

MyID MFA and PSM

Version 5.3.2

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:

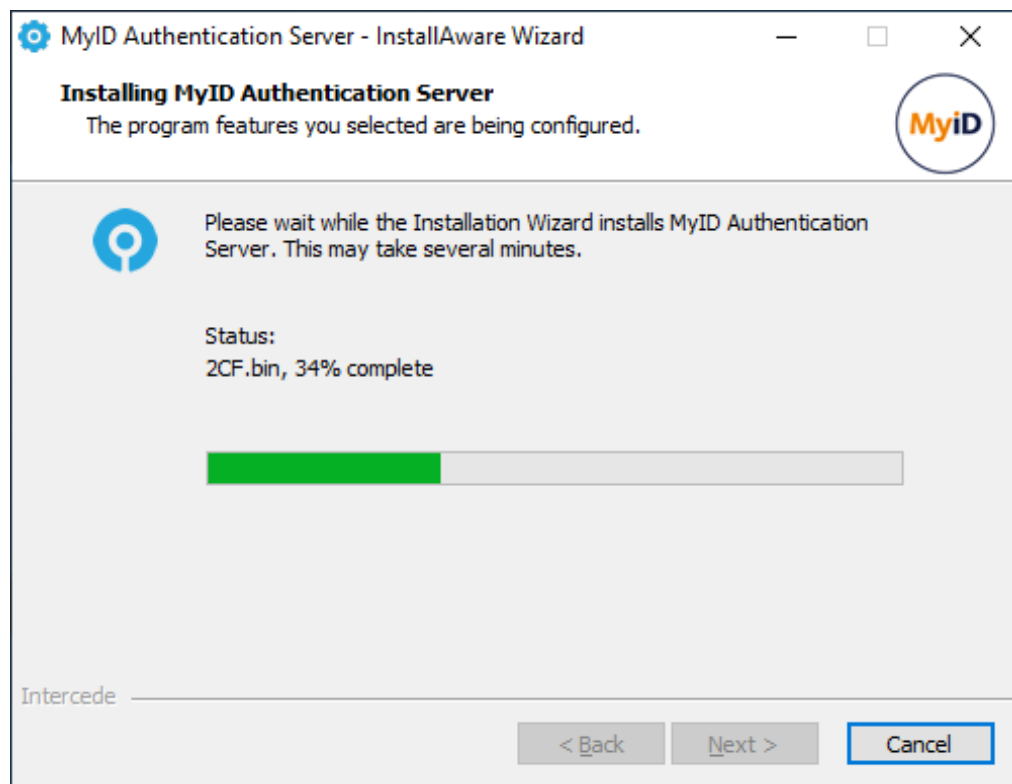
- Active Directory administrator credentials.
- SMTP server details: name, port, authentication requirements.
- The DNS name for the server.
- Understanding of which authentication technology to use.
- For FIDO and passkey tokens, MyID MFA requires a trusted certificate to be bound to MyID web sites;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

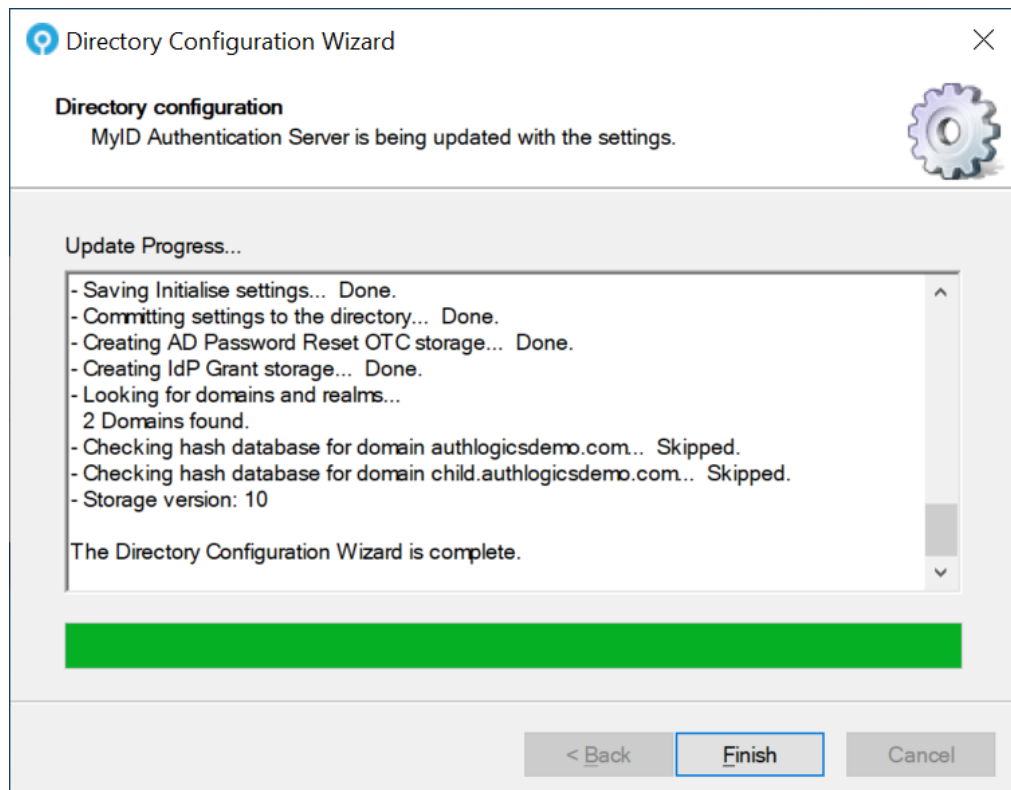
To install the MyID Authentication Server:

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](#).

