leostream®

Remote Desktop Access Platform

Certificate Authority Setup

Password-less SSO with Certificate-Based Authentication for Windows DCV Sessions

Version 2024.5

April 2026

Contacting Leostream

Leostream Corporation
77 Sleeper Street
PMB 02-123
Boston, MA 02210
USA

http://www.leostream.com
Telephone: +1 781 890 2019

To submit an enhancement request, email features@leostream.com.
To request product information or inquire about our future direction, email sales@leostream.com.

Copyright

Trademarks

The following are trademarks or registered trademarks of Leostream Corporation.

Leostream®
The Leostream graphical logo™

The absence of a product name or logo from this list does not constitute a waiver of the trademark or other intellectual property rights concerning that product, name, or logo by Leostream.

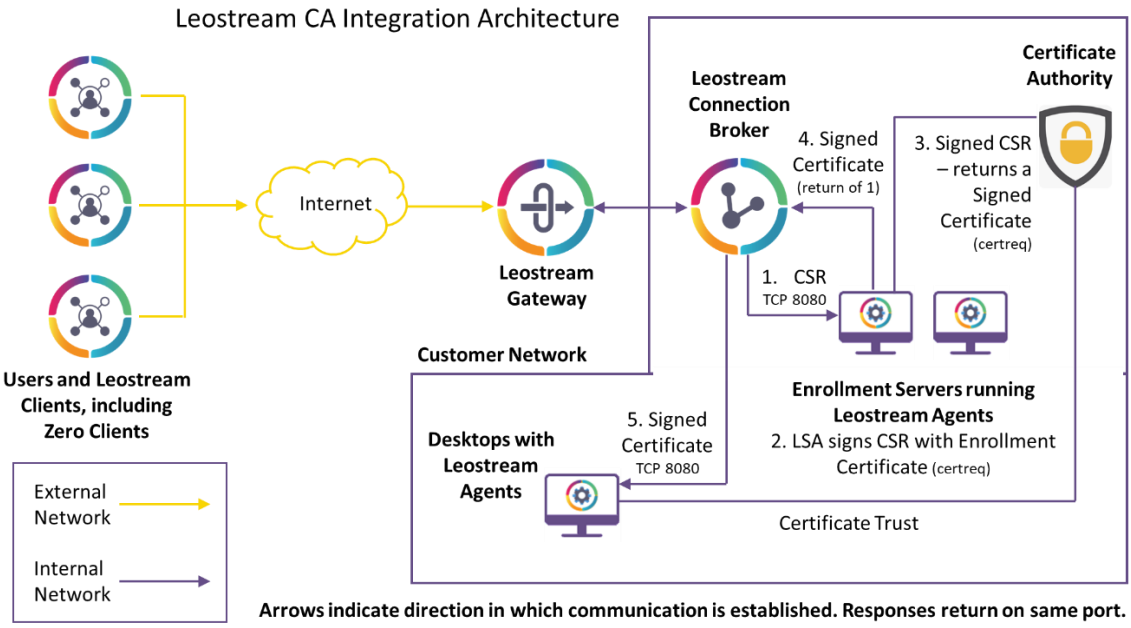
HP is a registered trademark that belong to Hewlett-Packard Development Company, L.P. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. UNIX is a registered trademark of The Open Group. OpenLDAP is a trademark of The OpenLDAP Foundation. Microsoft, Active Directory, SQL Server, Excel, Hyper-V, Windows, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Other brand and product names are trademarks or registered trademarks of their respective holders. Leostream claims no right to use of these marks.

Contents

Overview

In order to provide password-less single sign-on for a Leostream user connecting to a remote Windows operating system, the Leostream Platform leverages your corporate Certificate Authority to request a signed Certificate on behalf of the Leostream user. The certificate is generated from a Template that you must configure on your CA. The Leostream Platform-generated certificate is used by the DCV Server to log the user into the operating system

The workflow is displayed in the following high-level diagram.



The workflow enumerated on the previous diagram is, as follows.

1. When the user requests a connection to an offered desktop, the Connection Broker begins the certificate generation process. First, the Connection Broker generates a CSR for the user. This CSR requires the user's UPN, Domain name, and objectSid, which must be included in the SAML assertion that logs the user into Leostream, and assumes that the user's account and domain are in the same domain as the CA that will be used to generate the certificate.

   It is also assumed that this certificate is valid for logging into any desktop the user is offered, even if that desktop is in a different domain.

2. The Leostream Agent running on the Enrollment Servers signs the CSR with an existing Enrollment Certificate, as described in Configuring Enrollment Servers and Certificates.

   The Leostream Agent service must be running as a Service Account that has rights to enroll certificates using the Login Certificate Template referenced in the following step.

3. The Leostream Agent on the Enrollment Server uses the `certreq` command with the signed CSR to request a certificate on the behalf of the user using the template described in Login Certificate Template Setup.

4. The Leostream Agent on the Enrollment Server returns that signed certificate to the Connection Broker.

5. The Connection Broker then sends that certificate to the Leostream Agent on the user's remote desktop for use during the login process. The Leostream Agent, in turn, sends the certificate to the DCV Server on the remote desktop to perform the operating system login.

Step 1. Create a Leostream Service Account

In order to request a certificate on behalf of the user, the Leostream Agent service must be running as a Service Account with the following permissions

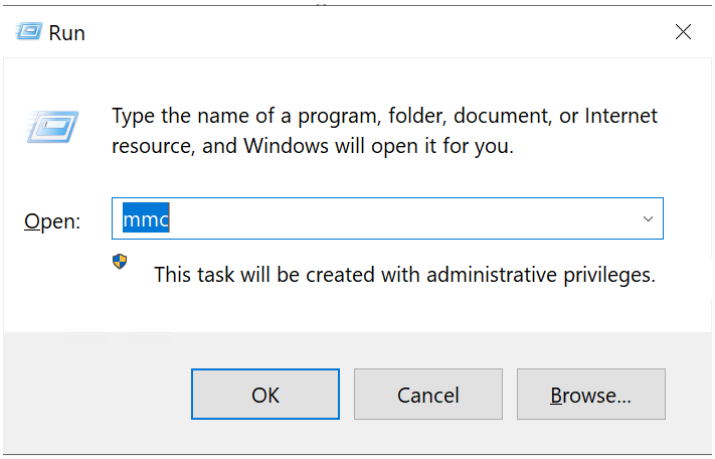
- View and Enroll permissions for the Login Certificate template, which is created in Login Certificate Template Setup
- Run permissions for Services on the Enrollment Servers
- Read permissions for the Enrollment Agent certificate private key

Leostream recommends creating a dedicated Service Account for running the Leostream Agent. Create this account on the domain associated with your Certificate Authorities.

