intercede

Multi-Factor Authentication

MyID MFA Quick Start Guide

Product Version: 5.0.6942.0

Call us on: +44 (0)1455 558 111 (UK & EMEA)
+1 408 706 2866 (US)

Email us: info@intercede.com

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 setup MyID Multi-Factor Authentication in a new environment. For detailed information about a specific feature or deployment scenario please see the MyID *Authentication Server Installation and Configuration Guide*.

Considerations

(1) MyID Multi-Factor Authentication requires a Windows Server and an Active Directory domain to be available prior to installation.
(2) A Domain Administrator / Enterprise Administrator account is required to perform the installation.
(3) Add AD accounts of MyID administrators to the Authlogics Administrators AD security group.
(4) After the installation the server will require a reboot.
(5) Internet access to https://*.authlogics.com is required.

Required information

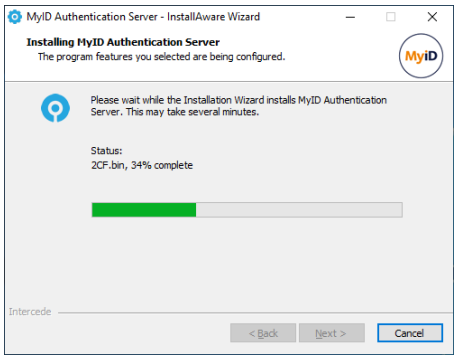
(1) AD administrator credentials.
(2) SMTP Server details: name, port, authentication requirements.
(3) The DNS name for the server.
(4) Understanding of which authentication technology to use.
(5) For FIDO and passkey tokens, MyID requires a trusted certificate to be bound to MyID web sites, self-signed certificates will 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.

Installing the Authentication Server

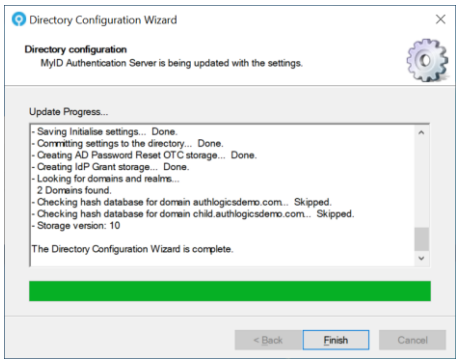
(1) Download the Authentication Server installer from https://www.intercede.com/support/downloads and extract the ZIP.

(2) Run the setup file in the *Install* folder.

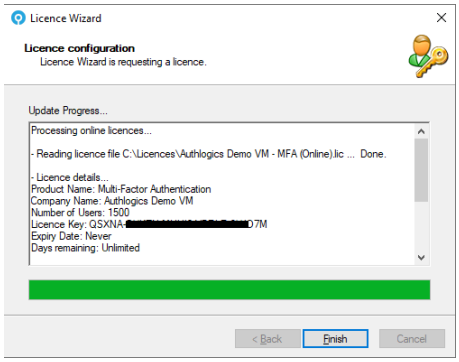
(3) Follow the Installation Wizard instructions to install the product binaries.



(4) Follow the Directory Configuration Wizard to setup the AD for use with MyID.



(5) Follow the Licence Wizard to configure a licence for MyID MFA. If you do not have a licence key the wizard can request a 30 day evaluation licence for you.



(6) **Reboot the Server** after the MyID Management Console loads to complete the initial setup.

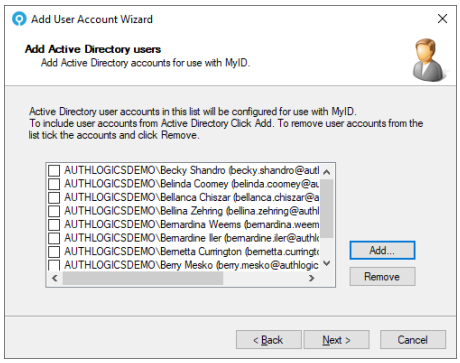
Configuring the Authentication Server

(1) Launch the MyID Management Console, right click “Authlogics MFA” and select properties.
(2) Configure the SMTP Server settings to be able to deliver alerts and new user emails.

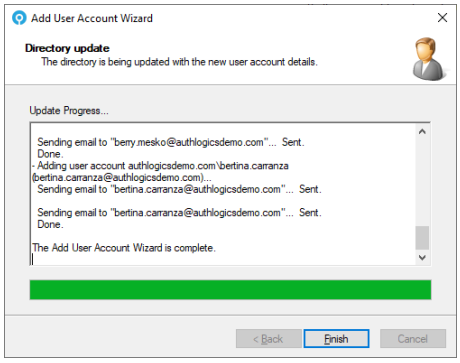
Adding MFA Users

(1) Expand domains and open the domain to add MFA users to.
(2) Click “Add Authlogics User Account” from the actions on the right to start the wizard.

(1) Select all the AD user which must be configured for MyID.

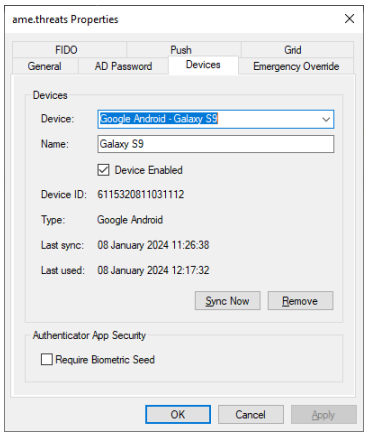


(3) Complete the Wizard.
(4) Select all the users to provision an MFA technology, e.g. Grid, One Time Code, YubiKey, then click “{*Technology*} Management” to start the wizard.
(5) Configure the technology settings for the selected users:



(6) Complete the Wizard.

(2) Double click a user account to view account properties.



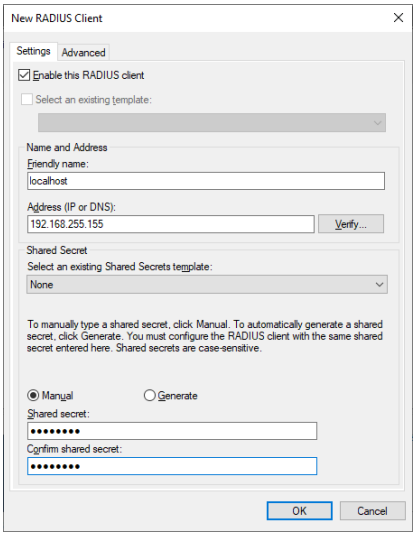
(7) Test the user login using the Self Service Portal via https://{server.authlogicsdemo.com}:14443/

Setting up RADIUS

(1) Launch the MyID Management Console, right click “Authlogics MFA” and select properties.

(2) Configure the RADIUS settings on the RADIUS tab as required.

(3) Click the “Open Network Policy Server” and add the local server as a RADIUS client using the local IP address and a shared secret.

