type: Boolean

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "message": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

message

A message indicating the result of the update operation.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2
- AWS SDK for Java V2
- AWS SDK for JavaScript V3
- AWS SDK for Kotlin
- AWS SDK for PHP V3
- AWS SDK for Python
- AWS SDK for Ruby V3

UpdateNetwork

Updates the properties of an existing Wickr network, such as its name or encryption key configuration.

Request Syntax

```
PATCH /networks/networkId HTTP/1.1
X-Client-Token: clientToken
Content-type: application/json


{
   "encryptionKeyArn": "string",
   "networkName": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

clientToken

A unique identifier for this request to ensure idempotency.

Length Constraints: Minimum length of 1. Maximum length of 64.

Pattern: `[a-zA-Z0-9-_:]+`

networkId

The ID of the Wickr network to update.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

networkName

The new name for the network. Must be between 1 and 20 characters.

Type: String

Pattern: [\S\s]*

Required: Yes

encryptionKeyArn

The ARN of the AWS KMS customer managed key to use for encrypting sensitive data in the network.

Type: String

Pattern: [\S\s]*

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
    "message": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

message

A message indicating that the network was updated successfully.

Type: String

Pattern: [\S\s]*

Errors

For information about the errors that are common to all actions, see [Common Errors](#).

[BadRequestError](#)

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

[ForbiddenError](#)

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

[InternalServerError](#)

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

[RateLimitError](#)

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

>   A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

[ResourceNotFoundError](#)

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

>   A message identifying which resource was not found.

HTTP Status Code: 404

[UnauthorizedError](#)

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

>   A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError](#)

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

>   A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)

- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateNetworkSettings

Updates network-level settings for a Wickr network. You can modify settings such as client metrics, data retention, and other network-wide options.

Request Syntax

```
PATCH /networks/networkId/settings HTTP/1.1
Content-type: application/json

{
   "settings": {
      "dataRetention": boolean,
      "enableClientMetrics": boolean,
      "readReceiptConfig": {
         "status": "string"
      }
   }
}
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network whose settings will be updated.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request accepts the following data in JSON format.

settings

A map of setting names to their new values. Each setting should be provided with its appropriate type (boolean, string, number, etc.).

Type: NetworkSettings object

Required: Yes

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "settings": [
      {
         "optionName": "string",
         "type": "string",
         "value": "string"
      }
   ]
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

settings

A list of the updated network settings, showing the new values for each modified setting.

Type: Array of Setting objects

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

[UnauthorizedError](#)

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

[ValidationError](#)

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)

- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateSecurityGroup

Updates the properties of an existing security group in a Wickr network, such as its name or settings.

Request Syntax

```
PATCH /networks/networkId/security-groups/groupId HTTP/1.1
Content-type: application/json

{
    "name": "string",
    "securityGroupSettings": {
        "alwaysReauthenticate": boolean,
        "atakPackageValues": [ "string" ],
        "calling": {
            "canStart11Call": boolean,
            "canVideoCall": boolean,
            "forceTcpCall": boolean
        },
        "checkForUpdates": boolean,
        "enableAtak": boolean,
        "enableCrashReports": boolean,
        "enableFileDownload": boolean,
        "enableGuestFederation": boolean,
        "enableNotificationPreview": boolean,
        "enableOpenAccessOption": boolean,
        "enableRestrictedGlobalFederation": boolean,
        "federationMode": number,
        "filesEnabled": boolean,
        "forceDeviceLockout": number,
        "forceOpenAccess": boolean,
        "forceReadReceipts": boolean,
        "globalFederation": boolean,
        "isAtoEnabled": boolean,
        "isLinkPreviewEnabled": boolean,
        "locationAllowMaps": boolean,
        "locationEnabled": boolean,
        "lockoutThreshold": number,
        "maxAutoDownloadSize": number,
        "maxBor": number,
        "maxTtl": number,
        "messageForwardingEnabled": boolean,
```

```
        "passwordRequirements": {
            "lowercase": number,
            "minLength": number,
            "numbers": number,
            "symbols": number,
            "uppercase": number
        },
        "permittedNetworks": [ "string" ],
        "permittedWickrAwsNetworks": [
            {
                "networkId": "string",
                "region": "string"
            }
        ],
        "permittedWickrEnterpriseNetworks": [
            {
                "domain": "string",
                "networkId": "string"
            }
        ],
        "presenceEnabled": boolean,
        "quickResponses": [ "string" ],
        "showMasterRecoveryKey": boolean,
        "shredder": {
            "canProcessManually": boolean,
            "intensity": number
        },
        "ssoMaxIdleMinutes": number
    }
}
```

URI Request Parameters

The request uses the following URI parameters.

groupId

The unique identifier of the security group to update.

Pattern: [\S\s]*

Required: Yes

networkId

The ID of the Wickr network containing the security group to update.

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

Request Body

The request accepts the following data in JSON format.

name

The new name for the security group.

Type: String

Pattern: `[\S\s]*`

Required: No

securityGroupSettings

The updated configuration settings for the security group.