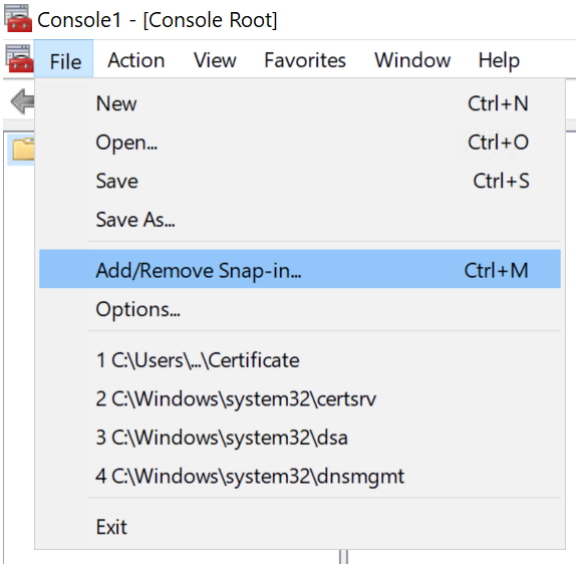
Step 2: Creating a Login Certificate Template

The Leostream Agent on your Enrollment Server queries your Certificate Authority for available Smartcard Logon templates, to use for generating certificates for users. Use the following procedure to make an appropriate certificate template for use with Leostream.

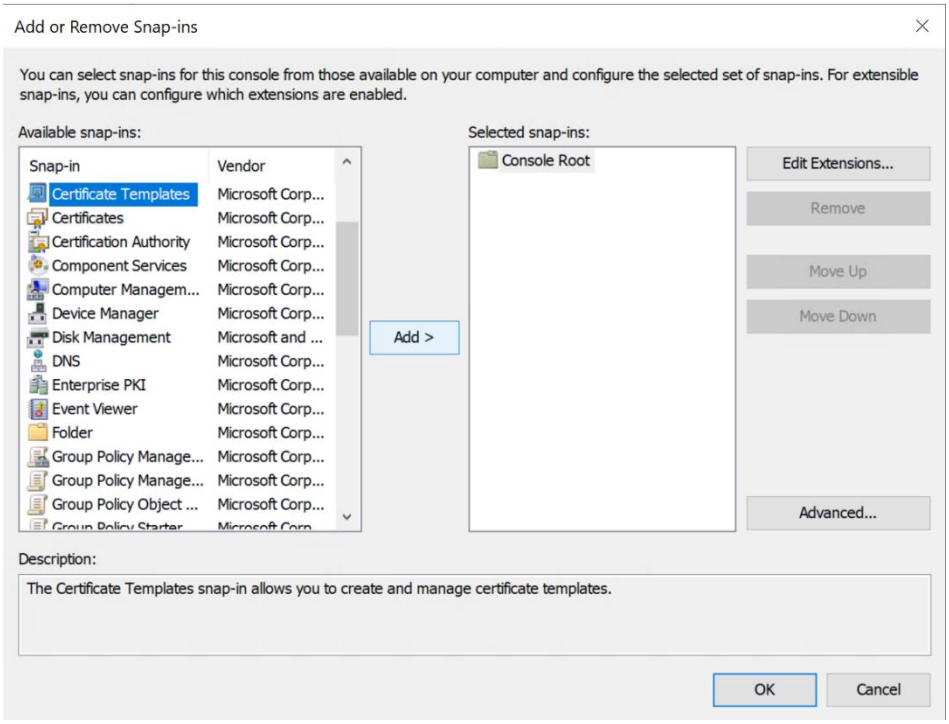
1. On your Certificate Authority, open a management console by running **mmc**, for example



2. In the **Management Console**, select **File > Add/Remove Snap-in**, as shown in the following figure.



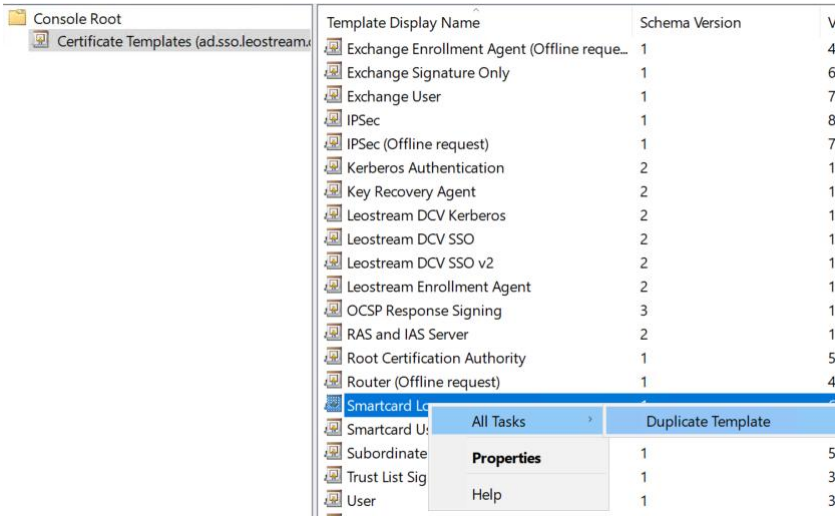
3. In the **Add or Remove Snap-ins** dialog, select **Certificate Templates** in the **Available snap-ins** list, as shown in the following figure.



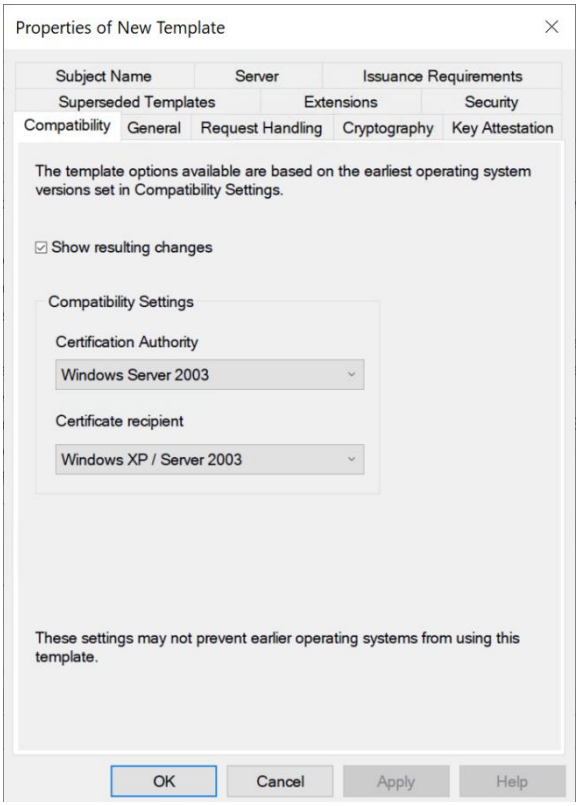
4. Click **Add >** to move the **Certificate Templates** to the **Selected snap-ins** list and then click **OK**.

