



MyID MFA and PSM

Version 5.1

Multi-Factor Authentication Quick Start Guide

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

Copyright

© 2001-2025 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non-disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

The Intercede® and MyID® word marks and the MyID® logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.

Conventions used in this document

- 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:
For example:
 - Copy the file *before* starting the installation.
 - Do *not* remove the files before you have backed them up.
- ***Bold and italic*** hyperlinks 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 installation 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

Multi-Factor Authentication Quick Start Guide	1
Copyright	2
Conventions used in this document	3
Contents	4
1 Introduction	5
1.1 Considerations	5
1.2 Required information	5
2 Installing the Authentication Server	6
3 Configuring the Authentication Server	9
3.1 Adding MFA users	9
3.2 Setting up RADIUS	12
3.3 Monitoring MFA usage	14
3.4 Configuring the Windows Desktop Agent	16
3.5 Configuring Passwordless Windows logons	18
4 Configuring a Certificate Authority	22
4.1 Installing the Certificate Authority	22
4.2 Configure Active Directory Certificate Services	28
5 Requesting a trusted certificate	35
5.1 Create a certificate request using the MyID PowerShell script	36

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:

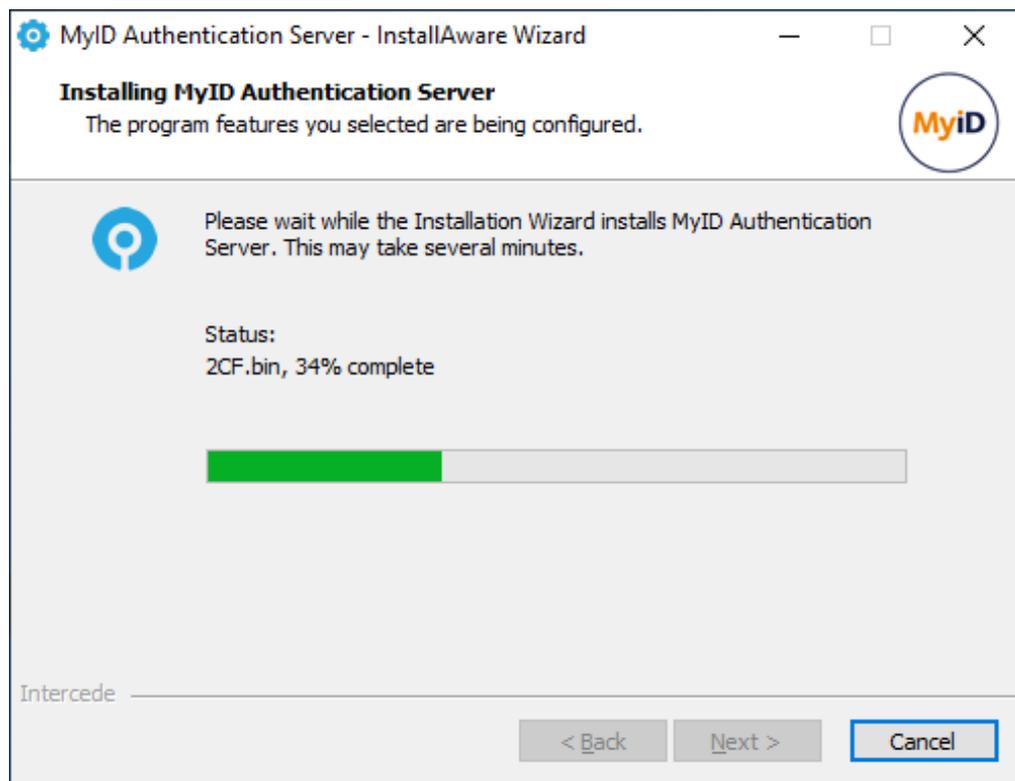
- Active Directory administrator credentials.
- SMTP server details: name, port, authentication requirements.
- The DNS name for the server.
- Understanding of which authentication technology to use.
- For FIDO and passkey tokens, MyID MFA requires a trusted certificate to be bound to MyID web sites; 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.

2 Installing the Authentication Server

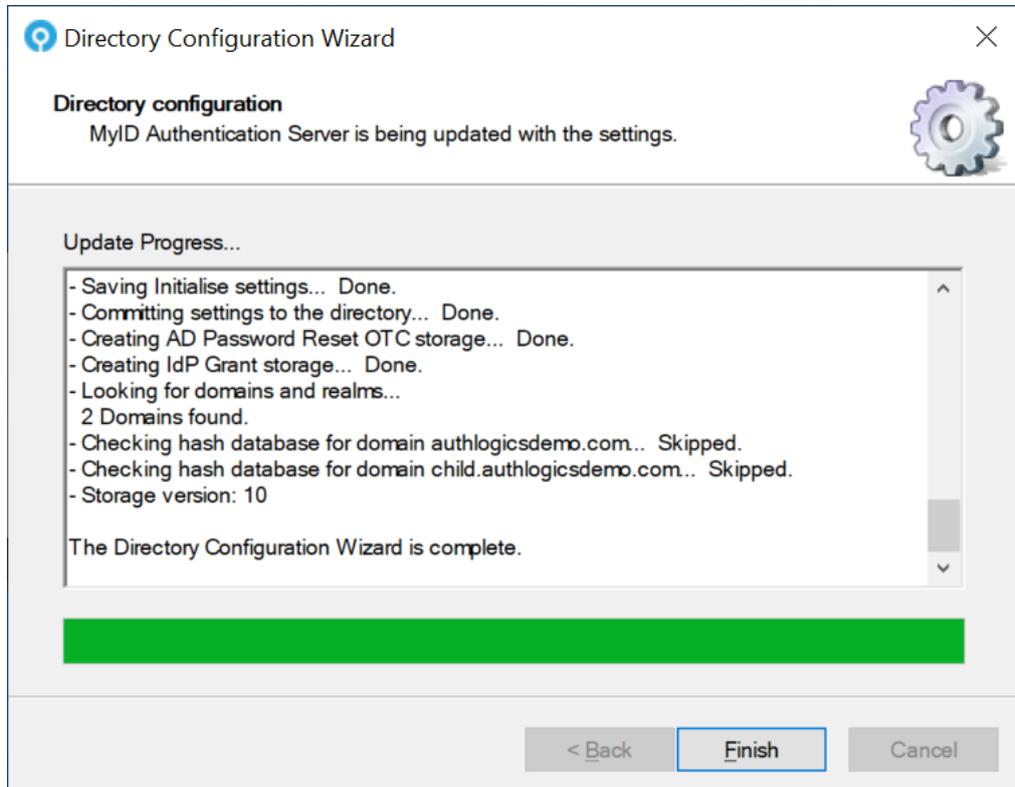
To install the MyID Authentication Server:

1. Download the Authentication Server installer from:
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.



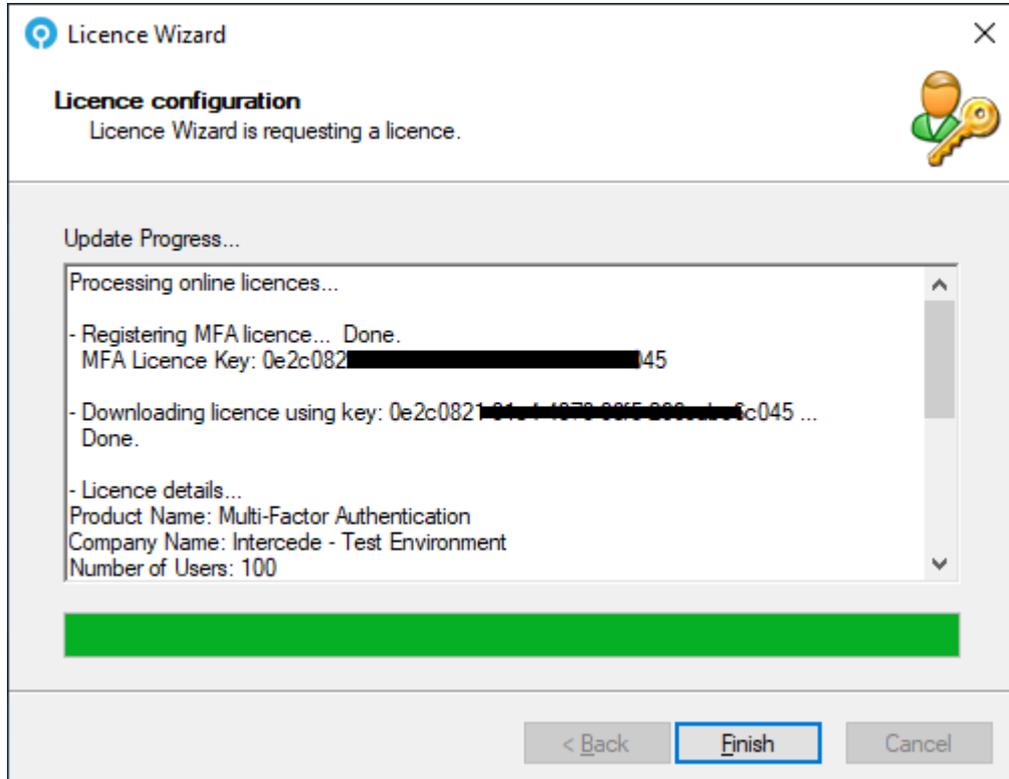
For more information, see the *Installing the MyID Authentication Server* section in the [MyID Authentication Server Installation and Configuration Guide](#).

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



For more information, see the *MyID Authentication Server Directory configuration* section in the [MyID Authentication Server Installation and Configuration Guide](#).

- 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.



For more information, see the *MyID license configuration* section in the [MyID Authentication Server Installation and Configuration Guide](#).

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

3 Configuring the Authentication Server

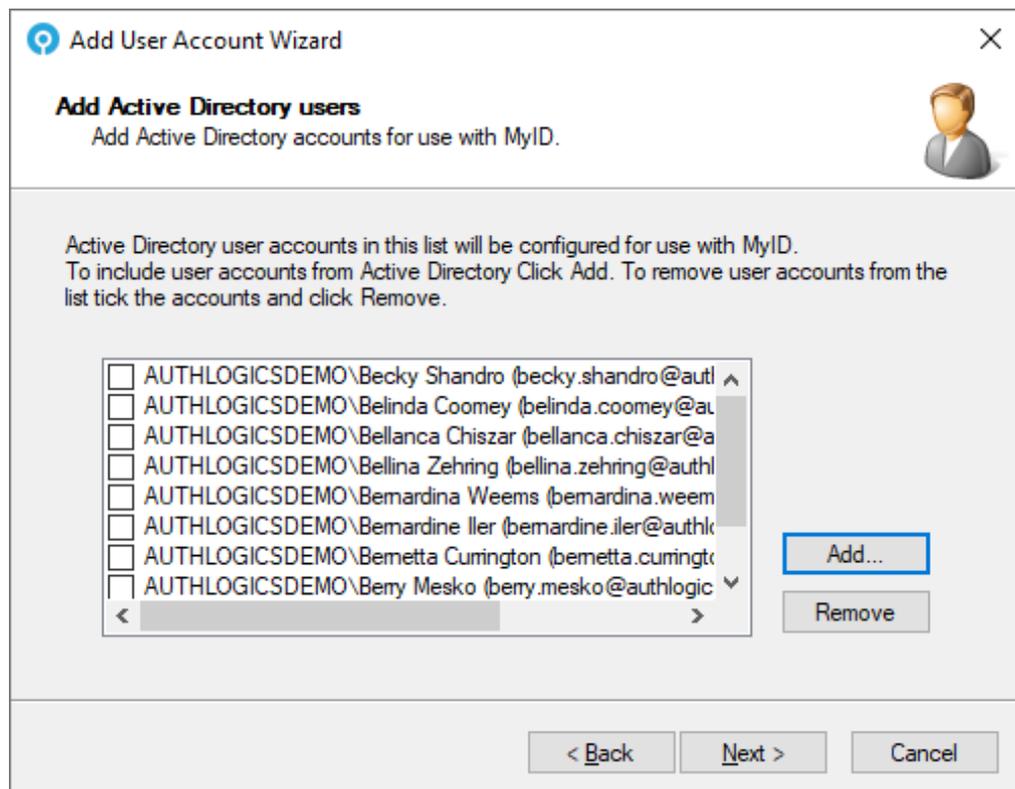
To begin the configuration of the MyID Authentication Server:

