

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

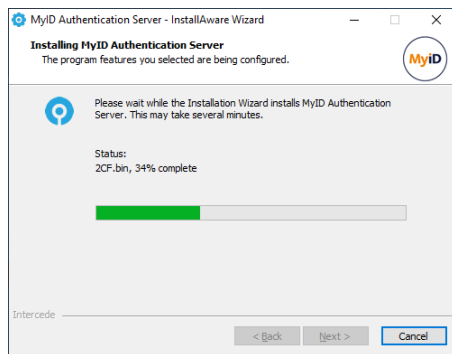
- (1) MyID Multi-Factor Authentication requires a Windows Server and an Active Directory domain to be available prior to installation.
- (2) A Domain Administrator / Enterprise Administrator account is required to perform the installation.
- (3) Add AD accounts of MyID administrators to the Authlogics 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

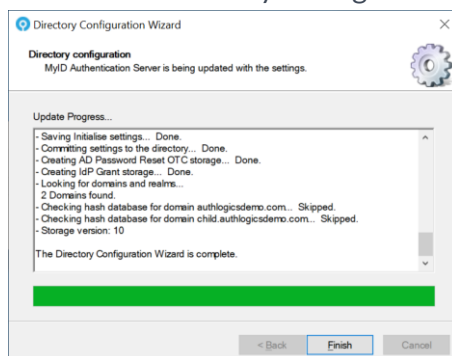
- (1) AD administrator credentials.
- (2) SMTP Server details: name, port, authentication requirements.
- (3) The DNS name for the server.
- (4) Understanding of which authentication technology to use.
- (5) For FIDO and passkey tokens, MyID requires a trusted certificate to be bound to MyID web sites,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

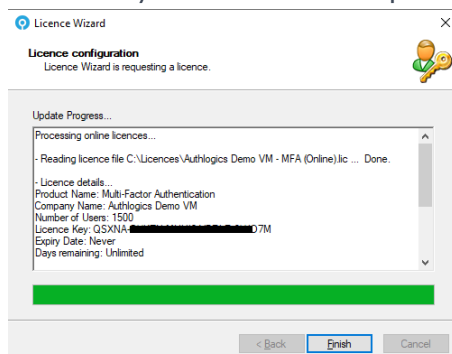
- (1) Download the Authentication Server installer from <https://www.intercede.com/support/downloads> and extract the ZIP.
- (2) Run the setup file in the *Install* folder.
- (3) Follow the Installation Wizard instructions to install the product binaries.



- (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.

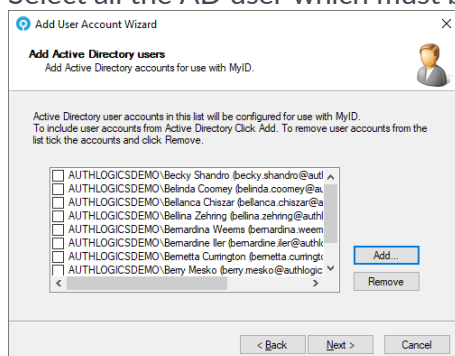
Configuring the Authentication Server

- (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.

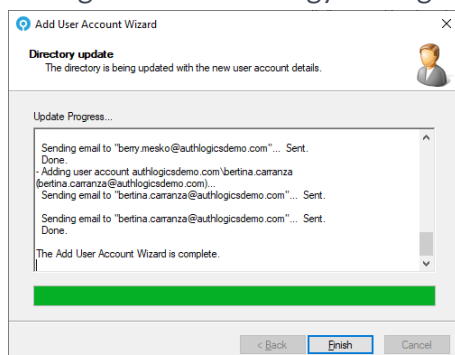
Adding MFA Users

- (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.

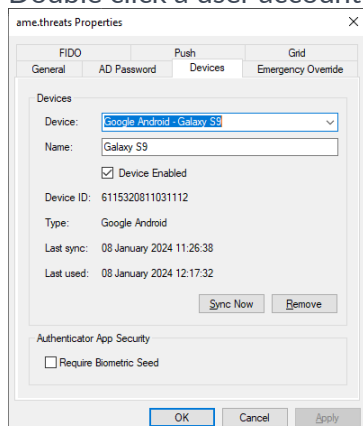


- (3) Complete the Wizard.
- (4) Select all the users to provision an MFA technology, e.g. Grid, One Time Code, YubiKey, then click “{ *Technology* } Management” to start the wizard.
- (5) Configure the technology settings for the selected users:



- (6) Complete the Wizard.

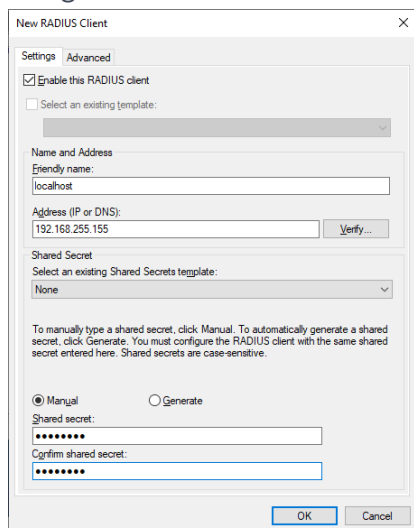
- (2) Double click a user account to view account properties.



- (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.



New RADIUS Client

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name: localhost

Address (IP or DNS): 192.168.255.155

Shared Secret

Select an existing Shared Secrets template: None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

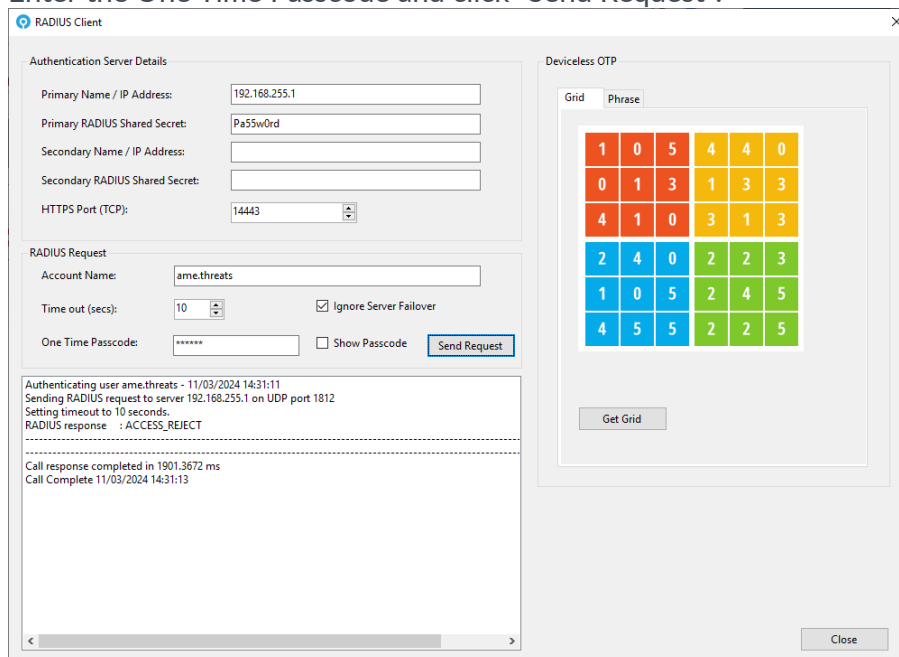
☒ Manual ☐ Generate

Shared secret: *****

Confirm 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”.