Federation mode - 0 (Local federation), 1 (Restricted federation), 2 (Global federation)

Type: SecurityGroupSettings object

Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "securityGroup": {
      "activeDirectoryGuid": "string",
      "activeMembers": number,
      "botMembers": number,
```

```
      "id": "string",
      "isDefault": boolean,
      "modified": number,
      "name": "string",
      "securityGroupSettings": {
         "alwaysReauthenticate": boolean,
         "atakPackageValues": [ "string" ],
         "calling": {
            "canStart11Call": boolean,
            "canVideoCall": boolean,
            "forceTcpCall": boolean
         },
         "checkForUpdates": boolean,
         "enableAtak": boolean,
         "enableCrashReports": boolean,
         "enableFileDownload": boolean,
         "enableGuestFederation": boolean,
         "enableNotificationPreview": boolean,
         "enableOpenAccessOption": boolean,
         "enableRestrictedGlobalFederation": boolean,
         "federationMode": number,
         "filesEnabled": boolean,
         "forceDeviceLockout": number,
         "forceOpenAccess": boolean,
         "forceReadReceipts": boolean,
         "globalFederation": boolean,
         "isAtoEnabled": boolean,
         "isLinkPreviewEnabled": boolean,
         "locationAllowMaps": boolean,
         "locationEnabled": boolean,
         "lockoutThreshold": number,
         "maxAutoDownloadSize": number,
         "maxBor": number,
         "maxTtl": number,
         "messageForwardingEnabled": boolean,
         "passwordRequirements": {
            "lowercase": number,
            "minLength": number,
            "numbers": number,
            "symbols": number,
            "uppercase": number
         },
         "permittedNetworks": [ "string" ],
         "permittedWickrAwsNetworks": [
```

```
            {
                "networkId": "string",
                "region": "string"
            }
        ],
        "permittedWickrEnterpriseNetworks": [
            {
                "domain": "string",
                "networkId": "string"
            }
        ],
        "presenceEnabled": boolean,
        "quickResponses": [ "string" ],
        "showMasterRecoveryKey": boolean,
        "shredder": {
            "canProcessManually": boolean,
            "intensity": number
        },
        "ssoMaxIdleMinutes": number
    }
  }
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

securityGroup

The updated security group details, including the new settings.

Type: SecurityGroup object

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS Command Line Interface V2
- AWS SDK for .NET
- AWS SDK for C++
- AWS SDK for Go v2

- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

UpdateUser

Updates the properties of an existing user in a Wickr network. This operation allows you to modify the user's name, password, security group membership, and invite code settings.

> ⓘ **Note**
>
> `codeValidation`, `inviteCode`, and `inviteCodeTtl` are restricted to networks under preview only.

Request Syntax

```
PATCH /networks/networkId/users HTTP/1.1
Content-type: application/json

{
   "userDetails": {
      "codeValidation": boolean,
      "firstName": "string",
      "inviteCode": "string",
      "inviteCodeTtl": number,
      "lastName": "string",
      "securityGroupIds": [ "string" ],
      "username": "string"
   },
   "userId": "string"
}
```

URI Request Parameters

The request uses the following URI parameters.

networkId

The ID of the Wickr network containing the user to update.

Length Constraints: Fixed length of 8.

Pattern: [0-9]{8}

Required: Yes

Request Body

The request accepts the following data in JSON format.

userId

    The unique identifier of the user to update.

    Type: String

    Length Constraints: Minimum length of 1. Maximum length of 10.

    Pattern: [0-9]+

    Required: Yes

userDetails

    An object containing the user details to be updated, such as name, password, security groups, and invite code settings.

    Type: UpdateUserDetails object

    Required: No

Response Syntax

```
HTTP/1.1 200
Content-type: application/json

{
   "codeValidation": boolean,
   "firstName": "string",
   "inviteCode": "string",
   "inviteExpiration": number,
   "lastName": "string",
   "middleName": "string",
   "modified": number,
   "networkId": "string",
   "securityGroupIds": [ "string" ],
```

```
    "status": number,
    "suspended": boolean,
    "userId": "string"
}
```

Response Elements

If the action is successful, the service sends back an HTTP 200 response.

The following data is returned in JSON format by the service.

networkId

The ID of the network where the user was updated.

Type: String

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

suspended

Indicates whether the user is suspended after the update.

Type: Boolean

userId

The unique identifier of the updated user.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: `[0-9]+`

codeValidation

Indicates whether the user can be verified through a custom invite code.

Type: Boolean

firstName

The updated first name of the user.

Type: String

Pattern: [\S\s]*

inviteCode

The updated invite code for the user, if applicable.

Type: String

Pattern: [\S\s]*

inviteExpiration

The expiration time of the user's invite code, specified in epoch seconds.

Type: Integer

lastName

The updated last name of the user.

Type: String

Pattern: [\S\s]*

middleName

The middle name of the user (currently not used).

Type: String

Pattern: [\S\s]*

modified

The timestamp when the user was last modified, specified in epoch seconds.

Type: Integer

securityGroupIds

The list of security group IDs to which the user now belongs after the update.

Type: Array of strings

Pattern: [\S]+

status

The user's status after the update.

Type: Integer

Errors

For information about the errors that are common to all actions, see Common Errors.

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

message

A detailed message explaining what was wrong with the request and how to correct it.

HTTP Status Code: 400

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

message

A message explaining why access was denied and what permissions are required.

HTTP Status Code: 403

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

message

A message describing the internal server error that occurred.

HTTP Status Code: 500

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

HTTP Status Code: 429

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

message

A message identifying which resource was not found.

HTTP Status Code: 404

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

message

A message explaining why the authentication failed.

HTTP Status Code: 401

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

HTTP Status Code: 422

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS Command Line Interface V2](#)
- [AWS SDK for .NET](#)
- [AWS SDK for C++](#)
- [AWS SDK for Go v2](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for JavaScript V3](#)
- [AWS SDK for Kotlin](#)
- [AWS SDK for PHP V3](#)
- [AWS SDK for Python](#)
- [AWS SDK for Ruby V3](#)

Data Types

The AWS Wickr API contains several data types that various actions use. This section describes each data type in detail.

> **ⓘ Note**
>
> The order of each element in a data type structure is not guaranteed. Applications should not assume a particular order.