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:

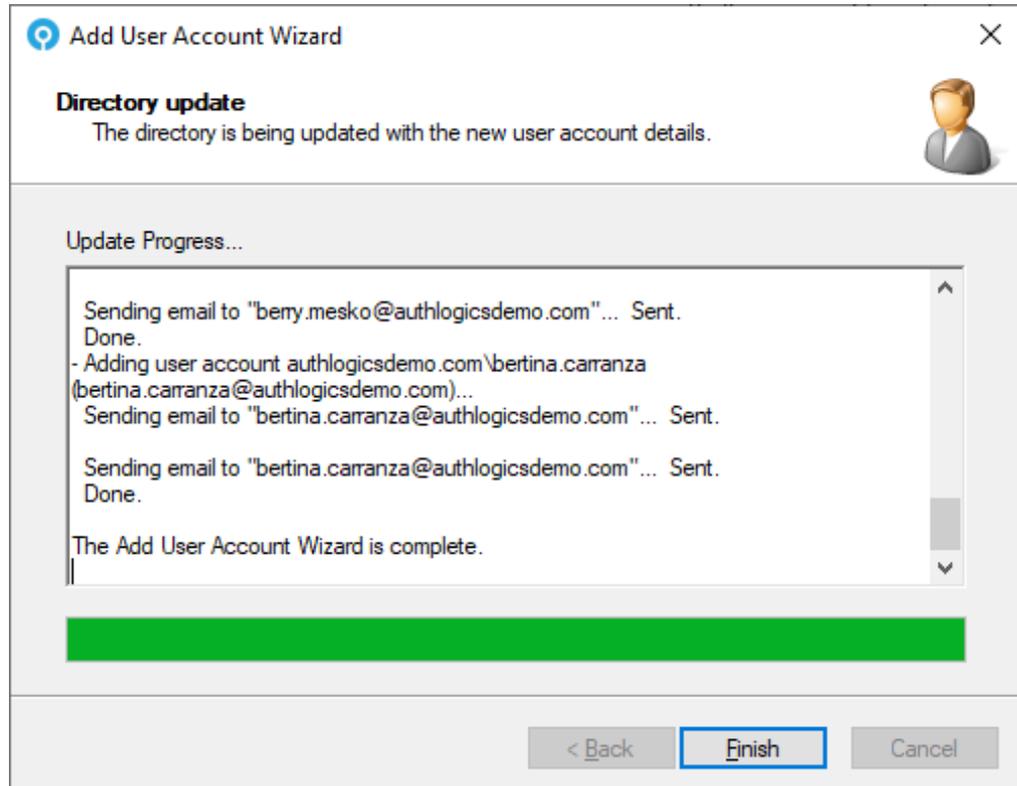
1. Expand the domains and open the domain into which you want to add MFA users.
2. Click the **Add User Account** action.
The Add User Account Wizard starts.
3. Select all the Active Directory users you want to configure for MyID MFA.



For more information on selecting user accounts, see the *Adding a new MyID user account* section in the [MyID Authentication Server Installation and Configuration Guide](#).

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.

ame.threats Properties

FIDO Push Grid
General AD Password Devices Emergency Override

Devices

Device: Google Android - Galaxy S9

Name: Galaxy S9

Device Enabled

Device ID: 6115320811031112

Type: Google Android

Last sync: 08 January 2024 11:26:38

Last used: 08 January 2024 12:17:32

Sync Now Remove

Authenticator App Security

Require Biometric Seed

OK Cancel Apply

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.

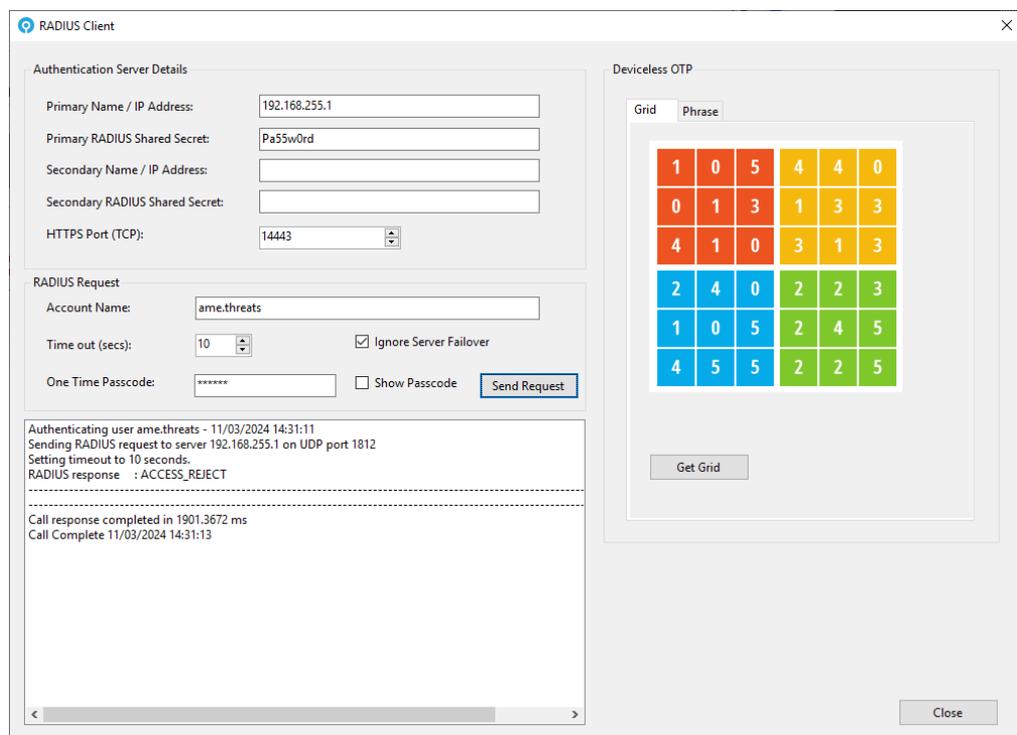
For more information on adding the local server as a RADIUS client, see the *Adding a RADIUS client* section in the **MyID Authentication Server Installation and Configuration Guide**.

5. Start the MyID RADIUS test client from:

```
C:\Program Files\Authlogics Authentication Server\
ResKit\Radius\Authlogics 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
```

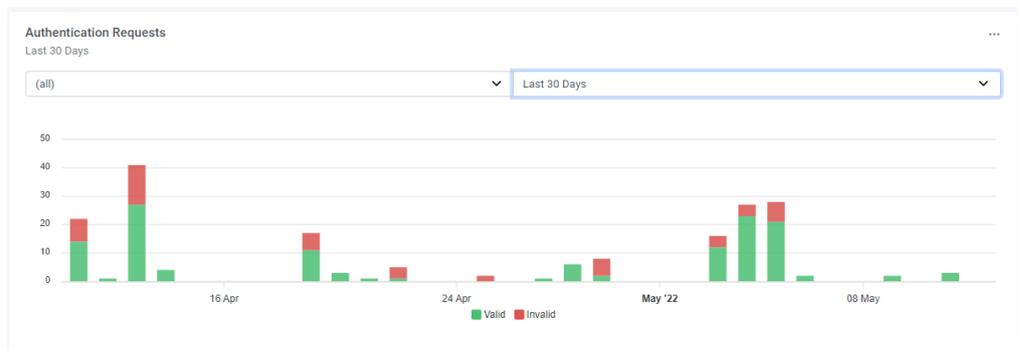
Where <servername> is the name of your server.

For more information on the Web Management Portal, see the *Web Management Portal dashboards* section in the [MyID Authentication Server Installation and Configuration Guide](#).

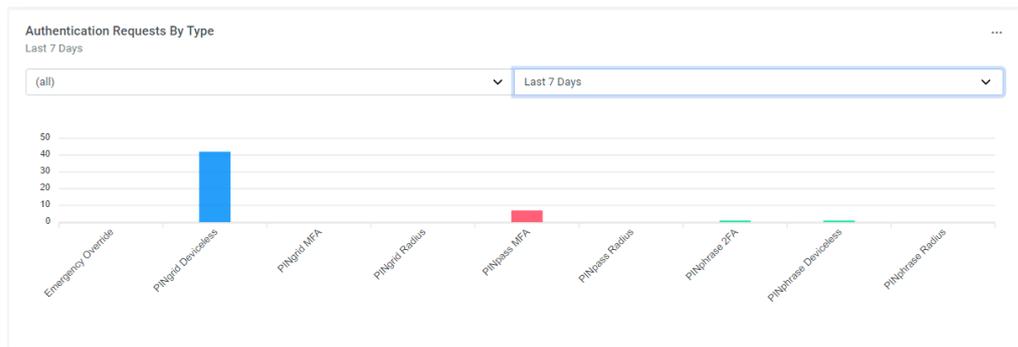
2. Under **System > Dashboards**, select **Multi-Factor Authentication**.

This dashboard reflects contains information on:

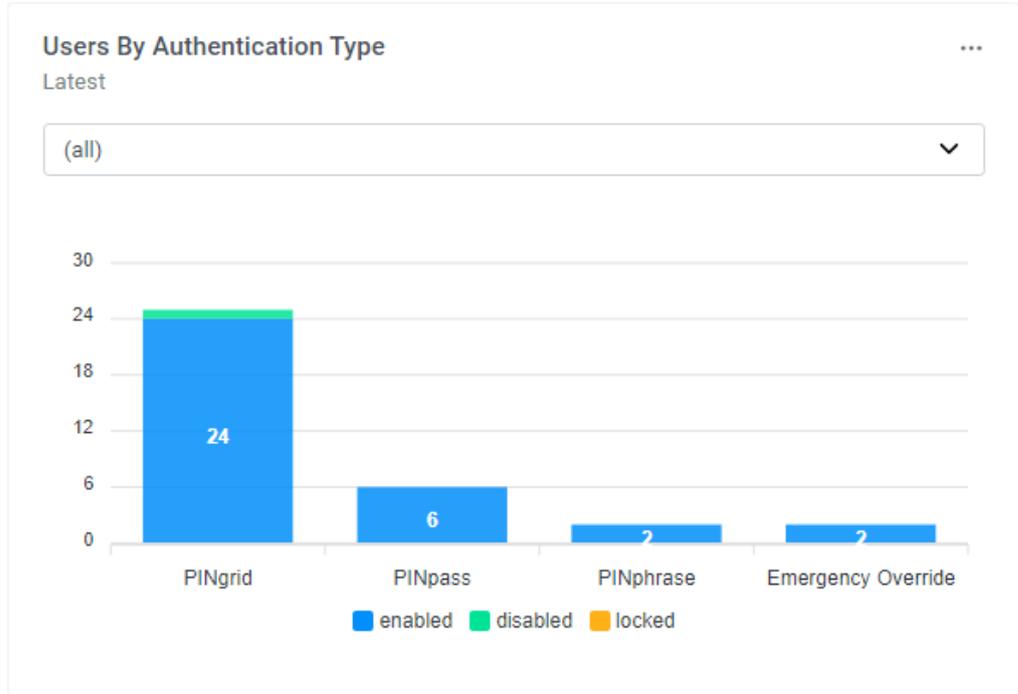
- **Authentication Requests**



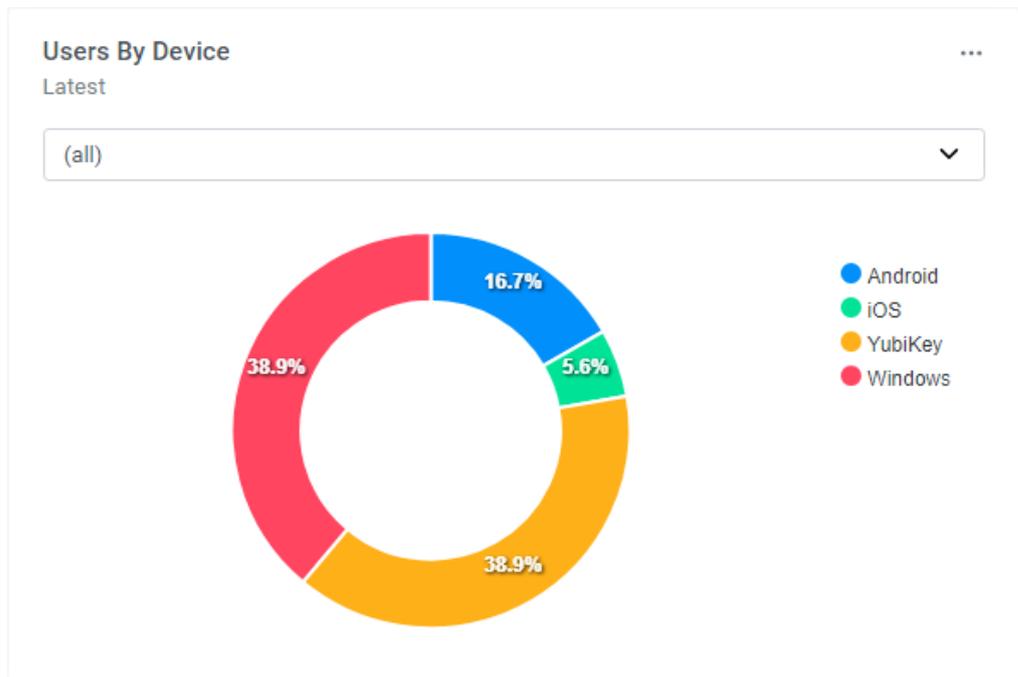
- **Authentication Requests By Type**



• Users By Authentication Type



• Users By Device



3.4 Configuring the Windows Desktop Agent

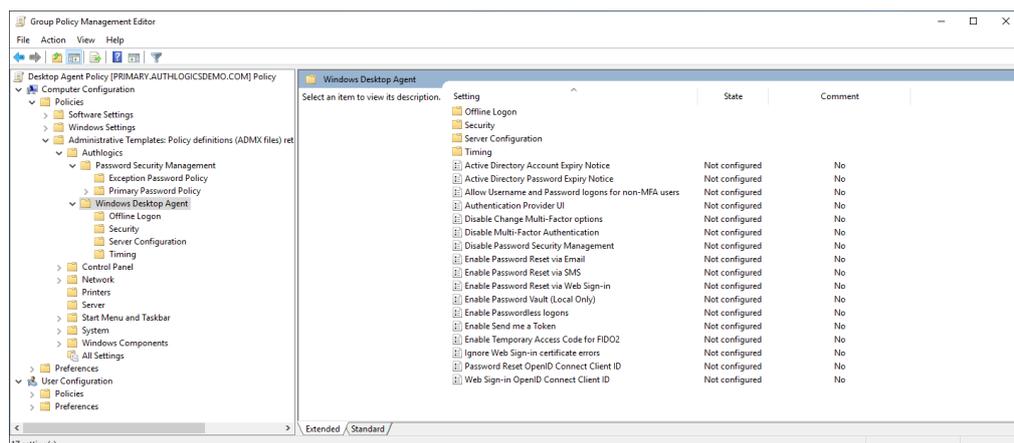
This section assumes that you are using a separate workstation test PC which is domain joined. You can deploy the MyID Windows Desktop Agent on non-domain joined PCs; however, you must apply the Group Policy Objects to these PCs manually.

Perform these actions on the server:

1. Download the Windows Desktop Agent installer from:
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.

For more information on importing the Group Policy ADMX Templates, see the *Adding Group Policy ADMX Templates to the local computer* section of the [Windows Desktop Agent Integration Guide](#).

4. Configure the following settings (assuming you are using Grid):
 - Authentication Provider UI: Enabled, Grid.
 - Disabled Windows Username and Password logons.

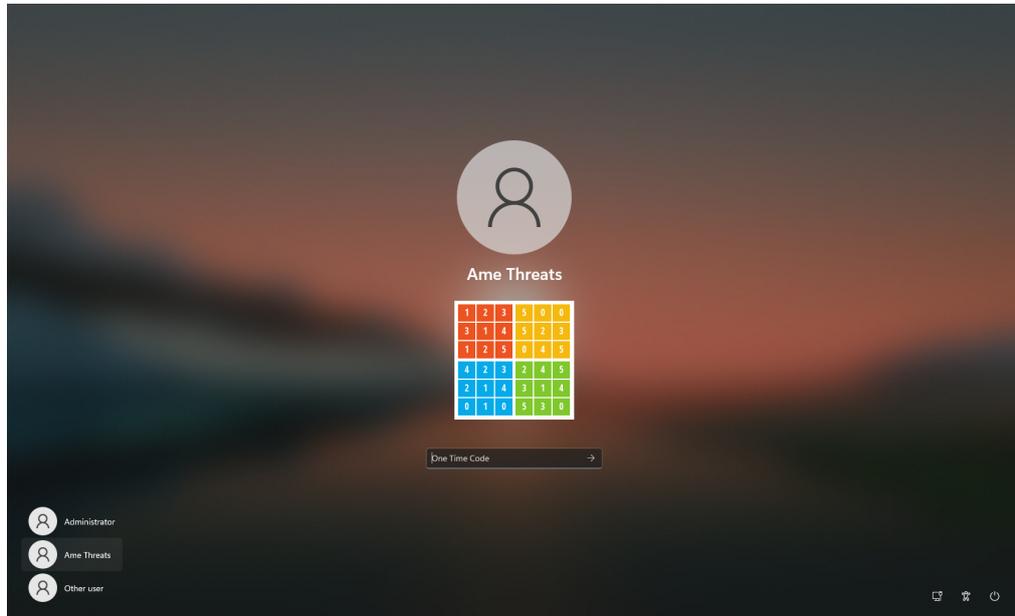


For more information on configuring the Windows Desktop Agent using group policies, see the *Configuring the MyID Windows Desktop Agent* section of the [Windows Desktop Agent Integration Guide](#).

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

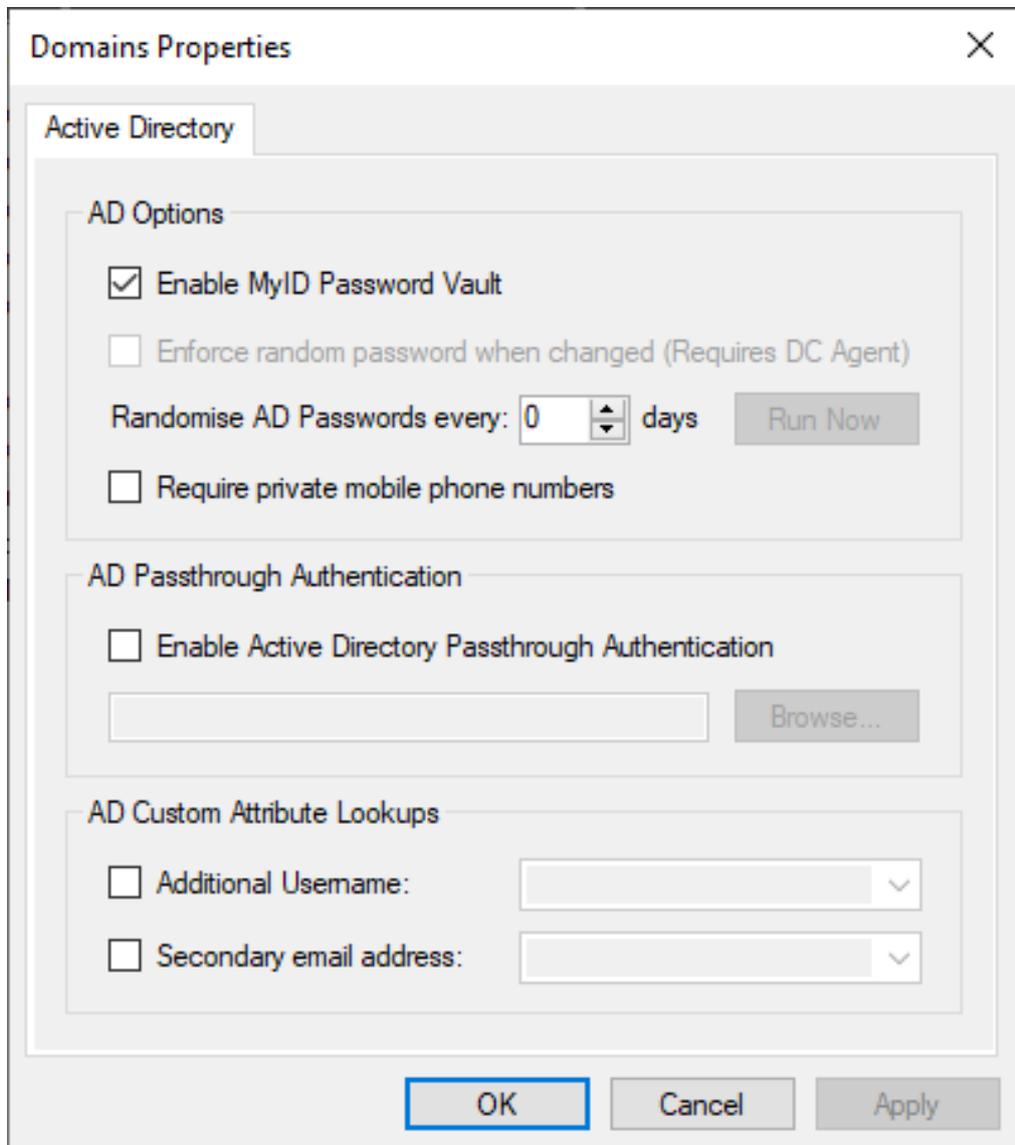
Perform these actions on the workstation:

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.



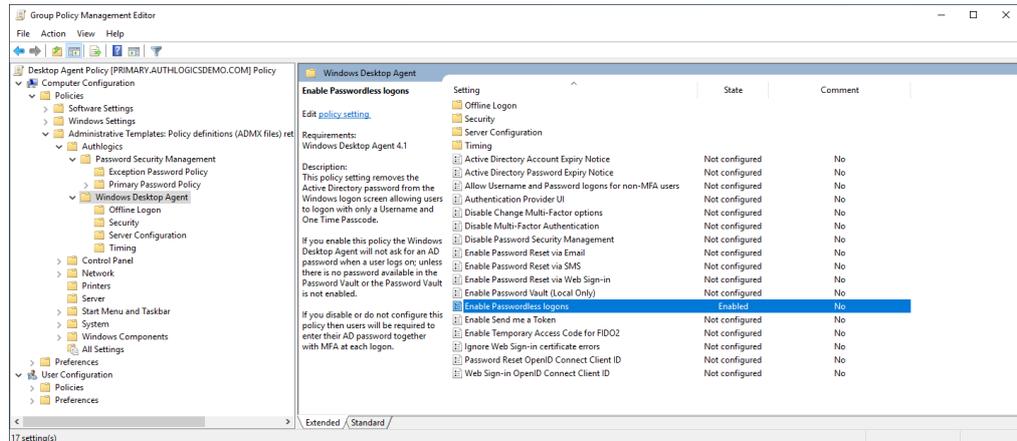
3.5 Configuring Passwordless Windows logons

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



2. Update the group policy settings.

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

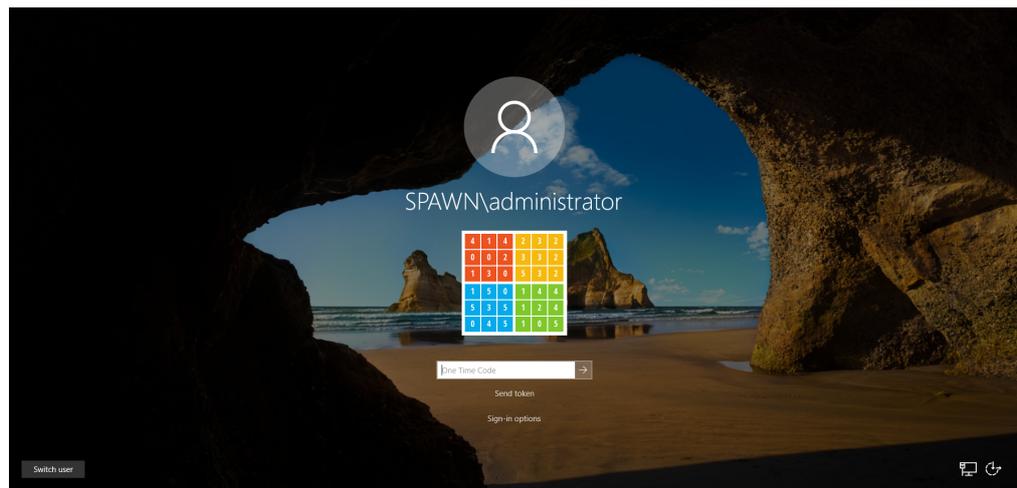


4. Ensure the GPO settings are applied to the PC by running:

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:

The screenshot shows a dialog box titled "ame.threats Properties" with a close button (X) in the top right corner. The dialog has four tabs: "General", "AD Password", "Devices" (which is selected and highlighted in blue), and "Emergency Override".