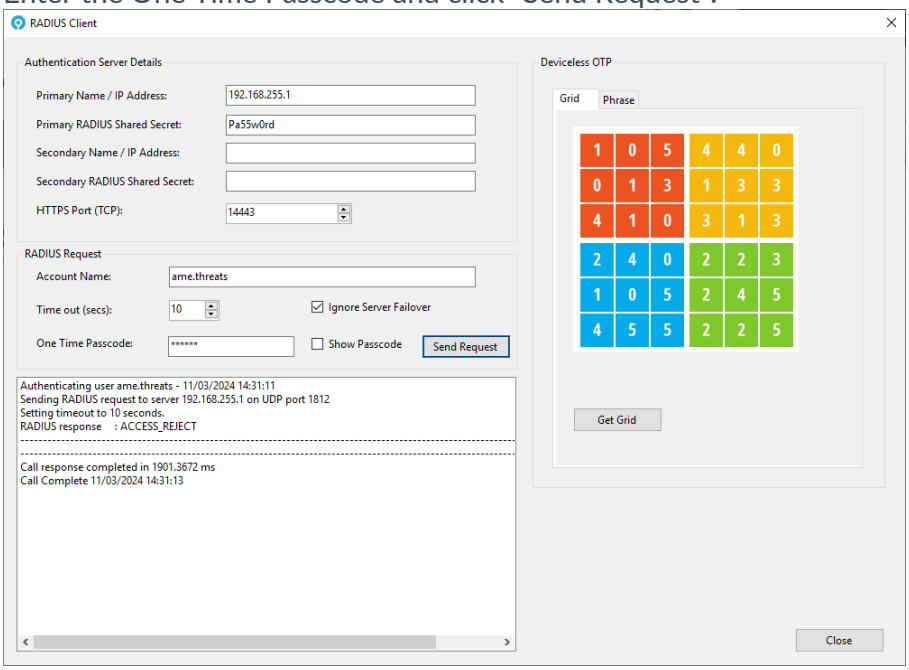


(4) Start the MyID RADIUS test client from: `C:\Program Files\Authlogics Authentication Server\ResKit\RadiusClient\Radius Client UI.exe`

   a. Enter the local server IP address and shared secret from step 3

   b. Enter the test user account name. Click “Grid” to show a grid if Grid is being used.

(3) Enter the One Time Passcode and click “Send Request”.



C. The RADIUS result is shown.

Monitoring MFA Usage

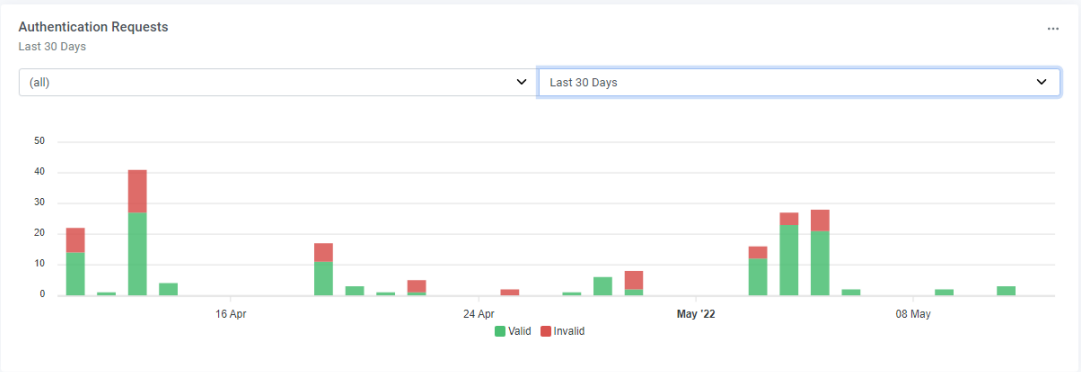
MyID Server includes a Dashboard to graphically display the state of your MFA deployment.

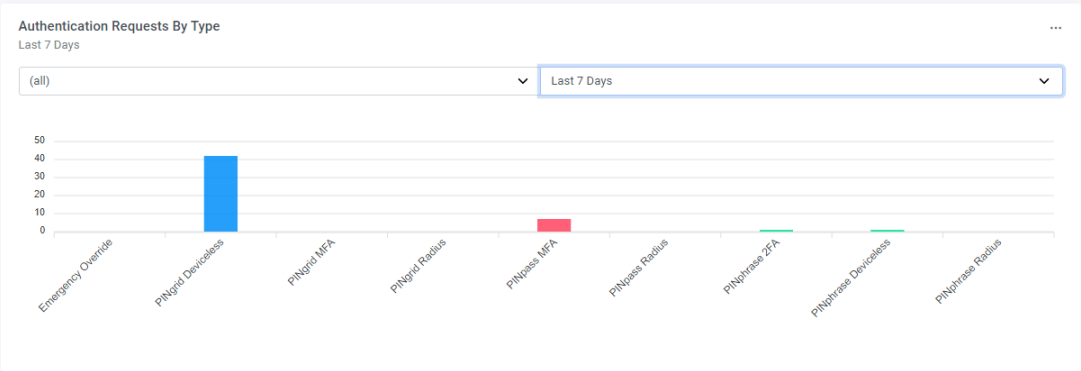
Launch the MyID Admin portal via https://{servername}:14443/admin.

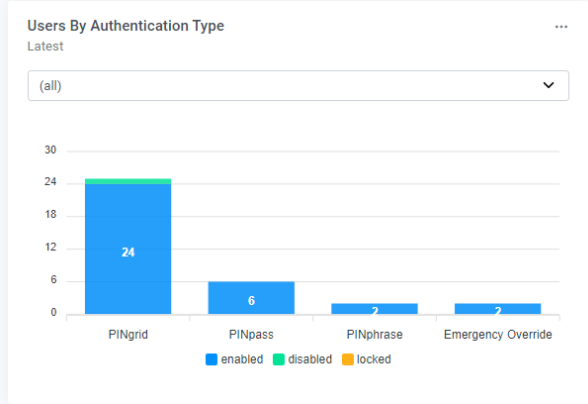
Select System – Dashboards – Multi-Factor Authentication.

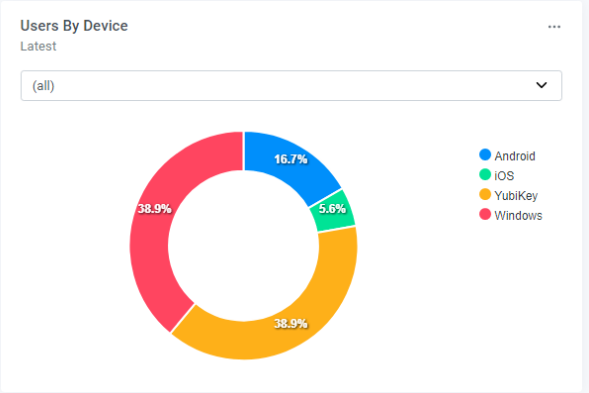
The dashboard reflects MFA actions for:

- Authentication Requests
- Authentication Requests By Type
- Users By Authentication Type
- Users By Device









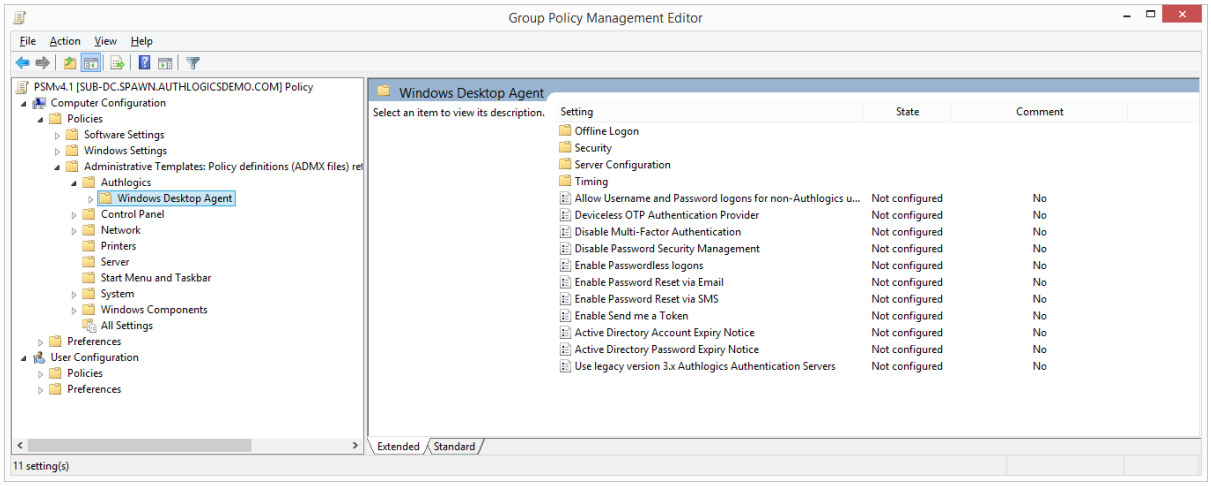
Configuring the Windows Desktop Agent

This section assumes a separate workstation test PC is being used which is domain joined. MyID Windows Desktop Agent can be deployed on non-domain joined PCs however, the Group Policy Objects will need to be applied to these PCs manually.