The following data types are supported:

- BasicDeviceObject
- BatchCreateUserRequestItem
- BatchDeviceErrorResponseItem
- BatchDeviceSuccessResponseItem
- BatchUnameErrorResponseItem
- BatchUnameSuccessResponseItem
- BatchUserErrorResponseItem
- BatchUserSuccessResponseItem
- BlockedGuestUser
- Bot
- CallingSettings
- ErrorDetail
- GuestUser
- GuestUserHistoryCount
- Network
- NetworkSettings
- OidcConfigInfo
- OidcTokenInfo
- PasswordRequirements
- PermittedWickrEnterpriseNetwork

- [ReadReceiptConfig](#)
- [SecurityGroup](#)
- [SecurityGroupSettings](#)
- [SecurityGroupSettingsRequest](#)
- [Setting](#)
- [ShredderSettings](#)
- [UpdateUserDetails](#)
- [User](#)
- [WickrAwsNetworks](#)

BasicDeviceObject

Represents a device where a user has logged into Wickr, containing information about the device's type, status, and login history.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

appId

The unique application ID for the Wickr app on this device.

Type: String

Pattern: [\S\s]*

Required: No

created

The timestamp when the device first appeared in the Wickr database.

Type: String

Pattern: [\S\s]*

Required: No

lastLogin

The timestamp when the device last successfully logged into Wickr. This is also used to determine SSO idle time.

Type: String

Pattern: [\S\s]*

Required: No

statusText

The current status of the device, either 'Active' or 'Reset' depending on whether the device is currently active or has been marked for reset.

Type: String

Pattern: [\S\s]*

Required: No

suspend

Indicates whether the device is suspended.

Type: Boolean

Required: No

type

The operating system of the device (e.g., 'MacOSX', 'Windows', 'iOS', 'Android').

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchCreateUserRequestItem

Contains the details for a single user to be created in a batch user creation request.

> **ⓘ Note**
>
> A user can only be assigned to a single security group. Attempting to add a user to multiple security groups is not supported and will result in an error.

> **ⓘ Note**
>
> `codeValidation`, `inviteCode`, and `inviteCodeTtl` are restricted to networks under preview only.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

securityGroupIds

A list of security group IDs to which the user should be assigned.

Type: Array of strings

Pattern: [\S]+

Required: Yes

username

The email address or username for the user. Must be unique within the network.

Type: String

Pattern: [\S\s]*

Required: Yes

codeValidation

Indicates whether the user can be verified through a custom invite code.

Type: Boolean

Required: No

firstName

The first name of the user.

Type: String

Pattern: [\S\s]*

Required: No

inviteCode

A custom invite code for the user. If not provided, one will be generated automatically.

Type: String

Pattern: [\S\s]*

Required: No

inviteCodeTtl

The time-to-live for the invite code in days. After this period, the invite code will expire.

Type: Integer

Required: No

lastName

The last name of the user.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchDeviceErrorResponseItem

Contains error information for a device operation that failed in a batch device request.

Contents

> **ℹ Note**
>
> In the following list, the required parameters are described first.

appId

The application ID of the device that failed to be processed.

Type: String

Pattern: [\S\s]*

Required: Yes

field

The field that caused the error.

Type: String

Pattern: [\S\s]*

Required: No

reason

A description of why the device operation failed.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchDeviceSuccessResponseItem

Contains information about a device that was successfully processed in a batch device operation.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

appId

The application ID of the device that was successfully processed.

Type: String

Pattern: `[\S\s]*`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchUnameErrorResponseItem

Contains error information for a username hash lookup that failed in a batch uname lookup request.

Contents

> **ℹ Note**
>
> In the following list, the required parameters are described first.

uname

The username hash that failed to be looked up.

Type: String

Required: Yes

field

The field that caused the error.

Type: String

Pattern: [\S\s]*

Required: No

reason

A description of why the username hash lookup failed.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchUnameSuccessResponseItem

Contains information about a username hash that was successfully resolved in a batch uname lookup operation.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

uname

The username hash that was successfully resolved.

Type: String

Required: Yes

username

The email address or username corresponding to the username hash.

Type: String

Pattern: [\S\s]*

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchUserErrorResponseItem

Contains error information for a user operation that failed in a batch user request.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

userId

   The user ID associated with the failed operation.

   Type: String

   Length Constraints: Minimum length of 1. Maximum length of 10.

   Pattern: [0-9]+

   Required: Yes

field

   The field that caused the error.

   Type: String

   Pattern: [\S\s]*

   Required: No

reason

   A description of why the user operation failed.

   Type: String

   Pattern: [\S\s]*

   Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BatchUserSuccessResponseItem

Contains information about a user that was successfully processed in a batch user operation.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

userId

The user ID that was successfully processed.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: [0-9]+

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

BlockedGuestUser

Represents a guest user who has been blocked from accessing a Wickr network.

Contents

> ℹ️ **Note**
>
> In the following list, the required parameters are described first.

admin

The username of the administrator who blocked this guest user.

Type: String

Pattern: [\S\s]*

Required: Yes

modified

The timestamp when the guest user was blocked or last modified.

Type: String

Pattern: [\S\s]*

Required: Yes

username

The username of the blocked guest user.

Type: String

Pattern: [\S\s]*

Required: Yes

usernameHash

The unique username hash identifier for the blocked guest user.

Type: String

Pattern: [\S\s]*

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Bot

Represents a bot account in a Wickr network with all its informational fields.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

botId

The unique identifier of the bot.

Type: String

Pattern: [\S\s]*

Required: No

displayName

The display name of the bot that is visible to users.

Type: String

Pattern: [\S\s]*

Required: No

groupId

The ID of the security group to which the bot belongs.