RADIUS Client

Authentication Server Details

Primary Name / IP Address: 192.168.255.1

Primary RADIUS Shared Secret: Pa55w0rd

Secondary Name / IP Address:

Secondary RADIUS Shared Secret:

HTTPS Port (TCP): 14443

RADIUS Request

Account Name: ame.threats

Time out (secs): 10 ☒ Ignore Server Failover

One Time Passcode: ***** ☐ Show Passcode

Authenticating user ame.threats - 11/03/2024 14:31:11
 Sending RADIUS request to server 192.168.255.1 on UDP port 1812
 Setting timeout to 10 seconds.
 RADIUS response : ACCESS_REJECT

Call response completed in 1901.3672 ms
 Call Complete 11/03/2024 14:31:13

Deviceless OTP

Grid Phrase

1	0	5	4	4	0
0	1	3	1	3	3
4	1	0	3	1	3
2	4	0	2	2	3
1	0	5	2	4	5
4	5	5	2	2	5

C. The RADIUS result is shown.

Monitoring MFA Usage

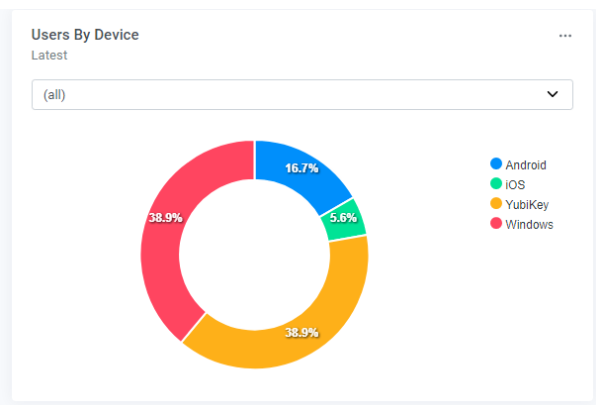
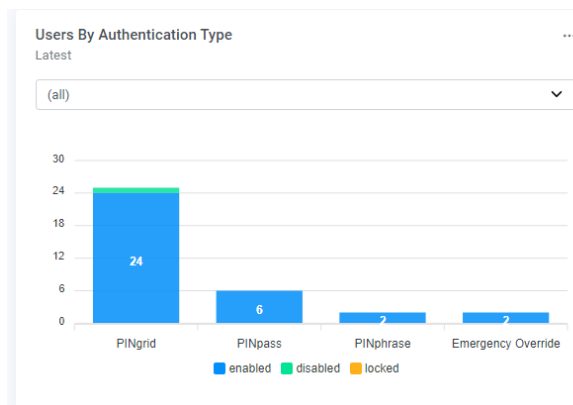
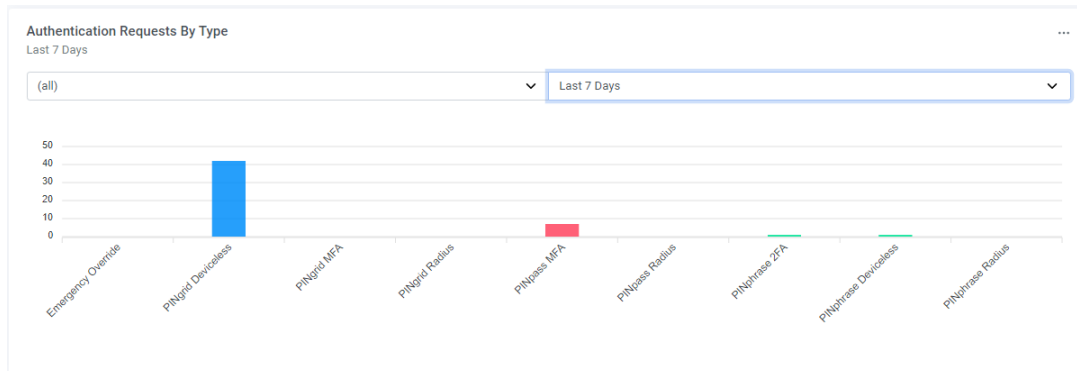
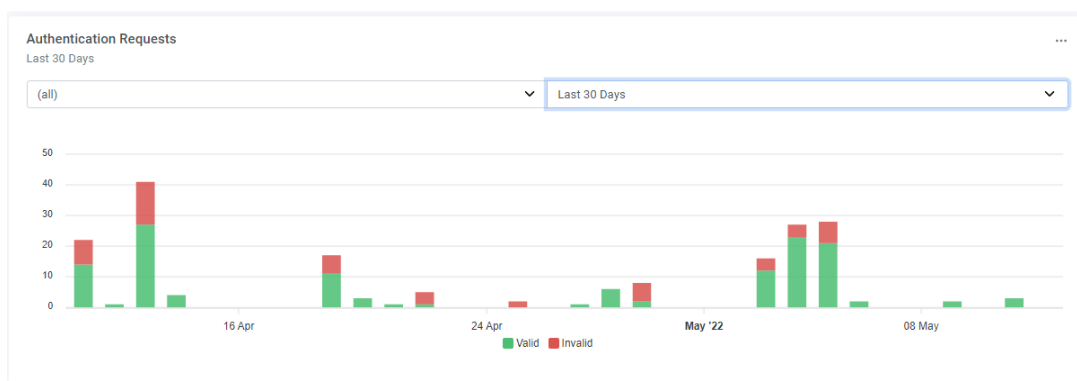
MyID Server includes a Dashboard to graphically display the state of your MFA deployment.