Under the "Devices" tab, there are three main sections:

- Reset Password:** This section contains the instruction "Reset the user's password in Active Directory and update it in the Password Vault, if enabled." Below this are two text input fields: "New Password:" and "Confirm Password:". At the bottom of this section is a checkbox labeled "User must change password at next logon" and a "Reset Password" button.
- Server Password Vault:** This section shows the text "AD Password stored in Server Password Vault: Yes" and a "Remove" button.
- Randomise Password:** This section contains a checkbox labeled "Randomise Password every 0 days" and a "Randomise Now" button.

At the bottom of the dialog box, there are three buttons: "OK", "Cancel", and "Apply". The "OK" button is highlighted with a blue border.

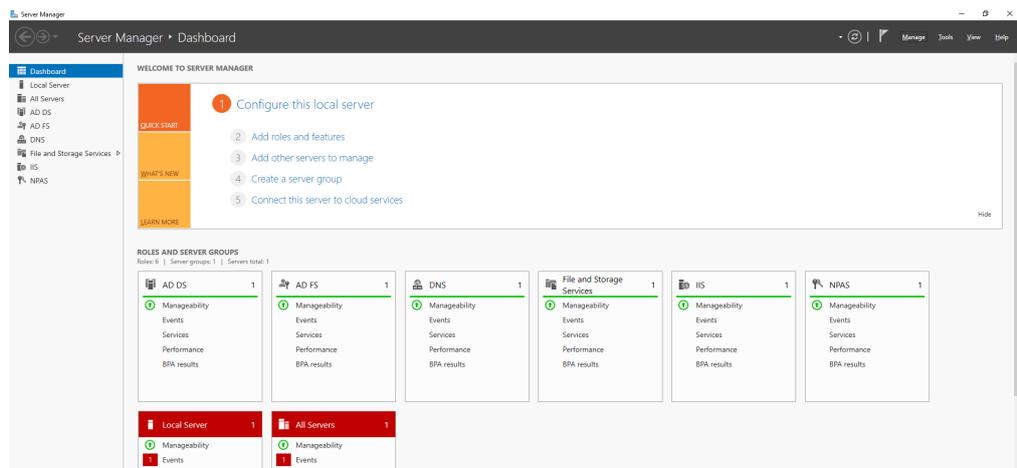
4 Configuring a Certificate Authority

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.

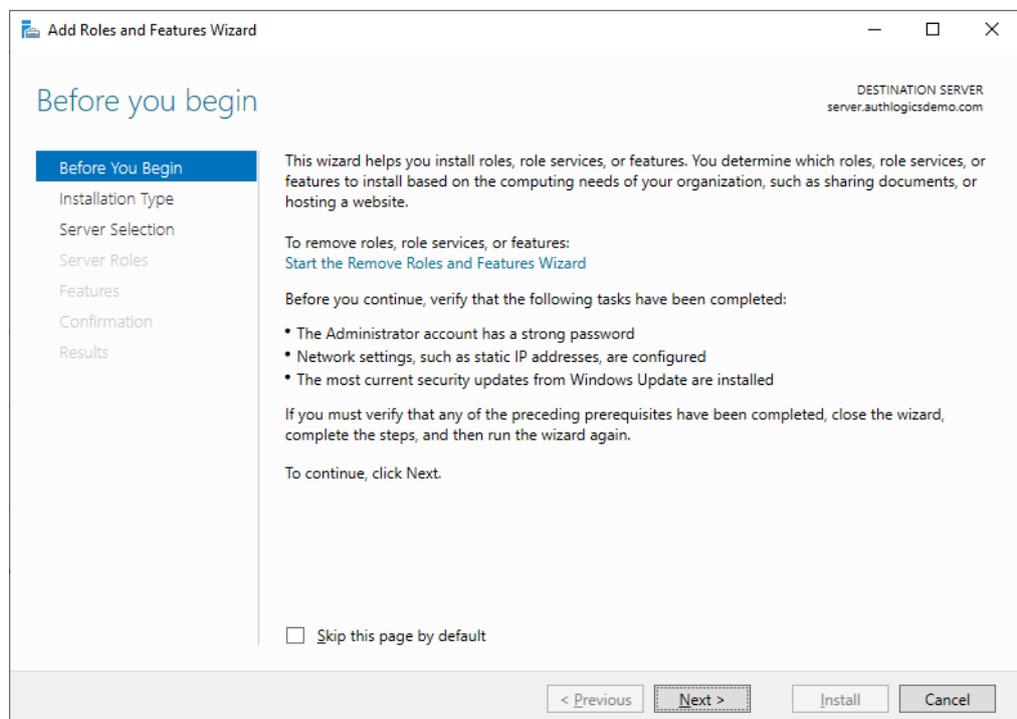
4.1 Installing the Certificate Authority

Perform these actions on the server:

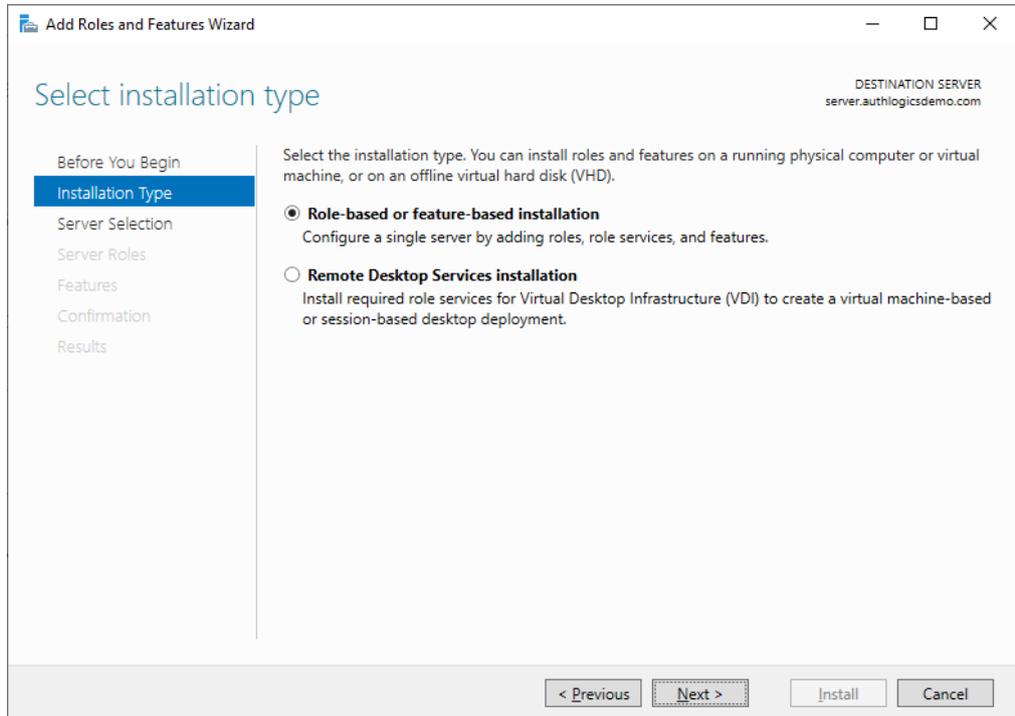
1. Open Server Manager.



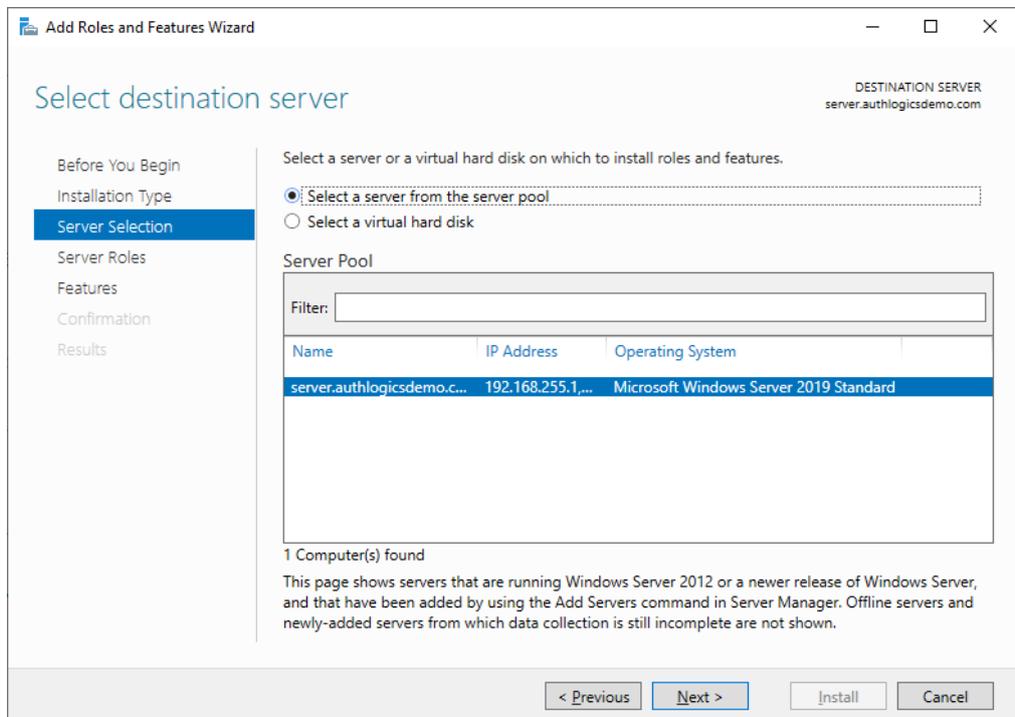
2. Under **Manage**, select **Add Roles and Features**.



