aws

Installation Guide

Access Amazon WorkSpaces with Common Access Cards

Access Amazon WorkSpaces with Common Access Cards : Installation Guide

Table of Contents

This whitepaper is for historical reference only. Some content might be outdated and some links might not be available.

Access Amazon WorkSpaces with Common Access Cards

Publication date: **March 08, 2021**

Abstract

The Department of Defense (DoD) requires the use of Common Access Cards (CAC) by its users to authenticate into and be authorized to use DoD computing resources. This implementation guide provides step-by-step guidance for implementing pre-authorization and in-session CAC access by DoD personnel into WorkSpaces.

Overview

Smart card authentication to [Amazon WorkSpaces](#) requires the implementation of a public key infrastructure (PKI) and proper configuration of active directory, domain controllers, group policy, and domain-joined Amazon WorkSpaces. This implementation guide provides step-by-step guidance to enable the use of DoD-issued Common Access Cards (CACs) with Amazon WorkSpaces.

This implementation guide details the steps required to create and configure:

- An Active Directory (AD) that will serve as the repository for account information, primarily user credentials, security group memberships, and certificate templates. The Active Directory also stores certificates, certificate revocation lists, and root and intermediate certificate authorities.

- An Enterprise Certificate Authority (CA) that is trusted by the Active Directory.

- An [Amazon Directory AD Connector](#) enabled to support CAC authentication and certificate revocations with registered root and intermediate certificate authorities.

- Amazon WorkSpaces enabled for pre-authorization access using a CAC as well as in-session pass-through use of CAC certificates to access protected content.

Considerations

You should consider and understand the following information prior to starting the instructions included in this guide.

- **Skill level** — Prior experience with Amazon Web Services (AWS) is required to complete this implementation. An understanding of core AWS technologies, including Amazon Virtual Private Cloud (Amazon VPC), Security Groups, AWS Directory Service AD Connector, Amazon WorkSpaces, AWS Command Line Interface (AWS CLI), Microsoft Active Directory, and Microsoft Certificate Authorities.

- **Increase service limits** — By default, AWS sets quotas (also referred to as limits) for the resources that you can create and the number of users who can use the service. You can request a quota increase using Service Quotas and AWS Support Center. If a service is not yet available in AWS Service Quotas, use AWS Support Center instead. Increases are not granted immediately. It might take a couple of days for your increase to become effective. For the service limit quotas for WorkSpaces, see the Amazon WorkSpaces endpoints and quotas page.

- **Supported Availability Zones** — Amazon Workspaces support for smart card pre-session authentication is available in the WorkSpaces AWS GovCloud (US-West) Region at this time. WorkSpaces support for smart card in-session authentication is available in all Regions where WorkSpaces Streaming Protocol (WSP) is supported.

Architecture overview

The following figure shows the high-level architecture of the Amazon WorkSpaces solution, depicting internet access by a customer to access an Amazon WorkSpaces Windows client over the internet to an Amazon WorkSpace.
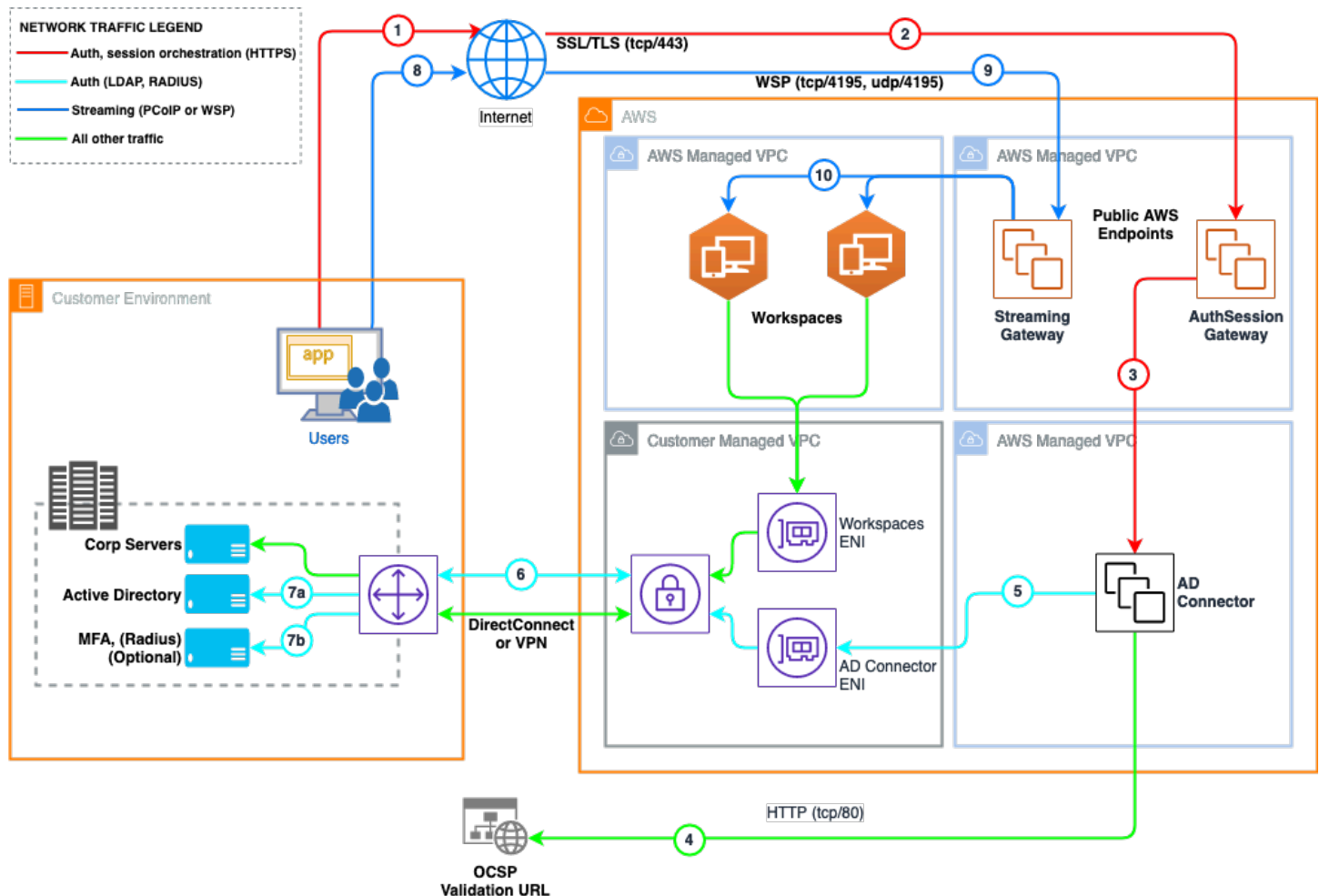
Amazon WorkSpaces smart card architecture diagram

Amazon Virtual Private Cloud

Region selection

Pre-session authentication is available only in the AWS GovCloud (US-West) Region at this time. In-session authentication is available in all Regions where WSP is supported.

VPC configuration

Amazon WorkSpaces launches your WorkSpaces in a virtual private cloud (VPC). Your WorkSpaces must have access to the internet, so you can install updates to the operating system and deploy applications using Amazon WorkSpaces Application Manager (Amazon WAM).

You can create a VPC with two private subnets for your WorkSpaces and a NAT gateway in a public subnet. Alternatively, you can create a VPC with two public subnets for your WorkSpaces and associate an Elastic IP address with each WorkSpace.

Your VPC's subnets must reside in different Availability Zones in the Region where you're launching WorkSpaces. Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single location. Each subnet must reside entirely within one Availability Zone, and cannot span zones.

For details on VPC configuration, see Configure a VPC for Amazon WorkSpaces.

Network connectivity

Connectivity from the Amazon WorkSpaces VPC to the associated Active Directory Domain Controllers to be used for authentication and authorization is required across a number of ports and protocols. This connectivity must be established before Amazon WorkSpaces can be successfully deployed.
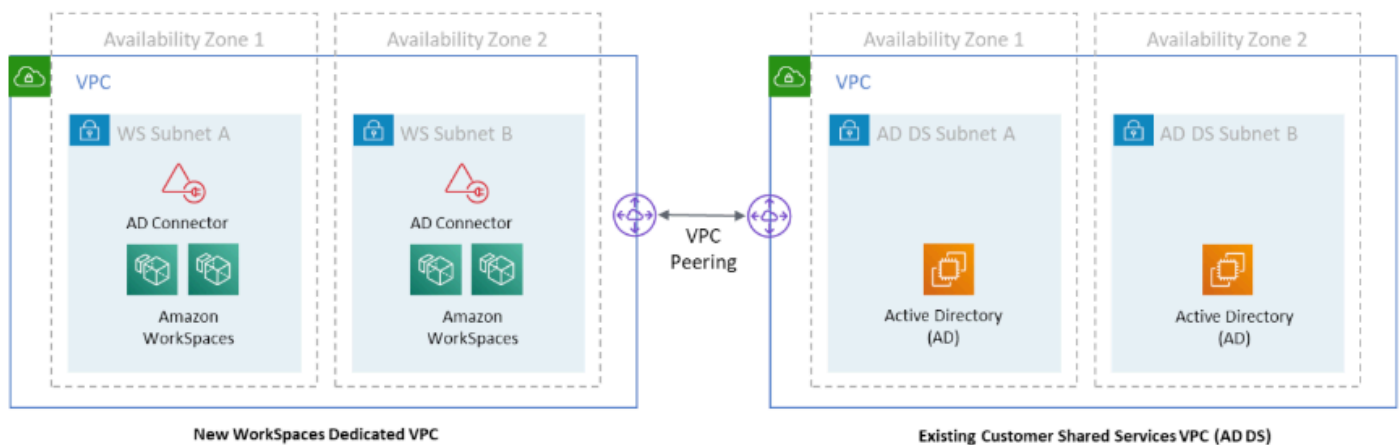
VPC peering

IP address and port requirements

The Amazon WorkSpaces client application requires outbound access on ports 443 (TCP) and 4195 (UDP and TCP).

Port 443 (TCP) is used for client application updates, registration, and authentication. The desktop client applications support the use of a proxy server for port 443 (HTTPS) traffic.

To enable the use of a proxy server:

1. Open the client application.

2. Choose **Advanced Settings**.

3. Choose **Use Proxy Server**.

4. Specify the address and port of the proxy server.

5. Choose **Save**.

Port 4195 (UDP and TCP) is used for streaming the WorkSpace desktop and for health checks. The desktop client applications do not support the use of a proxy server for port 4195 traffic; they require a direct connection to port 4195. This port must be open to the WorkSpaces Streaming Protocol (WSP) Gateway IP address ranges, and to the health check servers in the Region that the WorkSpace is in. For more information, refer to Health Check Servers and WSP Gateway Servers.