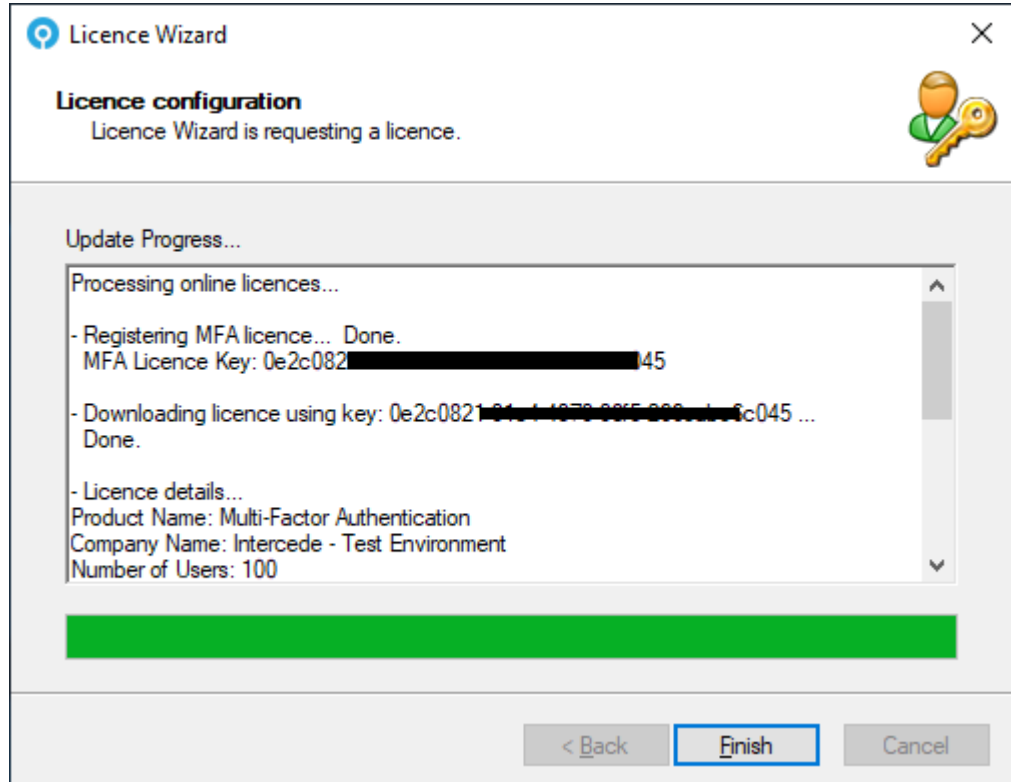
5. Follow the Directory Configuration Wizard to setup the Active Directory for use with MyID MFA.



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

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.



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

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

3 Configuring the Authentication Server

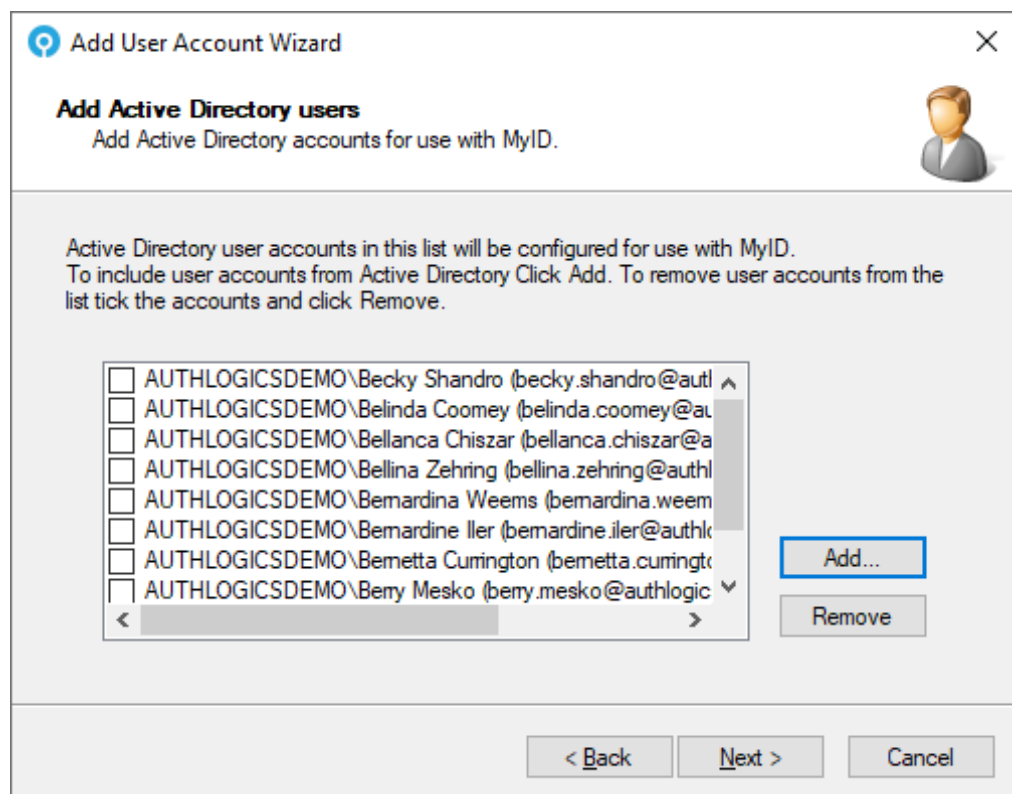
To begin the configuration of the MyID Authentication Server:

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:

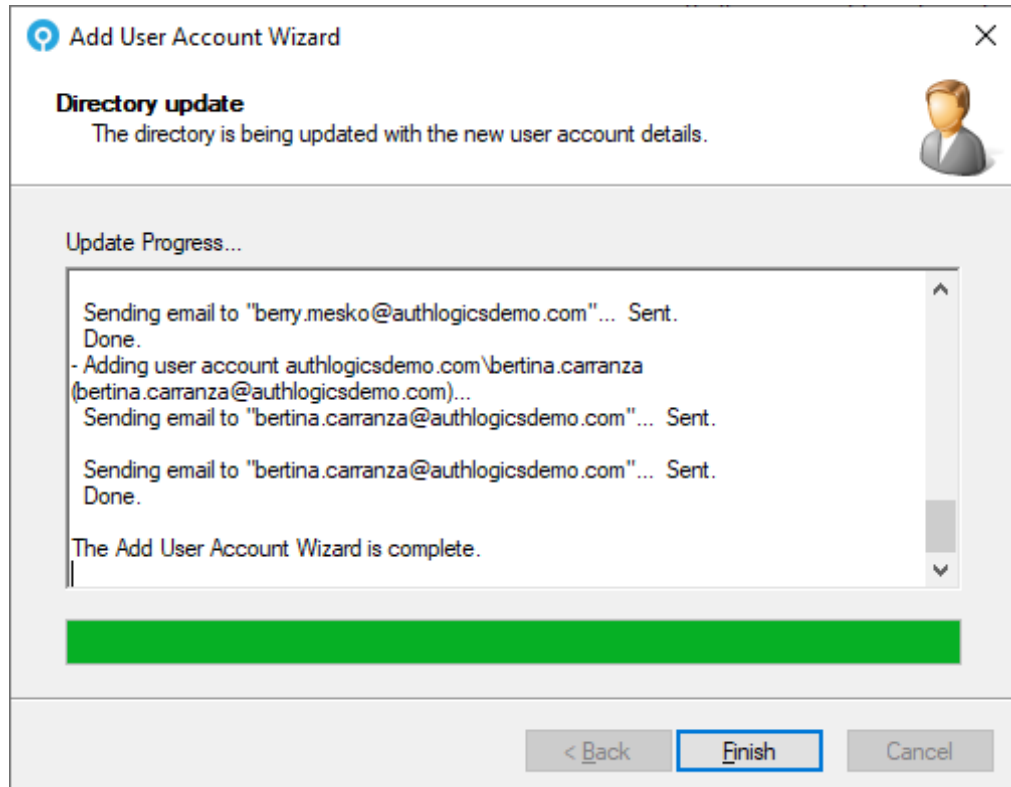
1. Expand the domains and open the domain into which you want to add MFA users.
2. Click the **Add User Account** action.
The Add User Account Wizard starts.
3. Select all the Active Directory users you want to configure for MyID MFA.



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](#).

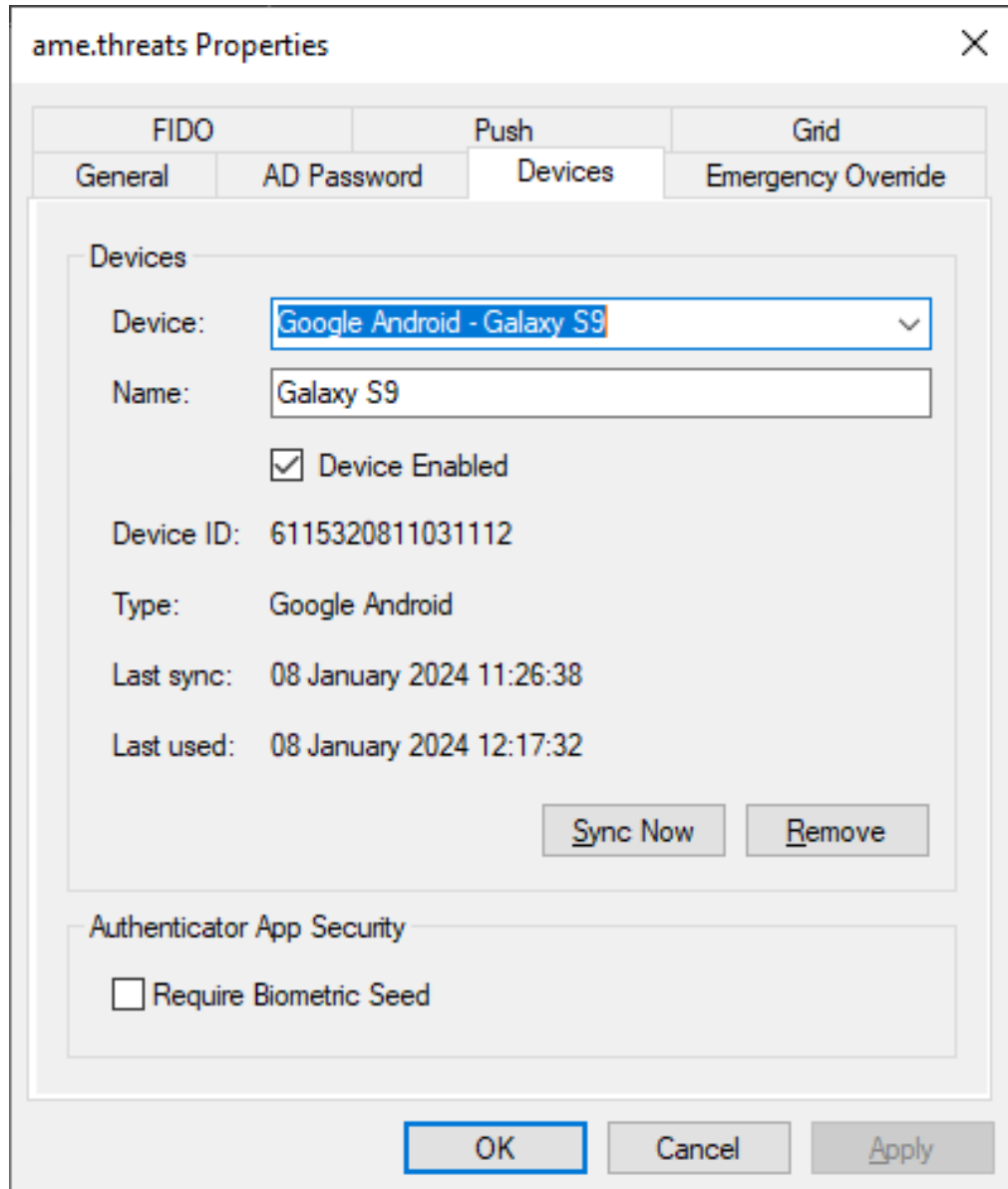
4. Complete the wizard.
5. Select all the users to provision an MFA technology.
For example, Grid, One Time Code, or YubiKey.
6. Click the **Management** option for the required technology to start the wizard.

