MyID MFA and PSM

Version 5.0.7

Multi-Factor Authentication Quick Start Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Copyright

Conventions

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.

- **Bold** is used for menu items and for labels.

  For example:
  - “Record a valid email address in **'From' email address**"
  - Select **Save** from the **File** menu.

- *Italic* is used for emphasis and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and Italic*** are used to identify the titles of other documents.

  For example: “See the ***Release Notes*** for further information.”

  Unless otherwise explicitly stated, all referenced documentation is available on the product media.

- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.

- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

Warning:	You must take a backup of your database before making any changes to it.

Contents

1 Introduction

Note: MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly. The term 'Authlogics' may still appear in certain areas of the product.

This guide provides an overview of the steps required to set up MyID Multi-Factor Authentication (MFA) in a new environment. For detailed information about a specific feature or deployment scenario, see the ***MyID Authentication Server Installation and Configuration Guide***.

1.1 Considerations

MyID Multi-Factor Authentication requires a Windows Server and an Active Directory domain to be available before installation.

You require a Domain Administrator / Enterprise Administrator account to perform the installation.

You must add Active Directory accounts of MyID administrators to the Authlogics Administrators AD security group.

After the installation, you must reboot the server.

The MyID MFA software requires Internet access to:

`https://*.authlogics.com`

1.2 Required information

Before you install the software, make sure you have the following information available:

- Active Directory administrator credentials.
- SMTP server details: name, port, authentication requirements.
- The DNS name for the server.
- Understanding of which authentication technology to use.
- For FIDO and passkey tokens, MyID MFA requires a trusted certificate to be bound to MyID web sites; self-signed certificates do not work.

  This document includes the steps required to create your own Certificate Authority on the MyID Server and generate trusted certificates if a public trusted certificate is not available.

1.3 Change history

Version	Description
INT2058-01	Reformatted and released with MyID MFA and PSM version 5.0.7.

2 Installing the Authentication Server

To install the MyID Authentication Server:

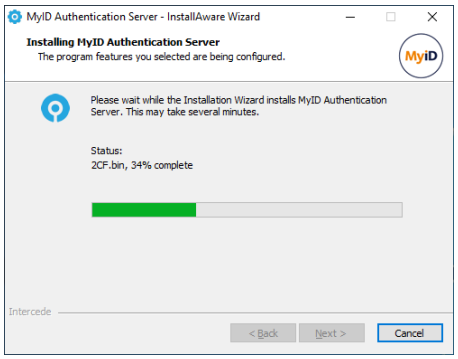
1. Download the Authentication Server installer from:

   https://www.intercede.com/support/downloads

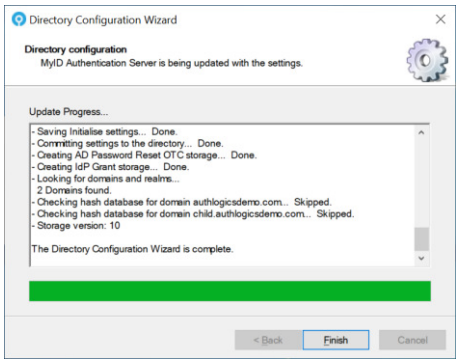
2. Extract the files from the zip archive.

3. Run the setup file in the `Install` folder.

4. Follow the Installation Wizard instructions to install the product binaries.

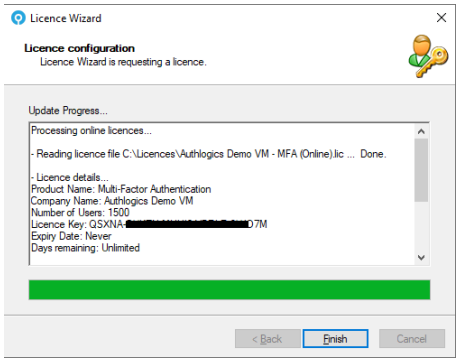


5. Follow the Directory Configuration Wizard to setup the Active Directory for use with MyID MFA.



6. Follow the Licence Wizard to configure a license for MyID MFA.

   If you do not have a license key the wizard can request a 30-day evaluation license for you.



7. Reboot the server after the MyID Management Console loads to complete the initial setup.

3 Configuring the Authentication Server

To begin the configuration of the MyID Authentication Server:

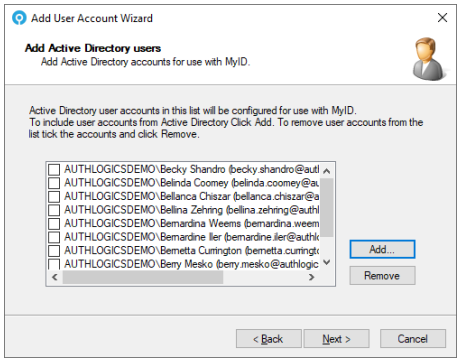
1. Launch the MyID Management Console.
2. Right-click **MyID MFA** and select **Properties**.
3. On the **SMTP Delivery** tab, configure the SMTP Server settings to be able to deliver alerts and new user emails.

3.1 Adding MFA users

To add MFA users:

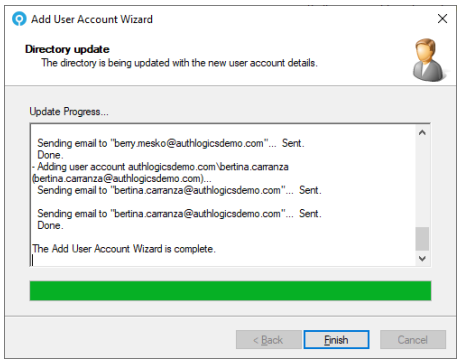
1. Expand the domains and open the domain into which you want to add MFA users.
2. Click the **Add User Account** action.

   The Add User Account Wizard starts.
3. Select all the Active Directory users you want to configure for MyID MFA.



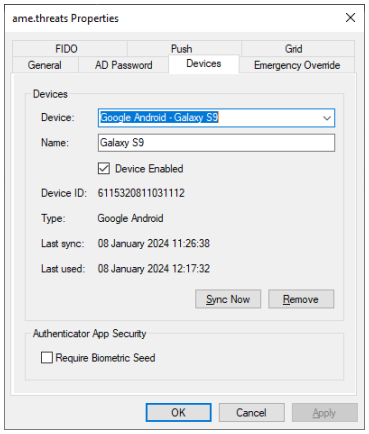
4. Complete the wizard.
5. Select all the users to provision an MFA technology.

   For example, Grid, One Time Code, or YubiKey.
6. Click the **Management** option for the required technology to start the wizard.
7. Configure the technology settings for the selected users:



8. Complete the wizard.

9. Double click a user account to view account properties.



10. Test the user login using the Self Service Portal:

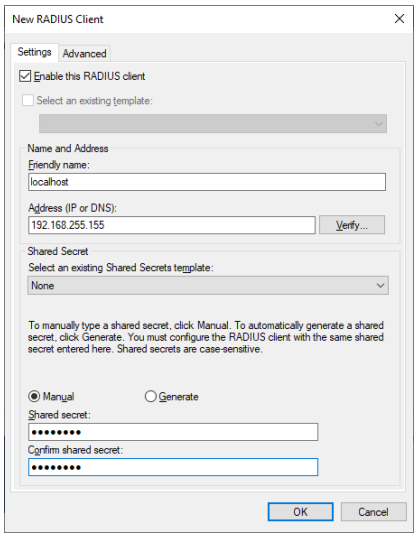
    `https:// <servername>:14443/`

    Where `<servername>` is the name of your server.