> ⓘ **Note**
>
> The TURN protocol is also used over port 4195 for client connections to the WorkSpaces Streaming Gateway. Refer to steps eight and nine in the *Architecture overview*.

Table 1 — Required ports and protocols

Source	Destination	Port	Type
WorkSpace Client	WorkSpaces	TCP 443	HTTPS
WorkSpace Client	WorkSpaces	TCP/UDP 4195	WSP
WorkSpaces	AD Domain Controller	TCP/UDP 53	DNS
WorkSpaces	AD Domain Controller	TCP/UDP 88	Kerberos Auth
WorkSpaces	AD Domain Controller	UDP 123	NTP
WorkSpaces	AD Domain Controller	TCP 135	RPC
WorkSpaces	AD Domain Controller	UDP 137 - 138	Netlogon
WorkSpaces	AD Domain Controller	TCP 139	Netlogon
WorkSpaces	AD Domain Controller	TCP/UDP 389	LDAP
WorkSpaces	AD Domain Controller	TCP/UDP 445	SMB

Source	Destination	Port	Type
WorkSpaces	AD Domain Controller	TCP/UDP 464	Kerberos
WorkSpaces	AD Domain Controller	TCP/UDP 636	LDAP
WorkSpaces	AD Domain Controller	TCP 49152 - 65535	Dynamic RPC
WorkSpaces	AD Domain Controller	UDP 1812	RADIUS
AD Connector	AD Domain Controller	TCP/UDP 53	DNS
AD Connector	AD Domain Controller	TCP/UDP 88	Kerberos Auth
AD Connector	AD Domain Controller	TCP/UDP 389	LDAP

Install and configure Active Directory and Certificate Authority

To install Active Directory on the server:

1. From the task bar, open the **Server Manager**.

2. From the **Server Manager** dashboard, select **Manage** and then **Add roles and features**. The Roles and Features Wizard launches. This wizard enables you to make modifications to the Windows Server instance.

3. On the **Installation Type** screen, select **Role-based or features-based** and select **Next**.

4. By default, the current server is selected. Choose **Next**.

5. On the **Server Roles** screen, choose the check box next to **Active Directory Domain Services**. A notice explains that you must also install additional roles, services, or features to install Domain Services. These additional capabilities include certificate services, federation services, lightweight directory services, and rights management.

6. To select additional capabilities, select **Add Features**. Choose **Next**.

7. On the **Select features** screen, select the check boxes next to the features that you want to install during the AD DS installation process. Choose **Next**.
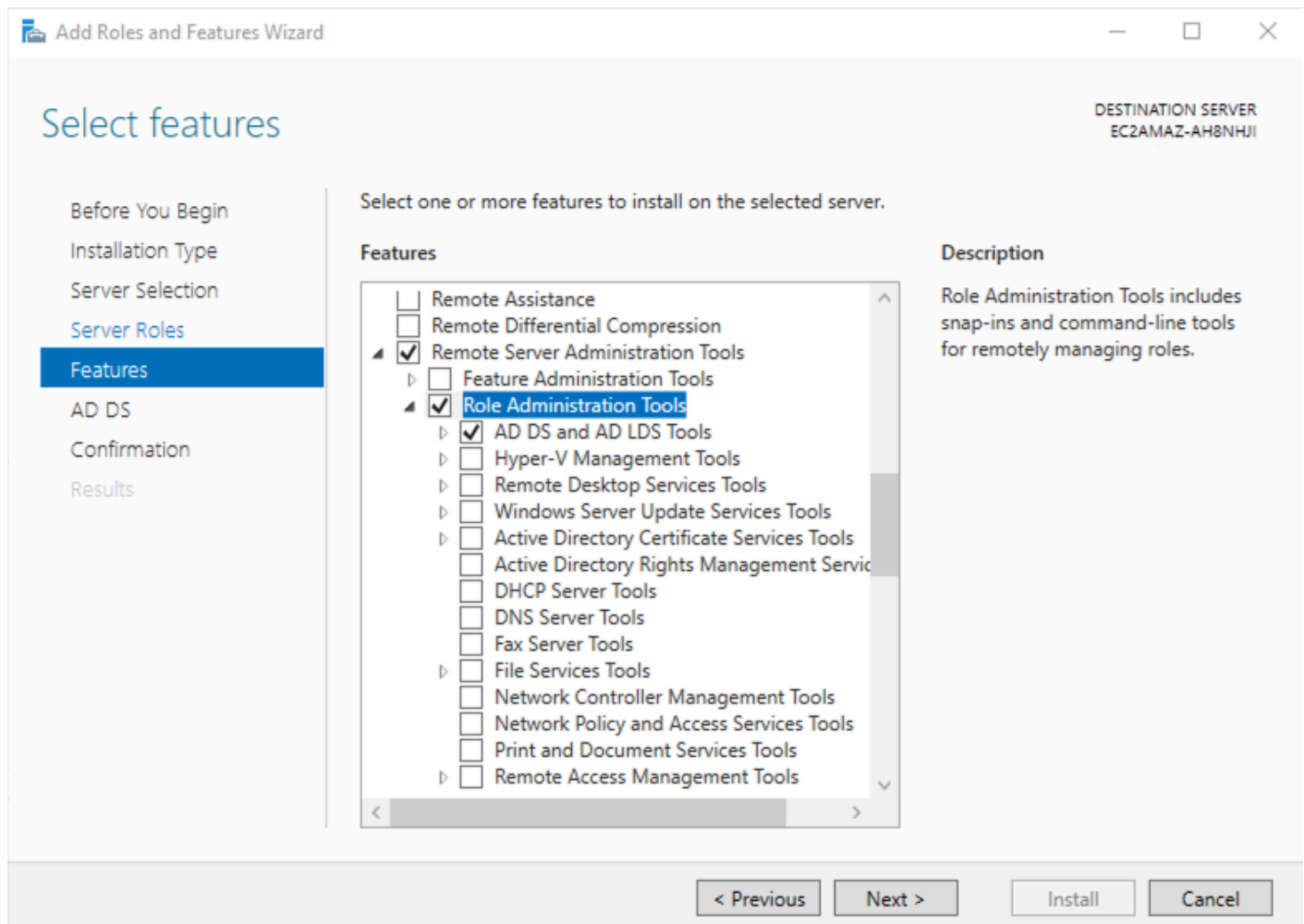
Active Directory feature installation

8. Review the information on the **AD DS** tab, then select **Next**.

9. Review the information on the **Confirm installation selections** screen, then select **Install**. Information on the progress of the installation displays. After the installation is complete, the AD DS role displays on the "Server Manager" landing page.

Configure Active Directory

After you have installed the AD DS role, you must configure the server for your domain.

To configure the server:

1. From the task bar, open the **Server Manager**.

2. Choose the triangular yellow notifications icon in the top navigation bar of the Server Manager window. The **Notifications** pane opens and displays a **Post-deployment Configuration** notification. Choose the **Promote this server to a domain controller** link that appears in the notification.
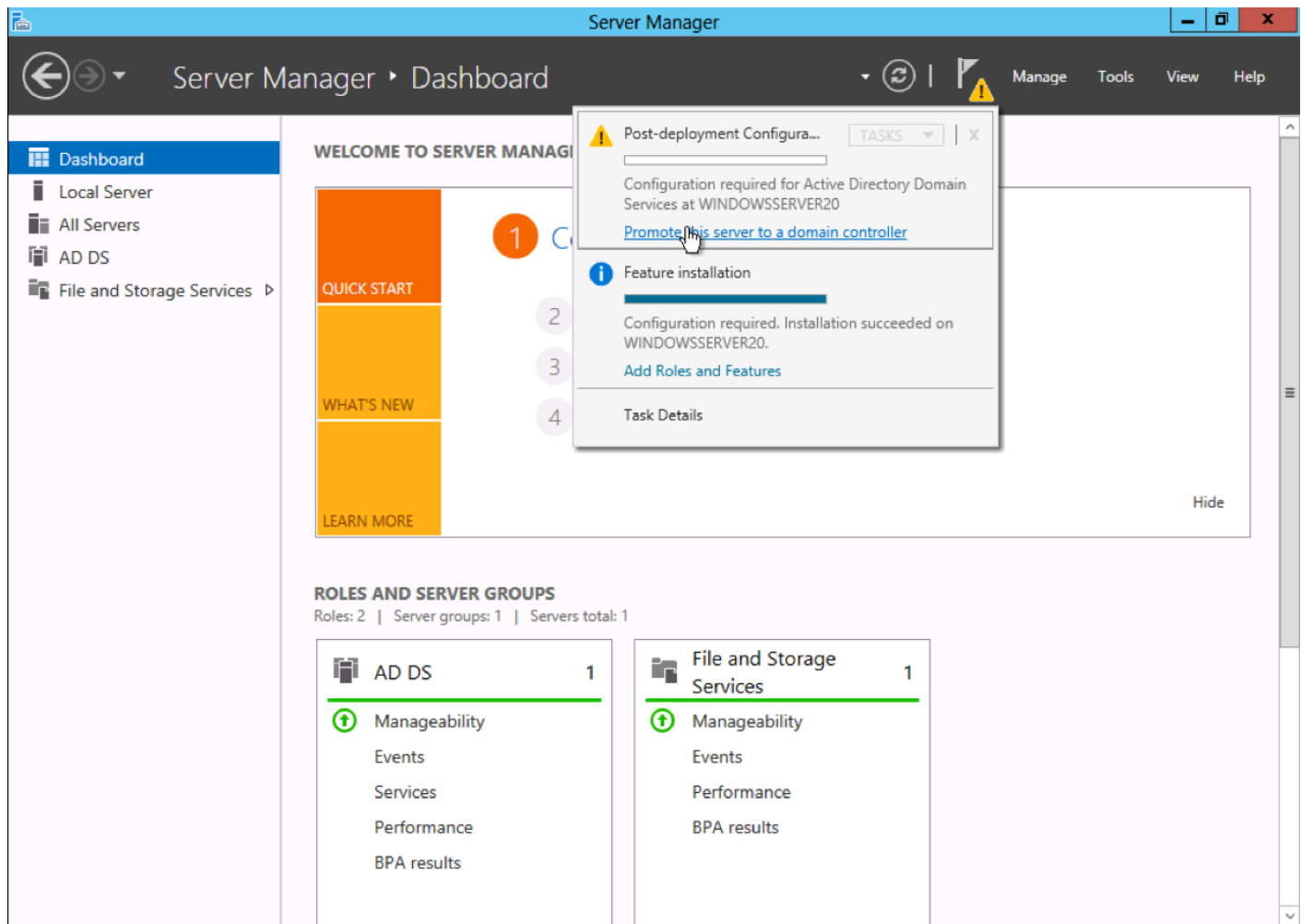
Active Directory post-deployment configuration

3. From the **Deployment Configuration** tab, choose **Radial options** > **Add a new forest**. Enter your root domain name in the **Root domain name** field and select **Next**.