7. Configure the technology settings for the selected users:



8. Complete the wizard.

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



The image shows a screenshot of the 'ame.threats Properties' dialog box. The dialog has a title bar with a close button (X). Below the title bar, there are four tabs: 'FIDO', 'Push', 'Grid', and 'Emergency Override'. The 'Push' tab is selected, and within it, the 'Devices' sub-tab is active. The 'Devices' section contains a list of devices. The first device is 'Google Android - Galaxy S9', which is selected. Below the device name, there is a text field for 'Name' containing 'Galaxy S9'. There is a checkbox labeled 'Device Enabled' which is checked. Below this, there are fields for 'Device ID' (6115320811031112), 'Type' (Google Android), 'Last sync' (08 January 2024 11:26:38), and 'Last used' (08 January 2024 12:17:32). At the bottom right of the device list, there are two buttons: 'Sync Now' and 'Remove'. Below the device list, there is a section titled 'Authenticator App Security' with a checkbox labeled 'Require Biometric Seed' which is unchecked. At the bottom of the dialog, there are three buttons: 'OK', 'Cancel', and 'Apply'.

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.

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 [Verify...](#)

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:
●●●●●●●●

OK Cancel

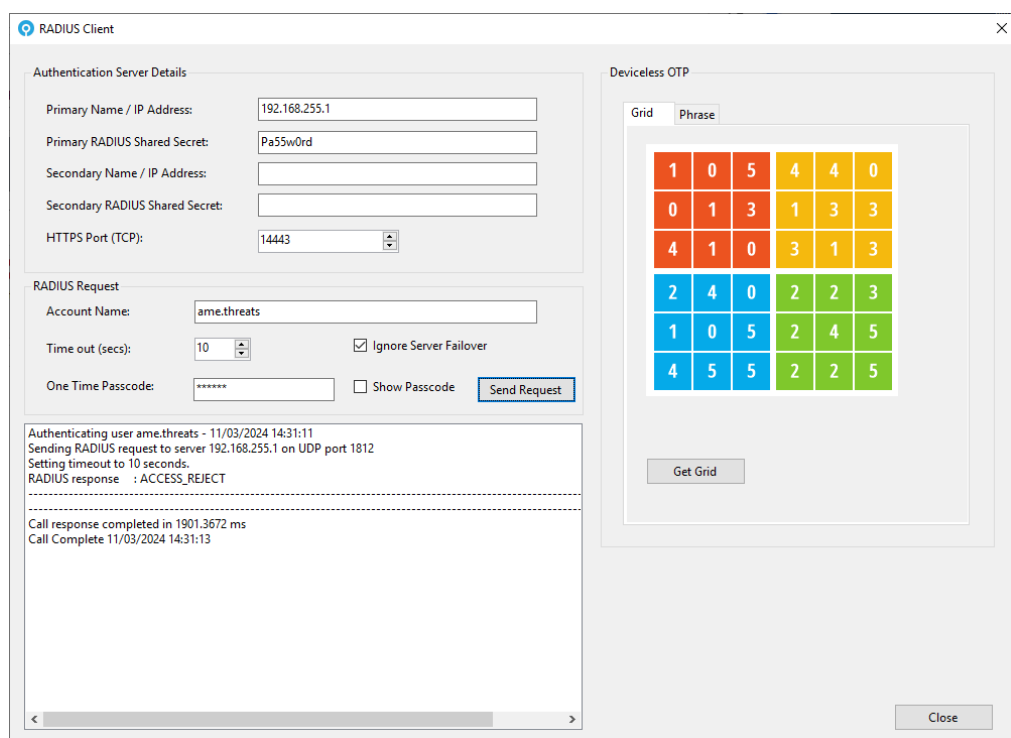
For more information on adding the local server as a RADIUS client, see the *Adding a RADIUS client* section in the [MyID Authentication Server Installation and Configuration Guide](#).

5. Start the MyID RADIUS test client from:

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

- Enter the local server IP address and shared secret you configured above.
- Enter the test user account name.
- Click **Grid** to show a grid if you are using a Grid.