Type: String

Pattern: [\S\s]*

Required: No

hasChallenge

Indicates whether the bot has a password set.

Type: Boolean

Required: No

lastLogin

The timestamp of the bot's last login.

Type: String

Pattern: [\S\s]*

Required: No

pubkey

The public key of the bot used for encryption.

Type: String

Pattern: [\S\s]*

Required: No

status

The current status of the bot (1 for pending, 2 for active).

Type: Integer

Required: No

suspended

Indicates whether the bot is currently suspended.

Type: Boolean

Required: No

uname

The unique username hash identifier for the bot.

Type: String

Pattern: [\S\s]*

Required: No

username

The username of the bot.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

CallingSettings

Defines the calling feature permissions and settings for users in a security group, controlling what types of calls users can initiate and participate in.

Contents

> ⓘ **Note**
>
> In the following list, the required parameters are described first.

canStart11Call

Specifies whether users can start one-to-one calls.

Type: Boolean

Required: No

canVideoCall

Specifies whether users can make video calls (as opposed to audio-only calls). Valid only when audio call(canStart11Call) is enabled.

Type: Boolean

Required: No

forceTcpCall

When enabled, forces all calls to use TCP protocol instead of UDP for network traversal.

Type: Boolean

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ErrorDetail

Contains detailed error information explaining why an operation failed, including which field caused the error and the reason for the failure.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

field

The name of the field that contains an error or warning.

Type: String

Pattern: [\S\s]*

Required: No

reason

A detailed description of the error or warning.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

GuestUser

Represents a guest user who has accessed the network from a federated Wickr network.

Contents

> **ℹ Note**
>
> In the following list, the required parameters are described first.

billingPeriod

The billing period when this guest user accessed the network (e.g., '2024-01').

Type: String

Pattern: [\S\s]*

Required: Yes

username

The username of the guest user.

Type: String

Pattern: [\S\s]*

Required: Yes

usernameHash

The unique username hash identifier for the guest user.

Type: String

Pattern: [\S\s]*

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

GuestUserHistoryCount

Contains the count of guest users for a specific billing period, used for tracking historical guest user activity.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

count

The number of guest users who have communicated with your Wickr network during this billing period.

Type: String

Pattern: [\S\s]*

Required: Yes

month

The month and billing period in YYYY_MM format (e.g., '2024_01').

Type: String

Pattern: [\S\s]*

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

Network

Represents a Wickr network with all its configuration and status information.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

accessLevel

The access level of the network (STANDARD or PREMIUM), which determines available features and capabilities.

Type: String

Valid Values: STANDARD | PREMIUM

Required: Yes

awsAccountId

The AWS account ID that owns the network.

Type: String

Pattern: [\S\s]*

Required: Yes

networkArn

The Amazon Resource Name (ARN) of the network.

Type: String

Pattern: [\S\s]*

Required: Yes

networkId

The unique identifier of the network.

Type: String

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

networkName

The name of the network.

Type: String

Pattern: `[\S\s]*`

Required: Yes

encryptionKeyArn

The ARN of the AWS KMS customer managed key used for encrypting sensitive data in the network.

Type: String

Pattern: `[\S\s]*`

Required: No

freeTrialExpiration

The expiration date and time for the network's free trial period, if applicable.

Type: String

Pattern: `[\S\s]*`

Required: No

migrationState

The SSO redirect URI migration state, managed by the SSO redirect migration wizard. Values: 0 (not started), 1 (in progress), or 2 (completed).

Type: Integer

Required: No

standing

The current standing or status of the network.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

NetworkSettings

Contains network-level configuration settings that apply to all users and security groups within a Wickr network.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

dataRetention

Indicates whether the data retention feature is enabled for the network. When true, messages are captured by the data retention bot for compliance and archiving purposes.

Type: Boolean

Required: No

enableClientMetrics

Allows Wickr clients to send anonymized performance and usage metrics to the Wickr backend server for service improvement and troubleshooting.

Type: Boolean

Required: No

readReceiptConfig

Configuration for read receipts at the network level, controlling the default behavior for whether senders can see when their messages have been read.

Type: ReadReceiptConfig object

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](AWS SDK for C++)
- AWS SDK for Java V2
- AWS SDK for Ruby V3

OidcConfigInfo

Contains the OpenID Connect (OIDC) configuration information for Single Sign-On (SSO) authentication, including identity provider settings and client credentials.

Contents

> ⓘ **Note**
>
> In the following list, the required parameters are described first.

companyId

Custom identifier your end users will use to sign in with SSO.

Type: String

Pattern: [\S\s]*

Required: Yes

issuer

The issuer URL of the identity provider, which serves as the base URL for OIDC endpoints and configuration discovery.

Type: String

Pattern: [\S\s]*

Required: Yes

scopes

The OAuth scopes requested from the identity provider, which determine what user information is accessible (e.g., 'openid profile email').

Type: String

Pattern: [\S\s]*

Required: Yes

applicationId

The unique identifier for the registered OIDC application. Valid range is 1-10.

Type: Integer

Valid Range: Minimum value of 1. Maximum value of 10.

Required: No

applicationName

The name of the OIDC application as registered with the identity provider.

Type: String

Pattern: [\S\s]*

Required: No

caCertificate

The X.509 CA certificate for validating SSL/TLS connections to the identity provider when using self-signed or enterprise certificates.

Type: String

Pattern: [\S\s]*

Required: No

clientId

The OAuth client ID assigned by the identity provider for authentication requests.

Type: String

Pattern: [\S\s]*

Required: No

clientSecret

The OAuth client secret used to authenticate the application with the identity provider.