3.2 Setting up RADIUS

To set up RADIUS:

1. Launch the MyID Management Console.
2. Right-click **MyID MFA** and select **Properties**.
3. On the **RADIUS** tab, configure the RADIUS settings as required.
4. Click **Open Network Policy Server** and add the local server as a RADIUS client using the local IP address and a shared secret.



5. Start the MyID RADIUS test client from:

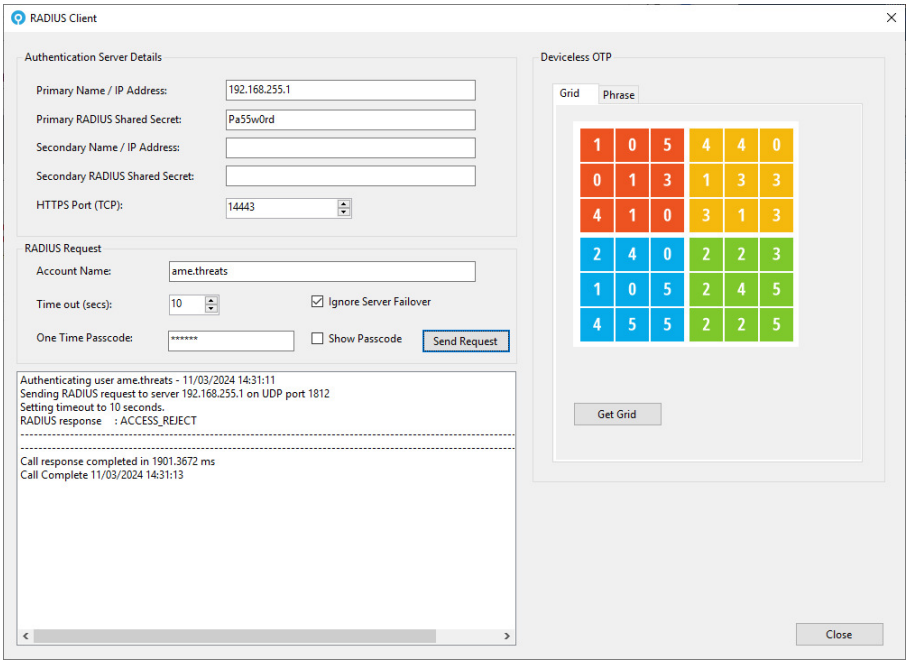
    ```
    C:\Program Files\Authlogics Authentication Server\
    ResKit\RadiusClient\Radius Client UI.exe
    ```

    a) Enter the local server IP address and shared secret you configured above.

    b) Enter the test user account name.

    c) Click **Grid** to show a grid if you are using a Grid.

6. Enter the One Time Passcode and click **Send Request**



The RADIUS result is shown.

3.3 Monitoring MFA usage

The MyID Authentication Server includes a dashboard to display the state of your MFA deployment.

1. Launch the MyID Web Management Portal.

   This is available at:

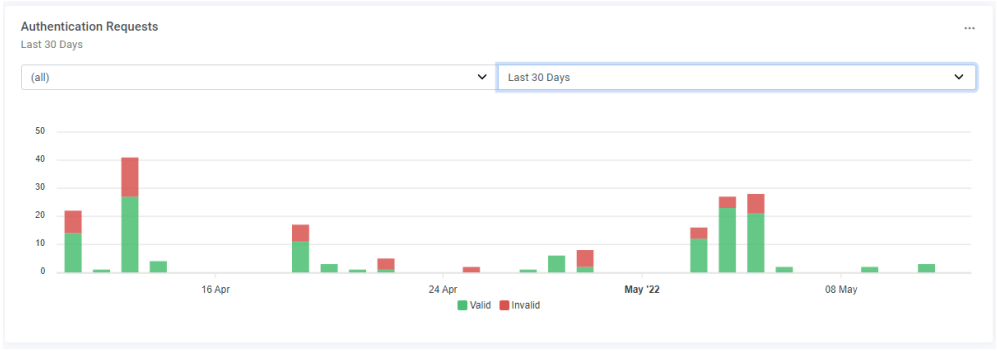
   `https://<servername>:14443/admin`

   Where `<servername>` is the name of your server.

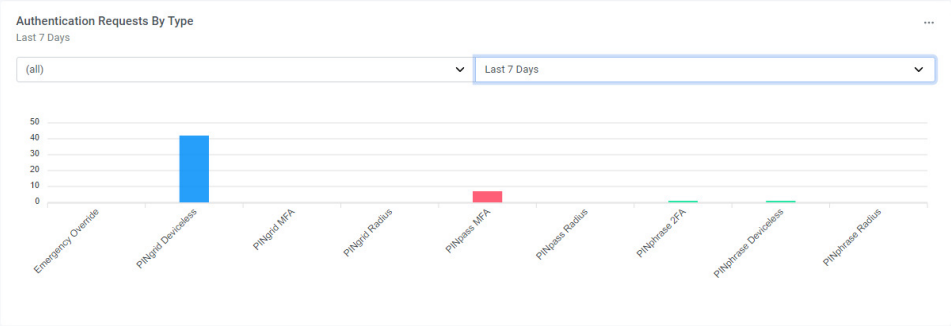
2. Under **System > Dashboards**, select **Multi-Factor Authentication**.

This dashboard reflects contains information on:

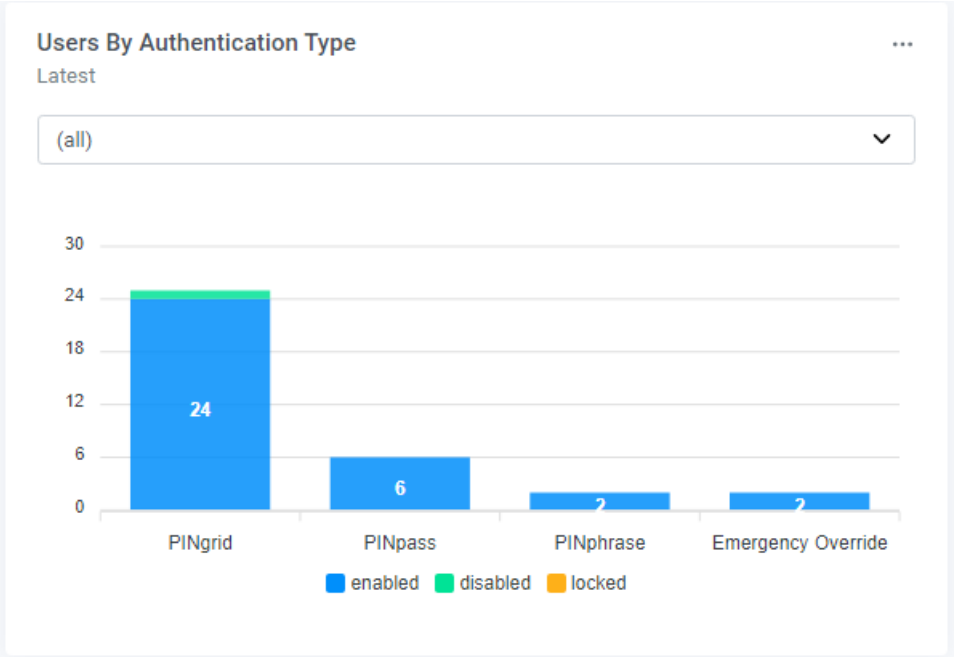
- Authentication Requests



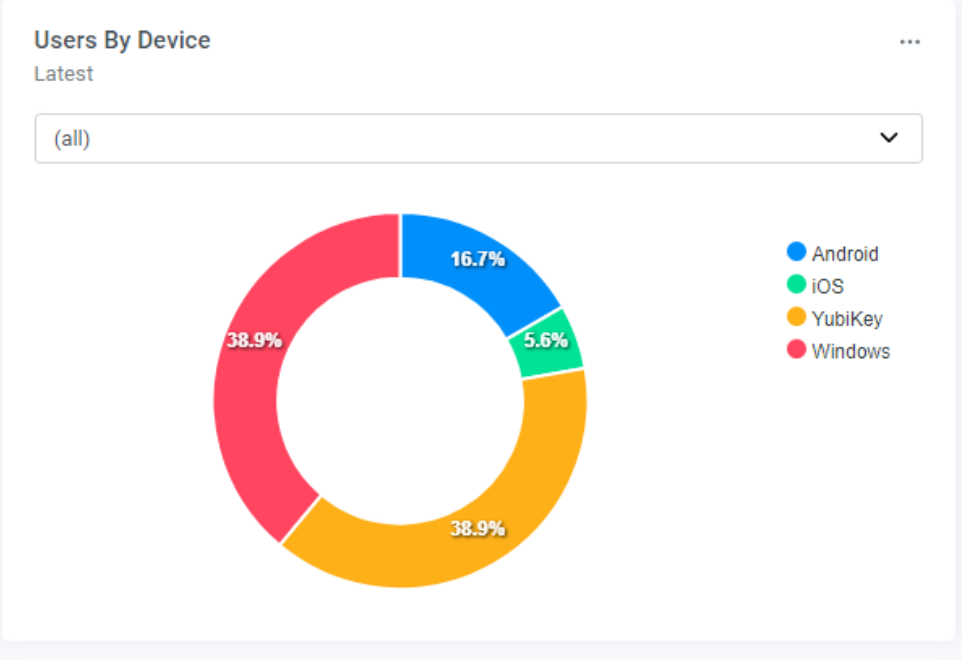
- Authentication Requests By Type



- Users By Authentication Type



- Users By Device



3.4 Configuring the Windows Desktop Agent

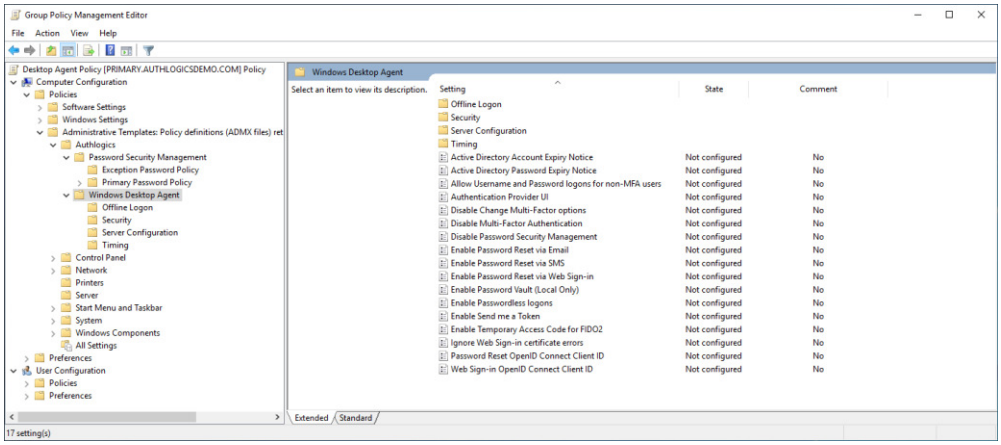
This section assumes that you are using a separate workstation test PC which is domain joined. You can deploy the MyID Windows Desktop Agent on non-domain joined PCs; however, you must apply the Group Policy Objects to these PCs manually.

Perform these actions on the server:

1. Download the Windows Desktop Agent installer from:

   https://www.intercede.com/support/downloads

2. Extract the files from the zip archive.
3. Import the `GPO\AuthlogicsWDA.admx` file into a new Group Policy object.
4. Configure the following settings (assuming you are using Grid):
   - Authentication Provider UI: Enabled, Grid.
   - Disabled Windows Username and Password logons.



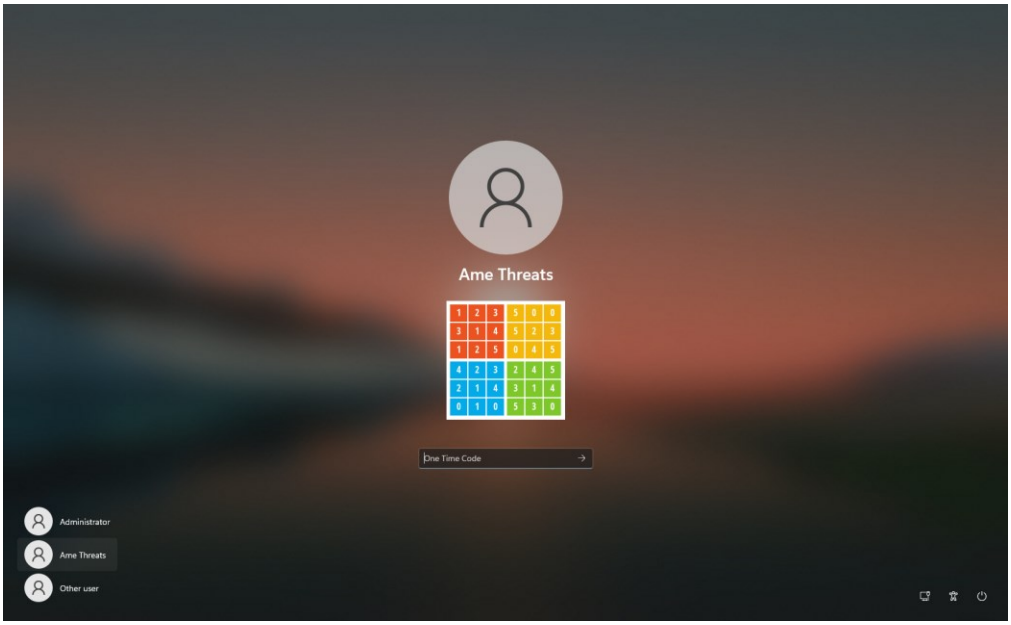
5. Apply the GPO to an OU containing the workstation computer account.

Perform these actions on the workstation:

1. Ensure the GPO settings are applied to the PC by running:

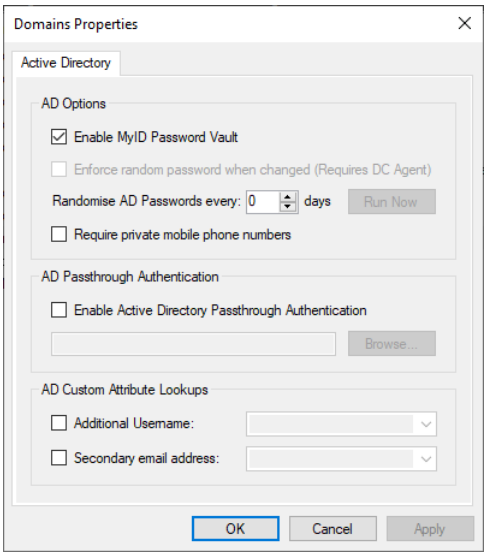
   ```
   GPUPDATE /FORCE
   ```

2. Install the Agent from the install folder.
3. Log off and log on with MFA.


Ame Threats
One Time Code
Administrator
Ame Threats
Other user

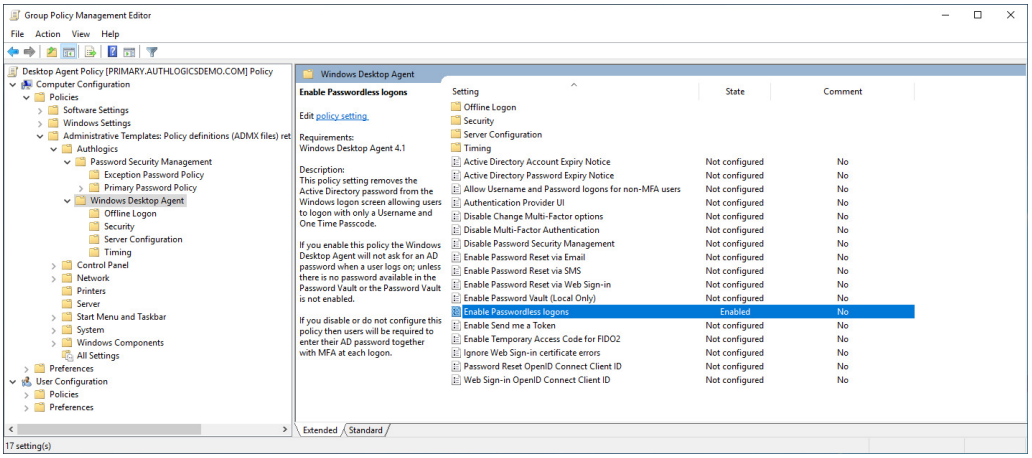
3.5 Configuring Passwordless Windows logons

1. On the Domain Properties dialog, enable the MyID Password Vault:



2. Update the group policy settings.

3. Enable the **Enable Passwordless logons** setting.

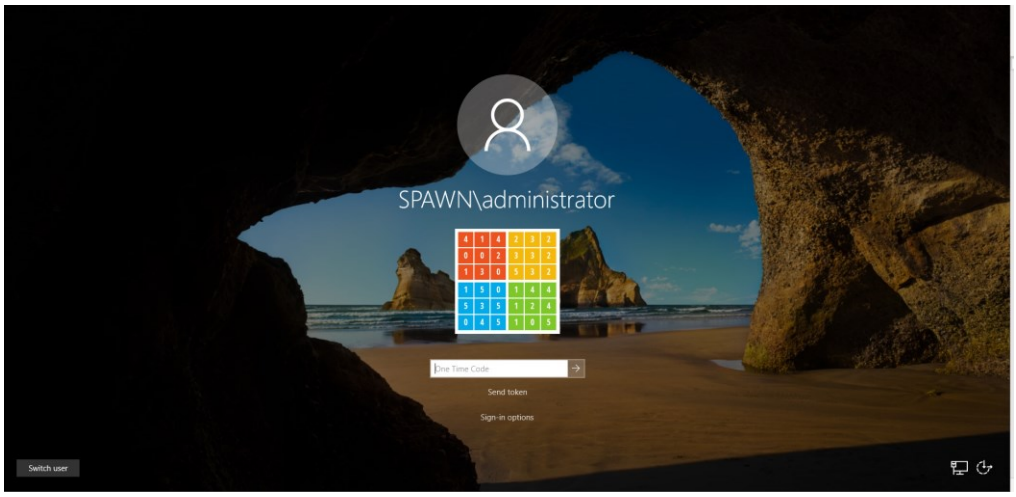


4. Ensure the GPO settings are applied to the PC by running:

```
GPUPDATE /FORCE
```

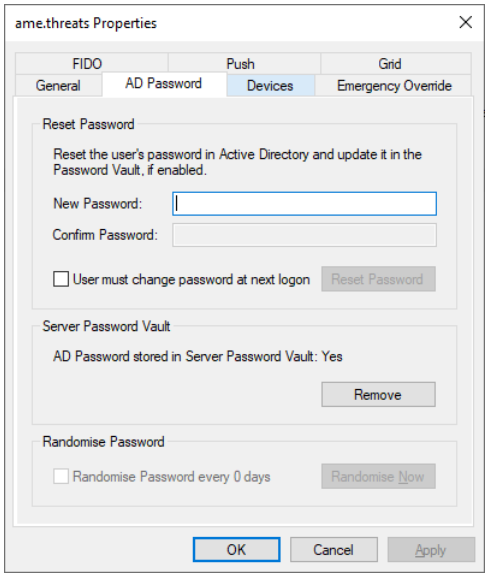
5. Reboot the workstation and log on as the test user.

   Note: There is no password option available:



6. On first attempt the login fails if there is no password in the vault. The password option automatically appears the second time.

7. After the login, the password is saved to the vault, and you can view this on the user account on the server:



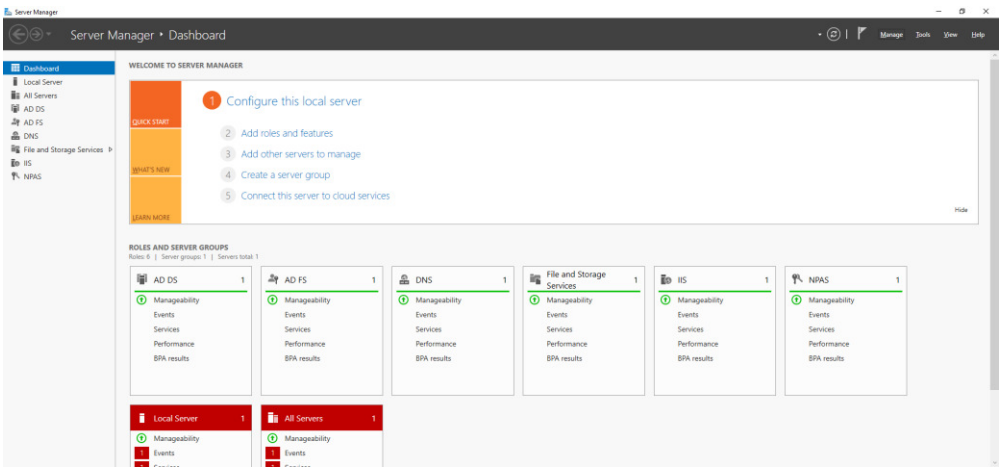
4 Configuring a Certificate Authority

This section details the steps required to set up a Certificate Authority on the MyID server to allow administrators to generate valid trusted certificates required for FIDO and passkey tokens.

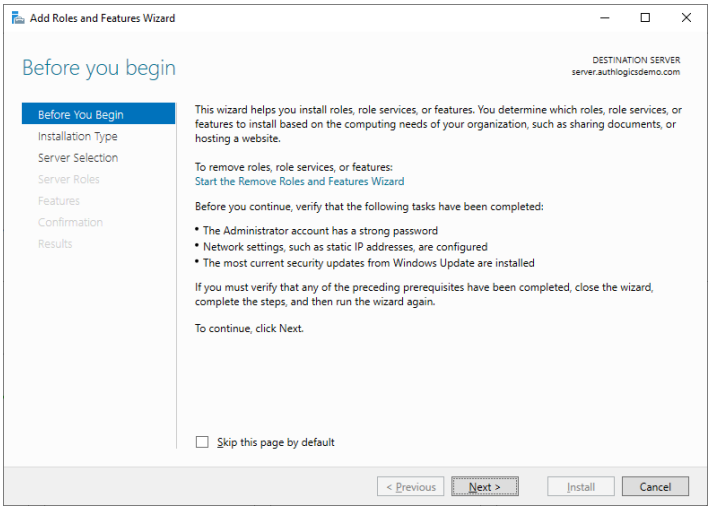
4.1 Installing the Certificate Authority