3. Click **Next**.

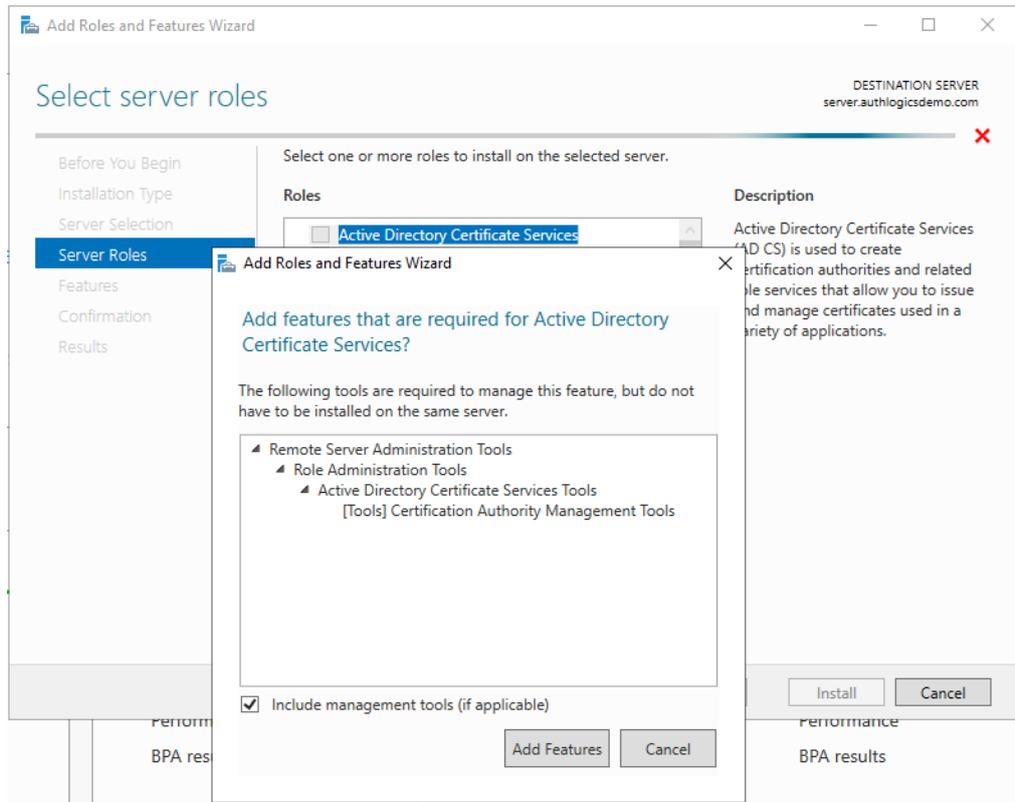


4. Select **Role-based or feature-based installation** and click **Next**.

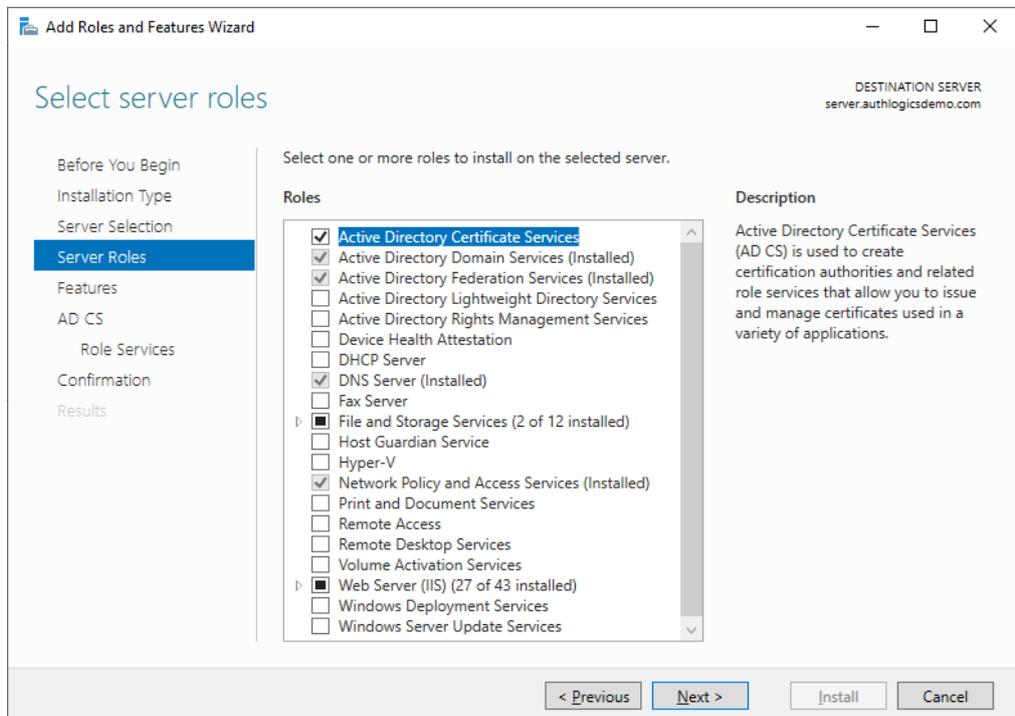


5. Select the local server as the server pool and click **Next**.

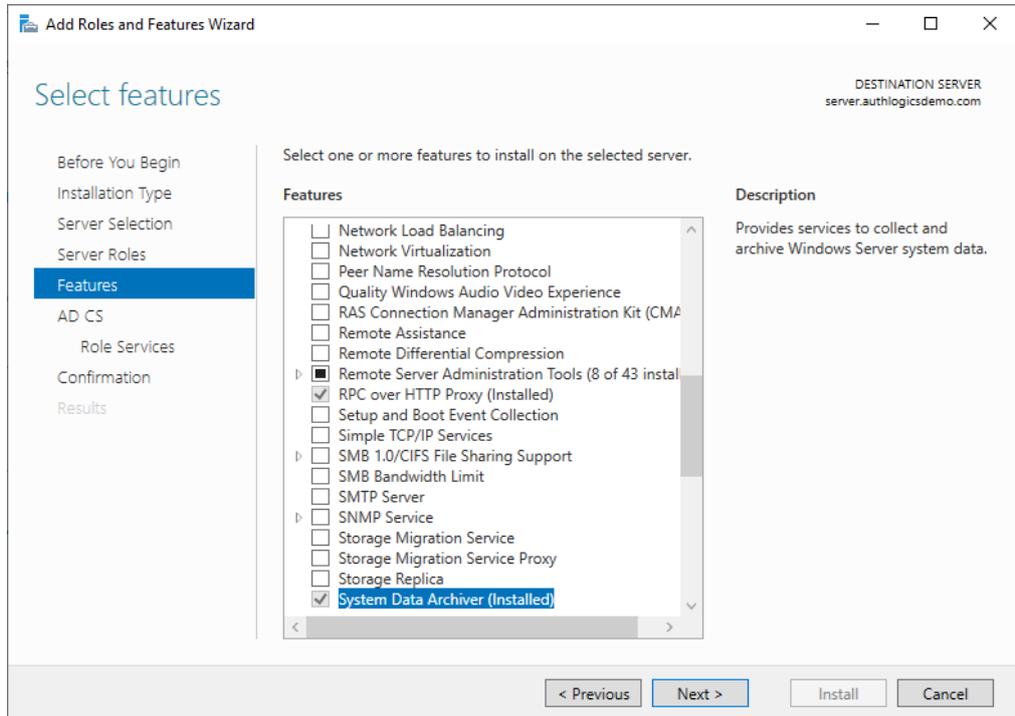
6. Enable **Active Directory Certificate Services**.



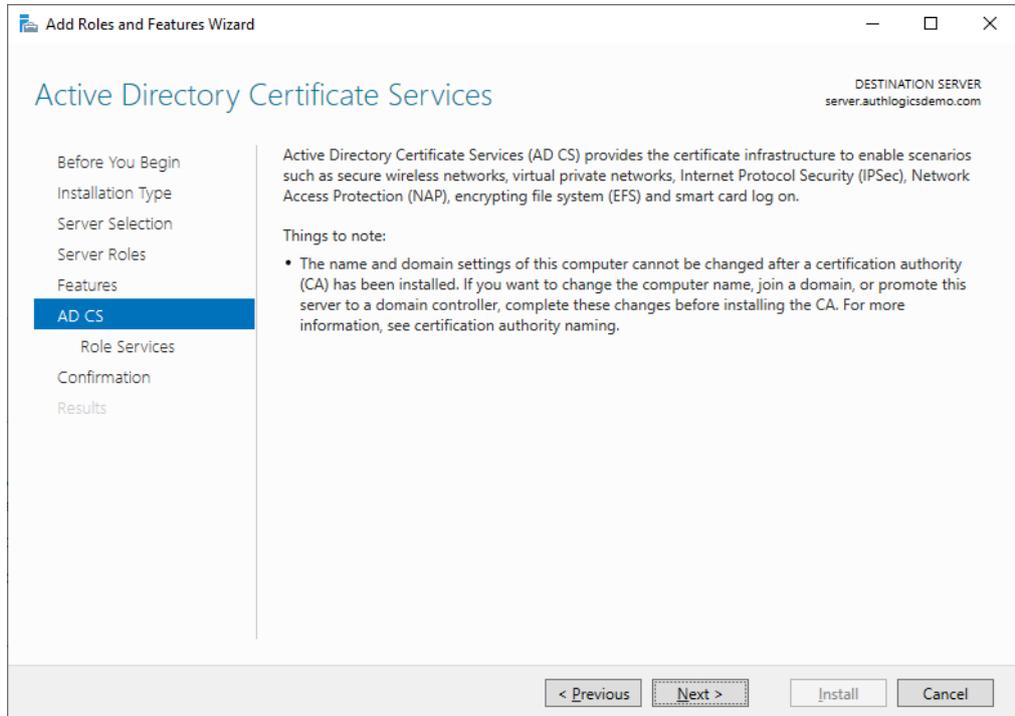
7. Click **Add Features** to add the features required for Active Directory Certificate Services.



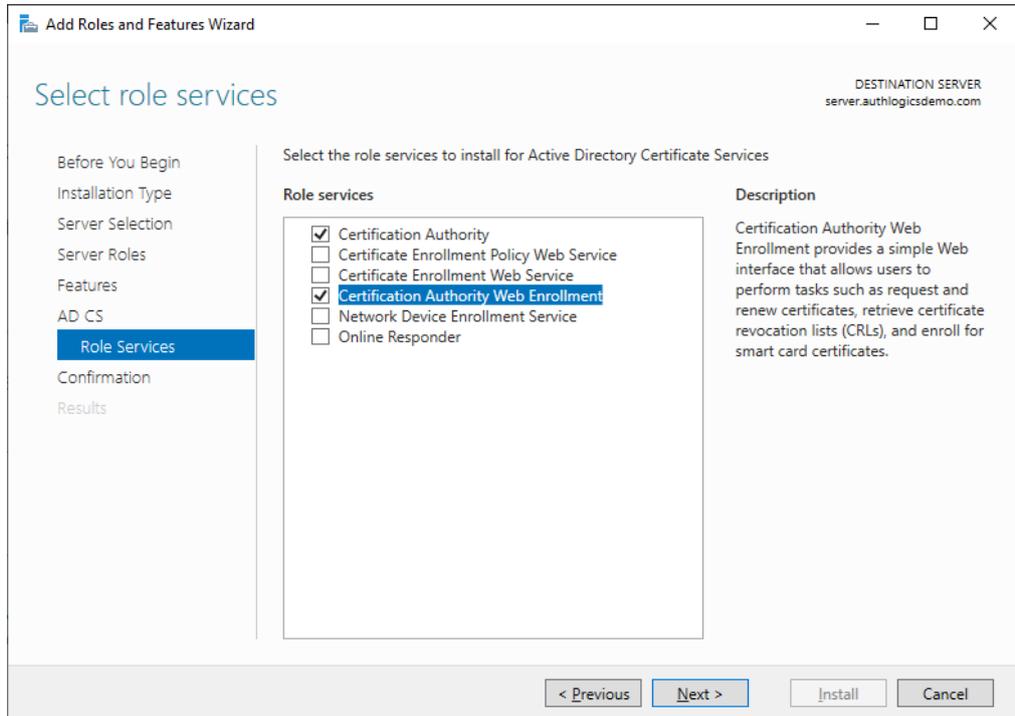
8. Click **Next**.