5. In the **Management Console**, select the **Certificate Templates** to list all the available certificate templates. Right-click on the **Smartcard Logon** template and select **All Tasks** > **Duplicate**

Template, as shown in the following figure.



6. In the **Properties of New Template** that opens, leave the **Compatibility** tab set to the defaults, shown in the following figure.



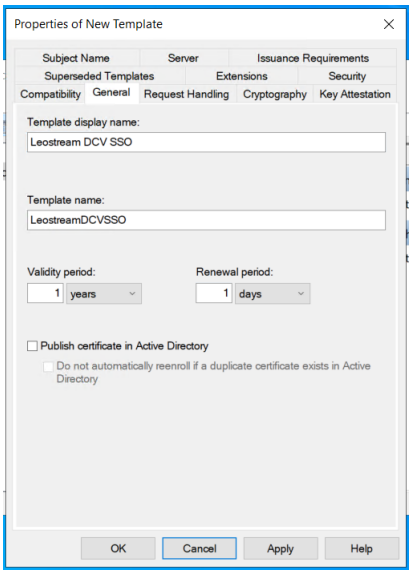
7. Go to **General** tab and enter a **Template display name**, which automatically updates the **Template name**.

   Also in this tab, enter a **Validity period** for the certificate. When a Leostream user first logs into

the Leostream Platform, the Connection Broker requests a certificate on behalf of that user. The generated certificate is valid for the length of time set by the **Validity period**. The Connection Broker stores the certificate and private key and continues to use that certificate for operating system logins for as long as the certificate is valid.

Storing the certificate improves the performance of subsequent logins as the Connection Broker does not need to regenerate a certificate. Choose the shortest **Validity period** that adheres to your corporate security guidelines.

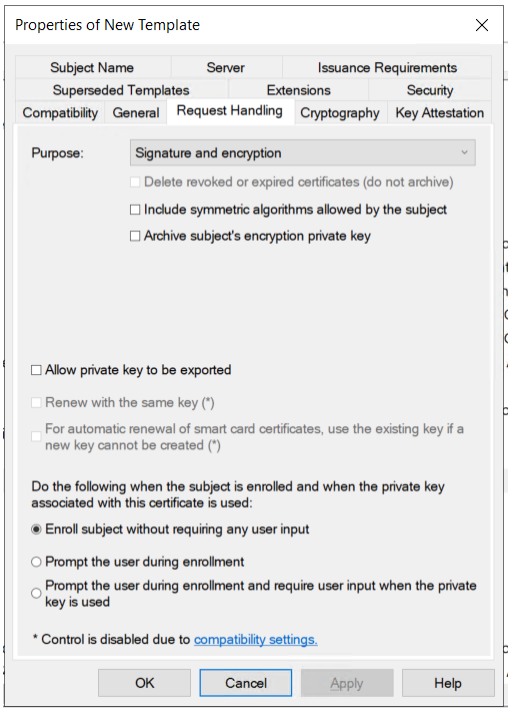
The following figure shows an example of a completed **General** tab.



8. On the **Request Handling** tab, ensure that the **Allow private key to be exported** is *unchecked*. The Connection Broker sends a CSR to the CA and, therefore, the Connection Broker stores the Private Key. Neither the CA, the Enrollment Server, nor the user's remote desktop will ever hold the private key.

   Also ensure that:

   a. The **Purpose** is set to **Signature and encryption**
   b. The **Enroll subject without requiring any user input** option is selected, as shown in the following figure.

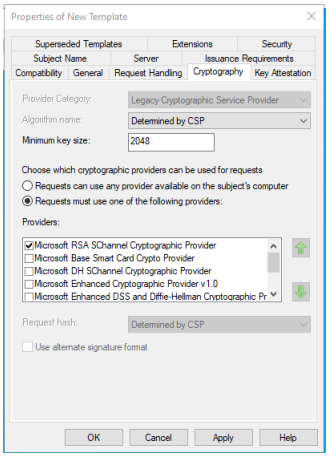


9. In the **Cryptography** tab:

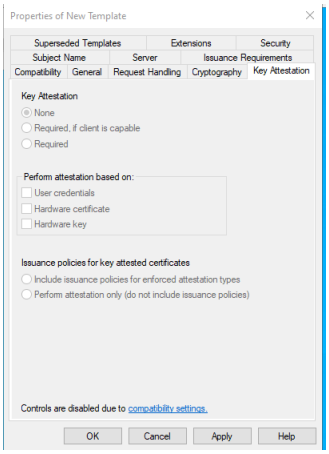
    a. Set **Minimum key size** to **2048** bits.
    b. Select **Requests must use one of the following providers** and check the following options:

    Microsoft RSA SChannel Cryptographic Provide
    Microsoft Base Smart Card Crypto Provider

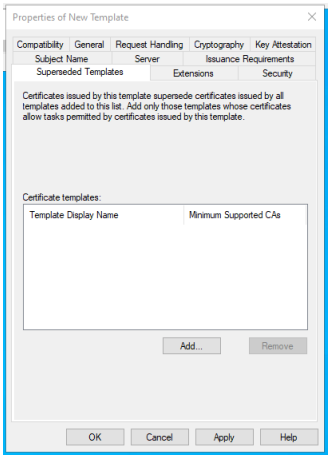
    NOTE: The selection in the **Providers** section may change based on discussions with the Amazon DCV team or on security requirements by Microsoft.



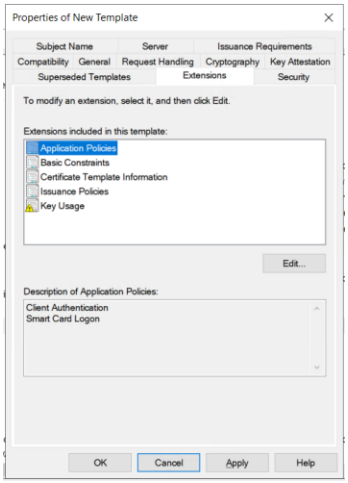
10. Leave the **Key Attestation** tab at its defaults.