Perform these actions on the server:

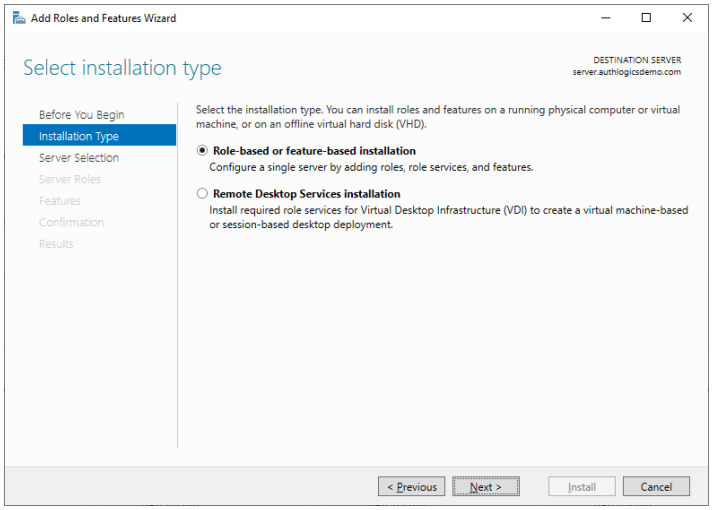
1. Open Server Manager.



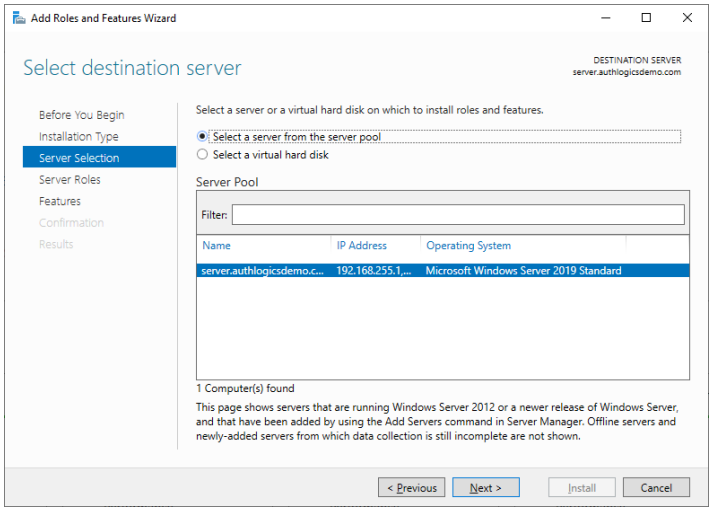
2. Under **Manage**, select **Add Roles and Features**.



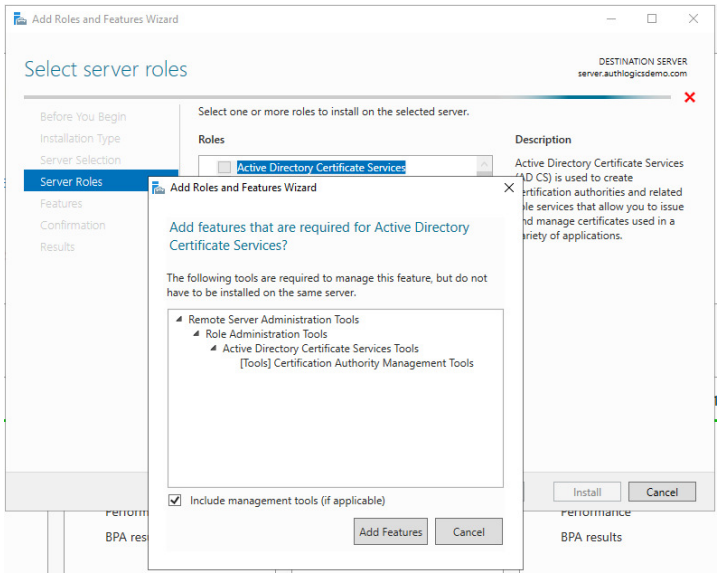
3. Click **Next**.



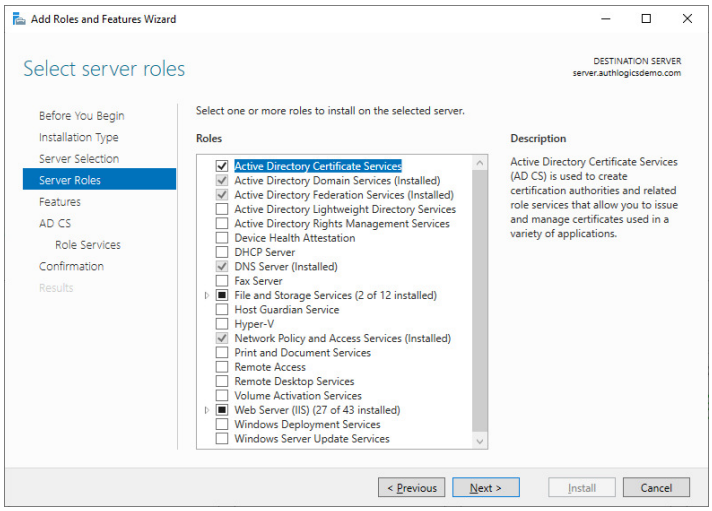
4. Select **Role-based or feature-based installation** and click **Next**.



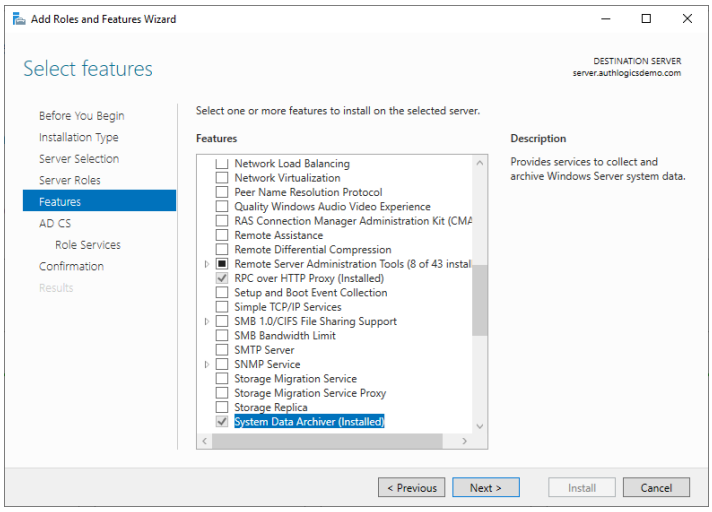
5. Select the local server as the server pool and click **Next**.
6. Enable **Active Directory Certificate Services**.



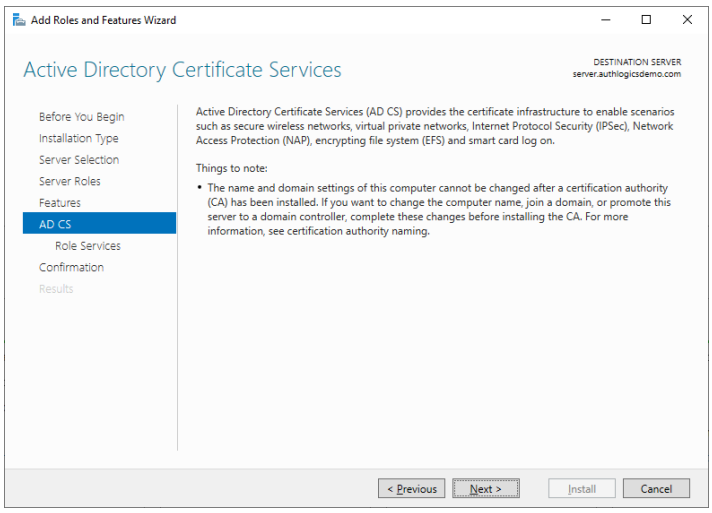
7. Click **Add Features** to add the features required for Active Directory Certificate Services.