4. Choose a **Domain** and a **Forest functional level**. (These selections affect features and server domain controller eligibility. For further information on domains and forest functional levels, see the official Microsoft documentation.)

5. Enter a password for Directory Services Restore Mode (DSRM) in the **Password** field. (The DSRM password is used when booting the Domain Controller into recovery mode.)

6. Review the warning on the **DNS Options** tab and select **Next**.

7. Confirm or enter a **NetBIOS name** and select **Next**.

8. Specify the locations of the **Database**, **Log files**, and **SYSVOL folders**, then select **Next**.

9. Review the configuration options and select **Next**.

10. The system checks if all of the necessary prerequisites are installed on the system. If the system passes these checks, select **Install**. The server automatically reboots after the installation is complete.

11. After the server reboots, reconnect to it by using Microsoft Remote Desktop Protocol (RDP).

Create a service account and delegate privileges

To connect to your existing directory, you must have the credentials for your AD Connector service account in the existing directory that has been delegated certain privileges. While members of the "Domain Admins" group have sufficient privileges to connect to the directory, as a best practice, you should use a service account that has only the minimum privileges necessary to connect to the directory. The following procedure demonstrates how to create a new group called "Connectors", delegate the necessary privileges needed to connect AWS Directory Service to this group, and then add a new service account to this group.

This procedure must be performed on a machine that is joined to your directory and has the "Active Directory User and Computers MMC" snap-in installed. You must also be logged in as a domain administrator.

To delegate privileges to your service account:

1. Open **Active Directory User and Computers** and select your domain root in the navigation tree.

2. In the list in the left-hand pane, right-click **Users**, select **New**, and then select **Group**.

3. Locate the **New Object - Group** dialog box.

4. For **Group name**, enter Connectors.

5. For **Group scope**, choose **Global**.

6. For **Group type**, enter Security.

7. Choose **OK**.

8. In the **Active Directory User** and **Computers** navigation tree, choose your domain root.

9. In the menu, choose **Action**, and then **Delegate Control**.

10. On the **Delegation of Control Wizard** page, select **Next**, then select **Add**.

11. In the **Select Users, Computers, or Groups** dialog box, enter **Connectors** and select **OK**. If more than one object is found, choose the **Connectors** group created above. Choose **Next**.

12.On the **Tasks to Delegate** page, select **Create a custom task to delegate**. Choose **Next**.

13.Choose **Only the following objects in the folder**, and then choose **Computer objects and User objects**.

14.Choose **Create selected objects in this folder** and **Delete selected objects in this folder**. Choose **Next**.

15.Choose **General** and **Property-specific**, **Read** and **Write**. Choose **Next**.

16.Verify the information on the **Completing the Delegation of Control Wizard** page, and select **Finish**.

17.Create a user with a strong password and add that user to the "Connectors" group. This user will be known as your AD Connector service account. Because this user it is now a member of the "Connectors" group, they now have sufficient privileges to connect AWS Directory Service to the directory.

Enable Kerberos Constrained Delegation for the AD Connector Service account

To use smart card authentication with AD Connector, you must enable Kerberos Constrained Delegation (KCD) for the AD Connector Service account to the Lightweight Active Directory Protocol. (LDAP) service in the on-premises AD directory.

Kerberos Constrained Delegation is a feature in Windows Server. This feature enables administrators to specify and enforce application trust boundaries by limiting the scope where application services can act on a user's behalf. For more information, see Kerberos constrained delegation.

1. Use the `SetSpn` command to set a Service Principal Name (SPN) for the AD Connector service account in the on-premises AD. This enables the service account for delegation configuration. The SPN can be any service or name combination, but not a duplicate of an existing SPN. The `-s` checks for duplicates.

2. Open an elevated command prompt using "Run as administrator".

3. Run this command:

```
setspn -s my/spn service_account
```

The following figure shows the successful result of running of the `SetSpn` command.

```
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -s my/spn adconnector
Checking domain DC=tfcwsp,DC=local

Registering ServicePrincipalNames for CN=ADConnector,CN=Users,DC=tfcwsp,DC=local
        my/spn
Updated object

C:\Users\Administrator>_
```

SetSpn command running

4. In **AD Users and Computers**, right-click on the AD Connector service account and choose **Properties**.

5. Choose the **Delegation** tab.

6. Choose the **Trust this user for delegation to specified service only** and **Use any authentication protocol** radio buttons.

7. Choose **Add**, **Users or Computers**, and then select **Advanced**.

8. Select **Find Now** to list all available resources, and then find your domain controller (DC) in the list.

Finding the domain controller in a list of resources

9. Select your domain controller and then choose **OK** to display a list of available services used for delegation.

10.Choose the LDAP service type that has a description of your forest and select **OK**.

11.Click **OK** again to save the configuration.

12.Repeat this process for other domain controllers in AD. Alternatively, you can automate the process using PowerShell.

Install Certificate Authority

For a DC to support Smart Card authentication, each DC must have a certificate issued by a trusted CA. This CA can be either a trusted third-party authority or a local Active Directory Certificate authority. Use the following directions to install Active Directory Certificate Services (ADCS) and create a new local enterprise CA.

To install ACDS and create a new local enterprise CA:

1. Log on as a member of both the "Enterprise Admins" group and the root domain's "Domain Admins" group.

2. In Server Manager, select **Manage**, and then select **Add Roles and Features**. The Add Roles and Features Wizard opens.

3. In **Select Installation Type**, ensure that **Role-Based or feature-based installation** is selected, and then select **Next**.

4. **Select destination server**, ensure that **Select a server from the server pool** is selected. In **Server Pool**, ensure that the **local computer** is selected. Choose **Next**.

5. In **Select Server Roles**, in **Roles**, select **Active Directory Certificate Services**. When you are prompted to add required features, select **Add Features**, and then select **Next**.

6. In **Select features**, select **Next**.

7. In **Active Directory Certificate Services**, read the provided information, and then select **Next**.

8. In **Confirm installation selections**, select **Install**. Do not close the wizard during the installation process.

9. When installation is complete, select **Configure Active Directory Certificate Services on the destination server**. The AD CS Configuration wizard opens. Read the credentials information and, if needed, provide the credentials for an account that is a member of the Enterprise Admins group. Choose **Next**.

10. In **Role Services**, select **Certification Authority**, and then select **Next**.

11. On the **Setup Type** page, verify that **Enterprise CA** is selected, and then choose **Next**.

12. On the **Specify the type of the CA** page, verify that **Root CA** is selected, and then choose **Next**.

13. On the **Specify the type of the private key** page, verify that **Create a new private key** is selected, and then choose **Next**.

14. On the **Cryptography for CA** page, keep the default settings for **CSP (RSA#Microsoft Software Key Storage Provider)** and **hash algorithm** (SHA256), and determine the best key character

length for your deployment. Large key character lengths provide optimal security; however, they can impact server performance and might not be compatible with legacy applications. It is recommended that you keep the default setting of 2048. Choose **Next**.

15.On the **CA Name** page, keep the suggested common name for the CA or change the name according to your requirements. Ensure that you are certain the CA name is compatible with your naming conventions and purposes, because you cannot change the CA name after you have installed AD CS. Choose **Next**.

16.On the **Validity Period** page, in **Specify the validity period**, type the number and select a time value (**Years**, **Months**, **Weeks**, or **Days**). The default setting of five years is recommended. Choose **Next**.

17.On the **CA Database** page, in **Specify the database locations**, specify the folder location for the certificate database and the certificate database log. If you specify locations other than the default locations, ensure that the folders are secured with access control lists (ACLs) that prevent unauthorized users or computers from accessing the CA database and log files. Choose **Next**.

18.In **Confirmation**, choose **Configure** to apply your selections, and then choose **Close**.

Alternatively, use the following PowerShell snippet to install and configure ADCS:

1. Install the ADCS Certificate Authority Windows Feature:

```
Install-WindowsFeature ADCS-Cert-Authority -IncludeManagementTools
```

2. Create the Enterprise Root CA.

```
    Install-ADcsCertificationAuthority `
    -CAType EnterpriseRootCa `
    -CACommonName `
    -CADistinguishedNameSuffix $domainDistinguishedName `
    -CryptoProviderName "RSA#Microsoft Software Key Storage
    Provider" `
    -KeyLength 2048 `
    -HashAlgorithmName "SHA256"
```

Install the Certificate Authority Trust Anchors

The most current root certificates must be installed on both servers and workstations. InstallRoot is a utility that manages certificates for DoD and Network Security Services (NSS)-trusted root and intermediate CAs on Microsoft servers and workstations.

To download, install, and run the NIPRNet InstallRoot application:

1. Open a web browser and navigate to the [DoD Cyber Exchange Public Tools and Configuration Files](#) page.
2. Under the Tools heading, download the latest Windows Installer (MSI) version of InstallRoot.
3. Run the InstallRoot installation tool.

> ⓘ **Note**
>
> Administrative rights are required when installing the InstallRoot application under the `C:\Program Files\` location on the system.

4. Run the tool as an administrator to install the DoD certificates into the Windows/Internet Explorer local machine trust store.

Publish DoD PKI certificates to the Active Directory NTAuth store using InstallRoot

Active Directory has an additional certificate store called NTAuth. The certificates that get installed in the Active Directory NTAuth store then get replicated to the local NTAuth store on the Domain Controllers. The Domain Controllers must have the intermediate and root CA certificates installed in their local NTAuth store to allow for smart card authentication using the certificates on the DoD CAC. These steps will install the CA certificates into the Active Directory NTAuth store using InstallRoot. InstallRoot version 4.1 or newer is required to install CA certificates into the NTAuth store.