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



The screenshot shows the 'RADIUS Client' application window. It has two main sections: 'Authentication Server Details' and 'RADIUS Request'. The 'Authentication Server Details' section contains fields for 'Primary Name / IP Address' (192.168.255.1), 'Primary RADIUS Shared Secret' (Pa55w0rd), 'Secondary Name / IP Address', 'Secondary RADIUS Shared Secret', and 'HTTPS Port (TCP)' (14443). The 'RADIUS Request' section contains 'Account Name' (ame.threats), 'Time out (secs)' (10), a checked 'Ignore Server Failover' checkbox, and a 'One Time Passcode' field with asterisks. A 'Send Request' button is at the bottom right of this section. Below these sections is a log area showing the following text: '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', and 'Call Complete 11/03/2024 14:31:13'. On the right side of the window is a 'Deviceless OTP' section with a 'Grid' tab selected. It displays a 4x6 grid of numbers: Row 1: 1, 0, 5, 4, 4, 0; Row 2: 0, 1, 3, 1, 3, 3; Row 3: 4, 1, 0, 3, 1, 3; Row 4: 2, 4, 0, 2, 2, 3; Row 5: 1, 0, 5, 2, 4, 5; Row 6: 4, 5, 5, 2, 2, 5. A 'Get Grid' button is below the grid, and a 'Close' button is at the bottom right of the window.

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`

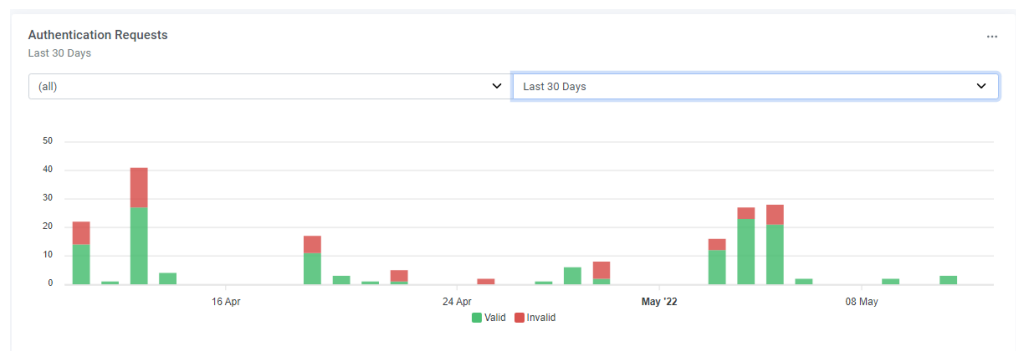
Where `<servername>` is the name of your server.

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

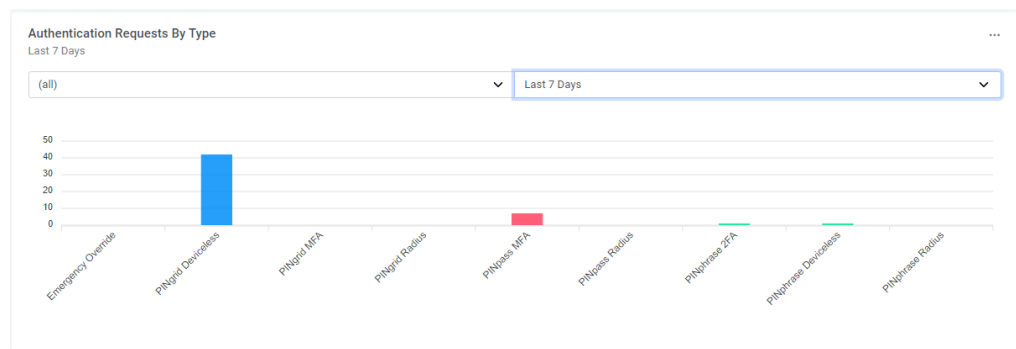
2. Under **System > Dashboards**, select **Multi-Factor Authentication**.

This dashboard reflects contains information on:

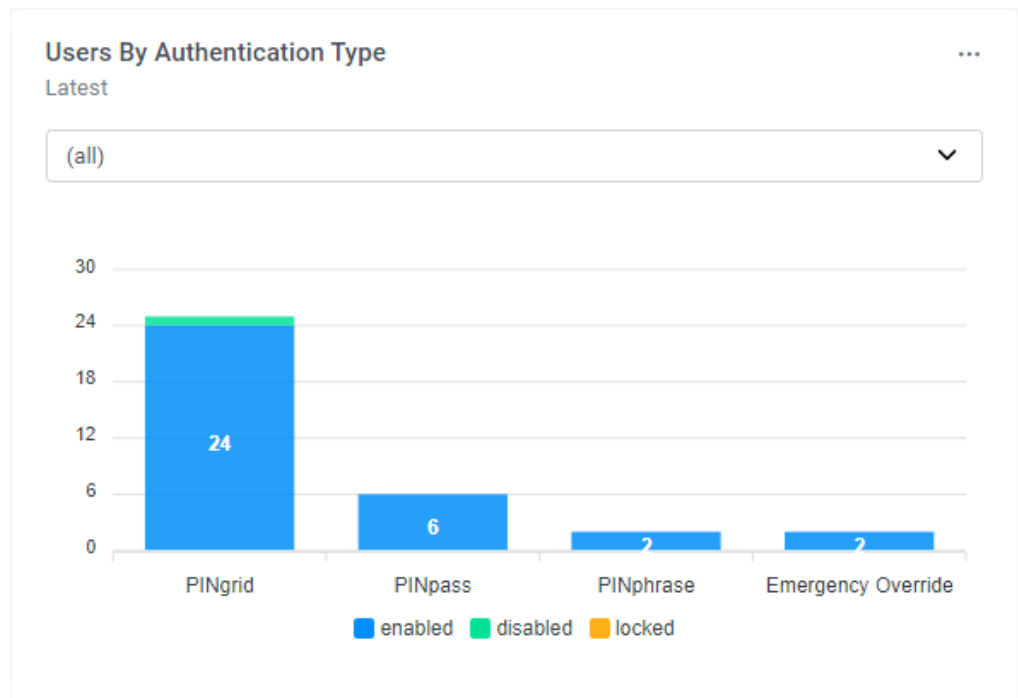
- **Authentication Requests**



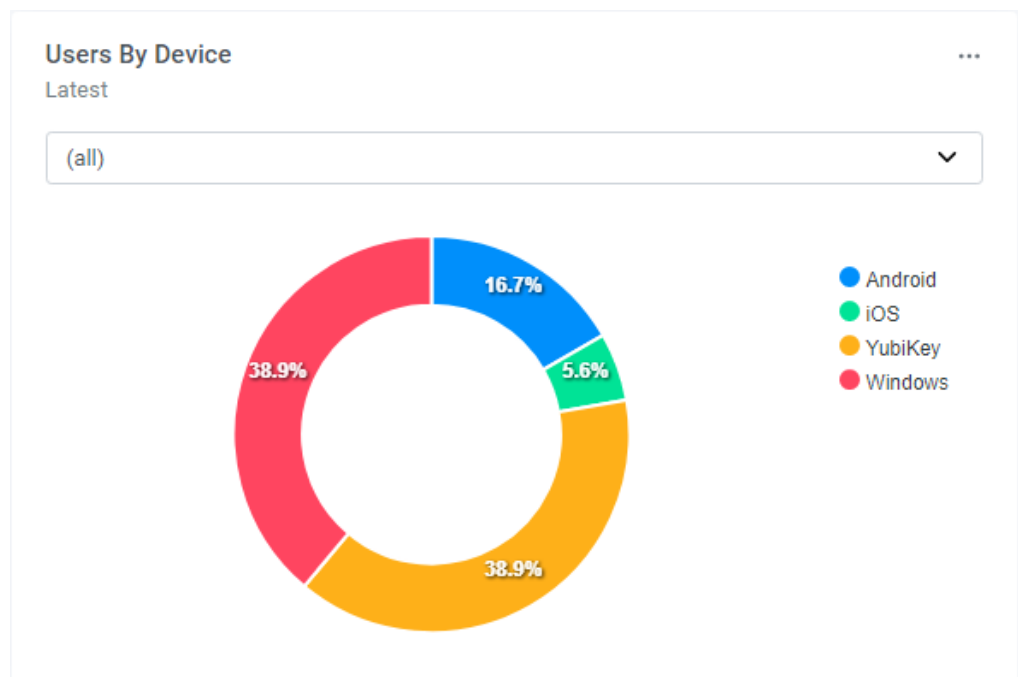
- **Authentication Requests By Type**



- Users By Authentication Type



- Users By Device



3.4 Configuring the Windows Desktop Agent

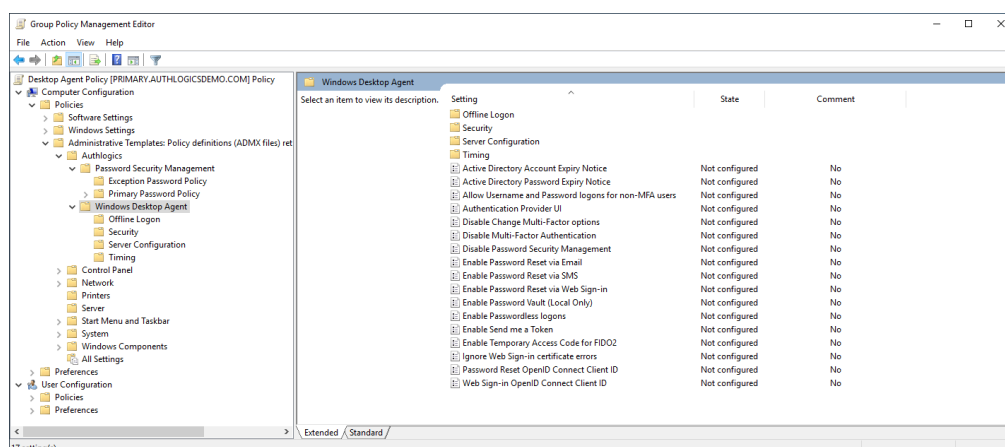
This section assumes that you are using a separate workstation test PC which is domain joined. You can deploy the MyID Windows Desktop Agent on non-domain joined PCs; however, you must apply the Group Policy Objects to these PCs manually.

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](#).