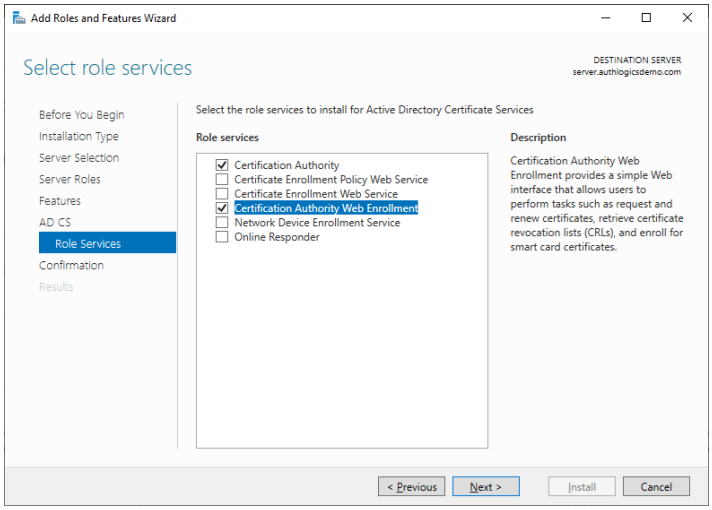
8. Click **Next**.



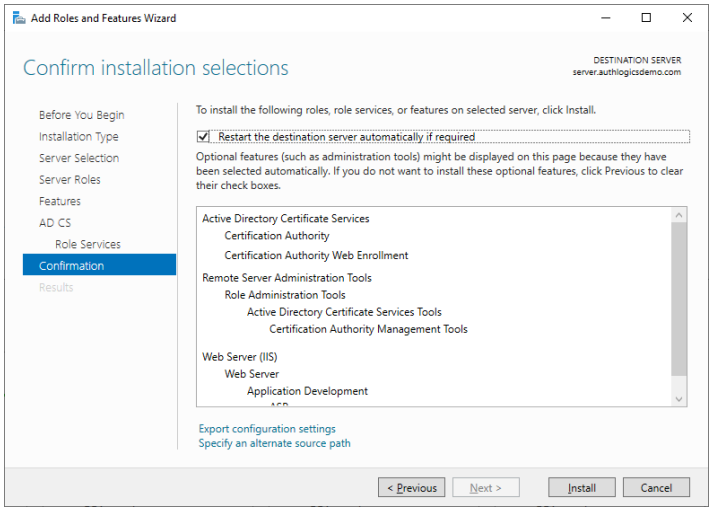
9. Click **Next**.