To install the CA certificates into the NTAuth store:

1. Right-click the **InstallRoot** utility and choose **run as administrator** when launching InstallRoot.

> **ⓘ Note**
>
> Active Directory Enterprise Administrator rights are required to successfully load the CA certificates into the NTAuth certificate store.

2. Choose the **Certificate** tab.

3. Expand the **Install DoD Certificates group** by choosing the ▾ **symbol**.

4. Highlight the **top certificate** (DoD Root CA2).

5. Choose **PEM Export** and select a directory to store the exported certificate (for example, c:\certs).

6. Open an **elevated command prompt** using **Run as administrator**, and navigate to the directory where the certificate was stored in the previous step.

7. Run this command:

```
certutil -dspublish -f "DoD_Root_CA_2__0x05__DoD_Root_CA_2.cer" NTAuthCA
```

Repeat step 4 through step 7 for the remaining DoD Root CAs.

The following figure shows the certificate successfully installed into the NTAuth store.


```
C:\Users\Administrator\Desktop>certutil -dspublish -f "DoD_Root_CA_3__0x01__DoD_Root_CA_3.cer" NTAuthCA
ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=tfcwsp,DC=local?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.

C:\Users\Administrator\Desktop>certutil -dspublish -f "DoD_Root_CA_4__0x01__DoD_Root_CA_4.cer" NTAuthCA
ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=tfcwsp,DC=local?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.

C:\Users\Administrator\Desktop>certutil -dspublish -f "DoD_Root_CA_5__0x0F__DoD_Root_CA_5.cer" NTAuthCA
ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=tfcwsp,DC=local?cACertificate

Certificate added to DS store.

CertUtil: -dsPublish command completed successfully.
```

*Publish certificate into the NTAuth certificate store*

8. In the **InstallRoot** utility, choose the **Store** tab.

9. Choose the **Active Directory NTAuth** icon.

10. A pop-up window appears with a security warning stating that any actions in the NTAuth store impact the entire domain. Choose **OK**.

11. A new store called NTAuth is created. Choose the **Active Directory NTAuth** tab.

12. Confirm there is a green check mark beside **Install DoD Certificates**.
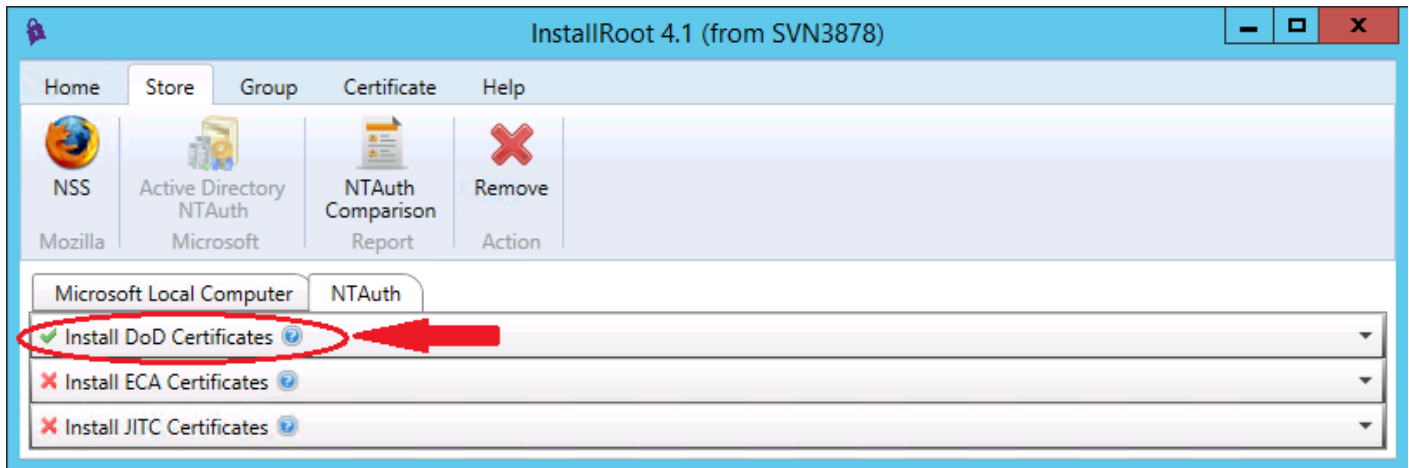
InstallRoot install DoD certificates

13. Choose the **Home** tab.

14. Choose the **Install Certificates** button. You may receive a prompt that configuration changes have been made and would you like to save those changes. Choose **Yes** to proceed.

15. A summary window displays the results. After checking the results, choose **OK**, then exit InstallRoot.

Enable smart card logon with third-party certification authorities

Smart Card Authentication to Active Directory requires that Smartcard workstations, Active Directory, and Active Directory domain controllers be configured properly. Active Directory must trust a certification authority to authenticate users based on certificates from that CA. Both Smartcard workstations and domain controllers must be configured with correctly configured certificates.

Download DoD root certificates

Export or download the third-party root certificate. How you obtain the party root certificate varies by vendor. The certificate must be in Base64 Encoded X.509 format.

The most current DoD certificates bundles can be downloaded from the DoD Cyber Exchange website. This zip file contains the DoD PKI CA certificates in PKCS#7 certificate bundles containing either Privately Enhanced Mail (PEM)-encoded or Distinguished Encoding Rules (DER)-encoded certificates. Separate PKCS#7 certificate bundles are also included for each root CA, for relying parties who may wish to accept only certificates issued with the key and signature hash combinations (for example, RSA-2048/SHA-256) issued by a given root. Instructions for verifying the integrity of all p7b files using the signed SHA-256 hashes file are included in the README.

To download the DOD root certificates:

1. Open a web browser and navigate to the [DoD Cyber Exchange Public Tools and Configuration Files](#) page.

2. Under the **Tools** heading, download the latest **PKI CA Certificate Bundles: PKCS#7 For DoD PKI Only - Version 5.6**.

Update default domain policy with third party root CAs

Add the Department of Defense third-party root CAs to the trusted roots in an Active Directory Group Policy object.

To configure Group Policy in the Windows domain to distribute the third-party CAs to the trusted root store of all domain computers:

1. Open **Group Policy Management**, choose your domain root in the navigation tree, and expand the **Group Policy Objects** container.

2. Choose the **Default Domain Policy Group Policy** object, and then choose **Edit**. A new window opens.

3. In the left pane, choose **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **Public Key Policies**.
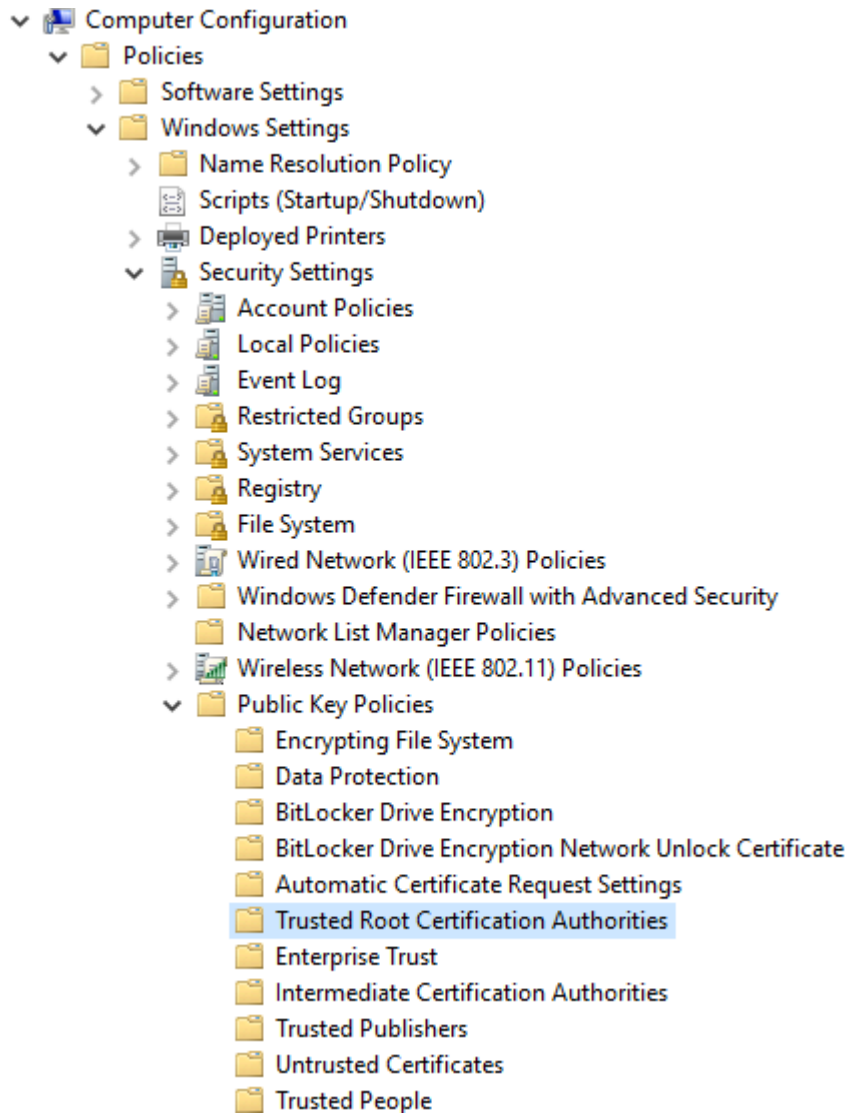
Trusted Root Certification Authorities folder location

4. Right-click **Trusted Root Certification Authorities**.

5. Select **All Tasks**, and then choose **Import**.

6. Follow the instructions in the wizard to import the certificate file
   `Certificates_PKCS7_v5.6_DoD.der`.

7. A confirmation window appears when the import is complete. Choose **OK**.

8. Drag and drop all of the **intermediate DoD certificate authorities** to the **Trusted Intermediate Certification Authorities** folder.