Type: String

Pattern: [\S\s]*

Required: No

customUsername

A custom field mapping to extract the username from the OIDC token when the standard username claim is insufficient.

Type: String

Pattern: [\S\s]*

Required: No

extraAuthParams

Additional authentication parameters to include in the OIDC authorization request as a query string. Useful for provider-specific extensions.

Type: String

Pattern: [\S\s]*

Required: No

redirectUrl

The callback URL where the identity provider redirects users after successful authentication. This URL must be registered with the identity provider.

Type: String

Pattern: [\S\s]*

Required: No

secret

An additional secret credential used by the identity provider for authentication.

Type: String

Pattern: [\S\s]*

Required: No

ssoTokenBufferMinutes

The grace period in minutes before the SSO token expires when the system should proactively refresh the token to maintain seamless user access.

Type: Integer

Required: No

userId

The claim field from the OIDC token to use as the unique user identifier (e.g., 'email', 'sub', or a custom claim).

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

OidcTokenInfo

Contains OAuth token information returned from the identity provider, including access tokens, ID tokens, and PKCE parameters used for secure authentication.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

accessToken

The OAuth access token that can be used to access protected resources on behalf of the authenticated user.

Type: String

Pattern: [\S\s]*

Required: No

codeChallenge

The PKCE code challenge, a transformed version of the code verifier sent during the authorization request for verification.

Type: String

Pattern: [\S\s]*

Required: No

codeVerifier

The PKCE (Proof Key for Code Exchange) code verifier, a cryptographically random string used to enhance security in the OAuth flow.

Type: String

Pattern: [\S\s]*

Required: No

expiresIn

The lifetime of the access token in seconds, indicating when the token will expire and need to be refreshed.

Type: Long

Required: No

idToken

The OpenID Connect ID token containing user identity information and authentication context as a signed JWT.

Type: String

Pattern: [\S\s]*

Required: No

refreshToken

The OAuth refresh token that can be used to obtain new access tokens without requiring the user to re-authenticate.

Type: String

Pattern: [\S\s]*

Required: No

tokenType

The type of access token issued, typically 'Bearer', which indicates how the token should be used in API requests.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

PasswordRequirements

Defines password complexity requirements for users in a security group, including minimum length and character type requirements.

Contents

> **Note**
>
> In the following list, the required parameters are described first.

lowercase

The minimum number of lowercase letters required in passwords.

Type: Integer

Required: No

minLength

The minimum password length in characters.

Type: Integer

Required: No

numbers

The minimum number of numeric characters required in passwords.

Type: Integer

Required: No

symbols

The minimum number of special symbol characters required in passwords.

Type: Integer

Required: No

uppercase

The minimum number of uppercase letters required in passwords.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

PermittedWickrEnterpriseNetwork

Identifies a Wickr enterprise network that is permitted for global federation, allowing users to communicate with members of the specified network.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

domain

The domain identifier for the permitted Wickr enterprise network.

Type: String

Pattern: `[\S\s]*`

Required: Yes

networkId

The network ID of the permitted Wickr enterprise network.

Type: String

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

ReadReceiptConfig

Configuration for read receipts at the network level, controlling whether senders can see when their messages have been read.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

status

The read receipt status mode for the network.

Type: String

Valid Values: `DISABLED | ENABLED | FORCE_ENABLED`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SecurityGroup

Represents a security group in a Wickr network, containing membership statistics, configuration, and all permission settings that apply to its members.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

activeMembers

The number of active user members currently in the security group.

Type: Integer

Required: Yes

botMembers

The number of bot members currently in the security group.

Type: Integer

Required: Yes

id

The unique identifier of the security group.

Type: String

Pattern: [\S\s]*

Required: Yes

isDefault

Indicates whether this is the default security group for the network. Each network has only one default group.

Type: Boolean

Required: Yes

modified

The timestamp when the security group was last modified, specified in epoch seconds.

Type: Integer

Required: Yes

name

The human-readable name of the security group.

Type: String

Pattern: [\S\s]*

Required: Yes

securityGroupSettings

The comprehensive configuration settings that define capabilities and restrictions for members of this security group.

Type: SecurityGroupSettings object

Required: Yes

activeDirectoryGuid

The GUID of the Active Directory group associated with this security group, if synchronized with LDAP.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SecurityGroupSettings

Comprehensive configuration settings that define all user capabilities, restrictions, and features for members of a security group. These settings control everything from calling permissions to federation settings to security policies.

Contents

> ⓘ **Note**
>
> In the following list, the required parameters are described first.

alwaysReauthenticate

Requires users to reauthenticate every time they return to the application, providing an additional layer of security.

Type: Boolean

Required: No

atakPackageValues

Configuration values for ATAK (Android Team Awareness Kit) package integration, when ATAK is enabled.

Type: Array of strings

Pattern: [\S\s]*

Required: No

calling

The calling feature permissions and settings that control what types of calls users can initiate and participate in.

Type: [CallingSettings](#) object

Required: No

checkForUpdates

Enables automatic checking for Wickr client updates to ensure users stay current with the latest version.

Type: Boolean

Required: No

enableAtak

Enables ATAK (Android Team Awareness Kit) integration for tactical communication and situational awareness.

Type: Boolean

Required: No

enableCrashReports

Allow users to report crashes.

Type: Boolean

Required: No

enableFileDownload

Specifies whether users can download files from messages to their devices.

Type: Boolean

Required: No

enableGuestFederation

Allows users to communicate with guest users from other Wickr networks and federated external networks.

Type: Boolean

Required: No

enableNotificationPreview

Enables message preview text in push notifications, allowing users to see message content before opening the app.