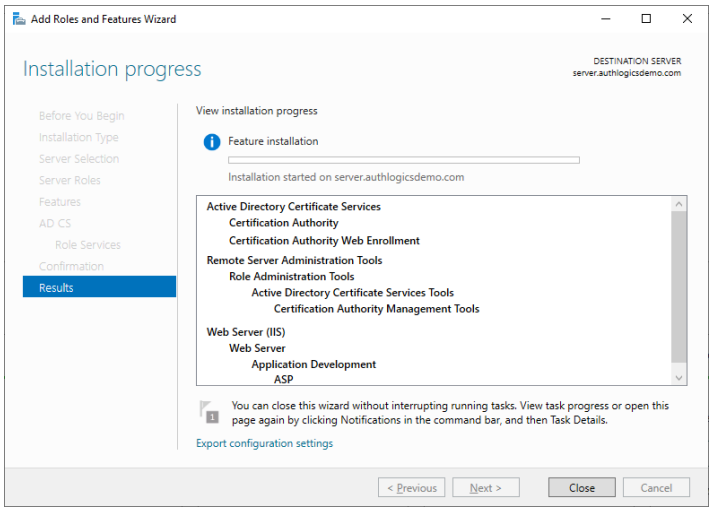
10. Click **Next.**



11. Enable the **Certificate Authority** and **Certificate Authority Web Enrollment** options.

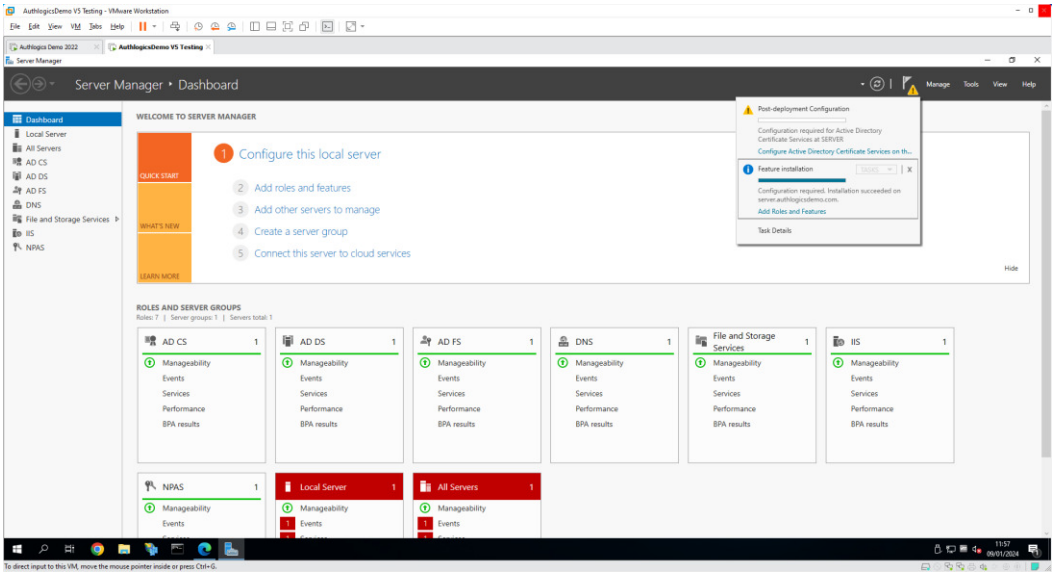


12. Enable the **Restart the destination server automatically if required** option and click **Install**.

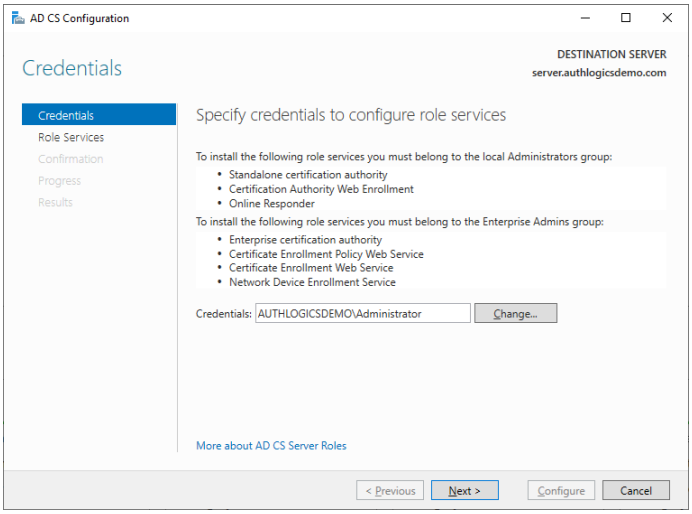


13. When the installation is complete, click **Close**.

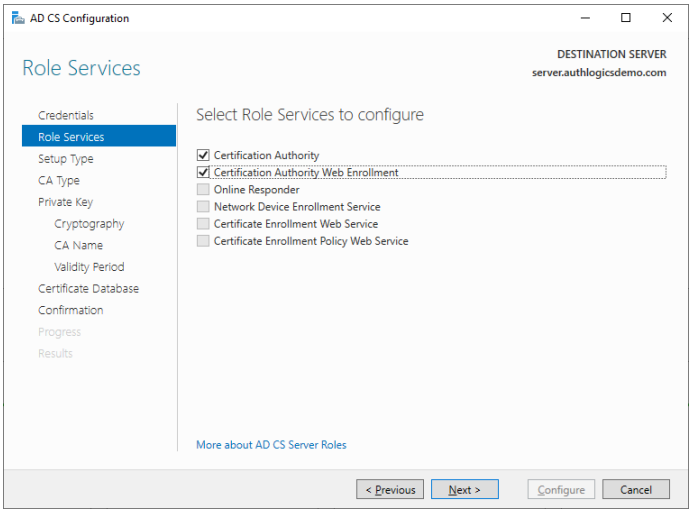
4.2 Configure Active Directory Certificate Services



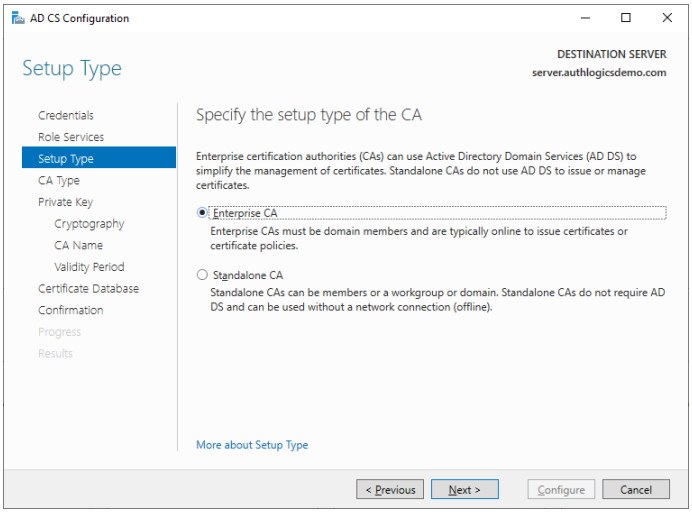
1. Select your Active Directory administrator credentials and the role to configure role services.



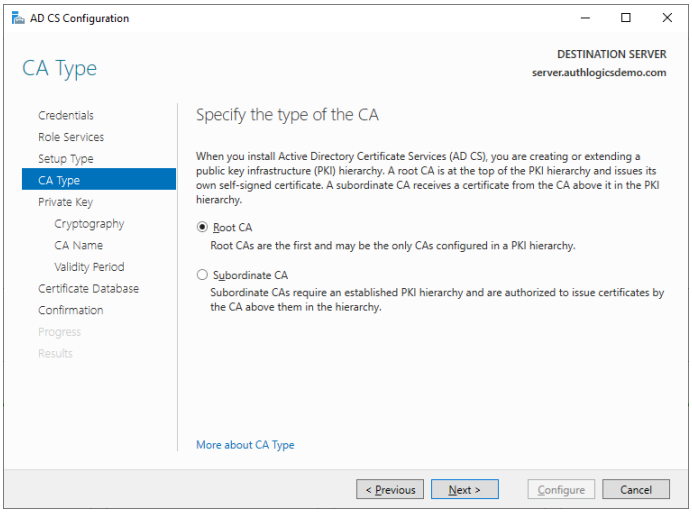
2. In the list of role services, enable the **Certification Authority** and **Certification Authority Web Enrollment** options.



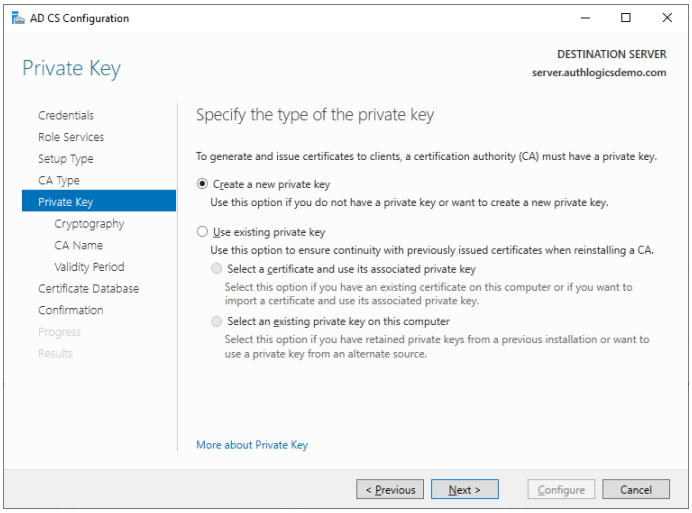
3. Select **Enterprise CA** and click **Next**.



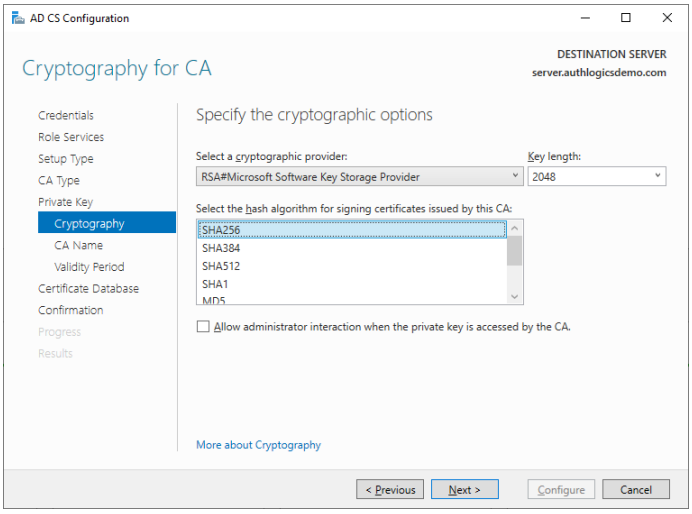
4. Select **Root CA** and click **Next**.



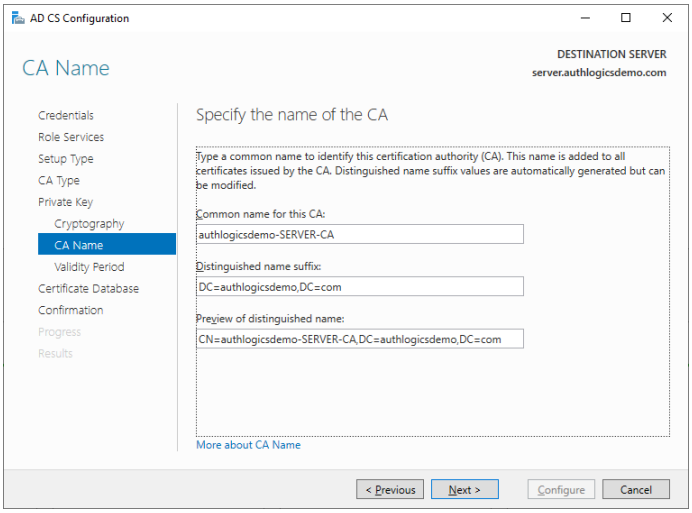
5. Create a new private key and click **Next**.