9. Close the **Group Policy** window.

Generate the issuing CA certificate

To generate the third party issuing the CA to the Group Policy object and the NTAuth store in AD:

1. Log into the Root Certification Authority server with an Administrator account.

2. Select **Start** > **Run** >, enter **Cmd**, and choose **Enter**.

3. To export the Root Certification Authority server to a new file name called ca_name.cer, enter:

```
certutil -ca.cert ca_name.cer
```

The following figure shows the certificate successfully installed into the NTAuth store.

```
C:\Users\Administrator\Desktop>certutil -ca.cert ca_demo.cer
CA cert[0]: 3 -- Valid
CA cert[0]:
-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIQUyFwyIxbgKpE7WK8PyyDajANBgkqhkiG9w0BAQsFADBT
MRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFjAUBgoJkiaJk/IsZAEZFgZ0ZmN3c3Ax
IjAgBgNVBAMTGXRmY3dzcC1FQzJBTUFaLUFIOE5ISkktQ0EwHhcNMjAxMjEwMTc0
MTMzWhcNMjUxMjEwMTc1MTMzWjBTMRUwEwYKCZImiZPyLGQBGRYFbG9jYWwxFjAU
BgoJkiaJk/IsZAEZFgZ0ZmN3c3AxIjAgBgNVBAMTGXRmY3dzcC1FQzJBTUFaLUFI
OE5ISkktQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC9pto6SyXH
u2op8cfdHZzLiHySgB3ywSZ90rOWf0U0JBFCkcsrtLS7J1U9/OknMl/gM8zWNlzM
5aRAc409RjuDHYIm9SpKx4JCZUjMMFjf7TtxQPQUzu0ftgorExN1jWm+imbDUYj0
e4KzbVtZFcxs+ZjbBYpgR2cznNayqdJyScI7GcCfHXDEl0m3tyOjf3XelB9+NC8K
poMbEAAiy+A2ev/EjrvOrZSEXY+w49X97kct85cGNEllFGzaQ2P95NF7AtDKn0zm
ZMKRBHYdbVzbUvBI52S5JyIxlLtWYxfPqVNZArBG6wvayRoee+OmzIi59FWVn4q5
3ePx83iKC9PJAgMBAAGjUTBPMAsGA1UdDwQEAwIBhjAPBgNVHRMBAf8EBTADAQH/
MB0GA1UdDgQWBBTqSWWAILQ6AJs4wbhK4OA7Tli6rzAQBgkrBgEEAYI3FQEEAwIB
ADANBgkqhkiG9w0BAQsFAAOCAQEAVuscuNM5oLDjSYxtkRpLrFO+2dc3zKRu3Iu0
V0C+EkIaoH3bp8MwTWR2ltI2fDhkfYp+IWYlnGq9E1T+qMCqkfzgteOTz7D/JeJK
Fbt8nAgfSAeW2ffzB2k/MW7hg84JliTxqGyoYV3MkR6mSwrVTpxgaq/JWrPLRVYJ
qCVdSbHfKbUJfhJj8kp6anQJV4/QtvqDYInPypi/PWqPMk3t6AemWnFWp27/xamv
+Y/A4f2bAMpzPKs17cefSou3+T2Tz0WY7RsY84/9pTE2QD0jzNf5bk+4loQ6ezST
Xwa3gUTYWFnxMb+zxqn+O0gh7k3qxH0PsvQuoLcagTy0gNYM9g==
-----END CERTIFICATE-----

CertUtil: -ca.cert command completed successfully.

C:\Users\Administrator\Desktop>dir ca_demo.cer
 Volume in drive C has no label.
 Volume Serial Number is E43B-9F7E

 Directory of C:\Users\Administrator\Desktop

12/11/2020  04:52 PM                 901 ca_demo.cer
               1 File(s)            901 bytes
               0 Dir(s)  15,032,414,208 bytes free
```

Use certutil to install the issuing CA certificate into NTAuth store

Update the default domain policy with the issuing party CA

Add the issuing CA to the trusted roots in an Active Directory Group Policy object.

To configure Group Policy in the Windows domain to distribute the issuing CA to the trusted root store of all domain computers:

1. Open **Group Policy Management**, select your domain root in the navigation tree, and expand the **Group Policy Objects** container.

2. Choose the **Default Domain Policy Group Policy** object, and then choose **Edit**. A new window opens.

3. In the left navigation pane, expand the following items:

   - **Computer Configuration**

   - **Policies**

   - **Windows Settings**

   - **Security Settings**

   - **Public Key Policy**

4. Right-click **Trusted Root Certification Authorities**.

5. Select **All Tasks**, then choose **Import**.

6. Follow the instructions in the wizard to import the certificate file generated in the Generate the issuing CA certificate, ca_name.cer.

7. A confirmation window appears when the import is complete. Choose **OK**.

8. Close the **Group Policy** window.

Import the issuing CA certificate into the Enterprise NTAuth store

In a command prompt, type the following command, and then press **ENTER**:

```
certutil -dspublish -f ca_name.cer NTAuthCA
```

The following figure shows the successful import of the certificate into the NTAuth store.

```
C:\Users\Administrator\Desktop\Issuing CA Cert> certutil -dspublish -f ca_demo.cer NTAuthCA
ldap:///CN=NTAuthCertificates,CN=Public Key Services,CN=Services,CN=Configuration,DC=tfcwsp,DC=local?cACertificate

Certificate already in DS store.

CertUtil: -dsPublish command completed successfully.
```

Import the issuing CA certificate into Enterprise NTAuth store

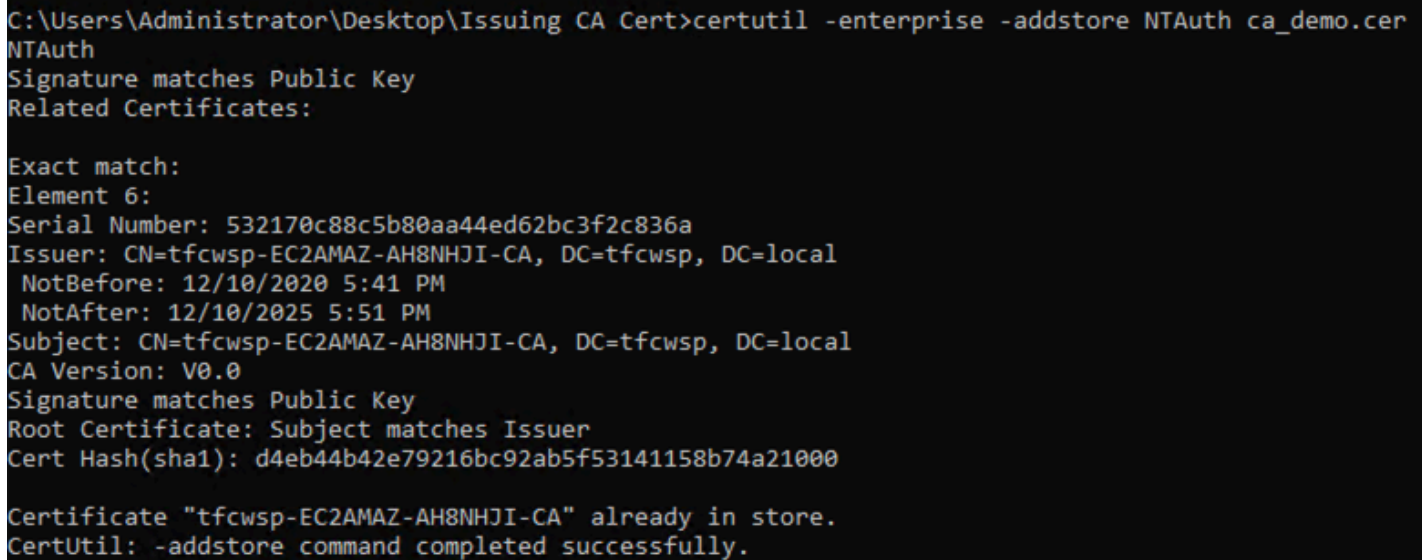The contents of the NTAuth store are cached in the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\EnterpriseCertificates\NTAuth\Certificates
```

This registry key is automatically updated to reflect the certificates that are published to the NTAuth store in the AD configuration container. This behavior occurs when Group Policy settings

are updated and when the client-side extension that is responsible for autoenrollment runs. In certain scenarios, such as AD replication latency or when the "Do not enroll certificates automatically" policy setting is enabled, the registry is not updated. In these scenarios, you can run the following command manually to insert the certificate into the registry location:

```
certutil -enterprise -addstore NTAuth issuing_ca_name.cer
```

The following figure shows the successful insert of the certificate into the registry location.

```
C:\Users\Administrator\Desktop\Issuing CA Cert>certutil -enterprise -addstore NTAuth ca_demo.cer
NTAuth
Signature matches Public Key
Related Certificates:

Exact match:
Element 6:
Serial Number: 532170c88c5b80aa44ed62bc3f2c836a
Issuer: CN=tfcwsp-EC2AMAZ-AH8NHJI-CA, DC=tfcwsp, DC=local
 NotBefore: 12/10/2020 5:41 PM
 NotAfter: 12/10/2025 5:51 PM
Subject: CN=tfcwsp-EC2AMAZ-AH8NHJI-CA, DC=tfcwsp, DC=local
CA Version: V0.0
Signature matches Public Key
Root Certificate: Subject matches Issuer
Cert Hash(sha1): d4eb44b42e79216bc92ab5f53141158b74a21000