Type: Boolean

Required: No

enableOpenAccessOption

Allow users to avoid censorship when they are geo-blocked or have network limitations.

Type: Boolean

Required: No

enableRestrictedGlobalFederation

Enables restricted global federation, limiting external communication to only specified permitted networks.

Type: Boolean

Required: No

federationMode

The local federation mode controlling how users can communicate with other networks. Values: 0 (none), 1 (federated), 2 (restricted).

Type: Integer

Required: No

filesEnabled

Enables file sharing capabilities, allowing users to send and receive files in conversations.

Type: Boolean

Required: No

forceDeviceLockout

Defines the number of failed login attempts before data stored on the device is reset. Should be less than lockoutThreshold.

Type: Integer

Required: No

forceOpenAccess

Automatically enable and enforce Wickr open access on all devices. Valid only if enableOpenAccessOption settings is enabled.

Type: Boolean

Required: No

forceReadReceipts

Allow user approved bots to read messages in rooms without using a slash command.

Type: Boolean

Required: No

globalFederation

Allows users to communicate with users on other Wickr instances (Wickr Enterprise) outside the current network.

Type: Boolean

Required: No

isAtoEnabled

Enforces a two-factor authentication when a user adds a new device to their account.

Type: Boolean

Required: No

isLinkPreviewEnabled

Enables automatic preview of links shared in messages, showing webpage thumbnails and descriptions.

Type: Boolean

Required: No

locationAllowMaps

Allows map integration in location sharing, enabling users to view shared locations on interactive maps. Only allowed when location setting is enabled.

Type: Boolean

Required: No

locationEnabled

Enables location sharing features, allowing users to share their current location with others.

Type: Boolean

Required: No

lockoutThreshold

The number of failed password attempts before a user account is locked out.

Type: Integer

Required: No

maxAutoDownloadSize

The maximum file size in bytes that will be automatically downloaded without user confirmation. Only allowed if fileDownload is enabled. Valid Values [512000 (low_quality), 7340032 (high_quality)]

Type: Long

Required: No

maxBor

The maximum burn-on-read (BOR) time in seconds, which determines how long messages remain visible before auto-deletion after being read.

Type: Integer

Required: No

maxTtl

The maximum time-to-live (TTL) in seconds for messages, after which they will be automatically deleted from all devices.

Type: Long

Required: No

messageForwardingEnabled

Enables message forwarding, allowing users to forward messages from one conversation to another.

Type: Boolean

Required: No

passwordRequirements

The password complexity requirements that users must follow when creating or changing passwords.

Type: PasswordRequirements object

Required: No

permittedNetworks

A list of network IDs that are permitted for local federation when federation mode is set to restricted.

Type: Array of strings

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: No

permittedWickrAwsNetworks

A list of permitted Wickr networks for global federation, restricting communication to specific approved networks.

Type: Array of WickrAwsNetworks objects

Required: No

permittedWickrEnterpriseNetworks

A list of permitted Wickr Enterprise networks for global federation, restricting communication to specific approved networks.

Type: Array of PermittedWickrEnterpriseNetwork objects

Required: No

presenceEnabled

Enables presence indicators that show whether users are online, away, or offline.

Type: Boolean

Required: No

quickResponses

A list of pre-defined quick response message templates that users can send with a single tap.

Type: Array of strings

Pattern: [\S\s]*

Required: No

showMasterRecoveryKey

Users will get a master recovery key that can be used to securely sign in to their Wickr account without having access to their primary device for authentication. Available in SSO enabled network.

Type: Boolean

Required: No

shredder

The message shredder configuration that controls secure deletion of messages and files from devices.

Type: [ShredderSettings](#) object

Required: No

ssoMaxIdleMinutes

The duration for which users SSO session remains inactive before automatically logging them out for security. Available in SSO enabled network.

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

SecurityGroupSettingsRequest

Contains the security group configuration settings that can be specified when creating or updating a security group. This is a subset of SecurityGroupSettings containing only the modifiable federation and security settings.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

enableGuestFederation

Guest users let you work with people outside your organization that only have limited access to Wickr. Only valid when federationMode is set to Global.

Type: Boolean

Required: No

enableRestrictedGlobalFederation

Enables restricted global federation to limit communication to specific permitted networks only. Requires globalFederation to be enabled.

Type: Boolean

Required: No

federationMode

The local federation mode. Values: 0 (none), 1 (federated - all networks), 2 (restricted - only permitted networks).

Type: Integer

Required: No

globalFederation

Allow users to securely federate with all AWS Wickr networks and AWS Enterprise networks.

Type: Boolean

Required: No

lockoutThreshold

The number of failed password attempts before a user account is locked out.

Type: Integer

Required: No

permittedNetworks

A list of network IDs that are permitted for local federation when federation mode is set to restricted.

Type: Array of strings

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: No

permittedWickrAwsNetworks

A list of permitted AWS Wickr networks for restricted global federation.

Type: Array of [WickrAwsNetworks](#) objects

Required: No

permittedWickrEnterpriseNetworks

A list of permitted Wickr Enterprise networks for restricted global federation.

Type: Array of [PermittedWickrEnterpriseNetwork](#) objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

Setting

Represents a single network-level configuration setting with its name, value, and data type. Settings control network-wide behaviors and features.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

optionName

The name of the network setting (e.g., 'enableClientMetrics', 'dataRetention').

Type: String

Pattern: [\S\s]*

Required: Yes

type

The data type of the setting value (e.g., 'boolean', 'string', 'number').

Type: String

Pattern: [\S\s]*

Required: Yes

value

The current value of the setting as a string. Boolean values are represented as 'true' or 'false'.