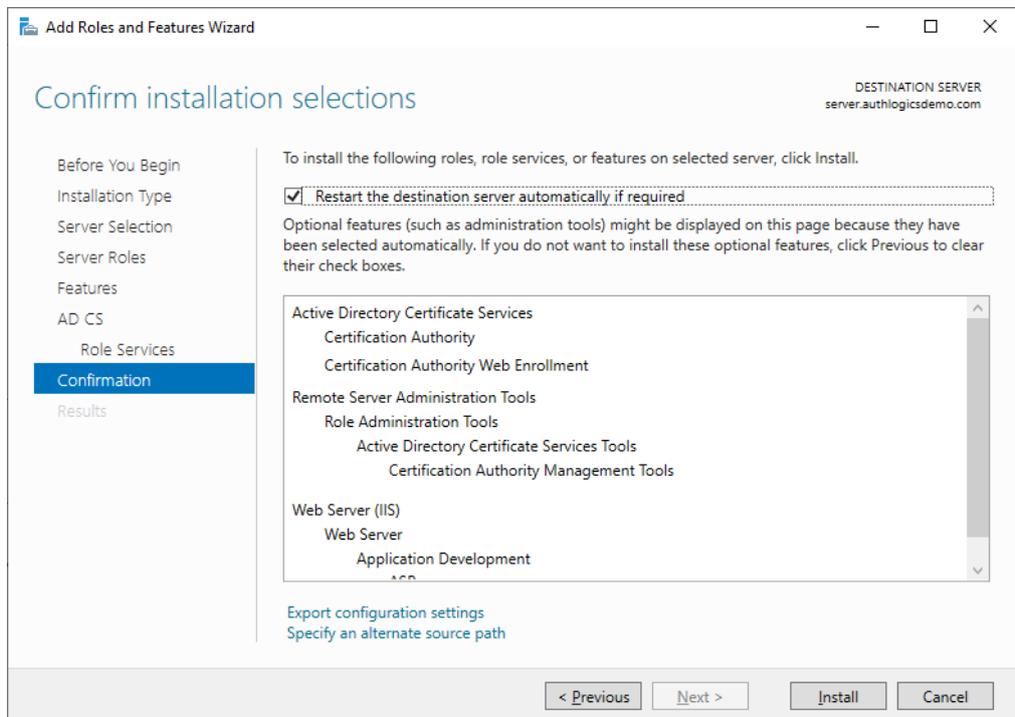
9. Click **Next**.



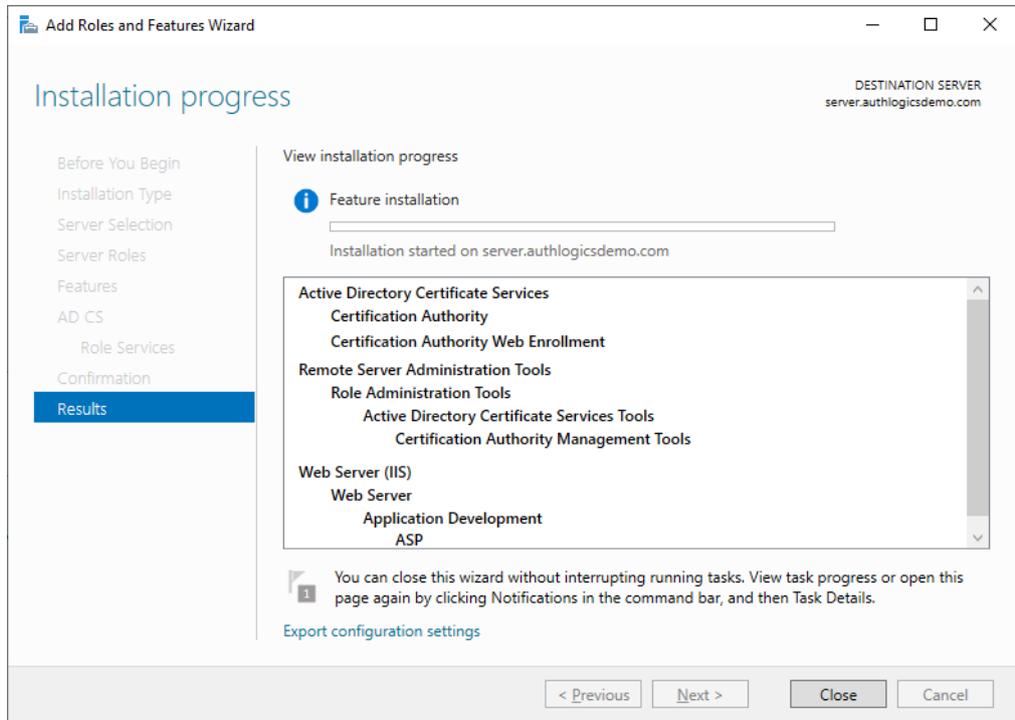
10. Click **Next**.



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

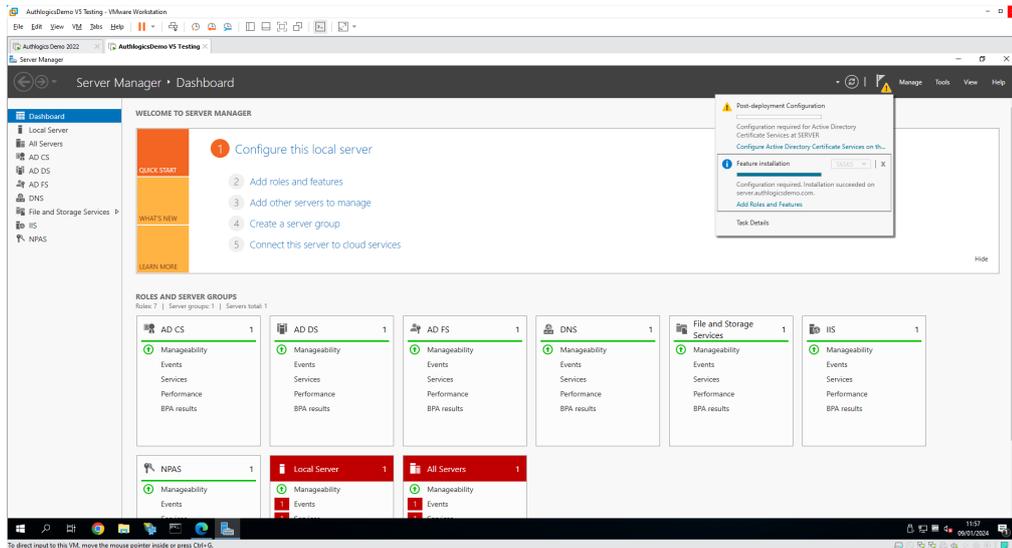


- 12. Enable the **Restart the destination server automatically if required** option and click **Install**.

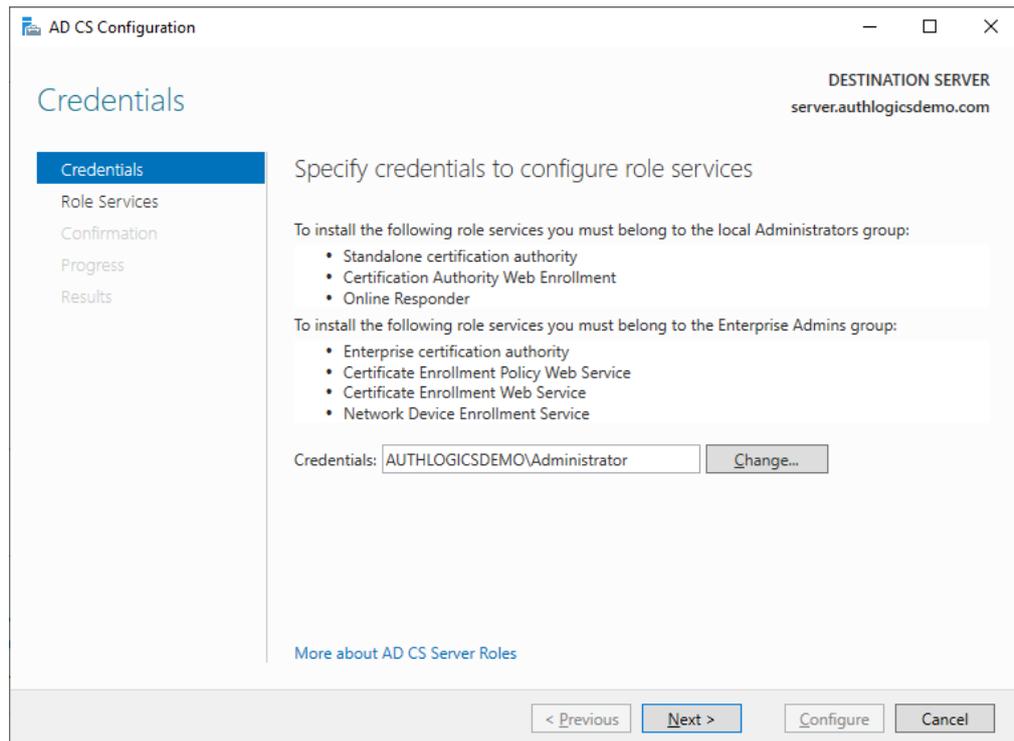


- 13. When the installation is complete, click **Close**.

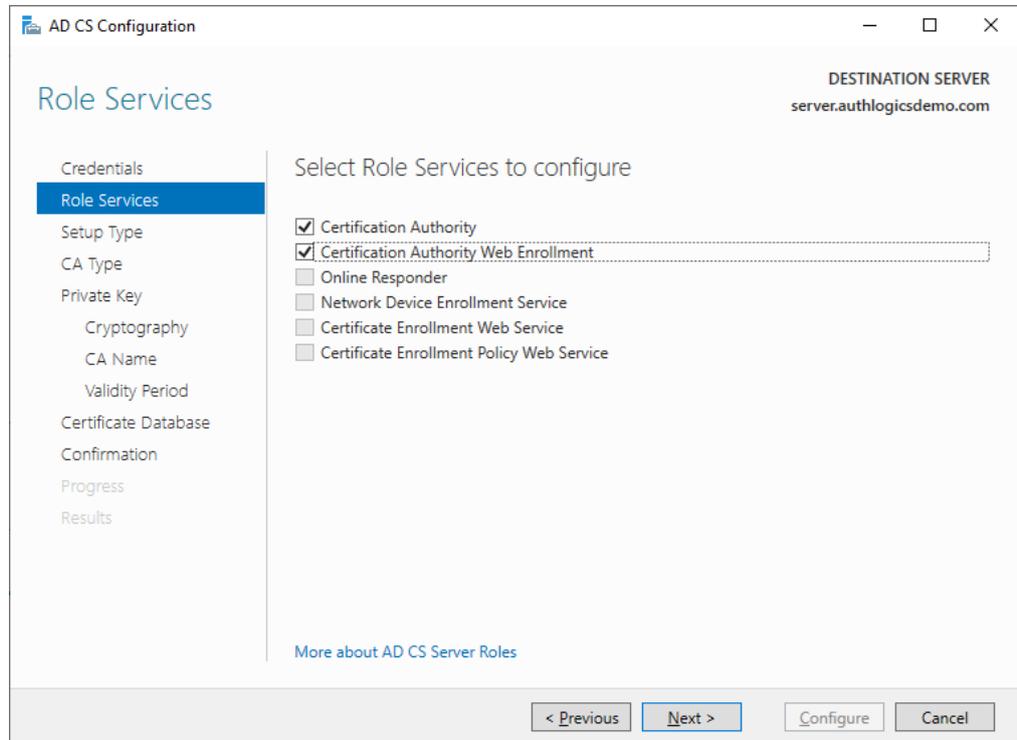
4.2 Configure Active Directory Certificate Services



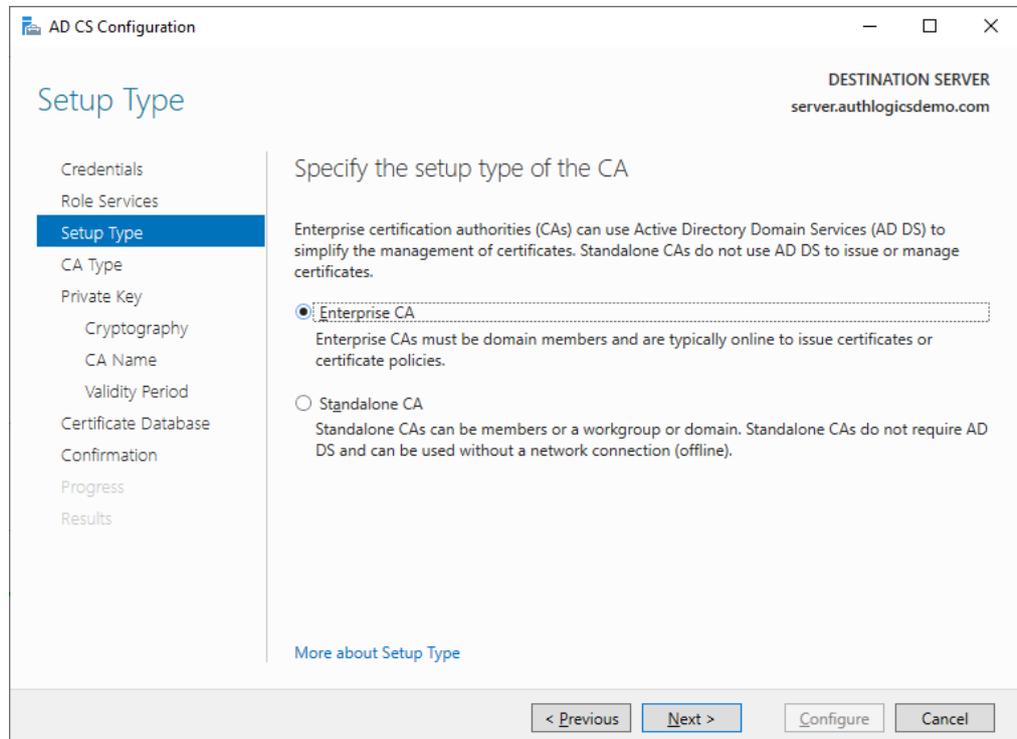
1. Select your Active Directory administrator credentials and the role to configure role services.