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



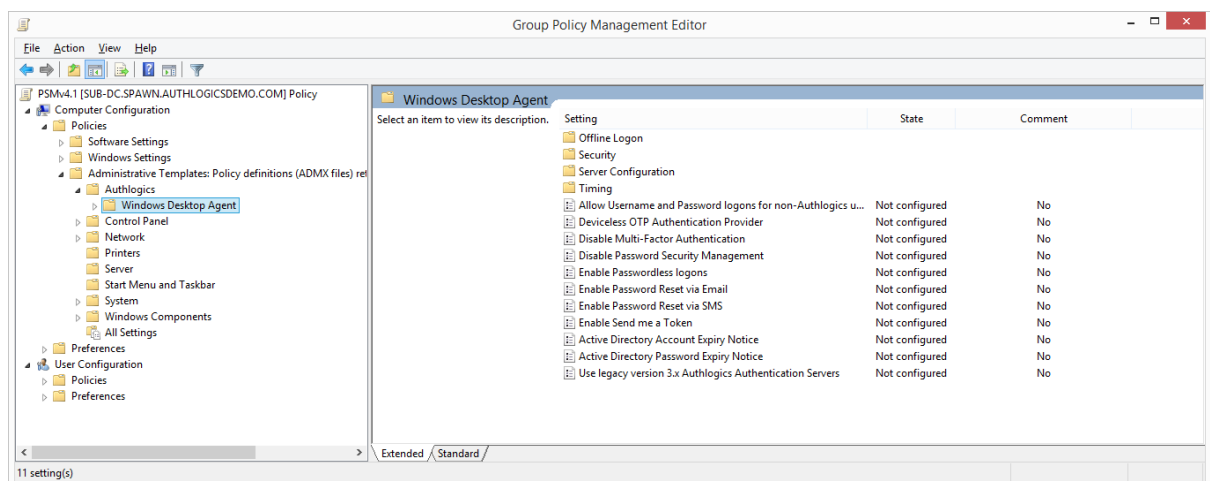
Configuring the Windows Desktop Agent

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

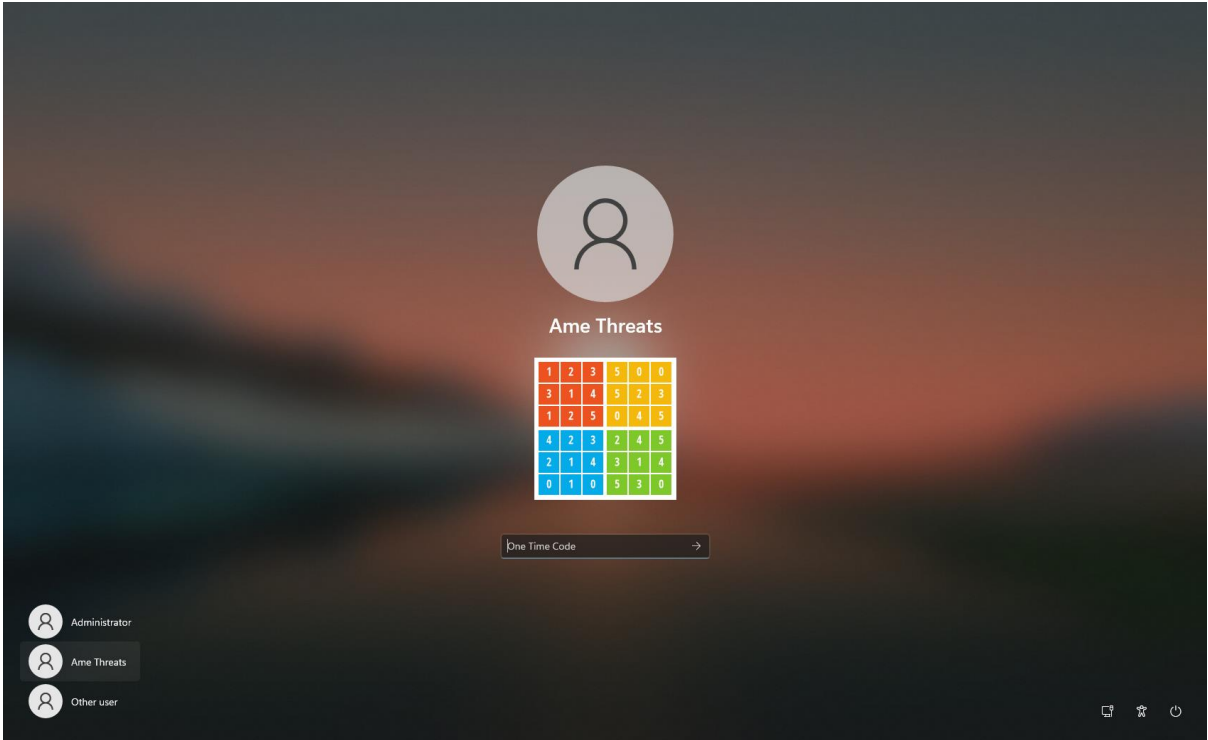


- (4) Apply the GPO to an OU containing the workstation computer account.

Perform these actions on the workstation:

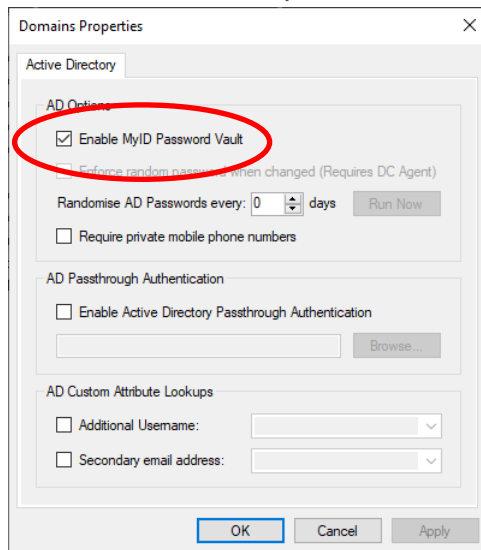
- (1) Ensure the GPO settings are applied to the PC by running `gpupdate /force`
- (2) Install the Agent from the install folder.

(3) Log off and log on with MFA



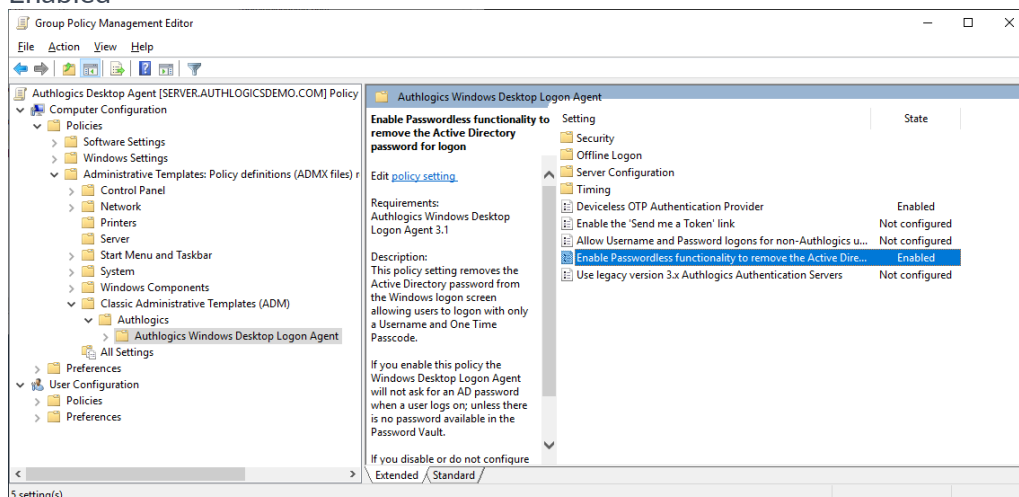
Configuring Passwordless Windows logons

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



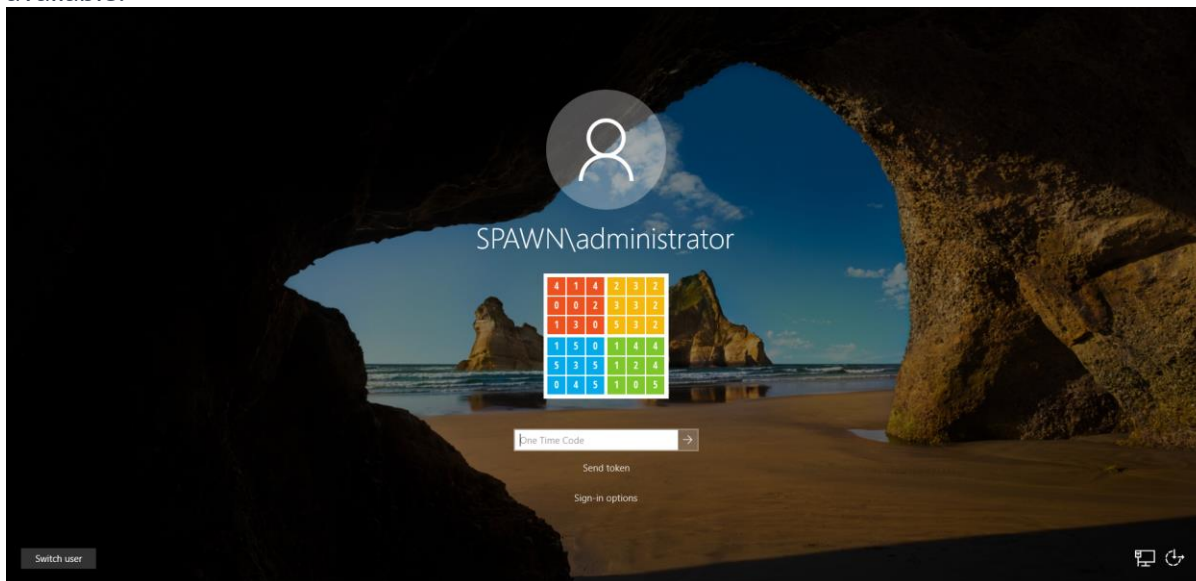
- (2) Update the group policy settings:

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

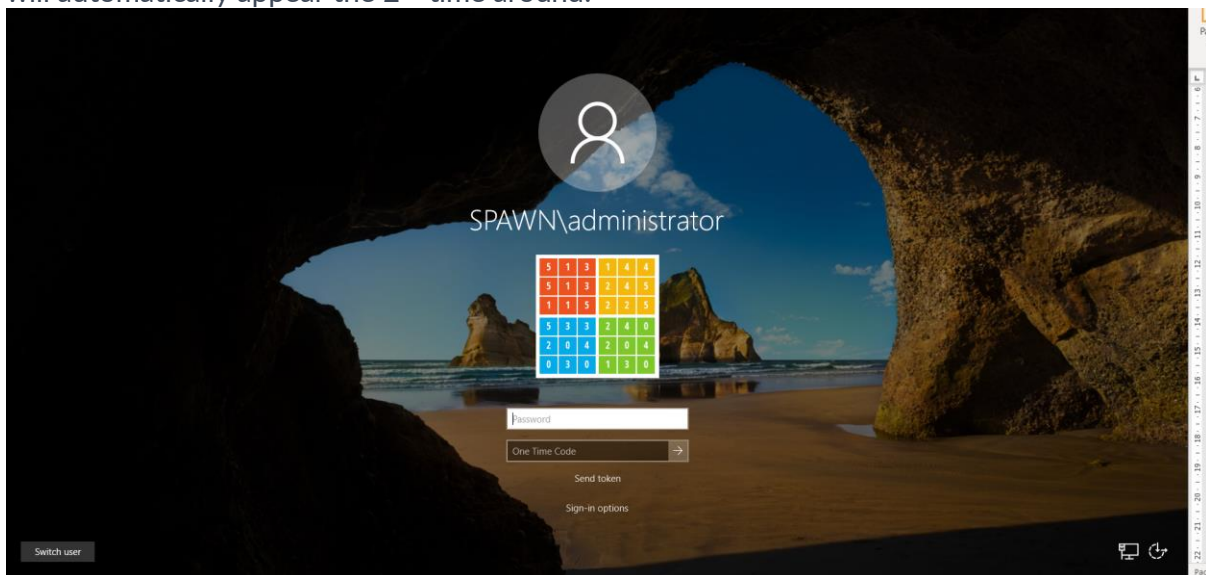


- (3) Ensure the GPO settings are applied to the PC by running `GPUPDATE /FORCE`

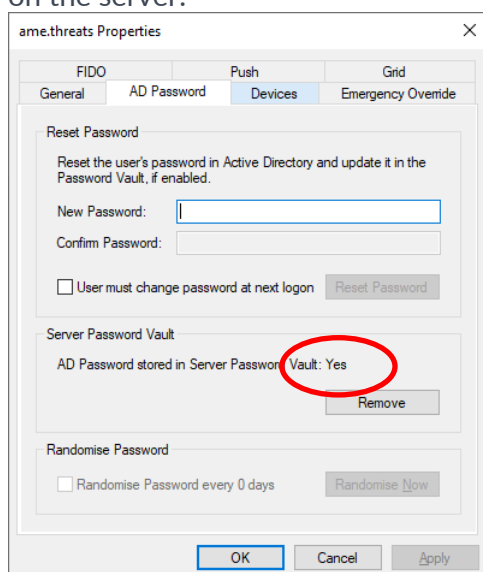
- (5) Reboot the workstation and logon as the test user – note that there is no password option available:



- (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:



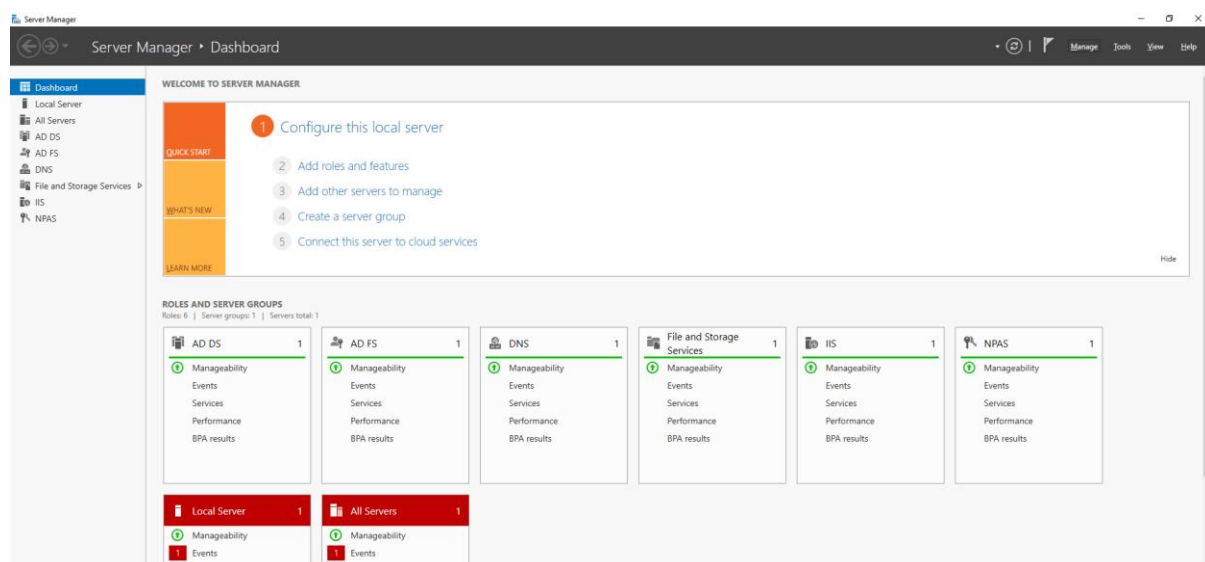
Configuring a Certificate Authority

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.

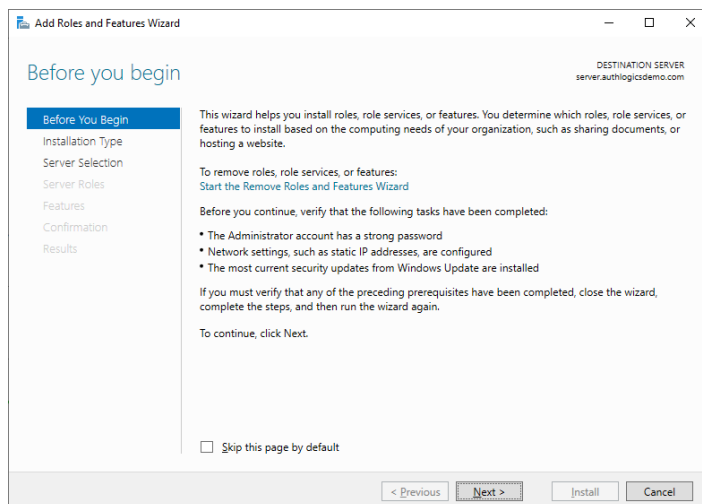
Installing the Certificate Authority

Perform these actions on the server:

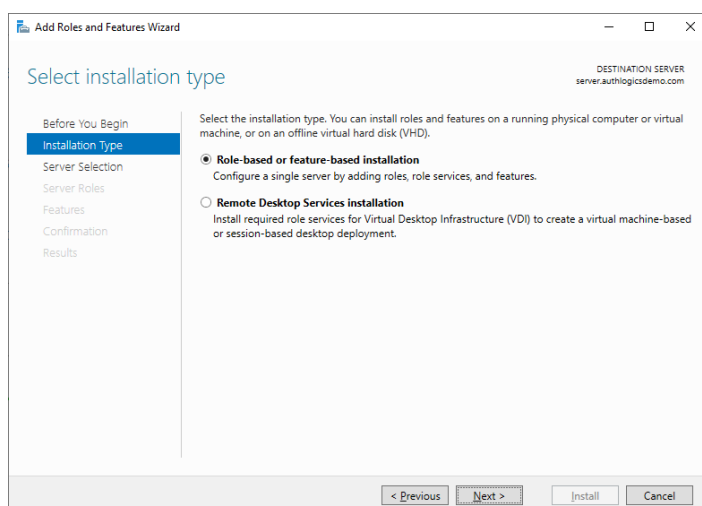
- (8) Open Server Manager



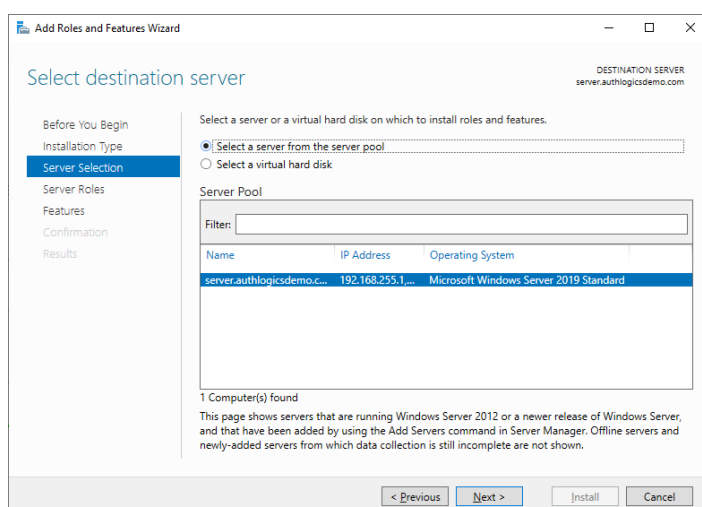
- (9) Select Manage



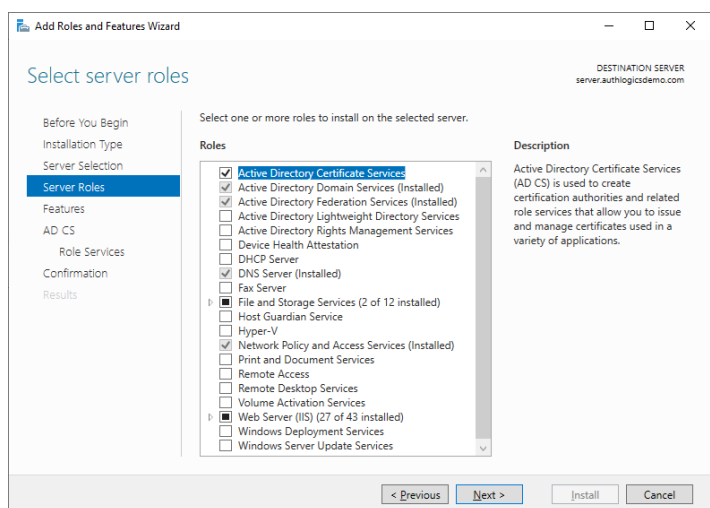
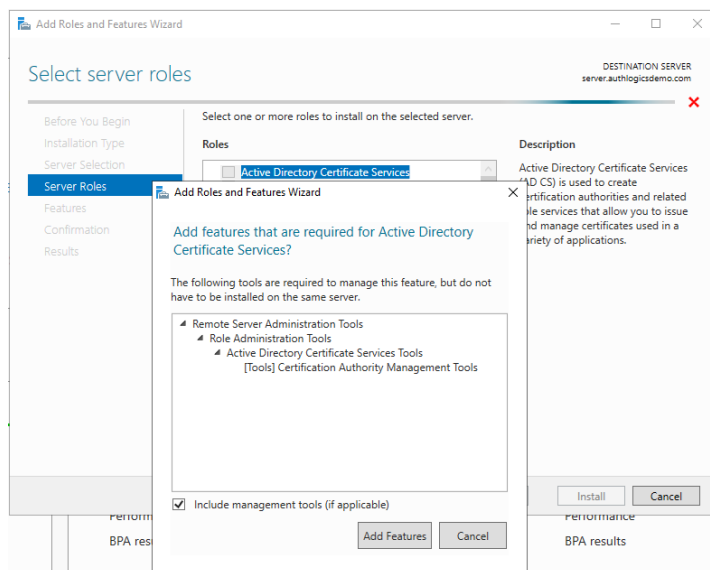
(10) Select Role-based or feature-based installation



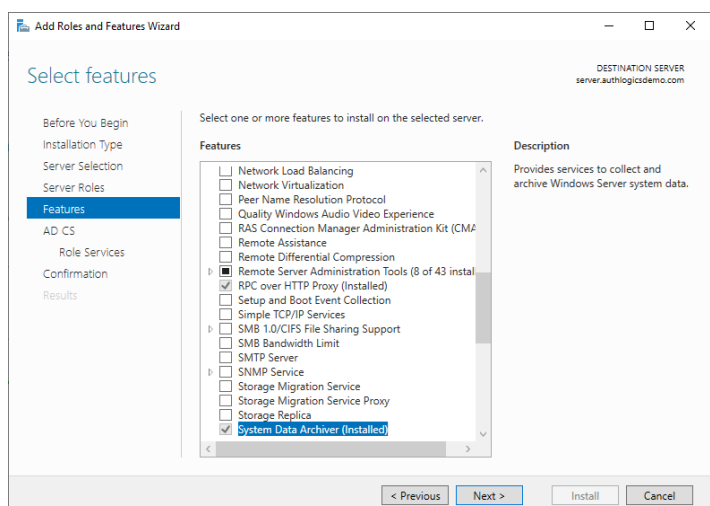
(11) Select the local server as the server pool



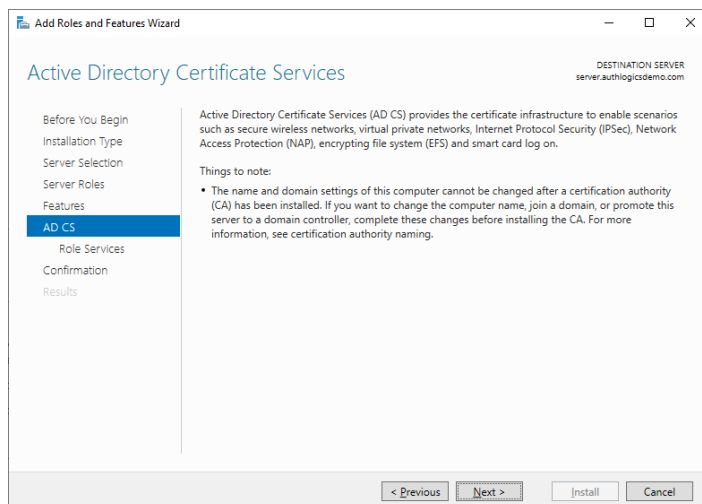
(12) Enable Active Directory Certificate Services and Add Features required for AD Certificate Services