Type: String

Pattern: [\S\s]*

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

ShredderSettings

Configuration for the message shredder feature, which securely deletes messages and files from devices to prevent data recovery.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

canProcessManually

Specifies whether users can manually trigger the shredder to delete content.

Type: Boolean

Required: No

intensity

Prevents Wickr data from being recovered by overwriting deleted Wickr data. Valid Values: Must be one of [0, 20, 60, 100]

Type: Integer

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

UpdateUserDetails

Contains the modifiable details for updating an existing user, including name, password, security group membership, and invitation settings.

> **ⓘ Note**
>
> A user can only be assigned to a single security group. Attempting to add a user to multiple security groups is not supported and will result in an error.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

codeValidation

Indicates whether the user can be verified through a custom invite code.

Type: Boolean

Required: No

firstName

The new first name for the user.

Type: String

Pattern: [\S\s]*

Required: No

inviteCode

A new custom invite code for the user.

Type: String

Pattern: [\S\s]*

Required: No

inviteCodeTtl

The new time-to-live for the invite code in days.

Type: Integer

Required: No

lastName

The new last name for the user.

Type: String

Pattern: [\S\s]*

Required: No

securityGroupIds

The updated list of security group IDs to which the user should belong.

Type: Array of strings

Pattern: [\S]+

Required: No

username

The new username or email address for the user.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

User

Represents a user account in a Wickr network with detailed profile information, status, security settings, and authentication details.

> ⓘ **Note**
>
> codeValidation, inviteCode and inviteCodeTtl are restricted to networks under preview only.

Contents

> ⓘ **Note**
>
> In the following list, the required parameters are described first.

cell

The phone number minus country code, used for cloud deployments.

Type: String

Pattern: [\S\s]*

Required: No

challengeFailures

The number of failed password attempts for enterprise deployments, used for account lockout policies.

Type: Integer

Required: No

codeValidation

Indicates whether the user can be verified through a custom invite code.

Type: Boolean

Required: No

countryCode

The country code for the user's phone number, used for cloud deployments.

Type: String

Pattern: [\S\s]*

Required: No

firstName

The first name of the user.

Type: String

Pattern: [\S\s]*

Required: No

inviteCode

The invitation code for this user, used during registration to join the network.

Type: String

Pattern: [\S\s]*

Required: No

isAdmin

Indicates whether the user has administrator privileges in the network.

Type: Boolean

Required: No

isInviteExpired

Indicates whether the user's email invitation code has expired, applicable to cloud deployments.

Type: Boolean

Required: No

isUser

Indicates whether this account is a user (as opposed to a bot or other account type).

Type: Boolean

Required: No

lastName

The last name of the user.

Type: String

Pattern: [\S\s]*

Required: No

otpEnabled

Indicates whether one-time password (OTP) authentication is enabled for the user.

Type: Boolean

Required: No

scimId

The SCIM (System for Cross-domain Identity Management) identifier for the user, used for identity synchronization. Currently not used.

Type: String

Pattern: [\S\s]*

Required: No

securityGroups

A list of security group IDs to which the user is assigned, determining their permissions and feature access.

Type: Array of strings

Pattern: [\S]+

Required: No

status

The current status of the user (1 for pending invitation, 2 for active).

Type: Integer

Required: No

suspended

Indicates whether the user is currently suspended and unable to access the network.

Type: Boolean

Required: No

type

The descriptive type of the user account (e.g., 'user').

Type: String

Pattern: [\S\s]*

Required: No

uname

The unique identifier for the user.

Type: String

Pattern: [\S\s]*

Required: No

userId

The unique identifier for the user within the network.

Type: String

Length Constraints: Minimum length of 1. Maximum length of 10.

Pattern: [0-9]+

Required: No

username

The email address or username of the user. For bots, this must end in 'bot'.

Type: String

Pattern: `[\S\s]*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)
- [AWS SDK for Ruby V3](#)

WickrAwsNetworks

Identifies a AWS Wickr network by region and network ID, used for configuring permitted networks for global federation.

Contents

> **ⓘ Note**
>
> In the following list, the required parameters are described first.

networkId

The network ID of the Wickr AWS network.

Type: String

Length Constraints: Fixed length of 8.

Pattern: `[0-9]{8}`

Required: Yes

region

The AWS region identifier where the network is hosted (e.g., 'us-east-1').

Type: String

Pattern: `[\S\s]*`

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for C++](#)
- [AWS SDK for Java V2](#)

- [AWS SDK for Ruby V3](#)

Service-specific Errors

The AWS Wickr API contains service-specific exceptions that various actions return. This section describes each exception in detail.

The following service-specific exceptions are returned:

- [BadRequestError](#)
- [ForbiddenError](#)
- [InternalServerError](#)
- [RateLimitError](#)
- [ResourceNotFoundError](#)
- [UnauthorizedError](#)
- [ValidationError](#)

BadRequestError

The request was invalid or malformed. This error occurs when the request parameters do not meet the API requirements, such as invalid field values, missing required parameters, or improperly formatted data.

HTTP Status Code returned: 400

Contents

message

A detailed message explaining what was wrong with the request and how to correct it.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for Ruby V3](#)

ForbiddenError

Access to the requested resource is forbidden. This error occurs when the authenticated user does not have the necessary permissions to perform the requested operation, even though they are authenticated.

HTTP Status Code returned: 403

Contents

message

A message explaining why access was denied and what permissions are required.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for Ruby V3](#)

InternalServerError

An unexpected error occurred on the server while processing the request. This indicates a problem with the Wickr service itself rather than with the request. If this error persists, contact AWS Support.

HTTP Status Code returned: 500

Contents

message

A message describing the internal server error that occurred.