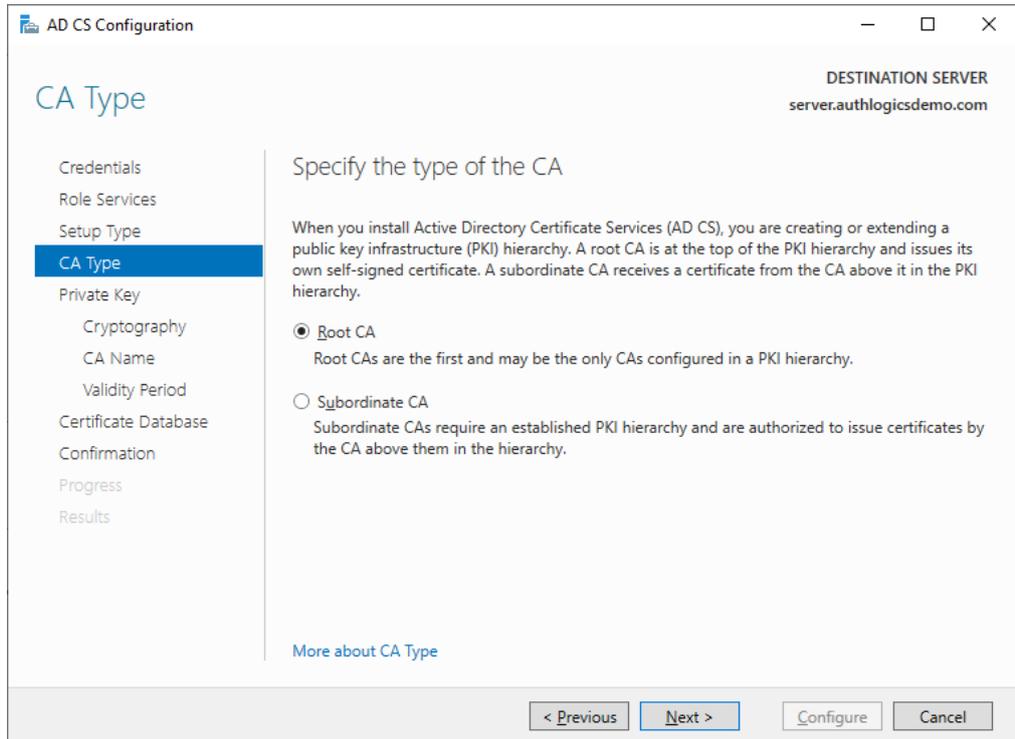
- In the list of role services, enable the **Certification Authority** and **Certification Authority Web Enrollment** options.



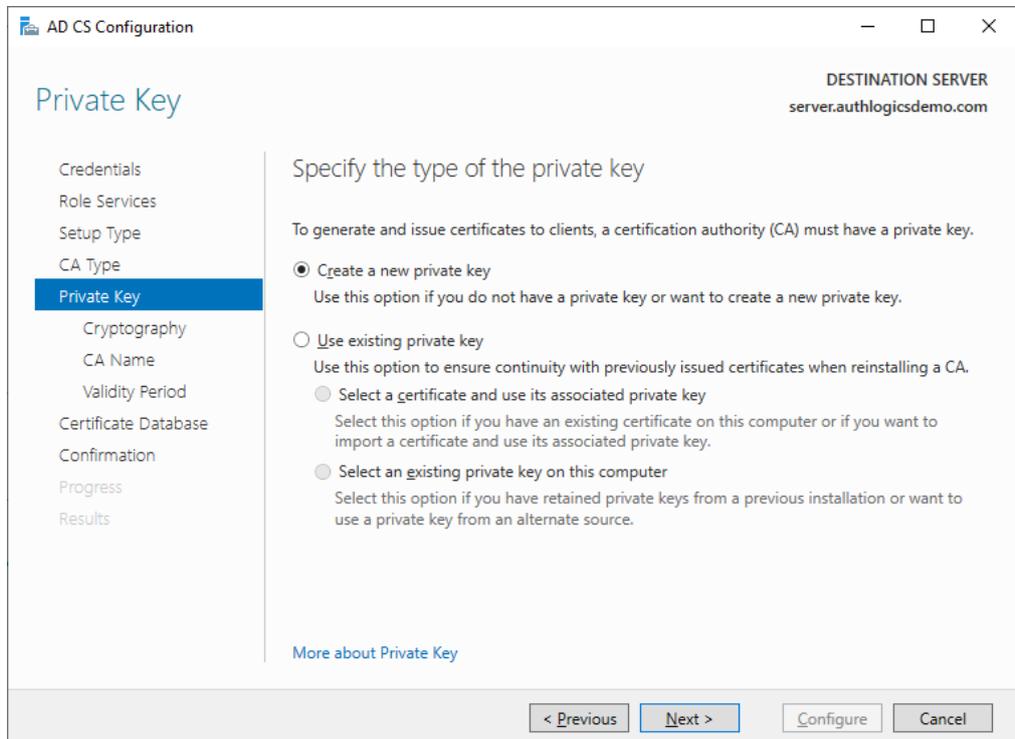
- Select **Enterprise CA** and click **Next**.



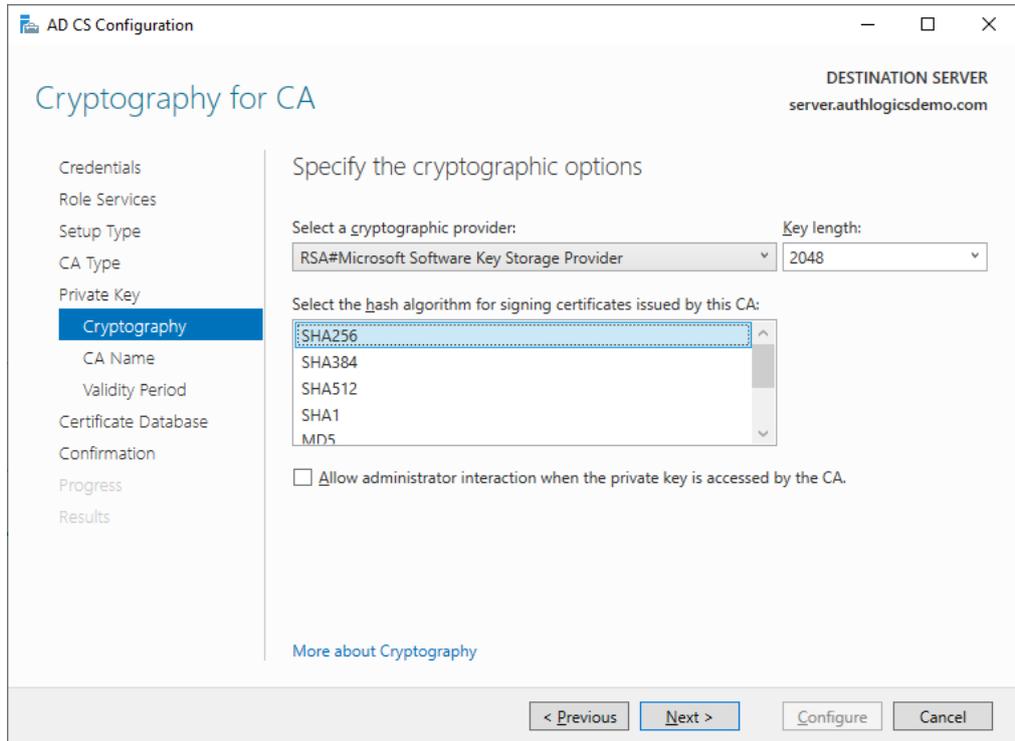
4. Select **Root CA** and click **Next**.



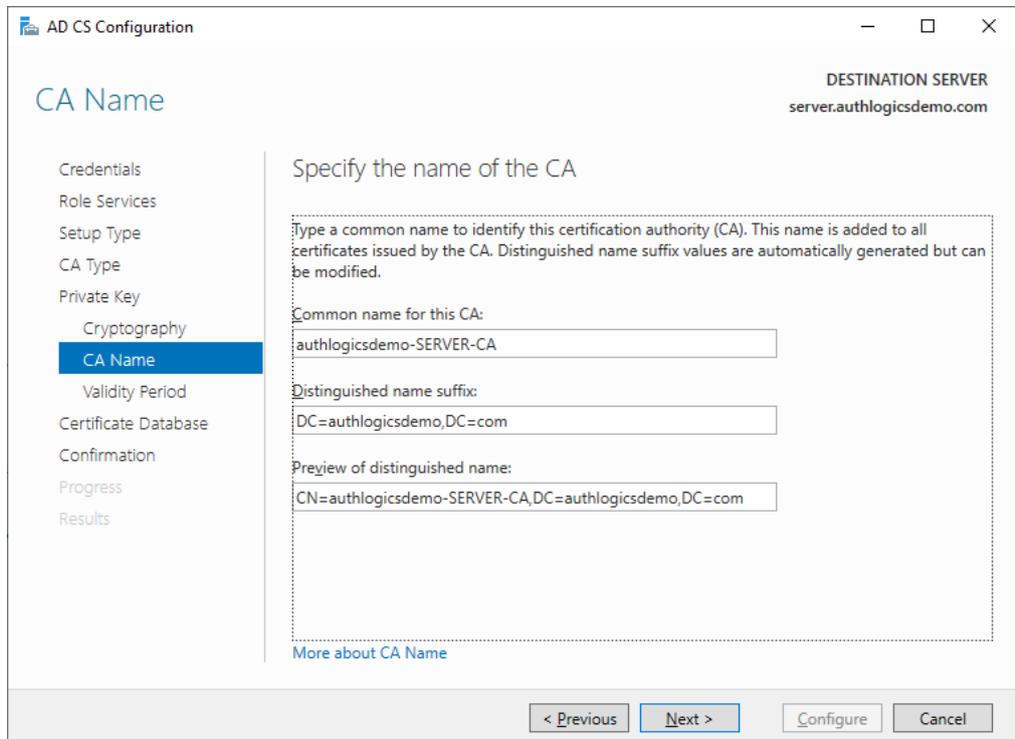
5. Create a new private key and click **Next**.