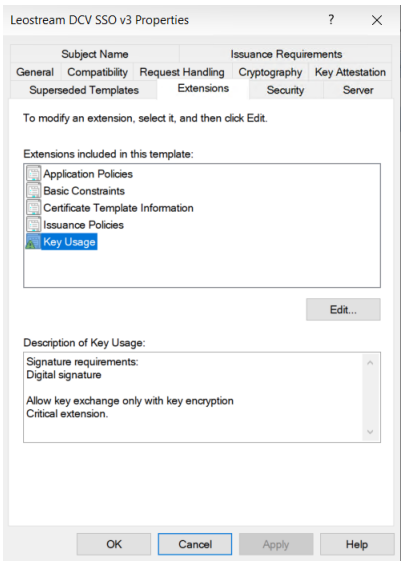


11. Leave the **Superseded Templates** tab at its defaults.



12. On the **Extensions** tab, confirm that the **Client Authentication** and **Smart Card Logon** Application Policies are listed and that the **Key Usage**, as shown in the following figures.

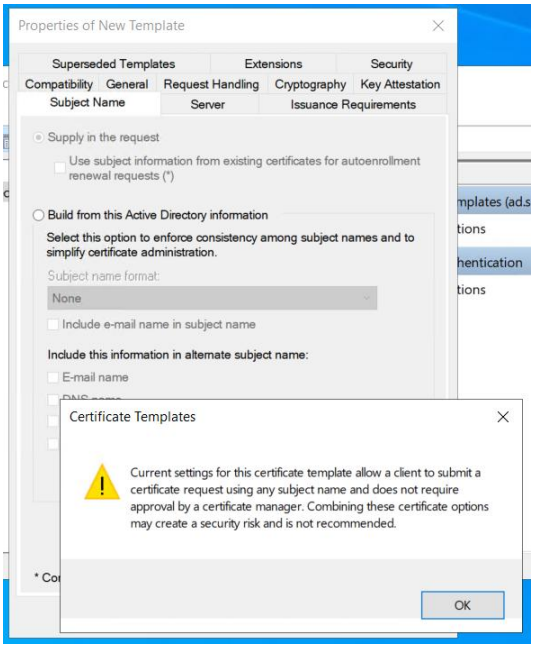




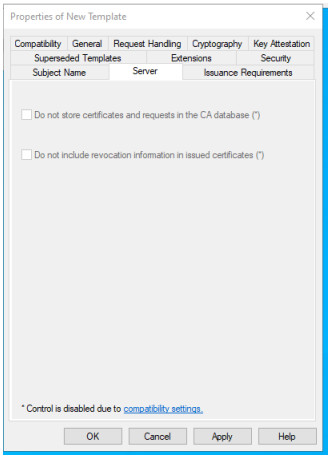
13. On the **Security** tab, ensure that the Service Account created in Step 1. Create a Leostream Service Account that runs the Leostream Agent service has **Enroll** and **Read** permissions.

14. On the **Subject Name** tab, select the **Supply in the request** radio button to allow the Connection Broker to request certificates. When you select the option, the warning shown in the following figure opens. Click **OK** on the warning dialog to return to the **Properties of New Template** dialog with the **Supply in the request** option selected.

    Because this template enables the **Supply in the request** option, ensure that the Connection Broker is the only application with permission to use this template.



15. Leave the **Server** tab at its defaults.

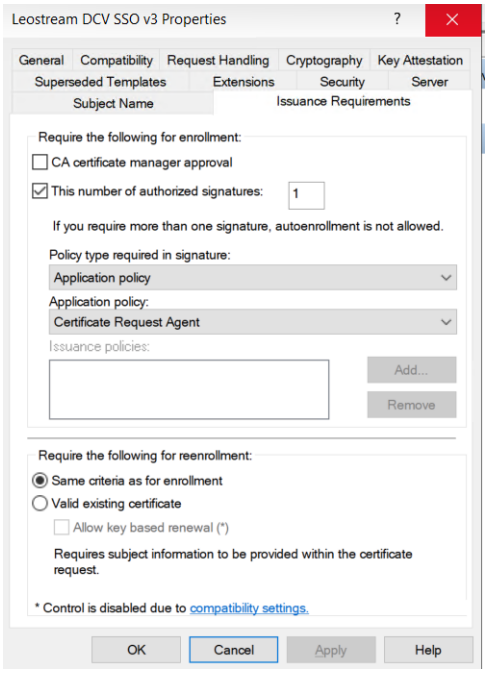


16. In the **Issuance Requirements** tab, select the **This number of authorized signatures** option and set the value to **1** to require an Enrollment Server to generate certifications from this template.

    Also, ensure that:

    a. The **Policy type required in signature** is set to **Application policy**
    b. The **Application policy** is set to **Certificate Request Agent**

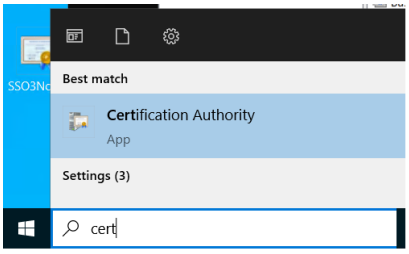
    The following figure shows an example of the **Issuance Requirements** tab.



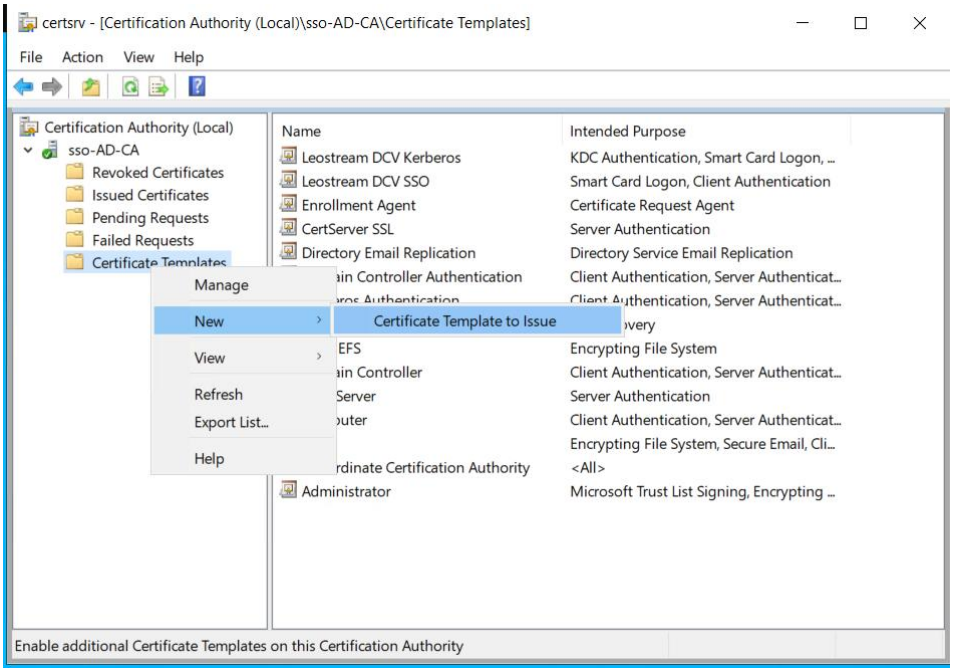
17. Click **OK** on the **Properties of New Template** to create the new certificate template.