Configuring the Windows Desktop Agent

Perform these actions on the server:

(1) Download the Windows Desktop Agent installer from https://www.intercede.com/support/downloads and extract the ZIP.
(2) Import the GPO\AuthlogicsWDA.admx file into a new Group Policy object
(3) Configure the following settings (assuming Grid):
    a. Deviceless OTP Authentication Provider: Enabled, Grid
    b. Disabled Windows Username and Password logons

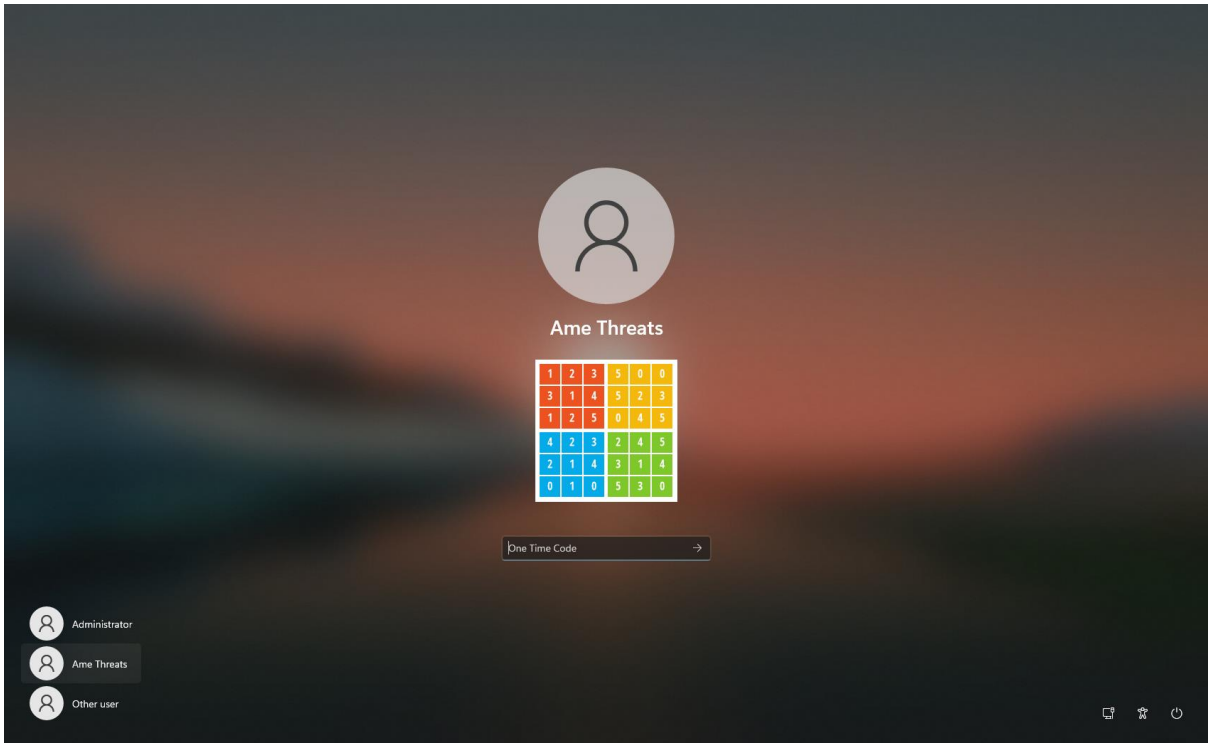


(4) Apply the GPO to an OU containing the workstation computer account.

Perform these actions on the workstation:

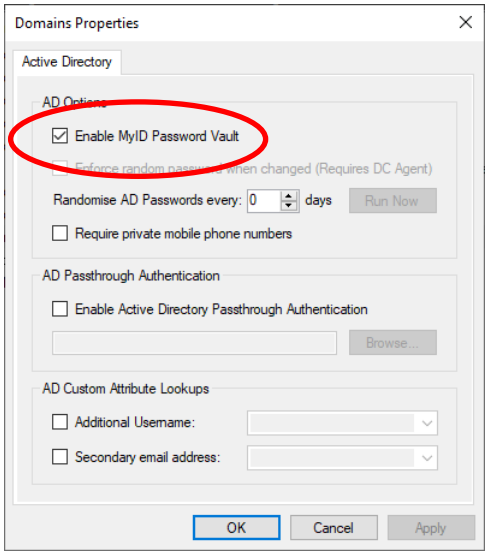
(1) Ensure the GPO settings are applied to the PC by running `GPUPDATE /FORCE`
(2) Install the Agent from the install folder.

(3) Log off and log on with MFA



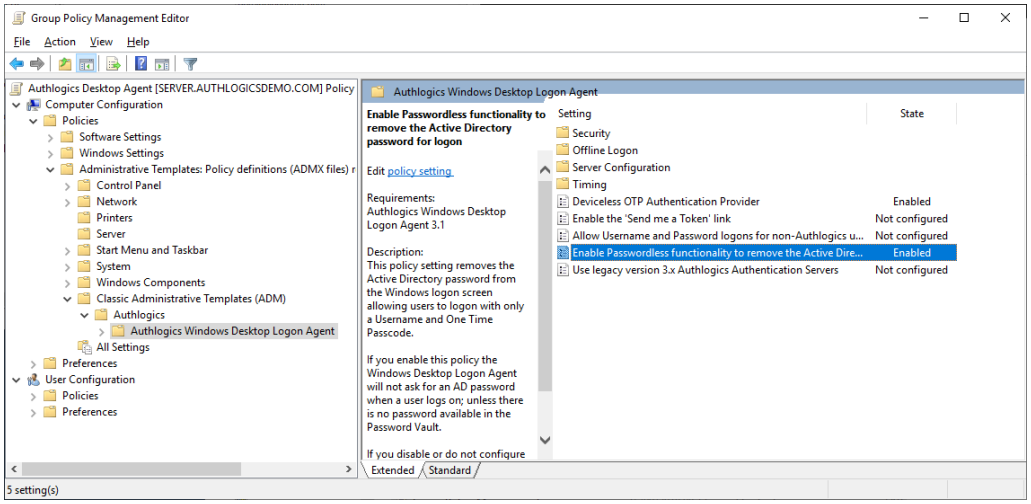
Configuring Passwordless Windows logons

(1) On the Domain – Properties tab, enable the MyID Password Vault:



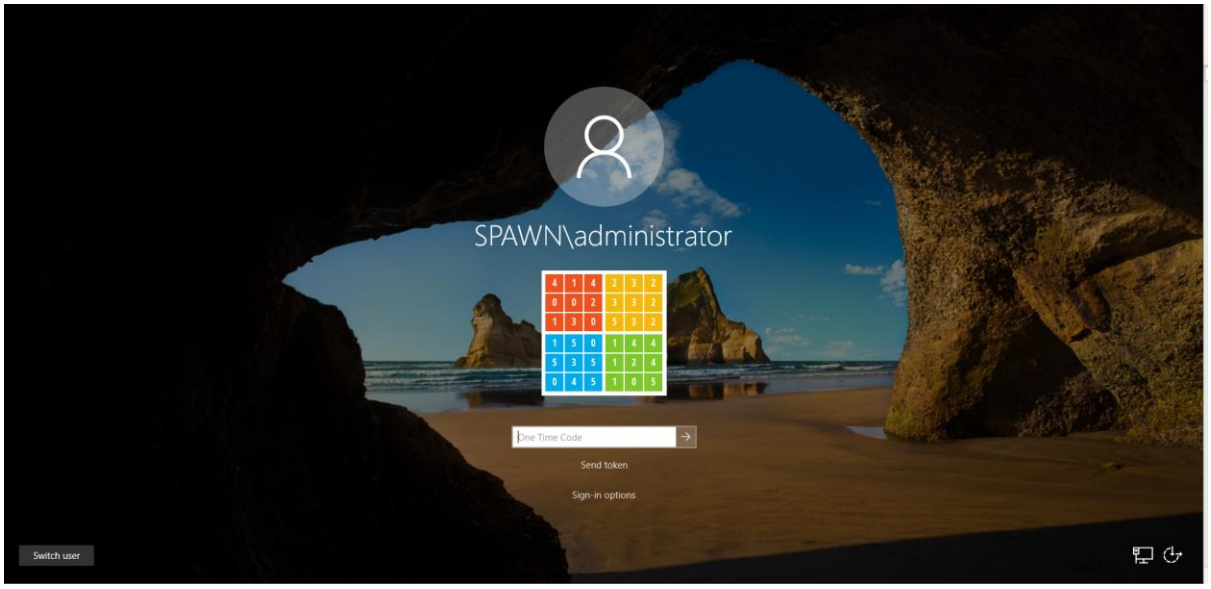
(2) Update the group policy settings:

(4) Enabled Passwordless functionality to remove the Active Directory password for logon: Enabled

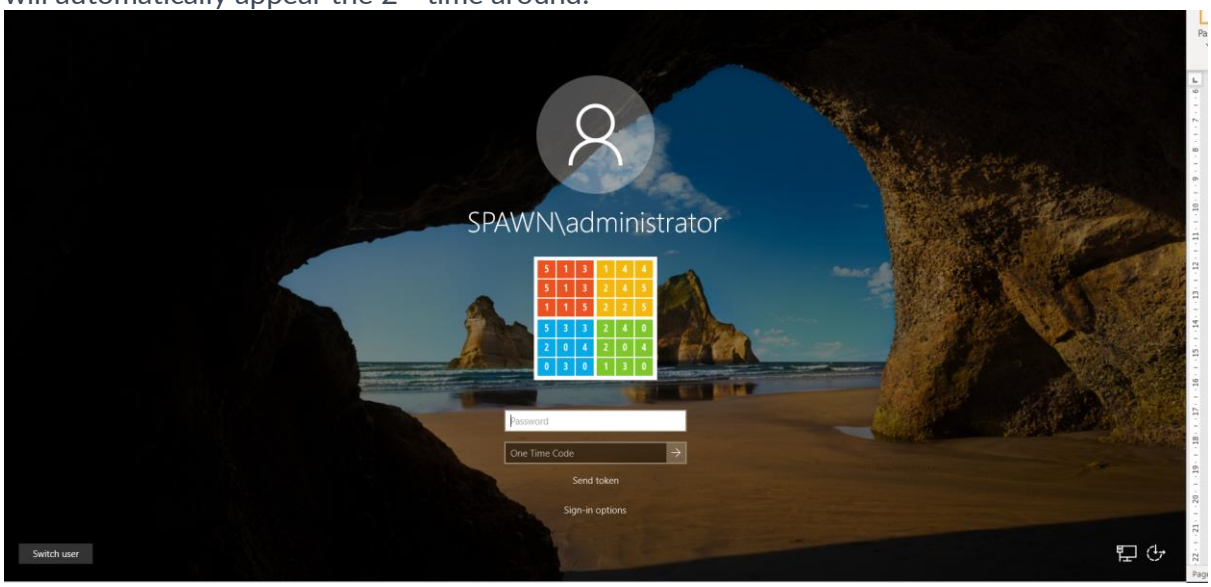


(3) Ensure the GPO settings are applied to the PC by running `GPUPDATE /FORCE`

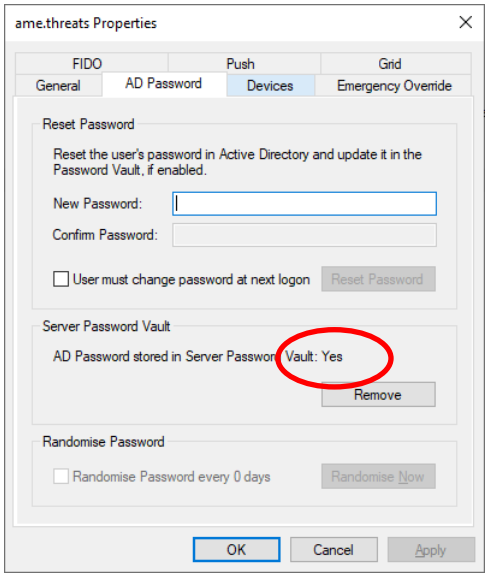
(5) Reboot the workstation and logon as the test user – note that there is no password option available:



(6) On first attempt the login will fail if there is no password in the vault. The password option will automatically appear the 2nd time around.



(7) After the login the password will be saved to the vault and can be seen on the user account on the server:



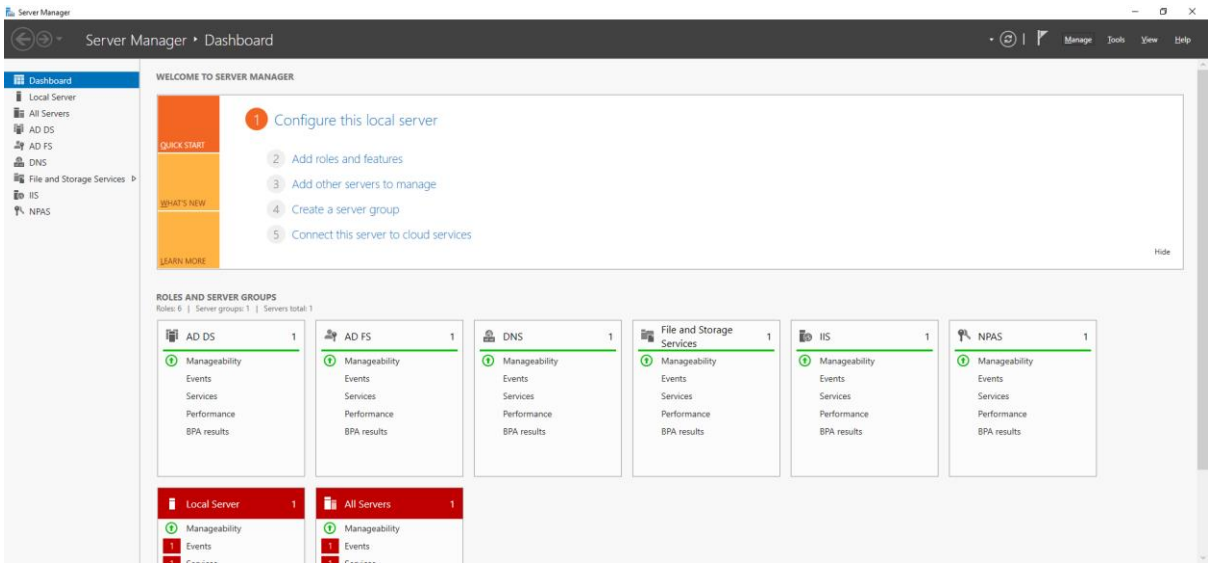
Configuring a Certificate Authority

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

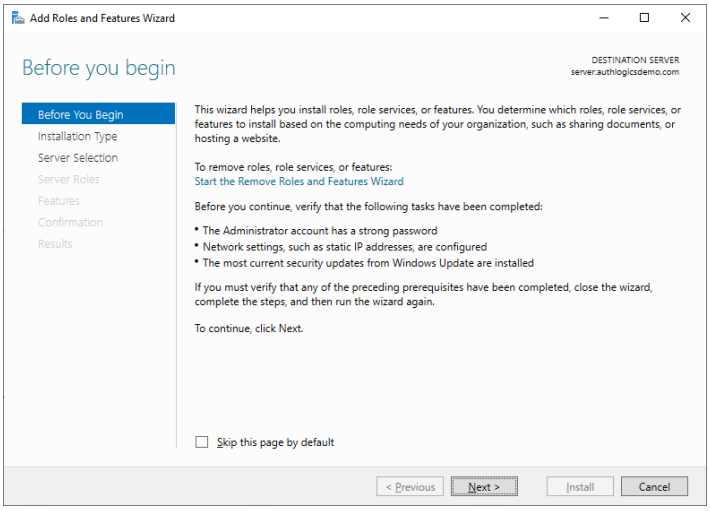
Installing the Certificate Authority

Perform these actions on the server:

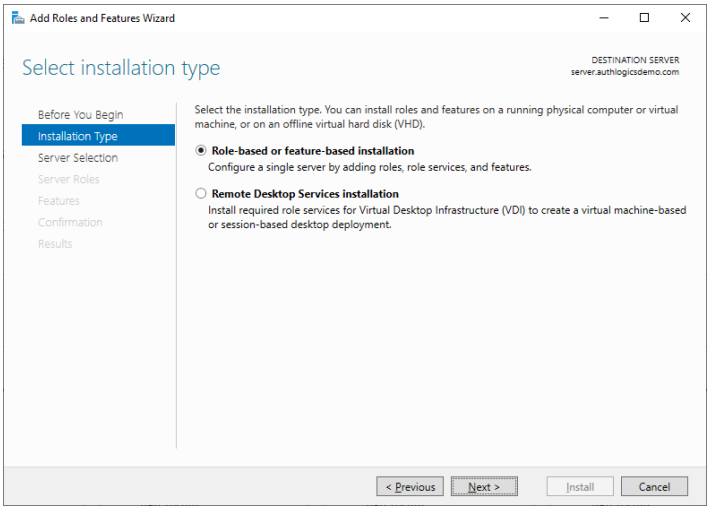
(8) Open Server Manager



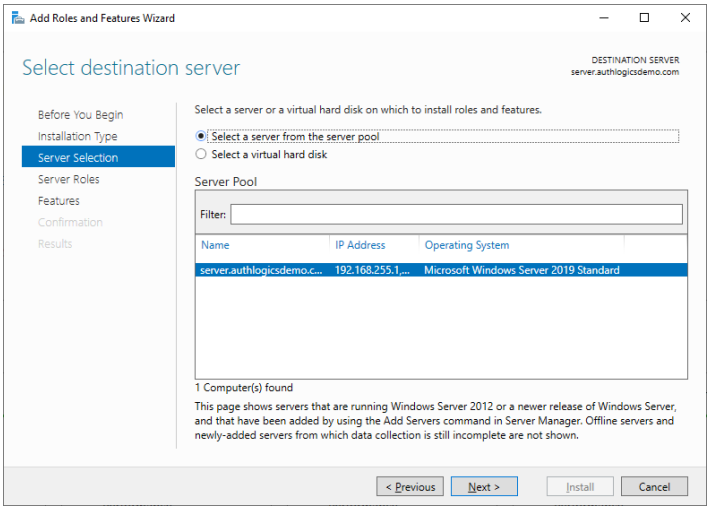
(9) Select Manage



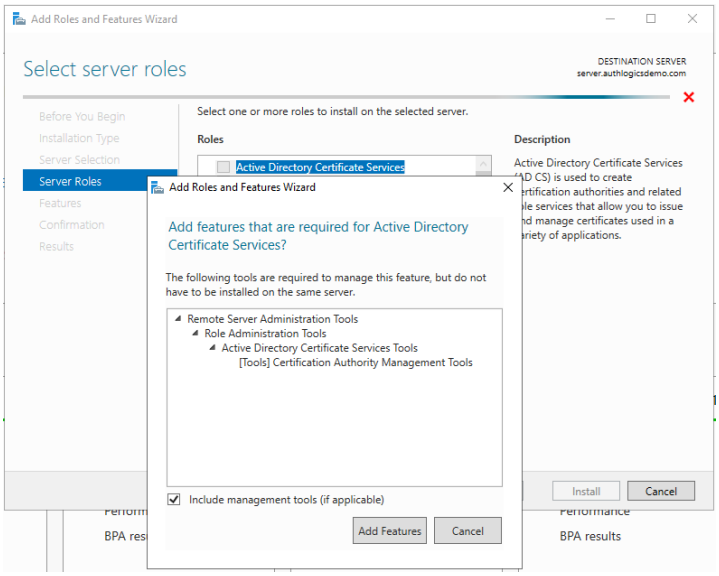
(10) Select Role-based or feature-based installation

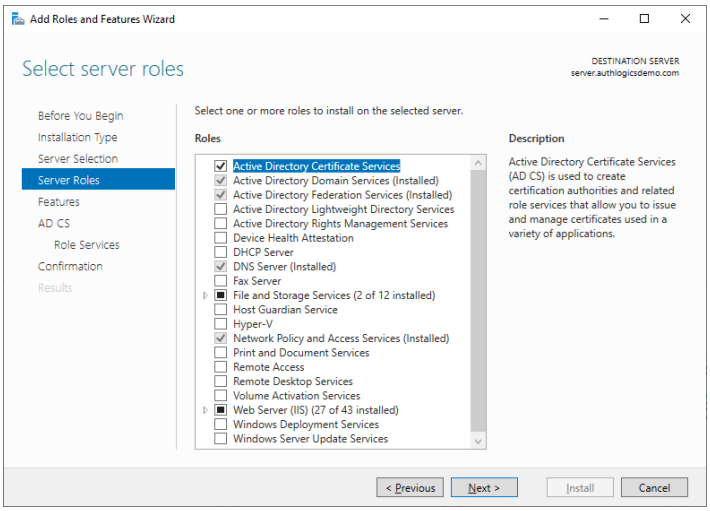


(11) Select the local server as the server pool

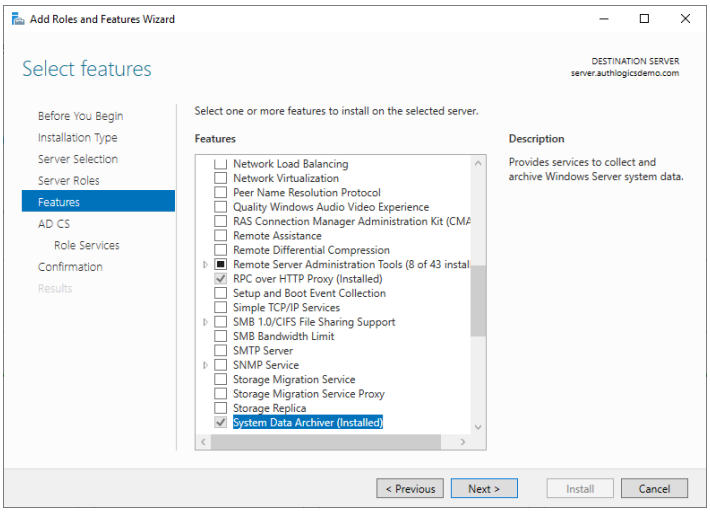


(12) Enable Active Directory Certificate Services and Add Features required for AD Certificate Services