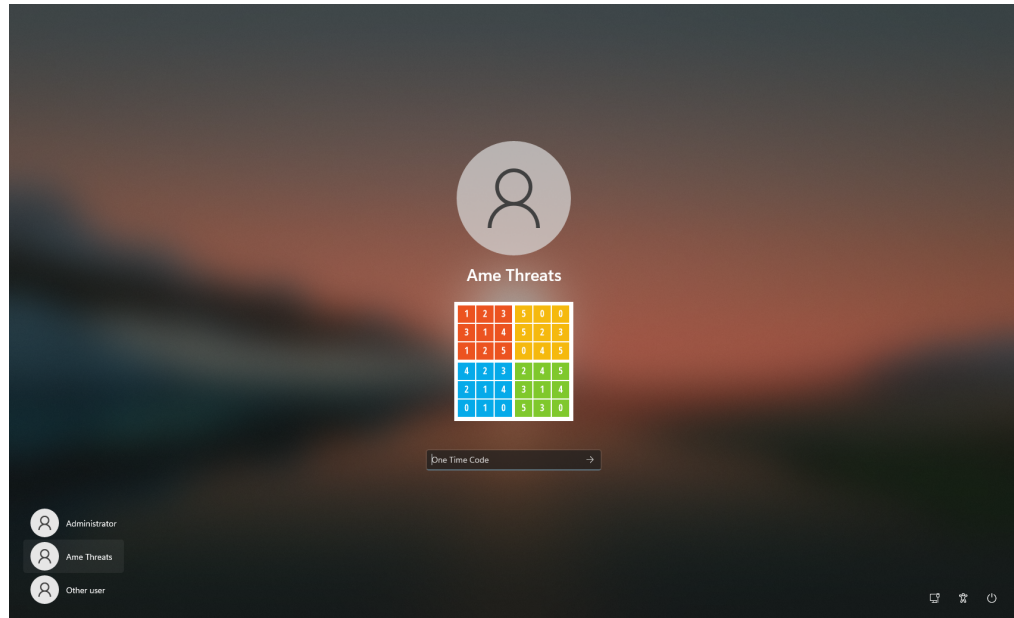
5. Apply the GPO to an OU containing the workstation computer account.

Perform these actions on the workstation:

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

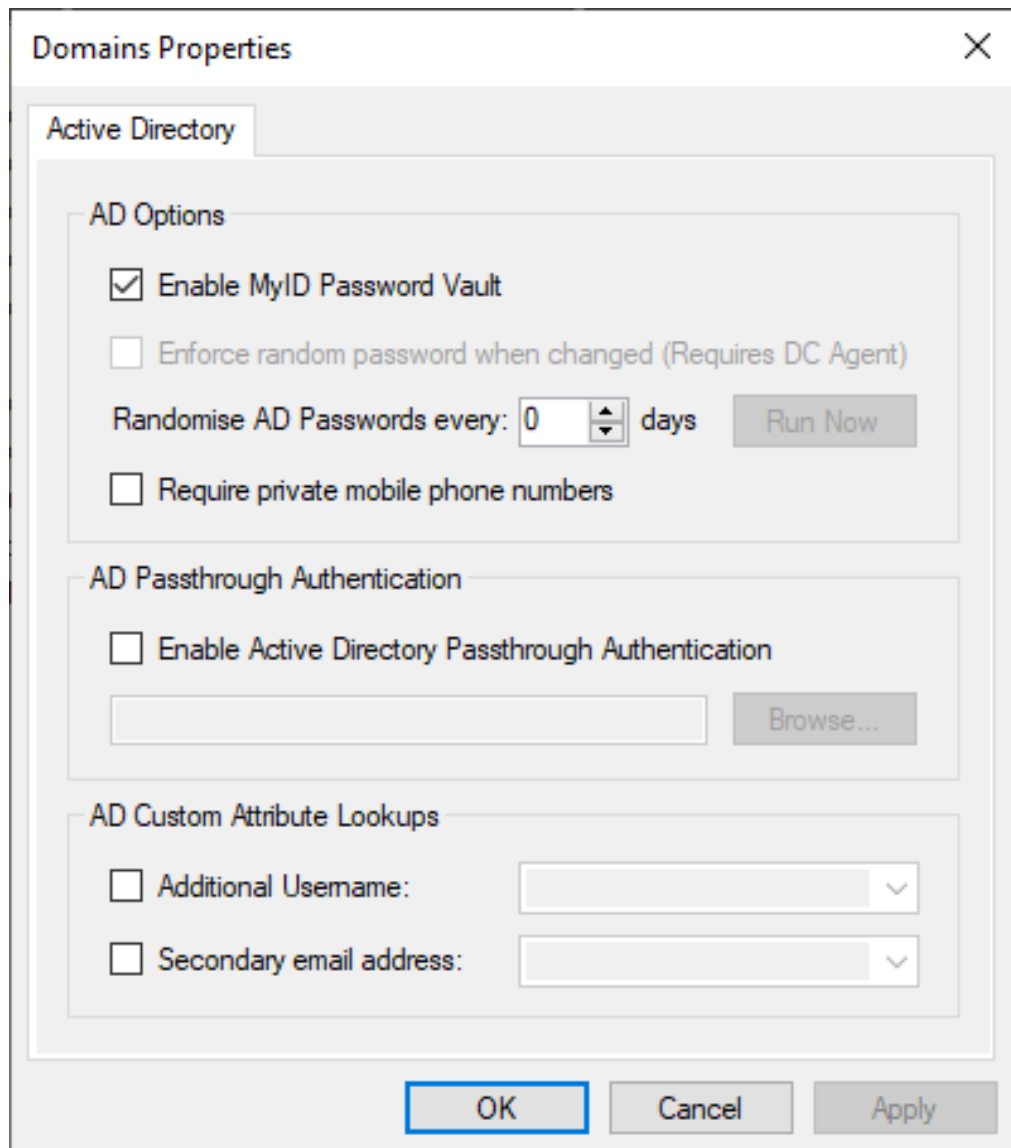
`GPUPDATE /FORCE`

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:



The screenshot shows the 'Domains Properties' dialog box with the 'Active Directory' tab selected. The 'AD Options' section contains the following settings:

- ☒ Enable MyID Password Vault
- ☐ Enforce random password when changed (Requires DC Agent)
- Randomise AD Passwords every: 0 days (with a 'Run Now' button)
- ☐ Require private mobile phone numbers

The 'AD Passthrough Authentication' section contains:

- ☐ Enable Active Directory Passthrough Authentication
- A text input field and a 'Browse...' button.