After creating the new template, you must make it available to the `certsrv` application, as follows.

1. Open the **Windows Start** menu and type `certsrv`. Select the **Certificate Authority** option that appears as the Best match, as shown in the following figure.



2. Right click on the **Certificate Templates** item in the **Certificate Authority** list on the left, and select **New > Certificate Template to Issue** as shown in the following figure.



3. In the **Enable Certificate Template** dialog that opens, locate and select the template you created in the previous procedure, then click **OK**.

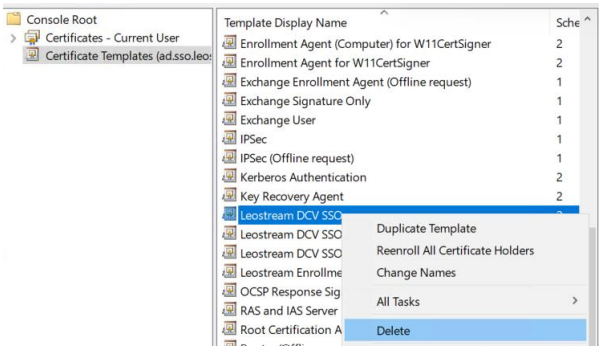
Your certificate authority is now ready to integrate with your Leostream Platform.

⚠ If you make changes to your certificate template after making it available to the `certsrv` application, you must remove the previous template and add your changes. To remove the previous template:

1. Open the **Certificate Authority** application as described in step 1 of the above procedure.

2. Select **Certificate Templates** in the tree on the left.

3. Right-click on the template to delete and select the **Delete** option, for example:



4. Click **Yes** in the **Certificate Templates** confirmation dialog.

5. Repeat the procedure to add the certificate template with the changes to the Certificate Authority.

Step 3: Configuring Enrollment Servers and Certificates

Designate one or more dedicated Windows machines as Enrollment Servers for your Leostream environment. To configure these machines to work with Leostream, you must complete the following steps, in order:

1. Create the Service Account that will run the Leostream Agent service on the Enrollment Server (as described in Step 1. Create a Leostream Service Account).

2. On your Certificate Authority, create an **Enrollment Agent (Computer) Template** for the Enrollment Server (as described in Create Enrollment Agent Template for Enrollment Server).

3. On the Enrollment Server, generate an **Enrollment Agent Certificate** from the template created in the previous step (as described in Generate an Enrollment Certificate on the Enrollment Server).

4. Grant **Private Key Access** to the Leostream Service Account that will run the Leostream Agent (as described in Grant Private Key Access to the Leostream Service Account).

5. On the Enrollment Server, install the Leostream Agent and update the Leostream Agent service so it runs as the Service Account defined in at the beginning of this procedure (as described in Install the Leostream Agent on the Enrollment Server).

After you install the Leostream Agent on each Enrollment Server, it automatically registers the machine with the Connection Broker as an Enrollment Server. If the machine is already inventoried by one of your Centers, that existing desktop record is converted to an Enrollment Server. Otherwise, the Connection Broker automatically creates an Uncategorized Desktops center to store the record. Enrollment Server

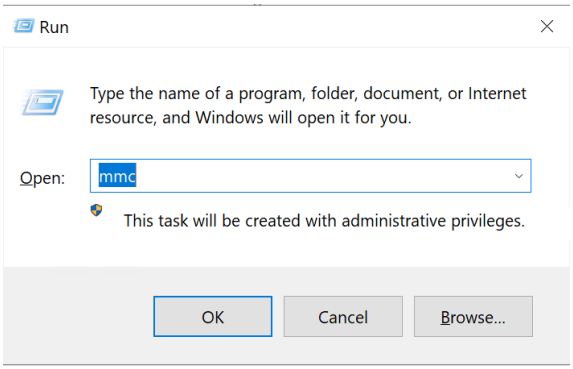
machines are listed on the **> Setup > Enrollment Servers** page and are removed from **> Resources > Desktops** page.

Create Enrollment Agent Template for Enrollment Server

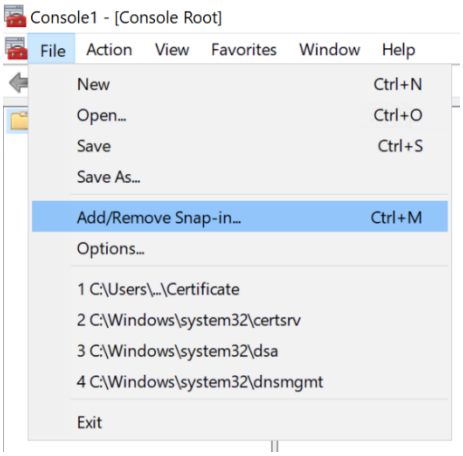
Use the following procedure to make an appropriate Enrollment Agent Template to use to create an Enrollment Certificate for your Enrollment Server. This template is used to issue a certificate that is valid only on the Enrollment Server.

1. Log into your Certificate Authority.

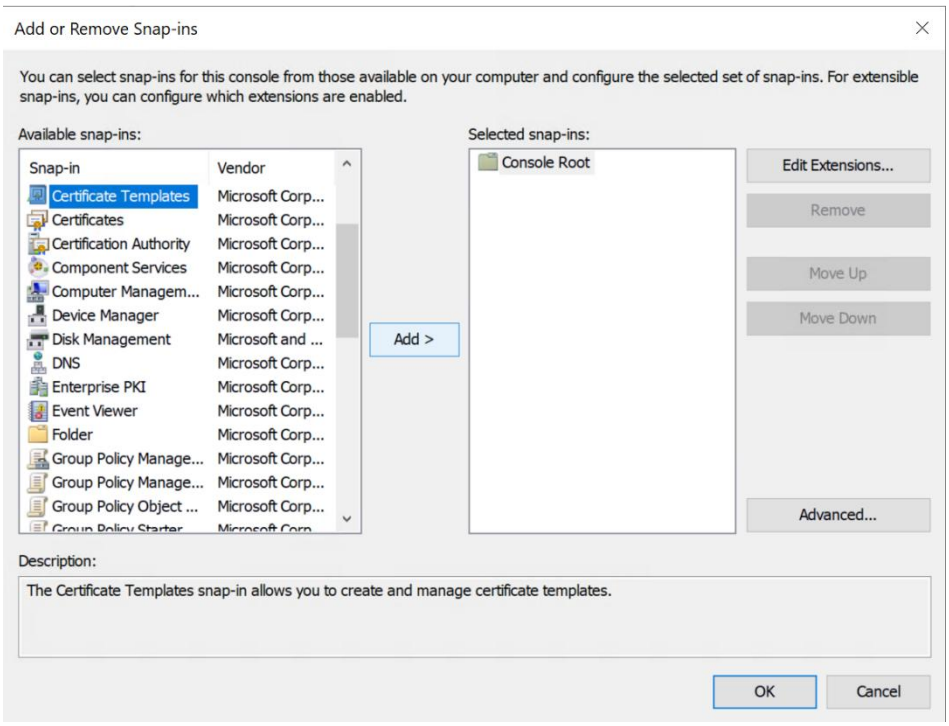
2. Open a management console by running **mmc**, for example:



3. In the **Management Console**, select **File > Add/Remove Snap-in**, as shown in the following figure.



4. In the **Add or Remove Snap-ins** dialog, select **Certificate Templates** in the **Available snap-ins** list, as shown in the following figure.