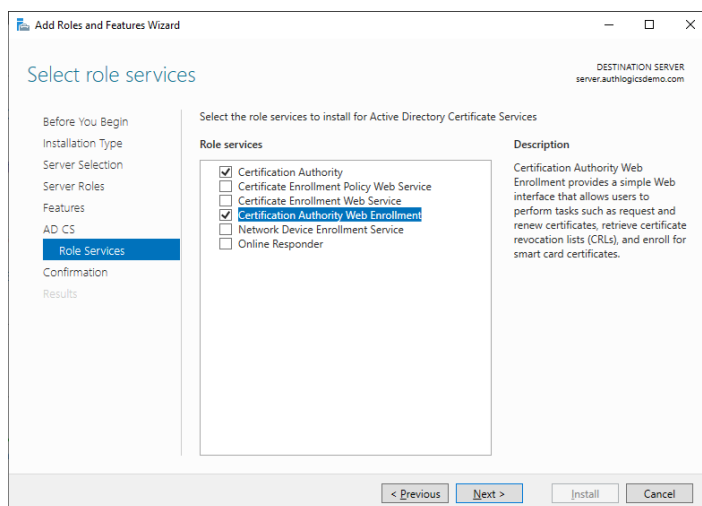
(13) Select Next



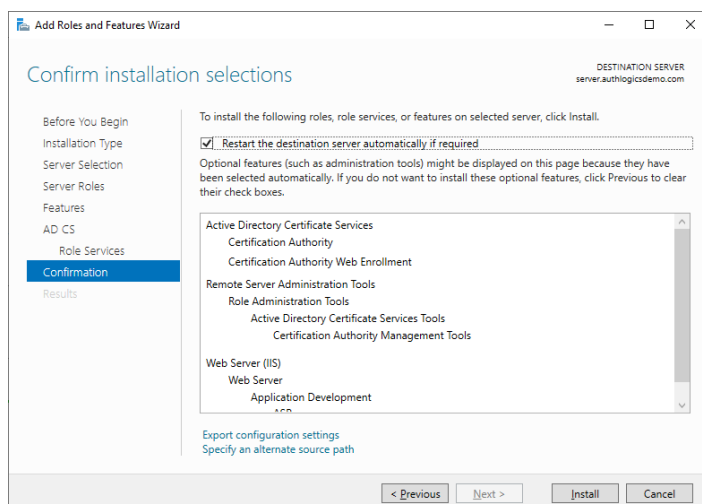
(14) Select Next

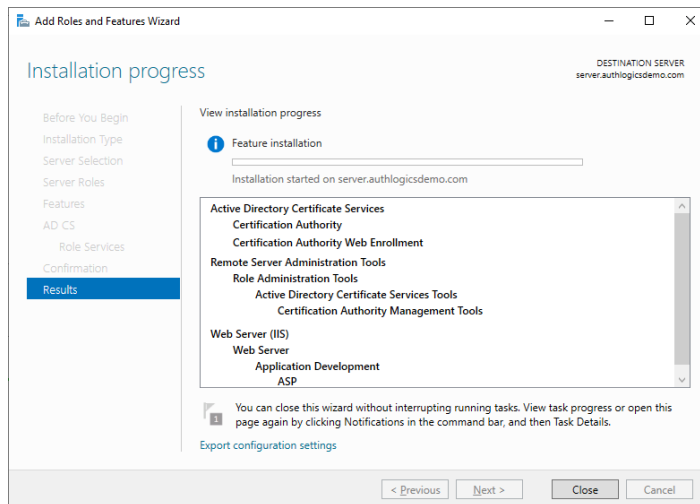


(15) Select Next and enable Certificate Authority and Certificate Authority Web Enrollment



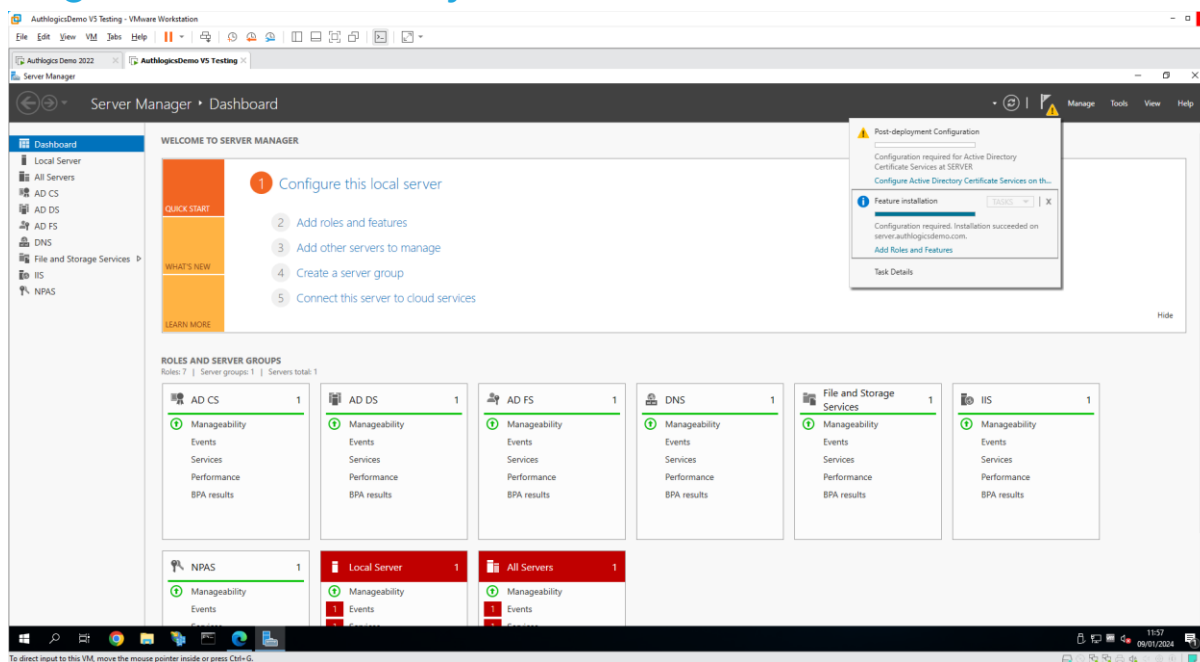
(16) Enable Restart the destination server automatically if required and select Install



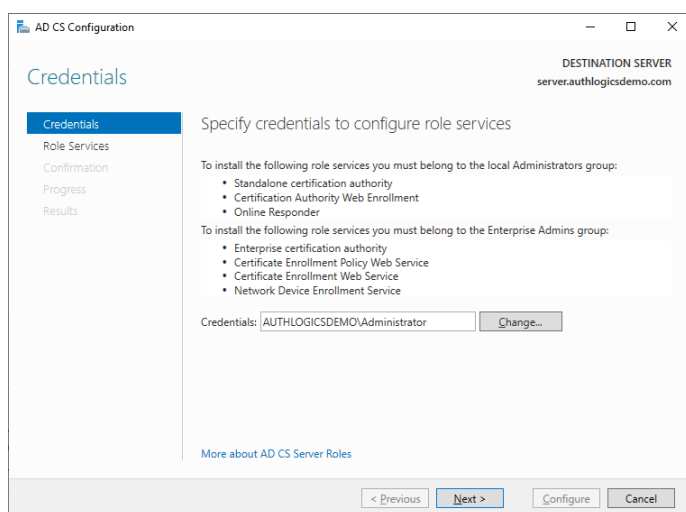


(17) Click Close when complete

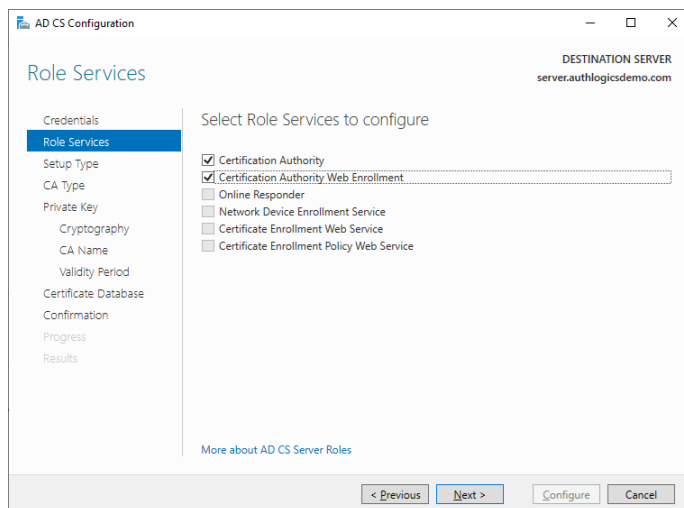
Configure Active Directory Certificate Services