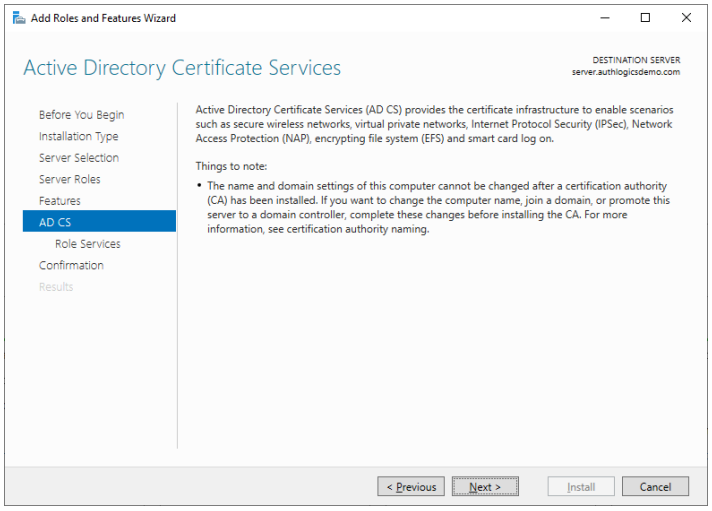




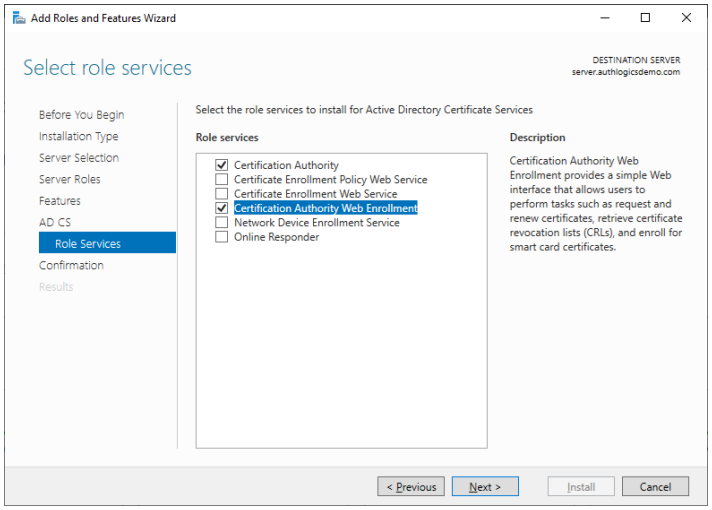
(13) Select Next



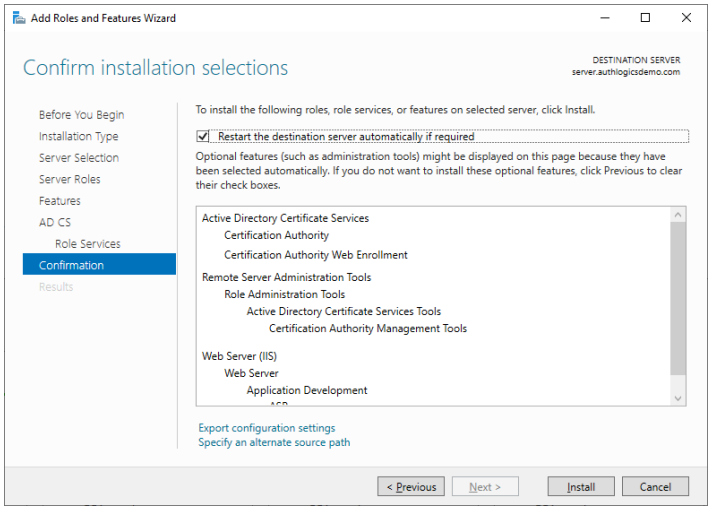
(14) Select Next

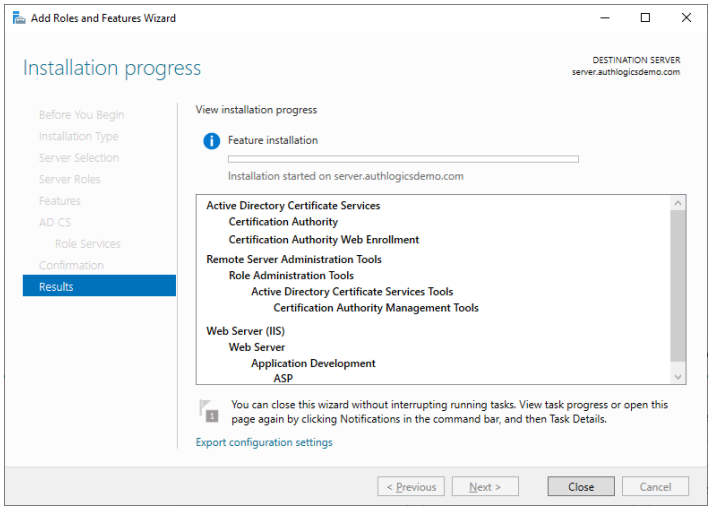


(15) Select Next and enable Certifcate Authority and Certificate Authority Web Enrollment



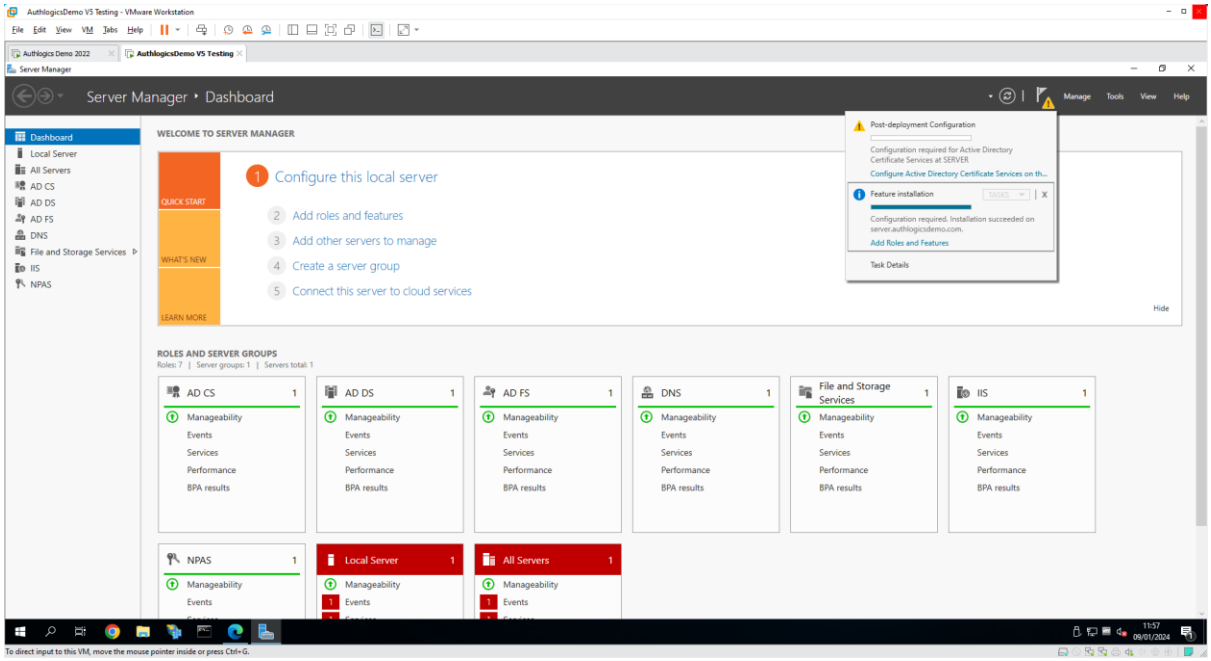
(16) Enable Restart the destination server automatically if required and select Install