5. Click **Add >** to move the **Certificate Templates** to the **Selected snap-ins** list and then click **OK**.

6. In the **Management Console**, select the **Certificate Templates** to list all the available certificate templates. Right-click on the **Enrollment Agent (Computer)** template and select **Duplicate Template**.

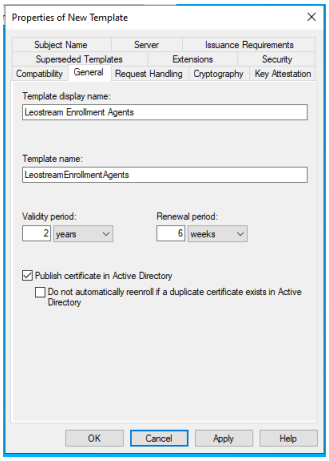
7. In the **General** tab, shown in the following figure:

    a. Enter a **Template display name**, which sets the template name (e.g., Leostream Enrollment Agents).

    b. Set the desired **Validity period** (e.g., 2 years).

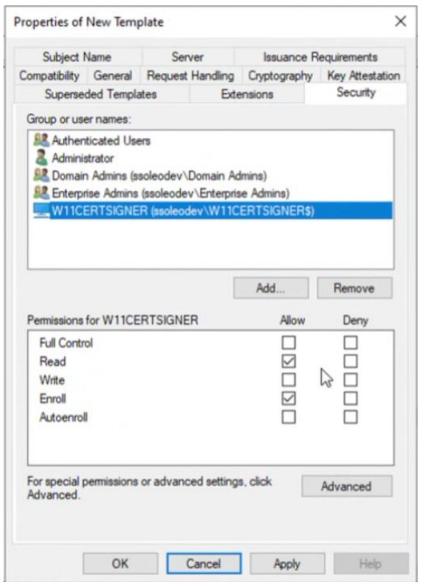
    c. Check the **Publish certificate in Active Directory** option.

    d. Click **Apply.**



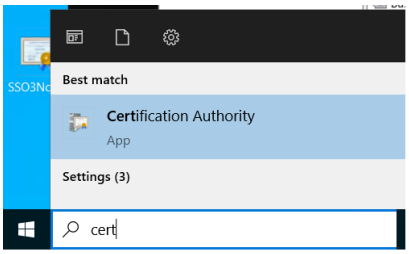
8. In the **Security** tab:

    a. Under the **Group or user names** field:
        i. Click the **Add** button.
        ii. In the **Select Users, Computers, Service Accounts, or Groups** dialog, click the **Obejct Types** button and ensure that **Computers** is checked in the **Object Types** dialog. Click **OK**.
        iii. Enter or search for the Computer record for your Enrollment Server that will request certificate using this template.
        iv. Click **OK**.
    b. Select that Computer and grant **Read** and **Enroll** permissions.
    c. Ensure Authenticated Users or other unnecessary groups do not have Enroll permissions to maintain security.

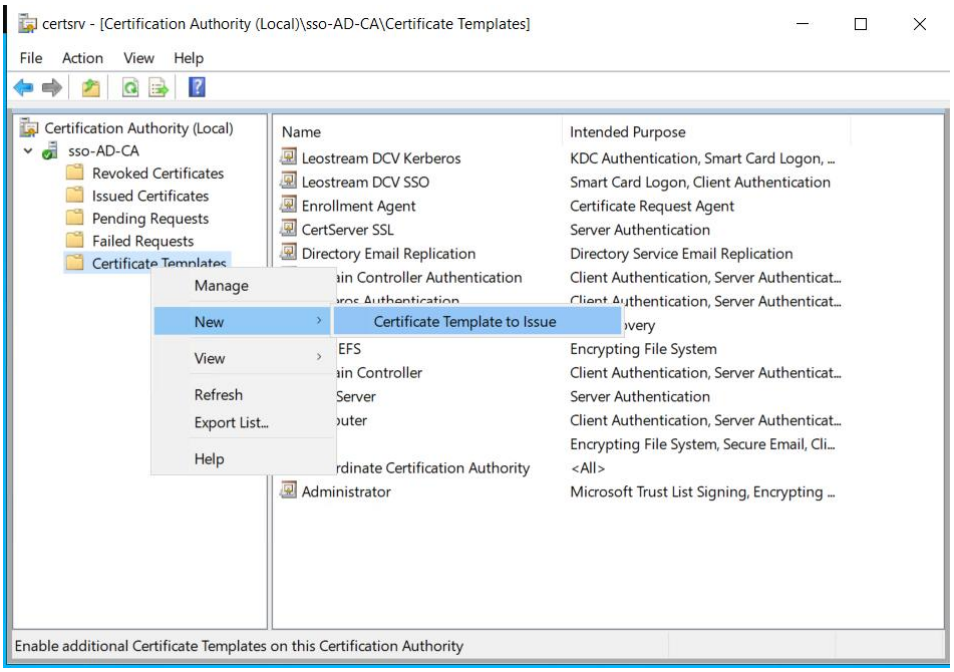


9. Leave all other settings in the **Properties of New Template** dialog at their defaults and click **OK**.

10. After creating the new template, publish it for use. Open the **Windows Start** menu and type `certsrv`. Select the **Certificate Authority** option that appears as the Best match, as shown in the following figure.



11. Right click on the **Certificate Templates** item in the **Certificate Authority** list on the left, and select **New > Certificate Template to Issue** as shown in the following figure.



12. In the **Enable Certificate Template** dialog that opens, locate and select the template you created in the previous procedure, then click **OK**.