- (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



AD CS Configuration

DESTINATION SERVER
server.authlogicsdemo.com

Role Services

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

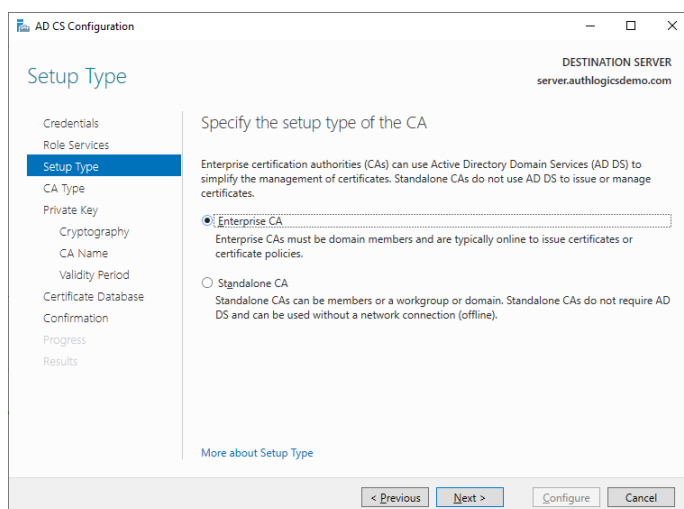
Select Role Services to configure

- ☒ Certification Authority
- ☒ Certification Authority Web Enrollment
- ☐ Online Responder
- ☐ Network Device Enrollment Service
- ☐ Certificate Enrollment Web Service
- ☐ Certificate Enrollment Policy Web Service

More about AD CS Server Roles

< Previous Next > Configure Cancel

(3) Select Enterprise CA and select Next



AD CS Configuration

DESTINATION SERVER
server.authlogicsdemo.com

Setup Type

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the setup type of the CA

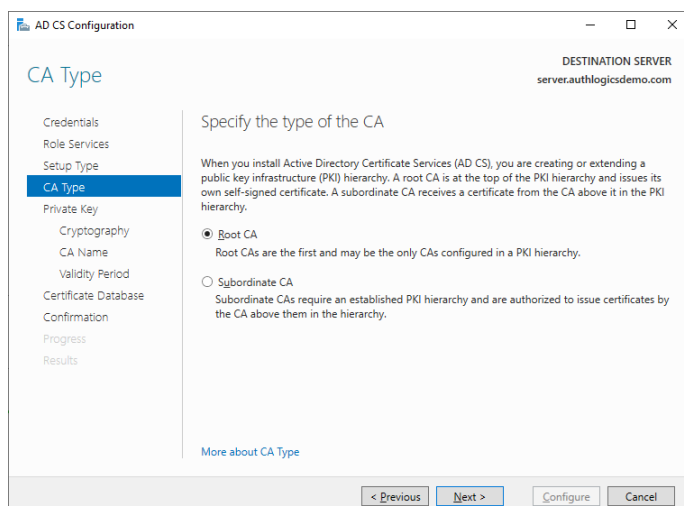
Enterprise certification authorities (CAs) can use Active Directory Domain Services (AD DS) to simplify the management of certificates. Standalone CAs do not use AD DS to issue or manage certificates.

- ☒ Enterprise CA
Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.
- ☐ Standalone CA
Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).

More about Setup Type

< Previous Next > Configure Cancel

(4) Select Root CA and Select Next



AD CS Configuration

DESTINATION SERVER
server.authlogicsdemo.com

CA Type

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the CA

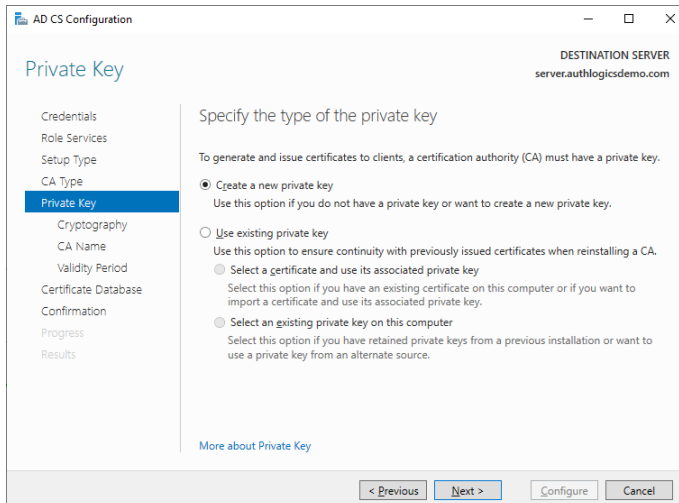
When you install Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. A root CA is at the top of the PKI hierarchy and issues its own self-signed certificate. A subordinate CA receives a certificate from the CA above it in the PKI hierarchy.

- ☒ Root CA
Root CAs are the first and may be the only CAs configured in a PKI hierarchy.
- ☐ Subordinate CA
Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.

More about CA Type

< Previous Next > Configure Cancel

(5) Create a new private key and Select Next



AD CS Configuration

DESTINATION SERVER
server.authlogicsdemo.com

Private Key

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the type of the private key

To generate and issue certificates to clients, a certification authority (CA) must have a private key.

☒ Create a new private key
Use this option if you do not have a private key or want to create a new private key.

☐ Use existing private key
Use this option to ensure continuity with previously issued certificates when reinstalling a CA.

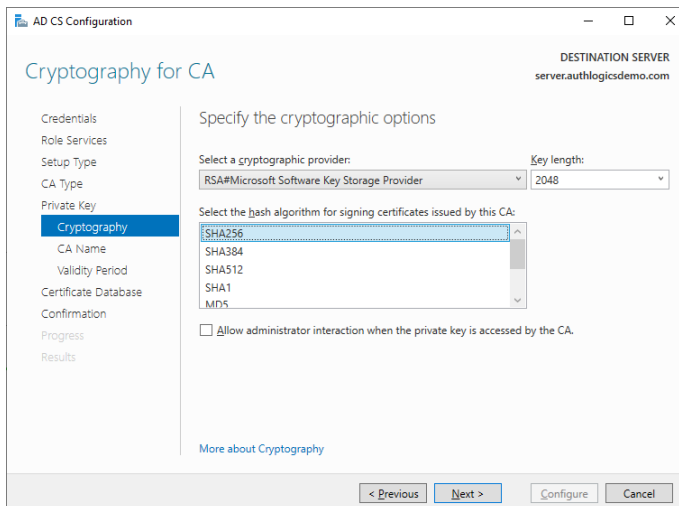
☐ Select a certificate and use its associated private key
Select this option if you have an existing certificate on this computer or if you want to import a certificate and use its associated private key.

☐ Select an existing private key on this computer
Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.

[More about Private Key](#)

< Previous Next > Configure Cancel

(6) Select Next



AD CS Configuration

DESTINATION SERVER
server.authlogicsdemo.com

Cryptography for CA

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the cryptographic options

Select a cryptographic provider:
RSA#Microsoft Software Key Storage Provider

Key length:
2048

Select the hash algorithm for signing certificates issued by this CA:

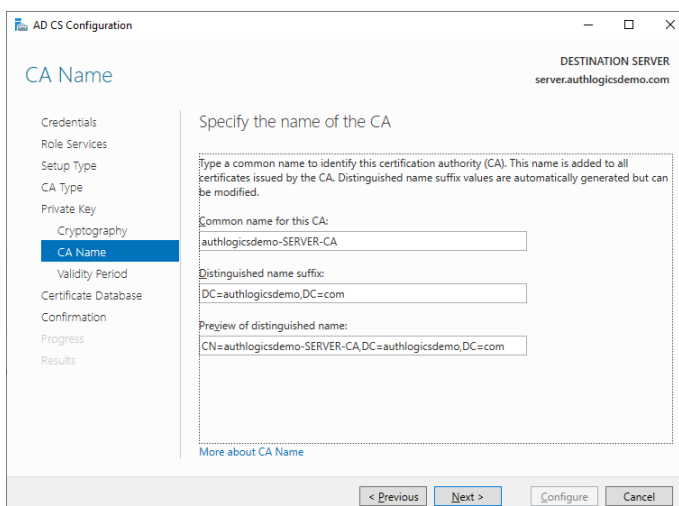
- SHA256
- SHA384
- SHA512
- SHA1
- MD5

☐ Allow administrator interaction when the private key is accessed by the CA.

[More about Cryptography](#)

< Previous Next > Configure Cancel

(7) Select Next



AD CS Configuration

DESTINATION SERVER
server.authlogicsdemo.com

CA Name

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the name of the CA

Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.