Type: String

Pattern: [\S\s]*

Required: Yes

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for Ruby V3](#)

RateLimitError

The request was throttled because too many requests were sent in a short period of time. Wait a moment and retry the request. Consider implementing exponential backoff in your application.

HTTP Status Code returned: 429

Contents

message

A message indicating that the rate limit was exceeded and suggesting when to retry.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for Ruby V3](#)

ResourceNotFoundError

The requested resource could not be found. This error occurs when you try to access or modify a network, user, bot, security group, or other resource that doesn't exist or has been deleted.

HTTP Status Code returned: 404

Contents

message

A message identifying which resource was not found.

Type: String

Pattern: `[\S\s]*`

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for Ruby V3](#)

UnauthorizedError

The request was not authenticated or the authentication credentials were invalid. This error occurs when the request lacks valid authentication credentials or the credentials have expired.

HTTP Status Code returned: 401

Contents

message

A message explaining why the authentication failed.

Type: String

Pattern: [\S\s]*

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- [AWS SDK for Ruby V3](#)

ValidationError

One or more fields in the request failed validation. This error provides detailed information about which fields were invalid and why, allowing you to correct the request and retry.

HTTP Status Code returned: 422

Contents

reasons

A list of validation error details, where each item identifies a specific field that failed validation and explains the reason for the failure.

Type: Array of ErrorDetail objects

Required: No

See Also

For more information about using this API in one of the language-specific AWS SDKs, see the following:

- AWS SDK for Ruby V3

Common Parameters

The following list contains the parameters that all actions use for signing Signature Version 4 requests with a query string. Any action-specific parameters are listed in the topic for that action. For more information about Signature Version 4, see [Signing AWS API requests](#) in the *IAM User Guide*.

Action

    The action to be performed.

    Type: string

    Required: Yes

Version

    The API version that the request is written for, expressed in the format YYYY-MM-DD.

    Type: string

    Required: Yes

X-Amz-Algorithm

    The hash algorithm that you used to create the request signature.

    Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

    Type: string

    Valid Values: `AWS4-HMAC-SHA256`

    Required: Conditional

X-Amz-Credential

    The credential scope value, which is a string that includes your access key, the date, the region you are targeting, the service you are requesting, and a termination string ("aws4_request"). The value is expressed in the following format: *access_key*/*YYYYMMDD*/*region*/*service*/aws4_request.

For more information, see [Create a signed AWS API request](#) in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-Date

The date that is used to create the signature. The format must be ISO 8601 basic format (YYYYMMDD'T'HHMMSS'Z'). For example, the following date time is a valid X-Amz-Date value: 20120325T120000Z.

Condition: X-Amz-Date is optional for all requests; it can be used to override the date used for signing requests. If the Date header is specified in the ISO 8601 basic format, X-Amz-Date is not required. When X-Amz-Date is used, it always overrides the value of the Date header. For more information, see [Elements of an AWS API request signature](#) in the *IAM User Guide*.

Type: string

Required: Conditional

X-Amz-Security-Token

The temporary security token that was obtained through a call to AWS Security Token Service (AWS STS). For a list of services that support temporary security credentials from AWS STS, see [AWS services that work with IAM](#) in the *IAM User Guide*.

Condition: If you're using temporary security credentials from AWS STS, you must include the security token.

Type: string

Required: Conditional

X-Amz-Signature

Specifies the hex-encoded signature that was calculated from the string to sign and the derived signing key.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

X-Amz-SignedHeaders

Specifies all the HTTP headers that were included as part of the canonical request. For more information about specifying signed headers, see Create a signed AWS API request in the *IAM User Guide*.

Condition: Specify this parameter when you include authentication information in a query string instead of in the HTTP authorization header.

Type: string

Required: Conditional

Common Errors

This section lists the errors common to the API actions of all AWS services. For errors specific to an API action for this service, see the topic for that API action.

AccessDeniedException

You do not have sufficient access to perform this action.

HTTP Status Code: 403

ExpiredTokenException

The security token included in the request is expired

HTTP Status Code: 403

IncompleteSignature

The request signature does not conform to AWS standards.

HTTP Status Code: 403

InternalFailure

The request processing has failed because of an unknown error, exception or failure.

HTTP Status Code: 500

MalformedHttpRequestException

Problems with the request at the HTTP level, e.g. we can't decompress the body according to the decompression algorithm specified by the content-encoding.

HTTP Status Code: 400

NotAuthorized

You do not have permission to perform this action.

HTTP Status Code: 401

OptInRequired

The AWS access key ID needs a subscription for the service.

HTTP Status Code: 403

RequestAbortedException

Convenient exception that can be used when a request is aborted before a reply is sent back (e.g. client closed connection).

HTTP Status Code: 400

RequestEntityTooLargeException

Problems with the request at the HTTP level. The request entity is too large.

HTTP Status Code: 413

RequestExpired

The request reached the service more than 15 minutes after the date stamp on the request or more than 15 minutes after the request expiration date (such as for pre-signed URLs), or the date stamp on the request is more than 15 minutes in the future.

HTTP Status Code: 400

RequestTimeoutException

Problems with the request at the HTTP level. Reading the Request timed out.

HTTP Status Code: 408

ServiceUnavailable

The request has failed due to a temporary failure of the server.

HTTP Status Code: 503

ThrottlingException

The request was denied due to request throttling.

HTTP Status Code: 400

UnrecognizedClientException

The X.509 certificate or AWS access key ID provided does not exist in our records.

HTTP Status Code: 403

UnknownOperationException

The action or operation requested is invalid. Verify that the action is typed correctly.

HTTP Status Code: 404

ValidationError

The input fails to satisfy the constraints specified by an AWS service.

HTTP Status Code: 400