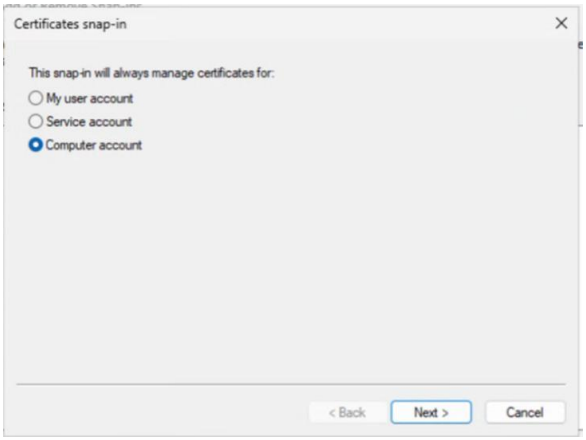
Generate an Enrollment Certificate on the Enrollment Server

To initialize the Enrollment Server, generate an Enrollment Certificate using the created Enrollment Agent (Computer) Template, as follows.

1. Log into the Enrollment Server.

2. Open the Certificates Snap-in:
   - Press Win + R, type **mmc**, and press **Enter**.
   - In the MMC console, go to **File** > **Add/Remove Snap-in**.

- Select **Certificates**, click **Add**
- Choose **Computer account**, as shown in the next figure, and click **Next**.



- With **Local computer** selected, click **Finish** to select the snap-in.
- Click **OK** in the **Add or Remove Snap-ins** dialog

3. Request the Enrollment Agent Certificate:
   - Under the Computer account, expand **Certificates** > **Personal**.
   - Right-click the **Certificates** folder, select **All Tasks** > **Request New Certificate**.
   - In the **Certificate Enrollment** wizard, click **Next**.
   - Select **Active Directory Enrollment Policy** and click **Next**.
   - Locate and check the box for the **Enrollment Agent (Computer)** template you created.
   - Click **Enroll**.
   - Complete the wizard to receive the certificate.

4. Verify the Certificate:
   - In the MMC console, navigate to **Personal** > **Certificates**.
   - Ensure the **Enrollment Agent** certificate appears with the intended purpose of Certificate Request Agent.

Grant Private Key Access to the Leostream Service Account

After verifying that the Enrollment Agent Certificate was enrolled successfully, you must grant access to the certificate's private key to the Service Account that will run your Leostream Agent. Because the certificate was enrolled into the Local Computer store, only SYSTEM and Administrators have access to the private key, by default. The Leostream Agent service runs as your Service Account and must be able to read this key.

In the MMC console with the Certificates (Local Computer) snap-in:

1. Navigate to **Personal > Certificates**.
2. Right-click the Enrollment Agent certificate and select **All Tasks > Manage Private Keys**.
3. In the Permissions dialog, click **Add**.
4. Enter the Service Account (e.g., _leostream.svc) and click **OK**.
5. Grant the account **Read** permission and click **OK**.

Install the Leostream Agent on the Enrollment Server

The Leostream Agent can be installed using the installation wizard. When stepping through the wizard:

- Do not select any additional tasks during installation.
- Enter the correct address for your Leostream Connection Broker environment so that the Leostream Agent can register with your Leostream Platform after installation.

  Your Connection Broker must contain a center to inventory the machines used as your Enrollment Servers. If a Desktop record does not already exist, create an Uncategorized Desktops center to store the Leostream Agent Registration.

After installation, switch the Leostream Agent service so it runs under the Service Account created in Step 1, instead of under the Local System account.

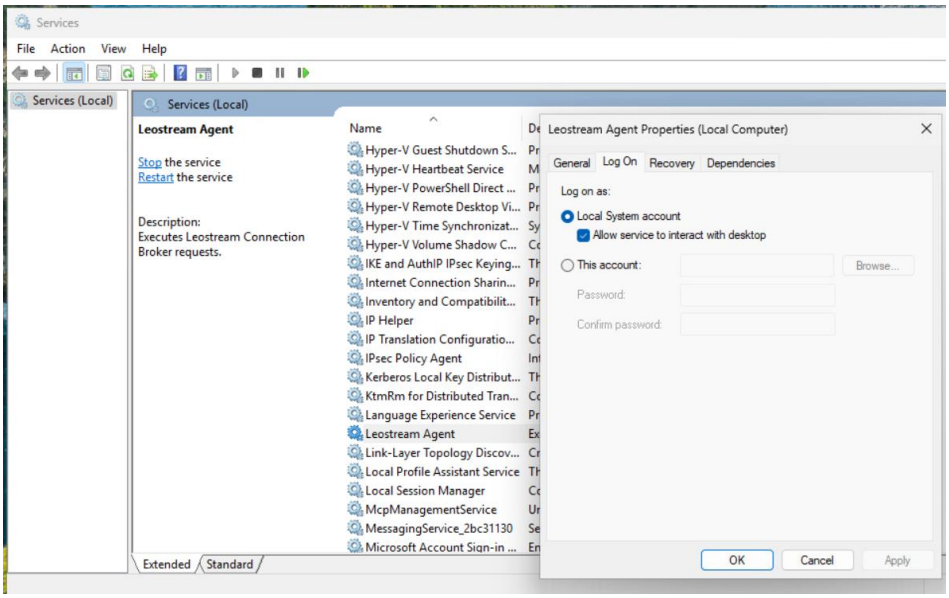
1. In the Windows Search bar, type “Services” to open the **System Services** dialog.

2. Scroll down to the **Leostream Agent** service.

3. Right click on the **Leostream Agent** service and select **Properties**.

4. In the **Leostream Agent Properties**, on the **General** tab, click the **Stop** button.

5. Go to the **Log On** tab.



6. Select the **This account** radio button.

7. Enter the username and password for the Service Account you created in Step 1.

8. Click **Apply** and click **OK** on the confirmation dialog that opens.

9. Go back to the **General** tab.

10. Click **Start**.

The Enrollment Server is now configured and appears in your Connection Broker on the **> Setup > Enrollment Servers** page. The Leostream Agent uses LDAP queries to discover the Certificate Authorities that it can use to generate logon certificates and inventory the available Smartcard Logon certificate templates on each CA. See Viewing your Enrollment Servers for more information.

Step 4: Configuring the Connection Broker

SAML Authentication Server Setup

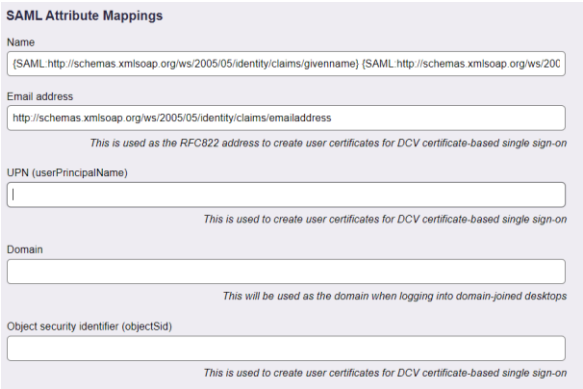
To generate a certificate on behalf of a Leostream user, the Connection Broker must have the user's UPN (userPrincipalName), Domain, and Object security identifier (objectSid). For users logging into your Leostream environment after authenticating with a SAML-based authentication server, the SAML assertion must return all of these attributes.