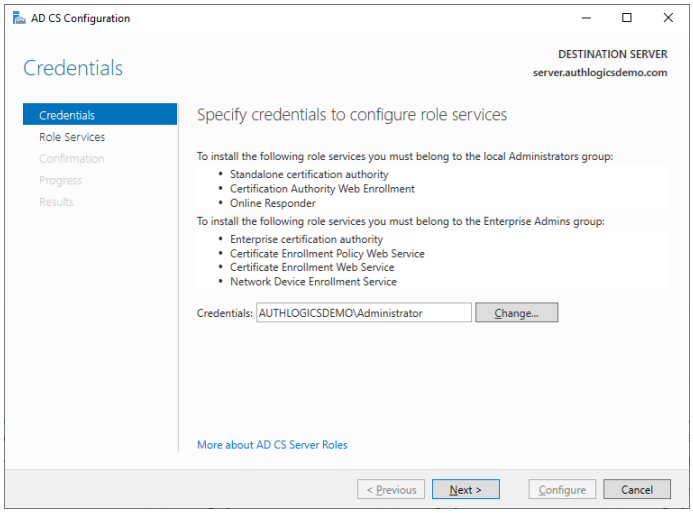


(17) Click Close when complete

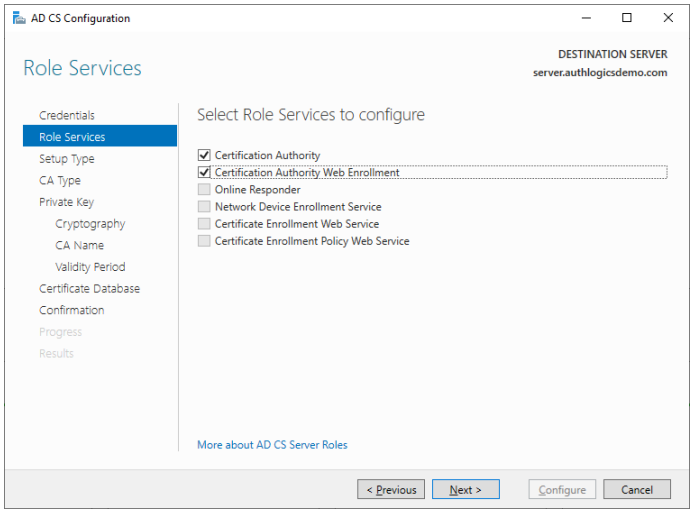
Configure Active Directory Certificate Services



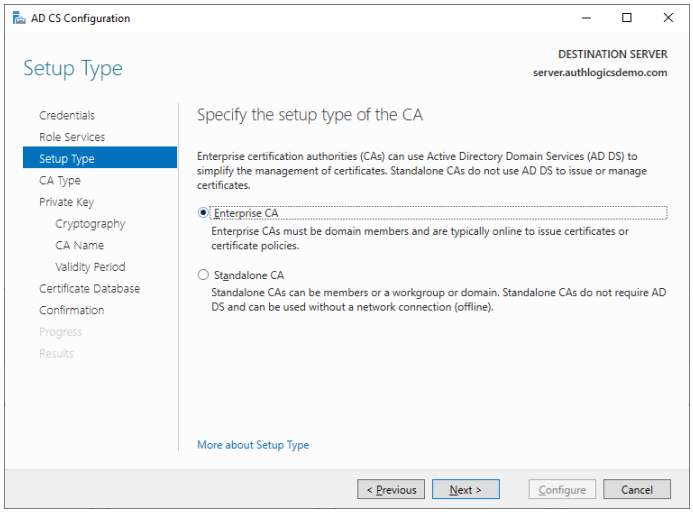
(1) Select your Active Directory administrator credentials and the role to configure role services



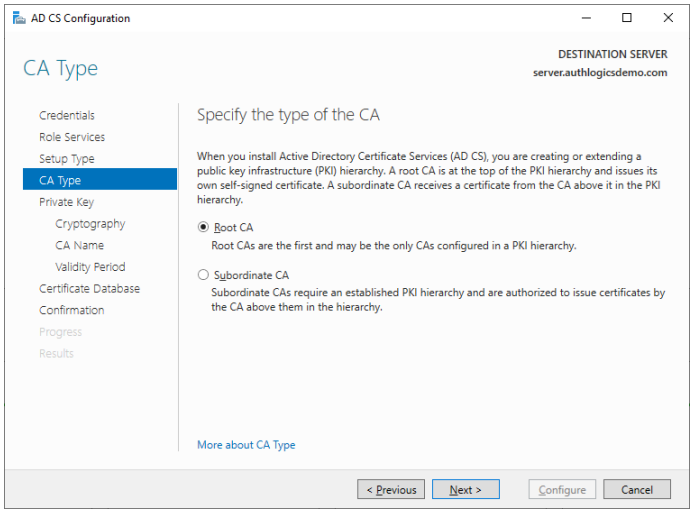
(2) Enable the roles Certification Authority and Certification Authority Web Enrollment options



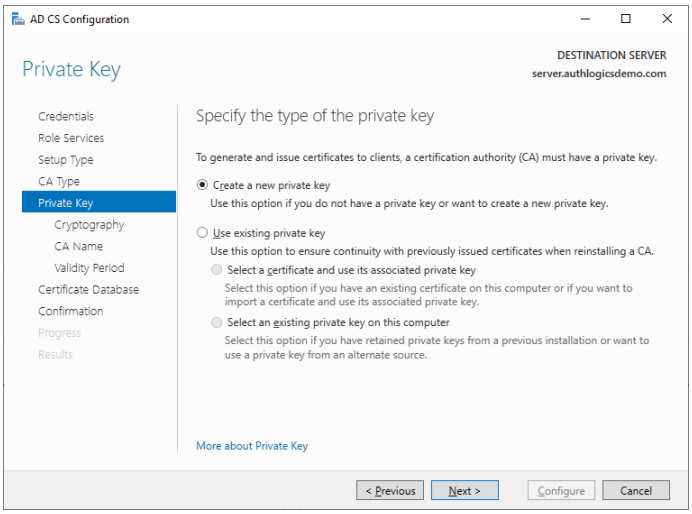
(3) Select Enterprise CA and select Next



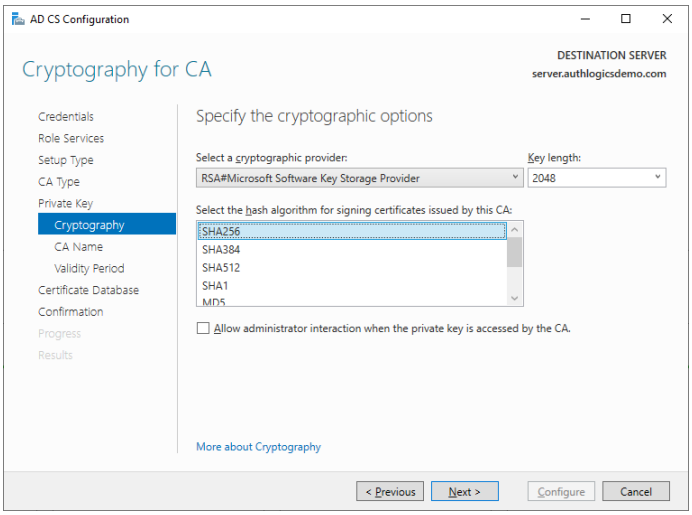
(4) Select Root CA and Select Next



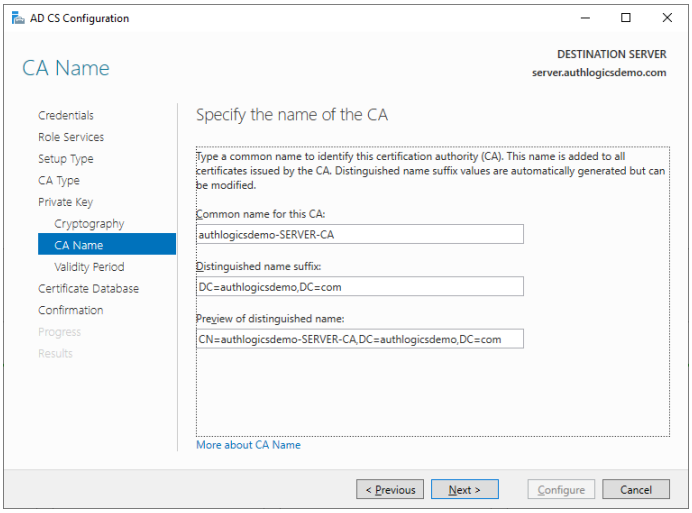
(5) Create a new private key and Select Next