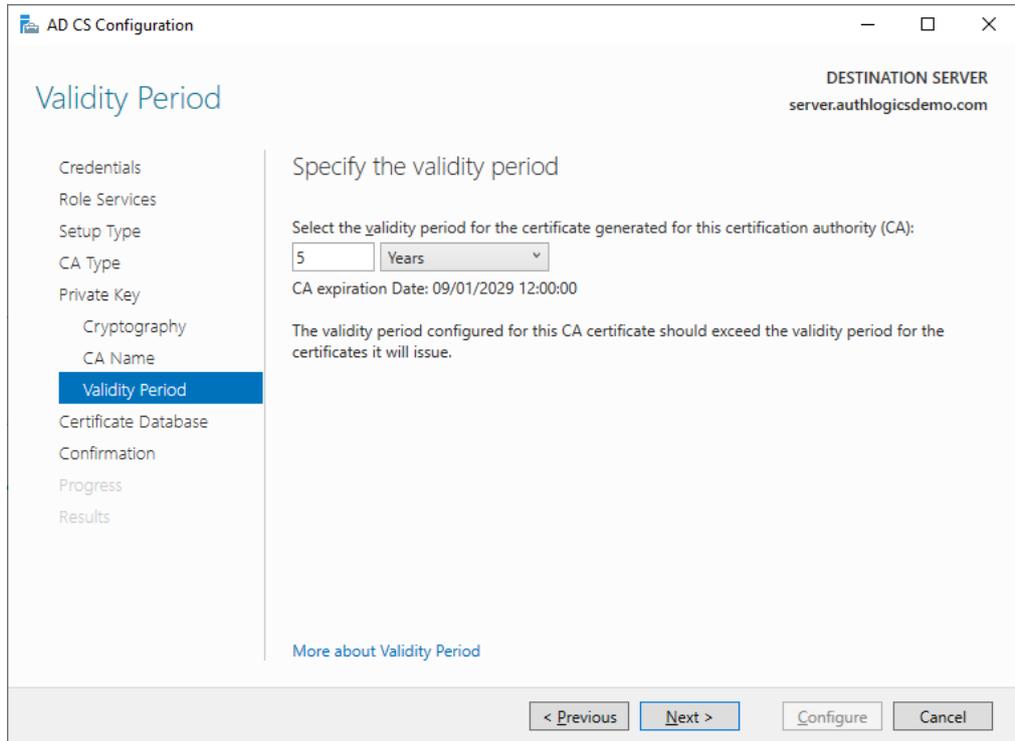
6. Click **Next**.



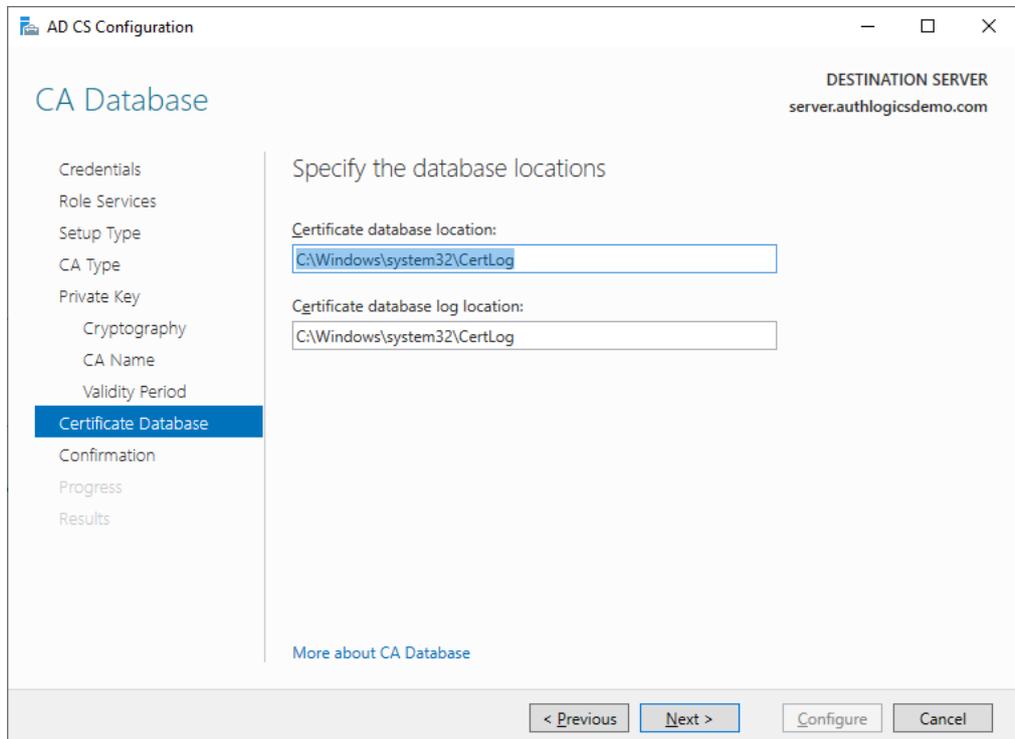
7. Click **Next**.



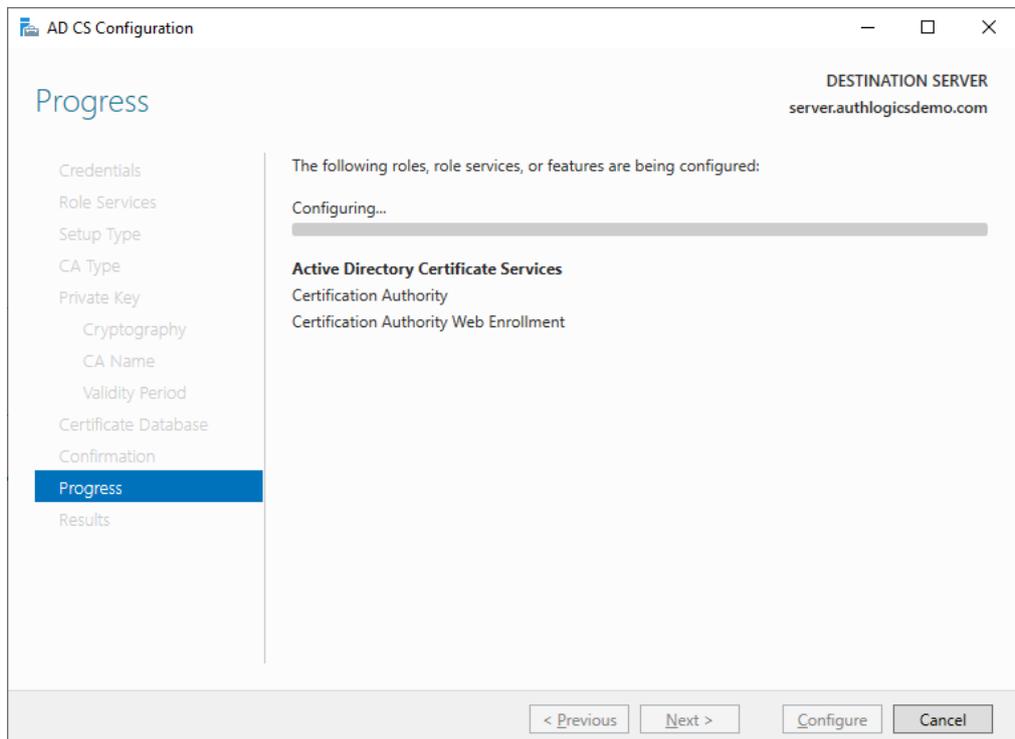
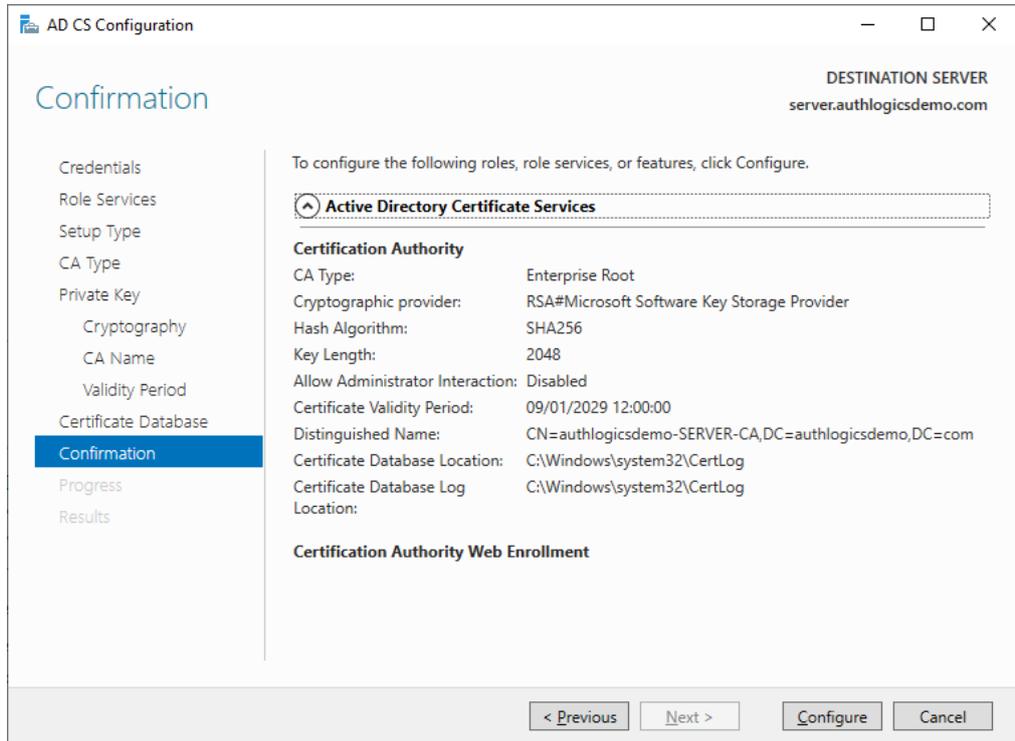
8. Click **Next**.



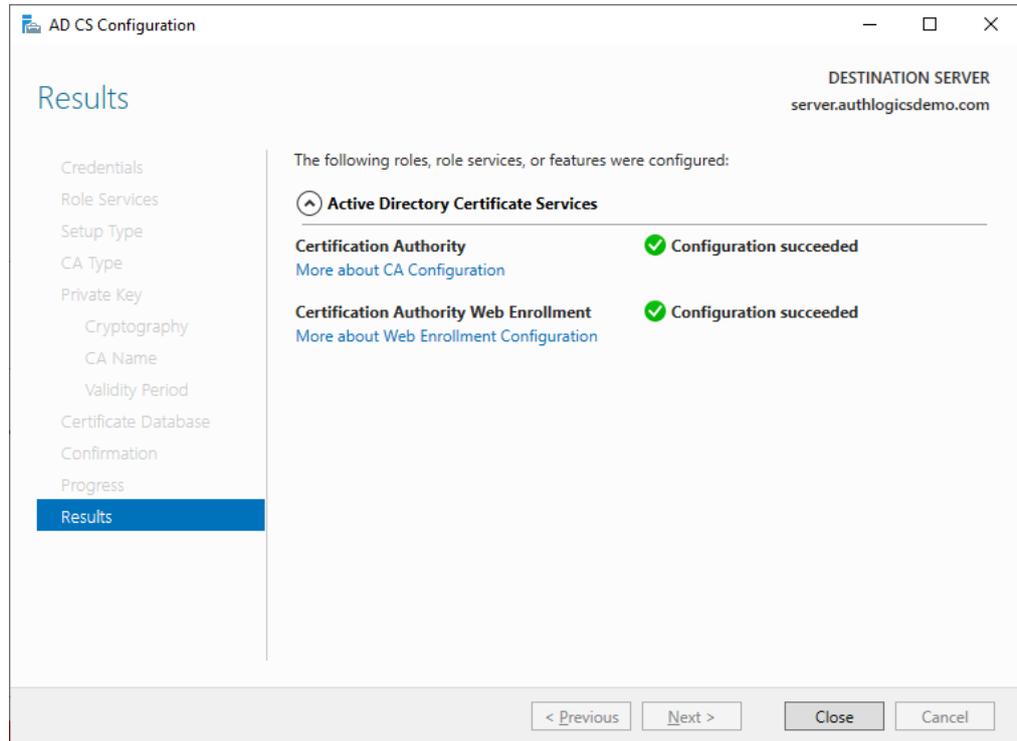
9. Click **Next**.



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.