Certificate "tfcwsp-EC2AMAZ-AH8NHJI-CA" already in store.
CertUtil: -addstore command completed successfully.
```

Import the issuing CA certificate into Enterprise NTAuth store

Domain controller certificate

Each domain controller that is going to authenticate smartcard users must have a domain controller certificate. Request and install a domain controller certificate on each domain controller.

If you install a Microsoft Enterprise CA in an AD forest, all domain controllers automatically enroll for a domain controller certificate.

Enable smart card logon

The Microsoft implementation for certificate-based authentication to AD requires a unique identifier called the User Principal Name (UPN) to be present in the Subject Alternative Name (SAN) field of the user's certificate. The DoD implements this value in the user's email signature certificate.

The UPN consists of two parts: the *generic name* and the *domain identifier suffix*. The DoD generic name is formatted as the individual's Electronic Data Interchange – Personnel Identifier (EDI-PI). The EDI-PI is appended with the domain identifier suffix: "@mil" for NIPRNet. This unique value (User_EDI-PI@mil) must match the UPN value listed in the user's account in AD for authentication to succeed.

> ⓘ **Note**
>
> Microsoft has updated their security best practices to implement strong attribution in Active Directory authentication using the altSecurityIdentities attributes for Users authenticating with certificates (for example, CAC Cards).
> For more information, go to [Certificate-based authentication changes on Windows domain controllers](#).

Alternative User Principal Name suffix

AD must be configured to accept the DoD-specific alternative UPN suffix. This is a one-time action that must be performed using **Active Directory Domains and Trusts**.

1. Open **Server Manager**. At the top of the dashboard, select **Tools** > **Active Directory Domains and Trusts**.

2. Right-click the **Active Directory Domains and Trusts** root node and select **Properties**.

3. In the **Alternative UPN Suffix** text box insert *mil* and choose **Add**.

4. Choose **OK**. Close the **Active Directory Domains and Trusts** window.

Users

To map a user's certificate to their AD account using the standard method of mapping (UPN), the certificate must contain two things:

- An Enhanced Key Usage (EKU) of "Smart Card Logon" or no EKU, and a Key Usage of "Digital Signature".

- A UPN value in the SAN attribute of the certificate. This UPN must be in the form of *xxxxx@domain_suffix*.

Their account User Logon Name must be renamed to match the UPN in the certificate. Existing users can be modified easily in Active Directory Users and Computers, and new users can be configured properly from the start using the existing new user wizard.

To remap existing users who currently authenticate via username/password:

1. Open **Server Manager**. At the top of the dashboard, select **Tools** > **Active Directory Users and Computers**.

2. Navigate to a user who will be migrated to smart card logon.

3. Right-click the user and select **Properties**.

4. Choose the **Account** tab. Note the user's logon name and UPN suffix.

5. Change the **User Logon Name** to match the **UPN** of this user.

6. Select the **@mil extension** from the **domain suffix** drop-down box to match the domain suffix in the user's certificate UPN value. Do not change the User logon name (pre-Windows 2000) fields.
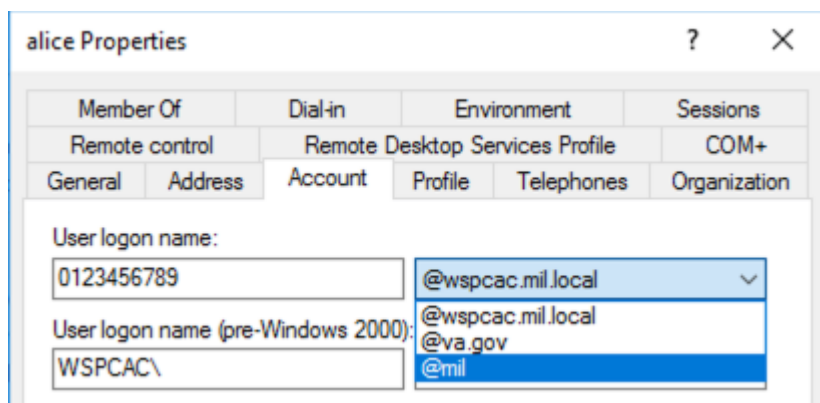
Select user's domain suffix to match UPN value

7. If your organizational policy requires users to log on with smart cards only (no username/ password allowed), scroll down to the **Account options** section and choose **Smart card is required for interactive logon**.

8. Choose **OK** to save the modifications.

To strongly map users in Active Directory using altSecurityIdentities

1. Open Server Manager, then choose **Tools**, **Active Directory Users and Computers**.

2. Choose **View**, **Advanced Features**.

3. Navigate to a user who will be migrated to smart card logon.

4. Right-click the user, then select **Properties**.

5. Choose **Attribute Editor**, find **altSecurityIdentities**, then select **Edit**.

6. In **Values to add**, add the strong attribution value for the user in this format: *X509IssuerSerialNumber*. An example of a strong mapping value might be **X509:<I>IssuerName<SR>1234567890**.

   In the following screenshot, the mapping value is **X509:<I>DC=com,DC=contoso,CN=CONTOSO-DC-CA<SR>1200000000AC11000000002B**.
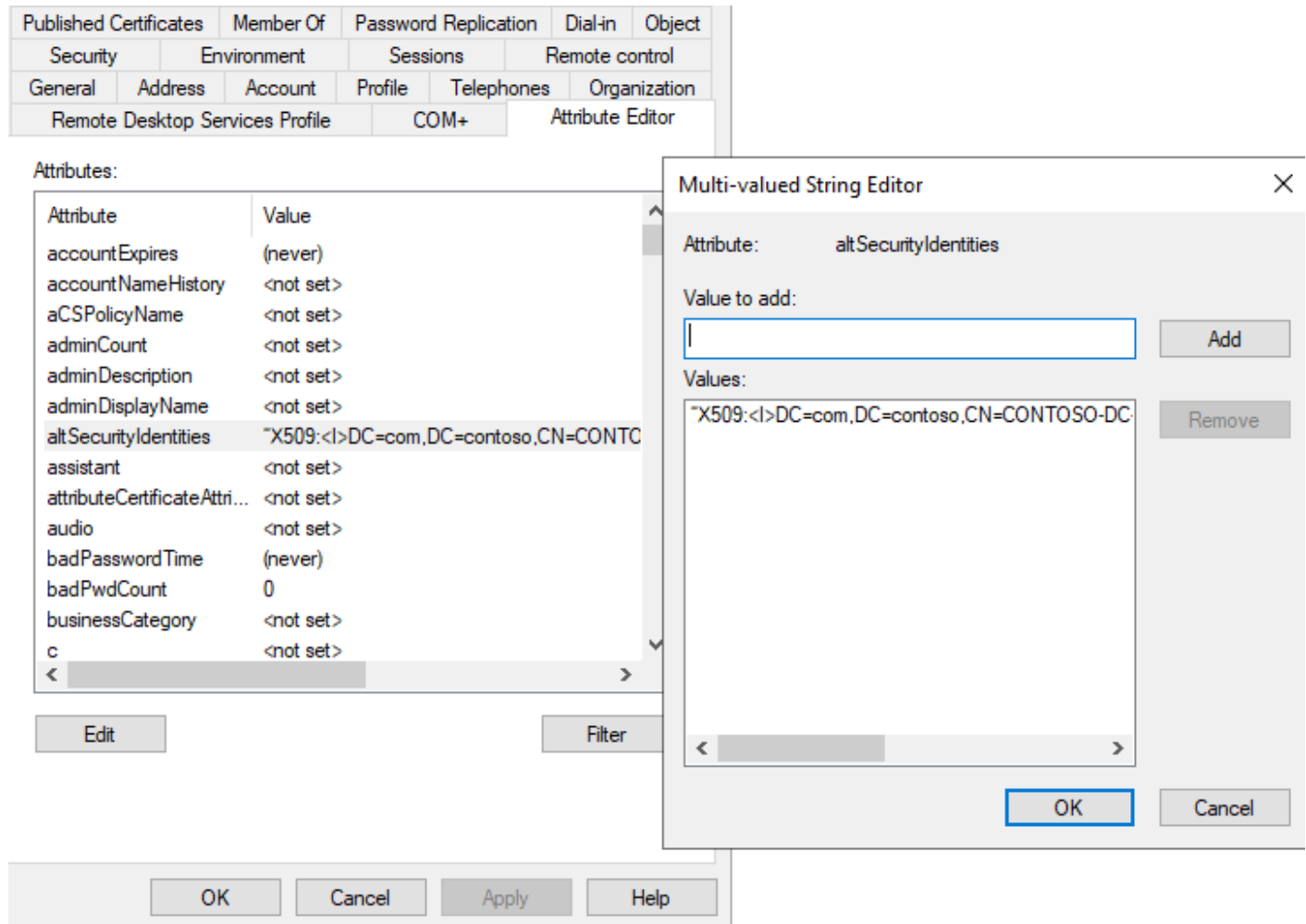
Adding a strong example mapping value

> **ⓘ Note**
>
> There are some fields associated with the certificate, such as Issuer, Subject, and Serial Number, that are reported in a *forward* format. Because of this, they will need to be reversed when you add them to the mapping string of the altSecurityIdentities

attribute. For example, when adding the *X509IssuerSerialNumber* mapping to a user to be authenticated, search for the `Issuer` and `Serial Number` fields of the certificate you intend to map to the user and reverse the order in which they are given. To find these values, find the certificate to map the user, double-click the file and choose **Details**.

See the following sample output:

- `Issuer: CN=CONTOSO-DC-CA, DC=contoso, DC=com`

- `SerialNumber: 2B0000000011AC0000000012`

Then, update the user's altSecurityIdentities attribute in Active Directory with the following string: **X509:<I>DC=com,DC=contoso,CN=CONTOSO-DC-CA<SR>1200000000AC11000000002B**

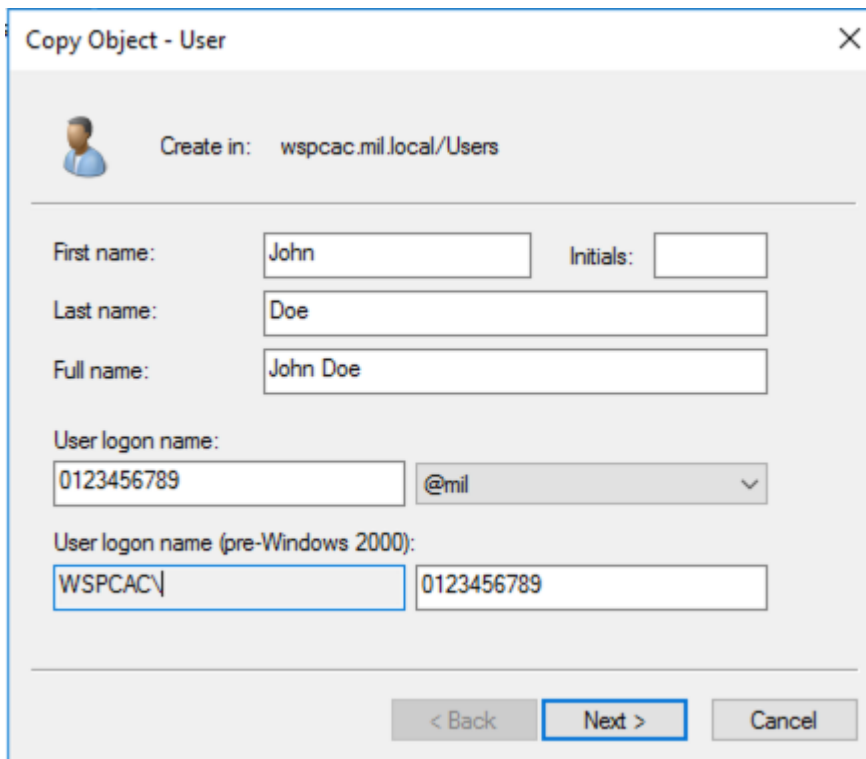Here are some other examples of strong attribution according to the Microsoft documentation:

X509IssuerSerialNumber	"X509:<I>IssuerName<SR>1234567890"	Strong	Recommended
X509SKI	"X509:<SKI>123456789abcdef"	Strong	
X509SHA1PublicKey	"X509:<SHA1-PUKEY>123456789abcdef"	Strong	

List of strong mapping value examples

7. Select **OK**, then **Apply**.

Manually Creating New Users

1. Open **Server Manager**. At the top of the dashboard, choose **Tools**, **Active Directory Users and Computers**.

2. Navigate to the OU container that will hold the new user. Right-click the container and choose **New**, **User**.

3. Enter the user's information, similar to the screen shot below. Enter the user's real name information, but for the **User Logon Name**, enter the EDI-PI of the user with the appropriate domain suffix: EDIPI@mil domain suffix

4. Form the **User Logon Name** (pre-Windows 2000) as it would conform to the proper username convention of your network. Choose **Next**.

Create new user with domain suffix and UPN value

5. Enter the appropriate temporary password for the user, selecting the standard options for your domain. Choose **Next**.

6. Choose **Finish**.

Install the Group Policy Administrative Template files for the WorkSpaces Streaming Protocol (WSP)

To use the Group Policy settings that are specific to Amazon WorkSpaces when using the WorkSpaces Streaming Protocol (WSP), you must add the Group Policy administrative template wsp.admx and wsp.adml files for WSP to the Central Store of the domain controller for your WorkSpaces directory. For more information about .admx and .adml files, see How to create and manage the Central Store for Group Policy Administrative Templates in Windows.

The following procedure describes how to create the Central Store and add the administrative template files to it. Perform the following procedure on a directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory.

To install the Group Policy administrative template files for WSP:

1. From a running Windows WorkSpace, make a copy of the `wsp.admx` and `wsp.adml` files in the `C:\Program Files\Amazon\WSP` directory.

2. On a directory administration WorkSpace or [Amazon Elastic Compute Cloud](#) (Amazon EC2) instance that is joined to your WorkSpaces directory, navigate to the domain's shared network folder. This folder will have your organization's fully qualified domain name (FQDN), such as \\example.com.