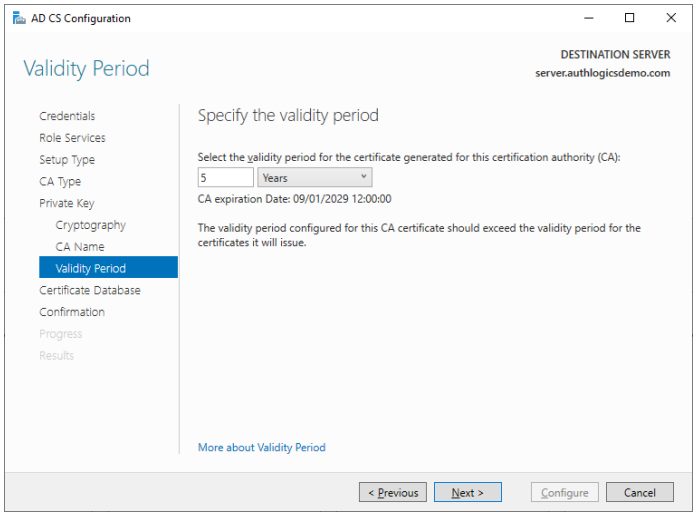
6. Click **Next**.



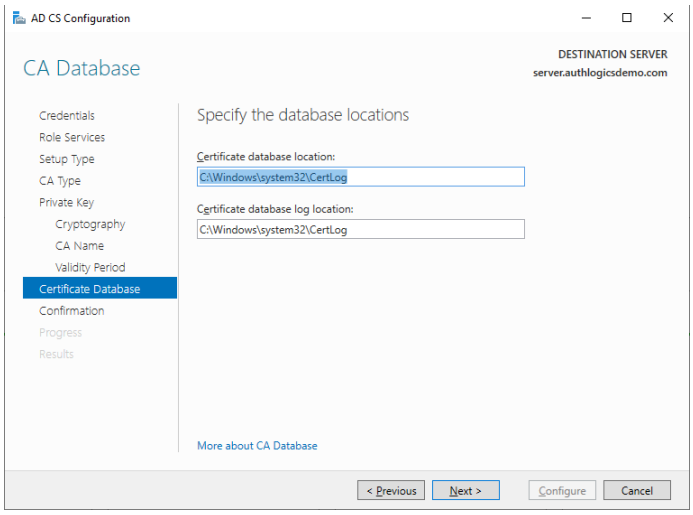
7. Click **Next**.



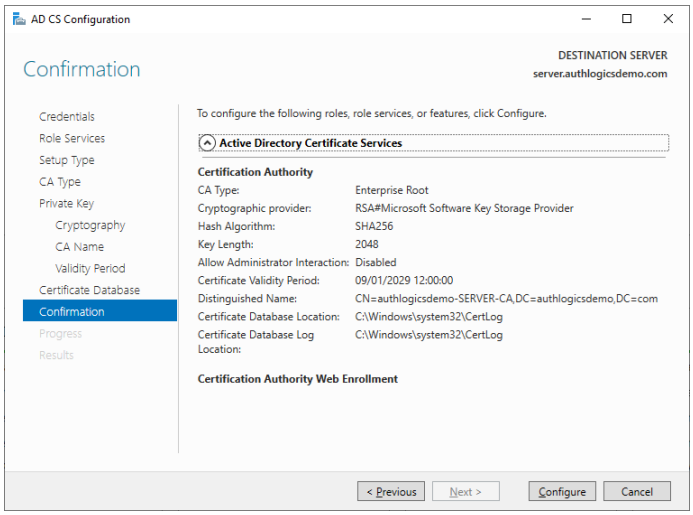
8. Click **Next**.

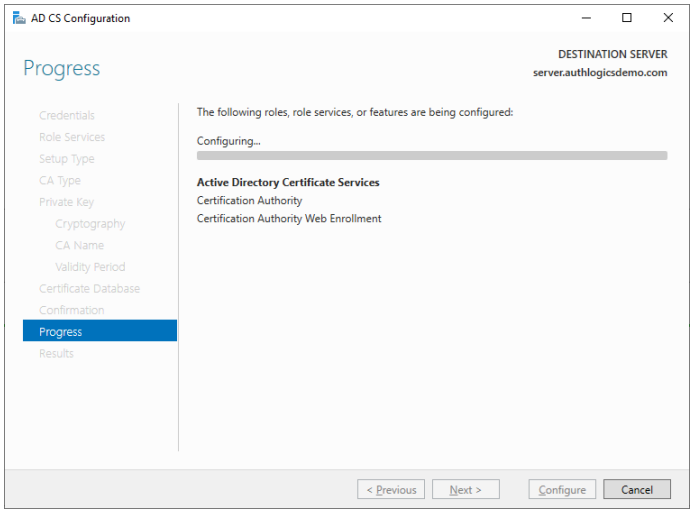


9. Click **Next**.

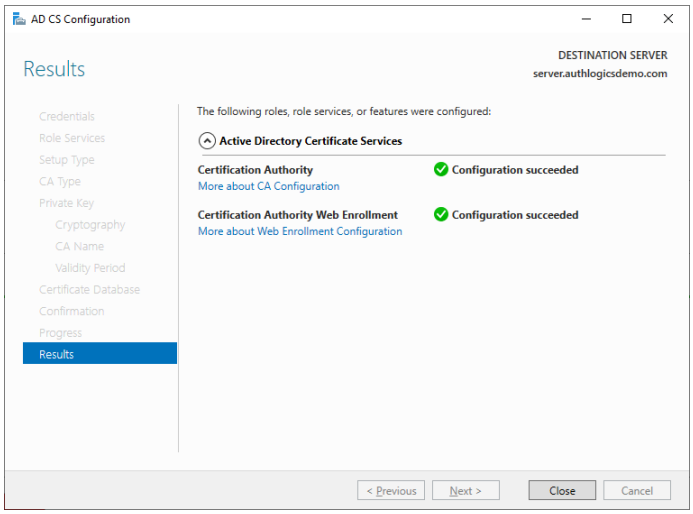


10. Click **Configure**.





11. Click **Close**.



At this stage, the server is now a Certificate Authority and available to issue trusted certificates.

5 Requesting a trusted certificate

This section details the steps required to request a trusted certificate from an on-premises certificate authority.

You can use the following methods to request a privately trusted certificate:

- Through the MyID provided PowerShell script.
- Using IIS.

This section describes the PowerShell script. For information on using IIS, consult your Microsoft documentation.

5.1 Create a certificate request using the MyID PowerShell script

Within the MyID Authentication Server installation folder, navigate to the following subfolder:

```
ResKit\Scripts\
```

Open a PowerShell ISE window using administrator credentials and run the following script:

```
RequestTrustedCert.ps1
```

The `RequestTrustedCert` PowerShell script requires the following inputs:

- `ServerName`

  This is the FQDN for the MyID Authentication Server or public name for Authentication Server web site.

- `CompanyName`
- `Department`
- `City`
- `State`
- `Country`

For example:

```
PS C:\Program Files\Authlogics Authentication Server\ResKit\Scripts>
.\RequestTrustedCert.ps1 -serverName dc.authlogicsdev.com -companyName
"Intercede" -department "IT" -city "Bracknell" -state "Berkshire" -
country "UK"
```

When you run the script, it creates a Web Server certificate and applies it to the Local Computer Personal Certificate Store, issued to the server name specified by the `ServerName` parameter.

Ensure that the `ServerName` parameter matches the Authentication Server's publicly accessible web site name.