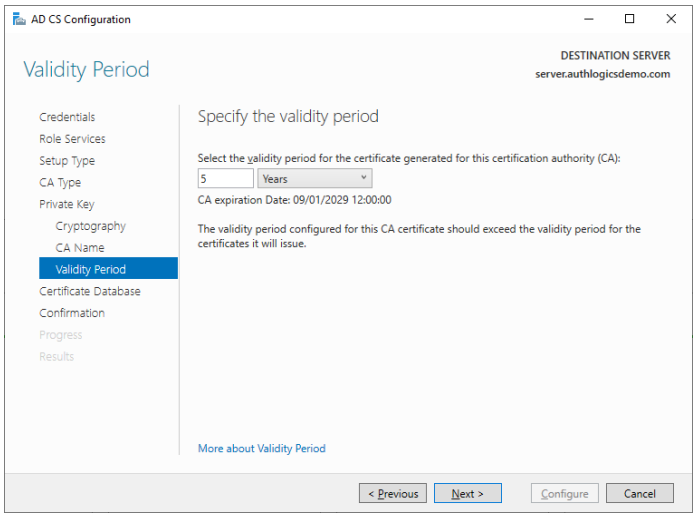
(6) Select Next



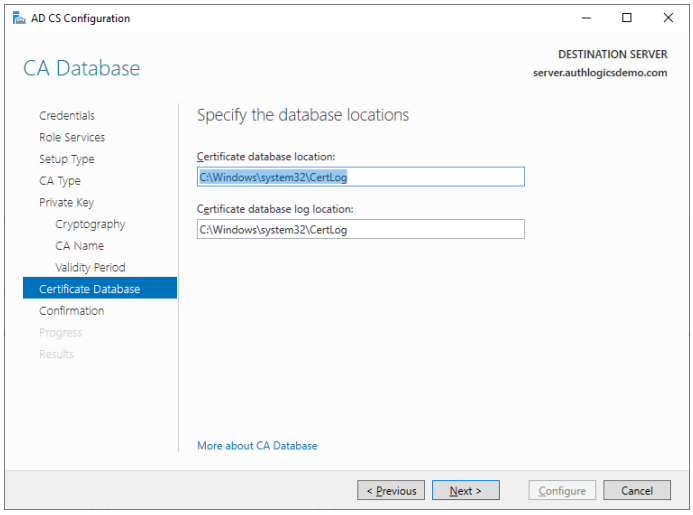
(7) Select Next



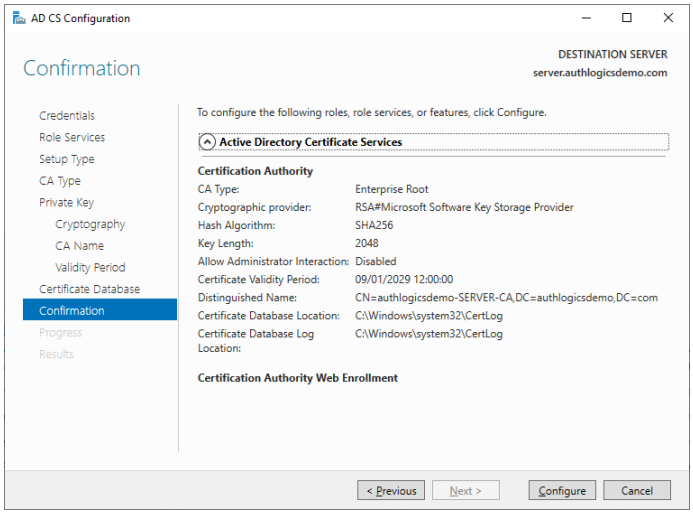
(8) Select Next

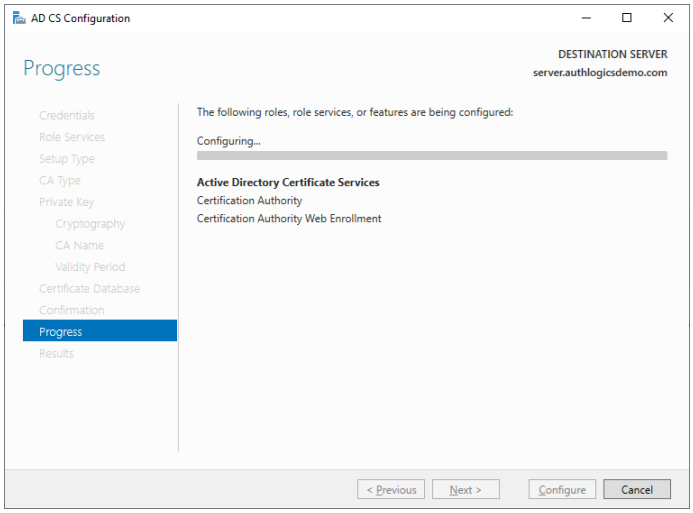


(9) Select Next

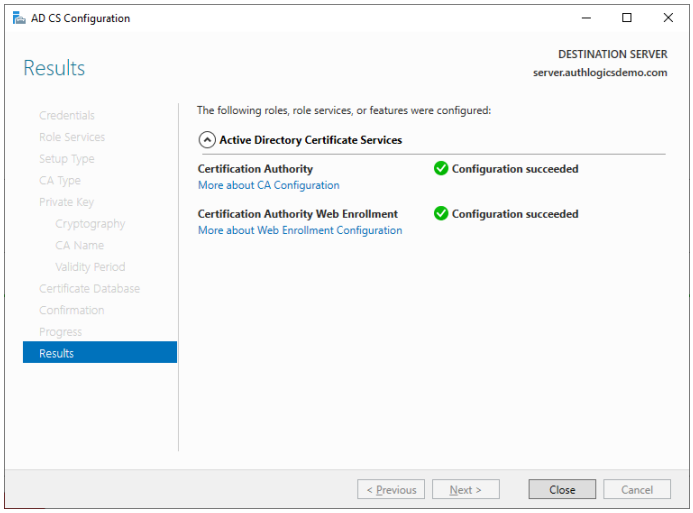


(10) Select Configure





(11) Select Close



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

Requesting a Trusted Certificate

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

There are 2 methods to request a privately trusted certificate. The first being through the MyID provided PowerShell script or secondly, by using IIS.

Create a Certificate Request using MyID PowerShell script

Within the MyID Authentication Server installation folder, ResKit\Scripts folder, using administrator credentials run the *RequestTrustedCert.ps1* through PowerShell ISE.

The RequestTrustedCert PowerShell script requires 6 inputs:

- ServerName
  This is the FQDN for the MyID Authentication Server or public name for Authentication Server web site.
- CompanyName
- Department
- City
- State
- Country

```
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 executed, a Web Server certificate will be created and applied 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 public accessible web site name.