You specify the attributes that returns the UPN, Domain, and objectSid, as follows.

1. In the Connection Broker Administrator Web interface, go to the **> Setup > Authentication Servers** tab.

2. Click the **Edit** action for your SAML authentication server or add a new authentication server. If you have not configured a SAML authentication server, see the Using SAML-Bsed Identity Providers with Leostream guide for complete instructions.

3. Scroll down to the **SAML Attribute Mappings** section, shown in the following figure, and ensure that you set the following attributes, at a minimum.



   a. In the **UPN (userPrincipalName)** edit field, enter the SAML attribute that returns the UPN.

b. In the **Domain** edit field, enter the SAML attribute that returns the user's domain. The value returned by this attribute must exactly match the **Domain** value specified in you Enrollment Servers, as described in the following section.

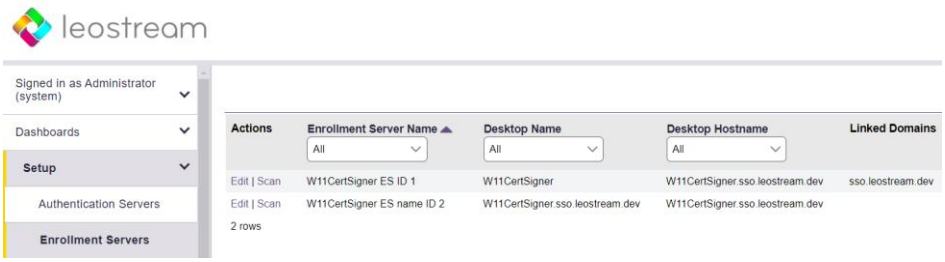
c. In the **Object security identifier (objectSid)**, enter the SAML attribute that returns the user's SID. The Connection Broker cannot generate valid certificates without this value.

4. Click the **Save** button at the bottom of the form.

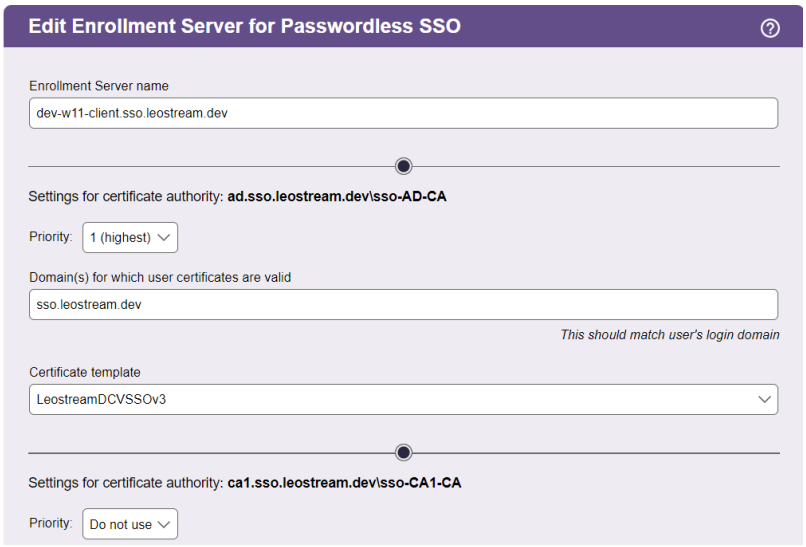
Viewing your Enrollment Servers

As soon as you install a Leostream Agent on your Enrollment Server, the agent registers the machine with the Connection Broker as an Enrollment Server. If the Windows machine was previously listed on the **> Resources > Desktops** page, the Connection Broker removes it.

The **> Setup > Enrollment Servers** page, shown in the following figure, lists the currently registered Enrollment Servers, for example:



Click the **Edit** action to view or edit the Enrollment Server properties, as shown in the following figure. The Enrollment Server lists all the Certificate Authorities available for generating Smartcard Logon certificates.



To configure the Enrollment Server:

1. In the **Enrollment Server Name**, enter a name for the record in the Connection Broker.

2. Set the **Priority** drop-down menu to **1 (highest)** for at least one of the listed Certificate Authority. Select **Do not use** for all Cas that should not be used for certificate generation.

   If you need to support failover to a secondary CA, select a **Priority** of **2**, **3**, etc. for the secondary, tertiary, etc. CAs.

3. In the **Domain(s) for which user certificates are valid** field, enter all the domain names that may be returned for users who need to request certificates from this Certificate Authority. These values must exactly match the value returned in the **Domain** field for the SAML authentication server. For example, if you have a mixture of FQDN and NetBIOS names, enter:

   ```
   sso.leostream.dev ssoleodev
   ```

   If the CA can generate certificate for multiple domains, enter all the domains in this field.

4. From the **Certificate template** drop-down menu, select the Smartcard Logon template to use when requesting certificates on behalf of users in this domain.

5. If multiple CAs are prioritized, ensure that each is configured correctly.

6. Click **Save**.

Enable DCV SSO in the Protocol Plan

Your Leostream Protocol Plans indicate which DCV connections leverage the passwordless SSO feature, as follows.

1. In the Connection Broker Administrator Web interface, go to the **> Configuration > Protocol Plans** tab.

2. Edit or create a new protocol plan for DCV SSO.

3. In the **Web browser** section of the Protocol Plan, set or ensure that the priority of **Amazon DCV** or **Amazon DCV HTML5 Viewer** is set to **1**.

4. Check the **Use DCV external authenticator with token** checkbox.

    Ensure that your DCV server is configured to use your Connection Broker for external authentication. See the Leostream Guide for Working with Display Protocols for instructions on configuring external authentication.

5. Check the **Use DCV certificate-based single sign-on** checkbox.

6. You can launch the DCV client using either a file download or URI.

7. Save the form.

Testing Certificate Generation

Create a policy that offers DCV-enabled desktops and uses your DCV SSO Protocol Plan, then ensure that the Assignments table for your SAML authentication server assigns that policy to the appropriate users.

To test the certificate generation, log into Leostream as a user who is assigned to that policy and launch a DCV connection. The Connection Broker generates a login certificate only after creating the DCV session.

 A generated certificate is reused until it expires, unless any of the user's SAML attributes changes. The certificate is regenerated when any of the user's SAML attributes change.

All generated certificates are listed on the **> Resources > Certificates** page. To force the Connection Broker to regenerate a user's certificate, click the **Remove** action associated with that certificate.