3. In Windows File Explorer or the Finder, go to **Network** > **FQDN**.

4. Open the **SYSVOL** folder.

5. Open the **FQDN** folder.

6. Open the **Policies** folder. You should now be in `\\FQDN\SYSVOL\FQDN\Policies`.

7. If it doesn't already exist, create a folder named **PolicyDefinitions**.

8. Open the **PolicyDefinitions** folder.

9. Copy the wsp.admx file into the `\\FQDN\SYSVOL\FQDN\Policies\PolicyDefinitions` folder.

10. Create a folder named **en-US** in the **PolicyDefinitions** folder.

11. Open the **en-US** folder.

12. Copy the wsp.adml file into the `\\FQDN\SYSVOL\FQDN\Policies\PolicyDefinitions\en-US` folder.

To verify that the administrative template files are correctly installed:

1. On your directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory, open the **Group Policy Management** tool (`gpmc.msc`).

2. Expand the forest (`Forest:FQDN`).

3. Expand **Domains**.

4. Expand your **FQDN** (for example, example.com).

5. Expand **Group Policy Objects**.

6. Select **Default Domain Policy**, open the context (**right-click**) menu, and choose **Edit**.

7. In the **Group Policy Management Editor**, choose **Computer Configuration, Policies, Administrative Templates**, **Amazon**, and **WSP**.

8. You can now use this WSP Group Policy object to modify the Group Policy settings that are specific to Amazon WorkSpaces when using WSP.

To enable or disable smart card redirection for Windows WorkSpaces:

By default, Amazon WorkSpaces are not enabled to support the use of smart cards for in-session authentication. If needed, you can enable in-session authentication for Windows WorkSpaces by using Group Policy settings.

1. Ensure that the most recent Amazon WorkSpaces Group Policy administrative template for WSP is installed in the Central Store of the domain controller for your WorkSpaces directory.

2. On your directory administration WorkSpace or Amazon EC2 instance that is joined to your WorkSpaces directory, open the **Group Policy Management** tool (gpmc.msc).

3. Expand the forest (Forest:FQDN).

4. Expand **Domains**.

5. Expand your **FQDN** (for example, example.com).

6. Expand **Group Policy Objects**.

7. Select **Default Domain Policy**, open the context (**right-click**) menu, and choose **Edit**.

8. In the **Group Policy Management** Editor, choose **Computer Configuration, Policies, Administrative Templates**, **Amazon**, and **WSP**.

9. Open the **Enable/disable smart card redirection** setting.

10. In the **Enable/disable smart card redirection** dialog box, choose **Enabled**.

11. Choose **OK**.

12. The Group Policy setting change takes effect after the next Group Policy update for the WorkSpace and after the WorkSpace session is restarted. To apply the Group Policy changes, do one of the following:

- Reboot the WorkSpace (in the Amazon WorkSpaces console, select the WorkSpace, then choose **Actions** > **Reboot WorkSpaces**).

- From an administrative command prompt, enter gpupdate /force.

AWS Directory Service Active Directory Connector

Create an AD Connector

Before starting this procedure, make sure you have completed the prerequisites identified in [AD Connector Prerequisites](#).

To connect to your existing directory with AD Connector:

1. In the [AWS Directory Service console](#) navigation pane, choose **Directories** and then choose **Set up directory**.
2. On the **Select directory type page**, choose **AD Connector**, and then choose **Next**.
3. On the **Enter AD Connector information** page, provide the following information:
   - Select **Directory size**. Choose either the **Small or Large** size option. For more information about sizes, see [Active Directory Connector](#).
   - Enter **Directory description** information.
   - Click **Next**.
4. On the **Choose VPC and subnets** page, select the following information:
   - Select **VPC** from the VPC dropdown.
   - Select two **subnets** for the domain controllers from the subnet dropdowns. The two selected subnets must be in different Availability Zones.
   - Click **Next**.
5. On the **Connect to AD** page, provide the following information:
   - **Directory DNS name** — The fully qualified name of your existing directory, such as corp.example.com.
   - **Directory NetBIOS name** — The short name of your existing directory, such as CORP.
   - **DNS IP addresses** — The IP address of at least one DNS server in your existing directory. These servers must be accessible from each subnet specified in the next section.
   - **Service account username** — The user name of a user in the existing directory. This service account name was created in the [Create service account and delegate privileges section](#). For more information about this service account, see [AD Connector Prerequisites](#).
   - **Service account password** — The password for the existing user.
   - **Confirm password** — Retype the password for the existing user.

6. Click **Next**.

7. On the **Review & create** page, review the directory information and make any necessary changes. When the information is correct, choose **Create directory**. It takes several minutes for the directory to be created. When the directory is created, the **Status** value changes to **Active**.

Smart card authentication requirements

CA certificate requirements

AD Connector requires a CA certificate, which represents the issuer of your user certificates, for smart card authentication. AD Connector matches CA certificates with the certificates presented by your users with their smart cards. Note the following CA certificate requirements:

- Before you can register a CA certificate, it must be more than 90 days away from expiration.

- CA certificates must be in Privacy-Enhanced Mail (PEM) format. If you export CA certificates from inside Active Directory, choose `Base64-encoded X.509 (.CER)` as the export file format.

- All root and intermediary CA certificates that chain from an issuing CA to user certificates must be uploaded for smart card authentication to succeed.

- A maximum of 100 CA certificates can be stored per AD Connector directory.

- AD Connector does not support the RSASSA-PSS signature algorithm for CA certificates.

Certificate revocation checking process

To perform smart card authentication, AD Connector must check the revocation status of user certificates using Online Certificate Status Protocol (OCSP). To perform certificate revocation checking, an OCSP responder URL must be internet accessible.

Obtain Department of Defense Certificates

The most current DoD approved external PKI certificate trust chains can be downloaded from the DoD Cyber Exchange website. This zip file contains certificate trust chains for DoD Approved External PKIs. Version 7.3 adds a rekeyed Treasury PKI root and new NASA issuance chain and removes several expired CAs.

1. Open a web browser and navigate to the [DoD Cyber Exchange Public Tools and Configuration Files](#) page.

2. Download the latest **DoD Approved External PKI Certificate Trust Chains - Version 7.3** under the **Tools** heading.

3. All DoD certificates have a OCSP responder URL of `http://ocsp.disa.mil`.

Alternatively, InstallRoot can extract certificates directly to PEM format (required for import to AWS Directory Services):

1. Open the InstallRoot application.

2. Choose the **Certificate** menu option.

3. Choose all installed DoD root and intermediate certificates that are desired for export.

4. Under **Export**, choose **PEM**.
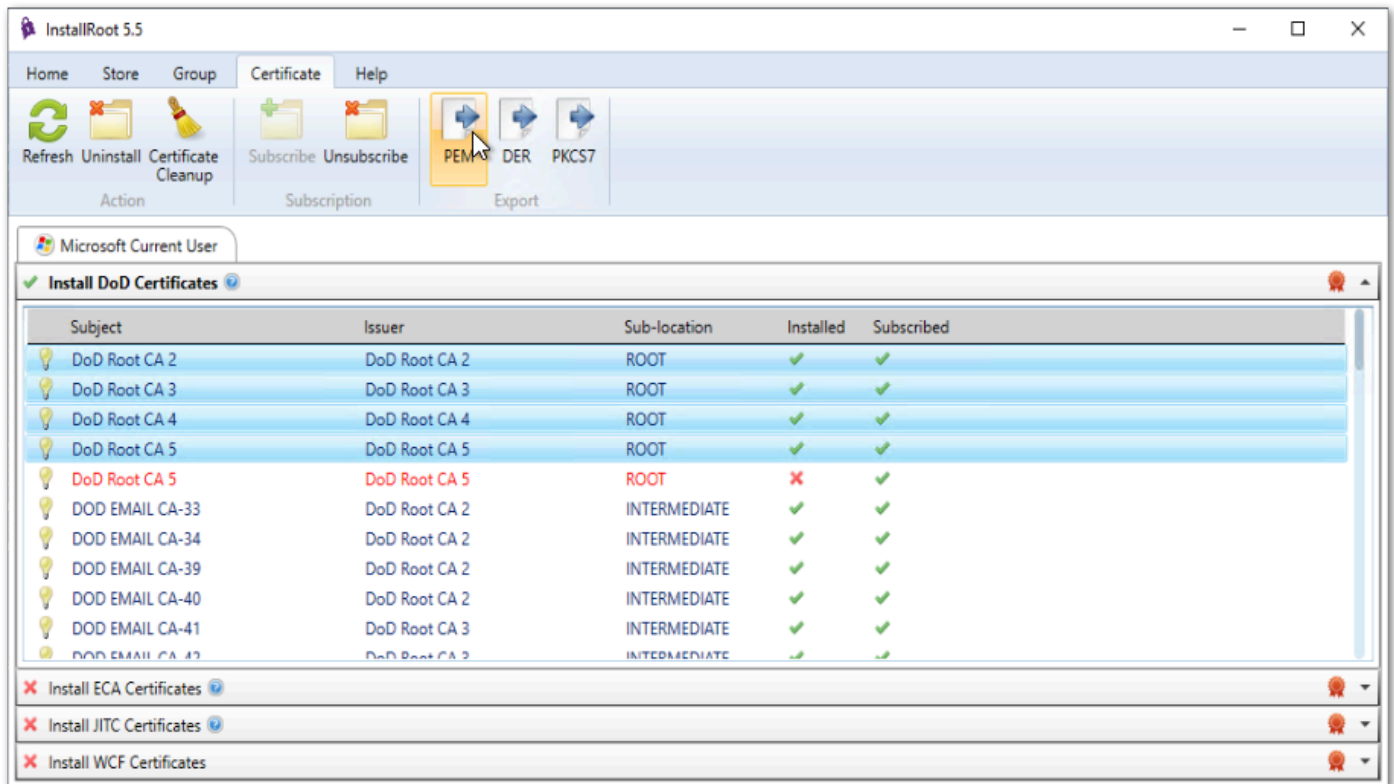
Export root and intermediate certificates with InstallRoot

5. Choose a directory to save the exported certificates, and click **OK**.

Register the CA Certificates with AD Connector

To register your CA certificate in AD Connector, use the following CLI command:

```
    aws ds register-certificate --directory-id your_directory_id --certificate-data
    file://your_file_path --type ClientCertAuth --client-cert-auth-settings
    '{"OCSPUrl":"http://your_OCSP_address"}' --region us-gov-west-1
```

For the certificate data, point to the location of your CA certificate. To provide a secondary OCSP responder address, use the optional ClientCertAuthSettings object. The response provides a certificate ID.

> ⓘ **Note**
>
>   Each certificate must be registered individually.

To upload multiple certificates, the following PowerShell command can be used on Windows-based systems where the AWS CLI V2 has been installed:

```
    Get-ChildItem "C:\{file location}" -Filter *.cer | Foreach-Object { aws ds
    register-certificate --directory-id your_directory_id --certificate-data file://
 $_ --type
    ClientCertAuth --client-cert-auth-settings
    '{\"OCSPUrl\":\"http://{your_ocsp_address}\"}' --endpoint
    https://ds-fips.us-gov-west-1.amazonaws.com }
```

To verify the status of a CA certificate registration or a list of registered CA certificates, run the following command:

```
    aws ds list-certificates --directory-id your_directory_id
```

The following screenshot shows the successful listing of certificates registered with the specified AD Connector.

```
f0189856da26 certs:  aws ds list-certificates --directory-id d-986738b317
CERTIFICATESINFO        c-9867319959    CN=DoD Interoperability Root CA 1,OU=PKI,OU=DoD,O=U.S. Government,C=US  2027-06-15T10:49:11-04:00       Registered      ClientCertAuth
CERTIFICATESINFO        c-9867319995a   CN=DoD Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US  2030-11-24T09:25:10-05:00       Registered      ClientCertAuth
CERTIFICATESINFO        c-9867319995b   CN=DoD Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US    2029-12-05T10:00:10-05:00       Registered      ClientCertAuth
CERTIFICATESINFO        c-9867319995c   CN=DoD Root CA 5,OU=PKI,OU=DoD,O=U.S. Government,C=US    2041-06-14T13:17:27-04:00       Registered      ClientCertAuth
CERTIFICATESINFO        c-9867319995d   CN=DOD EMAIL CA-33,OU=PKI,OU=DoD,O=U.S. Government,C=US  2021-09-22T09:34:57-04:00       Registered      ClientCertAuth
CERTIFICATESINFO        c-9867319995e   CN=DOD EMAIL CA-34,OU=PKI,OU=DoD,O=U.S. Government,C=US  2021-09-22T09:41:54-04:00       Registered      ClientCertAuth
CERTIFICATESINFO        c-9867319995f   CN=DOD EMAIL CA-39,OU=PKI,OU=DoD,O=U.S. Government,C=US  2021-11-08T09:14:47-05:00       Registered      ClientCertAuth
CERTIFICATESINFO        c-9867319980    CN=DOD SW CA-56,OU=PKI,OU=DoD,O=U.S. Government,C=US     2022-11-23T10:48:22-05:00       Registered      ClientCertAuth
```

List certificates registered with AD Connector

Enable smart card authentication for Amazon WorkSpaces

To enable smart card authentication for Amazon WorkSpaces in AD Connector, use the following
CLI command:

```
    aws ds enable-client-authentication --directory-id your_directory_id --type
  SmartCard
```

If successful, AD Connector returns an HTTP 200 response with an empty HTTP body.

```
f0189856da26 certs:  aws ds enable-client-authentication --directory-id d-986738b317 --type SmartCard
f0189856da26 certs:  █
```

Enable smart card authentication on AD Connector

For details about enabling smart card authentication in AD Connector, see Enable smart card
authentication in AD Connector.

Amazon WorkSpaces

WorkSpaces Directory registration

Use the WorkSpaces portal to register the AD Connector Directory with WorkSpaces. Details about registering a directory with WorkSpaces can be found on the Register a Directory with Amazon WorkSpaces page. Once registration of the Directory is completed, update the Directory configuration within the WorkSpaces Console. Details for updating the Directory can be found on the Update Directory Details for Your WorkSpaces page.

WorkSpaces image and customer bundle creation

Amazon WorkSpaces come with a default set of applications that includes Internet Explorer 11 and Firefox. You can choose to add "Plus" application bundles to your Amazon WorkSpaces with Windows 10, which include Microsoft Office Professional 2016 and Trend Micro Worry-Free Business Security.

A custom WorkSpace image and bundle can be created by following the steps located on the Create a Custom WorkSpaces Image and Bundle page. The custom WorkSpace image and bundle is used to create WorkSpaces for your users.

Launch WorkSpaces

Using the WorkSpaces Console, follow the launch wizard to configure and launch a WorkSpace associated with specific user.

During the "Select Bundle" step of the wizard, be sure to select **only WSP enabled WorkSpace Bundles**. You must select a WSP-enabled bundle to use smart card authentication.

*Select **WSP Bundle** to use smart cards with WorkSpaces*

For details about launching Amazon WorkSpaces, see Launch a WorkSpace Using AD Connector.

Security

Strong authentication

Strong authentication is provided through the user of a Common Access Card/Personal Identity Verification (CAC/PIV) card, which is a smart card used to identify active-duty military personnel, selected reservists, US Department of Defense (DoD) civilian employees, and eligible contractor personnel. In addition to providing physical access to buildings and protected areas, it also allows access to DoD computer networks and systems, satisfying two-factor authentication, digital security, and data encryption. It leverages a Public Key Infrastructure (PKI) Security Certificate to verify a cardholder's identity prior to allowing access to protected resources. Data from the user's CAC is accessed to validate the user, but neither the CAC certificate data or the pin are stored.

Services accreditation

Table 2 provides a list of AWS Services and features utilized in the Amazon WorkSpaces Common Access Card solution. The current AWS Service DoD SRG accreditation status can be found on the [AWS Services in Scope by Compliance Program](#) page.

Table 2 - AWS Services and Accreditation status for the Amazon WorkSpaces smart card capability

VPC	Security Groups	IL2/4/5/6
VPC	Subnets	IL2/4/5/6
Directory	AD Connector	IL2/4/5
Directory	Smart Card Capabilities	Pending JAB/DISA
WorkSpaces	Workspace Instances	IL2/4/5
WorkSpaces	Smart Card Capabilities	Pending JAB/DISA

Configuring WorkSpaces Directory for FIPS 140-2

To comply with the [Federal Risk and Authorization Management Program (FedRAMP)](#) or the [Department of Defense Cloud Computing Security Requirements Guide](#), you must configure

Amazon WorkSpaces to use Federal Information Processing Standards (FIPS) endpoint encryption at the directory level. You must also use a US AWS Region that has FedRAMP authorization or is DoD SRG compliant. For details on updating the Directory, see [Set Up Amazon WorkSpaces for FedRAMP Authorization or DoD SRG Compliance](#).

Security Groups

Using the AWS Console or CLI, create Security Groups that allow for communication to and from your WorkSpaces interfaces. Security Groups should include all ports and protocols required by the Amazon WorkSpaces service, as well as ports and protocols required by Active Directory between domain controllers and domain members. For details about WorkSpaces ports and protocols , see [IP Address and Port Requirements for Amazon WorkSpace](#).

Conclusion

Following the details in this implementation guide, you have configured your Active Directory, Certificate Authority, AWS Directory AD Connector, and Amazon WorkSpaces environments to allow for the use of Common Access Cards.

Specifically, you have completed the following:

- Set up an Active Directory that serves as the repository for account information; primarily user credentials, security group memberships, and certificate templates. This directory also stores group policy, certificates, certificate revocation lists, and root and intermediate certificate authorities to allow for pre-authorization and in-session use of CACs with Amazon WorkSpaces.
- Set up an Active Directory Enterprise Certificate Authority used to issue domain controller certificates.
- Created an Amazon Directory AD Connector enabled to support smart card authentication. You registered the DoD root and intermediate certificate authorities with the AD Connector and associated a secondary OCSP address for each certificate using the AWS CLI.
- Created an Amazon WorkSpaces WSP instance associated with the smart card-enabled Amazon Directory Service AD Connector, allowing for pre-authorization access using a CAC, as well as in-session pass-through use of CAC certificates to access protected content.

Contributors

Contributors to this document include:

- Isi Lawson, Sr. Solutions Architect, Amazon Web Services
- Adam Hesch, Principal Architect, Amazon Web Services
- Chris Chiott, Solutions Architect, Amazon Web Services

Additional resources

For additional information, see:

- [Amazon WorkSpaces Administration Guide](#)
- [AWS Directory Service Administration Guide](#)

Document revisions

To be notified about updates to this whitepaper, subscribe to the RSS feed.

Change	Description	Date
Whitepaper updated	Refreshed smart card logon section and made other minor changes to account for UI updates.	November 22, 2022
Minor update	Fixed missing quotation mark in the `certutil` command example.	April 12, 2022
Initial publication	Whitepaper first published	March 8, 2021

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided "as is" without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.