Common name for this CA:
authlogicsdemo-SERVER-CA

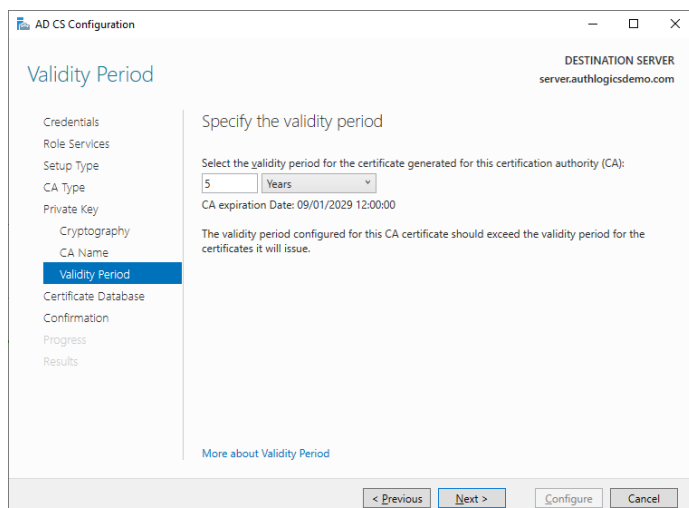
Distinguished name suffix:
DC=authlogicsdemo,DC=com

Preview of distinguished name:
CN=authlogicsdemo-SERVER-CA,DC=authlogicsdemo,DC=com

[More about CA Name](#)

< Previous Next > Configure Cancel

(8) Select Next



AD CS Configuration

DESTINATION SERVER
server.authlogicsdemo.com

Validity Period

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the validity period

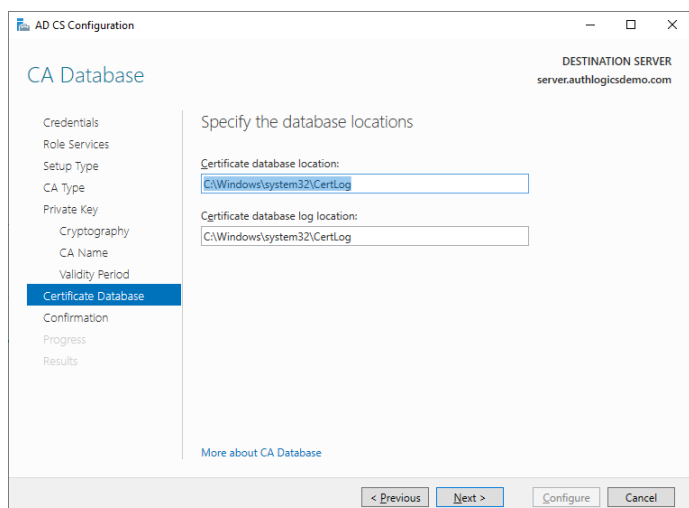
Select the validity period for the certificate generated for this certification authority (CA):
5 Years
CA expiration Date: 09/01/2029 12:00:00

The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.

[More about Validity Period](#)

< Previous Next > Configure Cancel

(9) Select Next



AD CS Configuration

DESTINATION SERVER
server.authlogicsdemo.com

CA Database

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

Specify the database locations

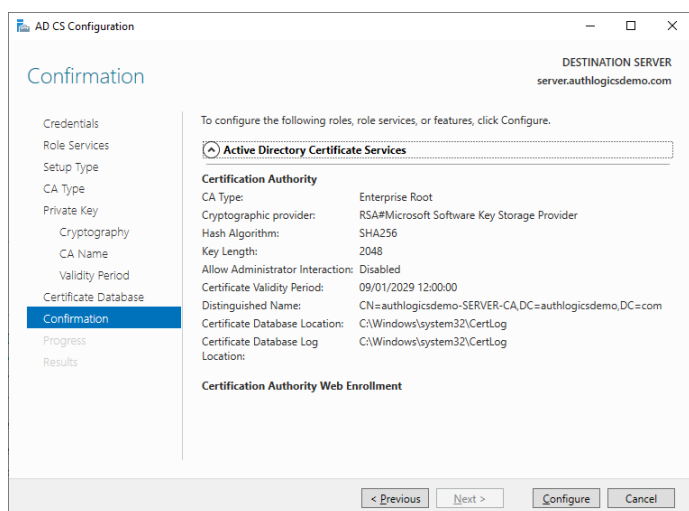
Certificate database location:
C:\Windows\system32\CertLog

Certificate database log location:
C:\Windows\system32\CertLog

[More about CA Database](#)

< Previous Next > Configure Cancel

(10) Select Configure



AD CS Configuration

DESTINATION SERVER
server.authlogicsdemo.com

Confirmation

Credentials
Role Services
Setup Type
CA Type
Private Key
Cryptography
CA Name
Validity Period
Certificate Database
Confirmation
Progress
Results

To configure the following roles, role services, or features, click Configure.

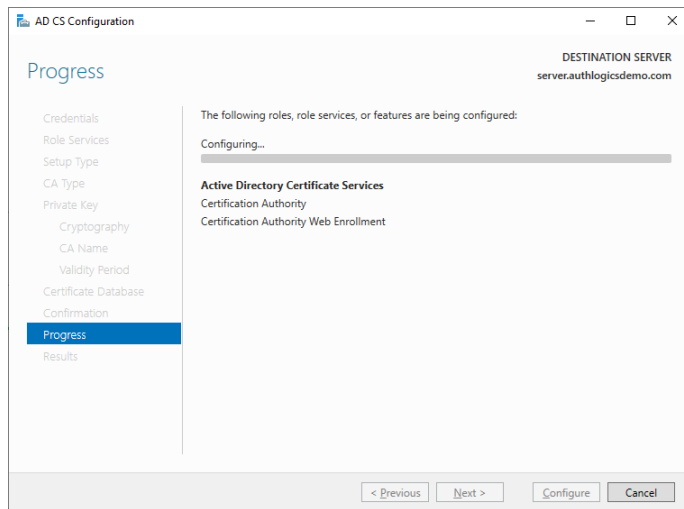
Active Directory Certificate Services

Certification Authority

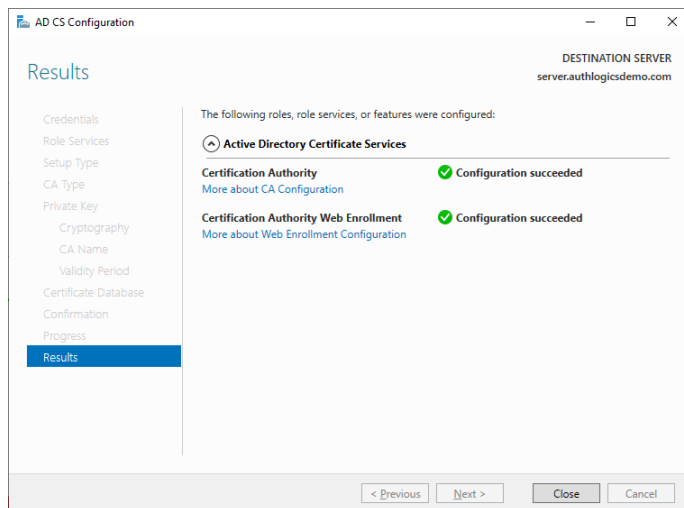
CA Type: Enterprise Root
Cryptographic provider: RSA#Microsoft Software Key Storage Provider
Hash Algorithm: SHA256
Key Length: 2048
Allow Administrator Interaction: Disabled
Certificate Validity Period: 09/01/2029 12:00:00
Distinguished Name: CN=authlogicsdemo-SERVER-CA,DC=authlogicsdemo,DC=com
Certificate Database Location: C:\Windows\system32\CertLog
Certificate Database Log Location: C:\Windows\system32\CertLog

Certification Authority Web Enrollment

< Previous Next > Configure Cancel



(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.