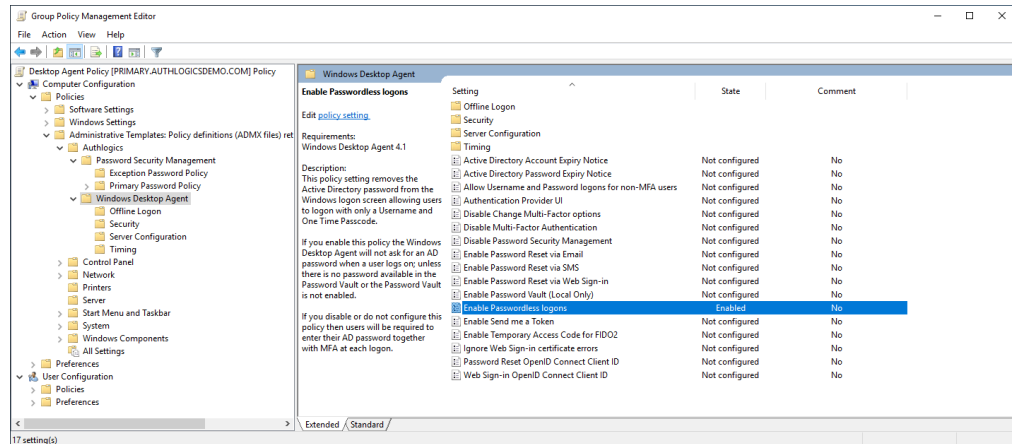
The 'AD Custom Attribute Lookups' section contains:

- ☐ Additional Username: (with a dropdown menu)
- ☐ Secondary email address: (with a dropdown menu)

At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

2. Update the group policy settings.

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

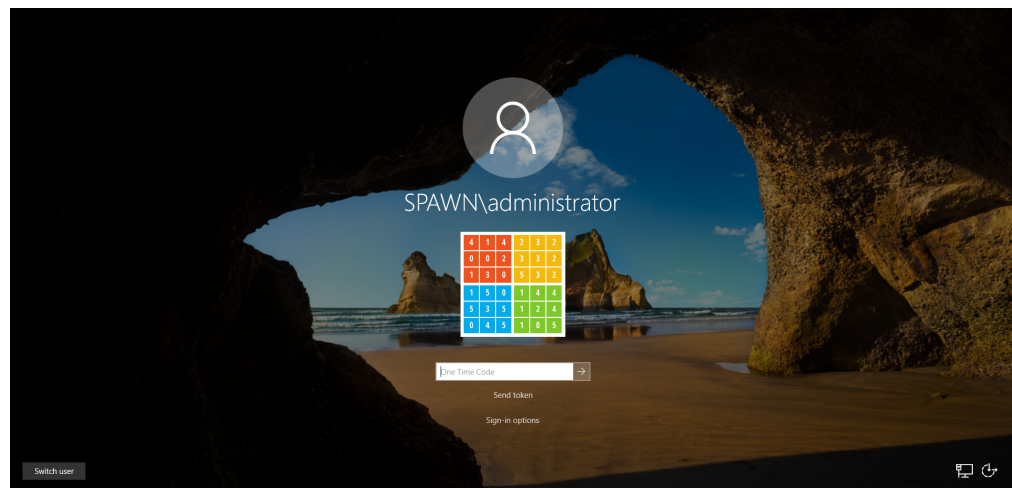


4. Ensure the GPO settings are applied to the PC by running:

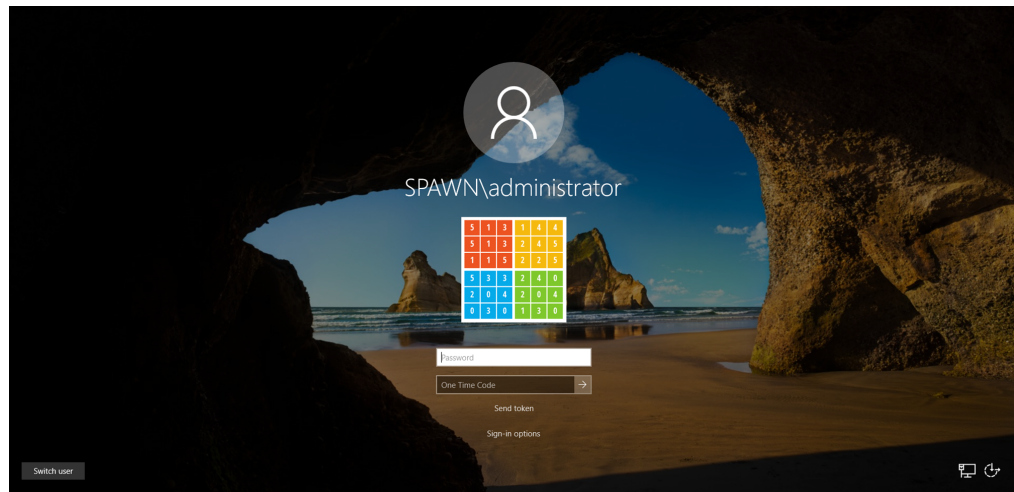
GPUPDATE /FORCE

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

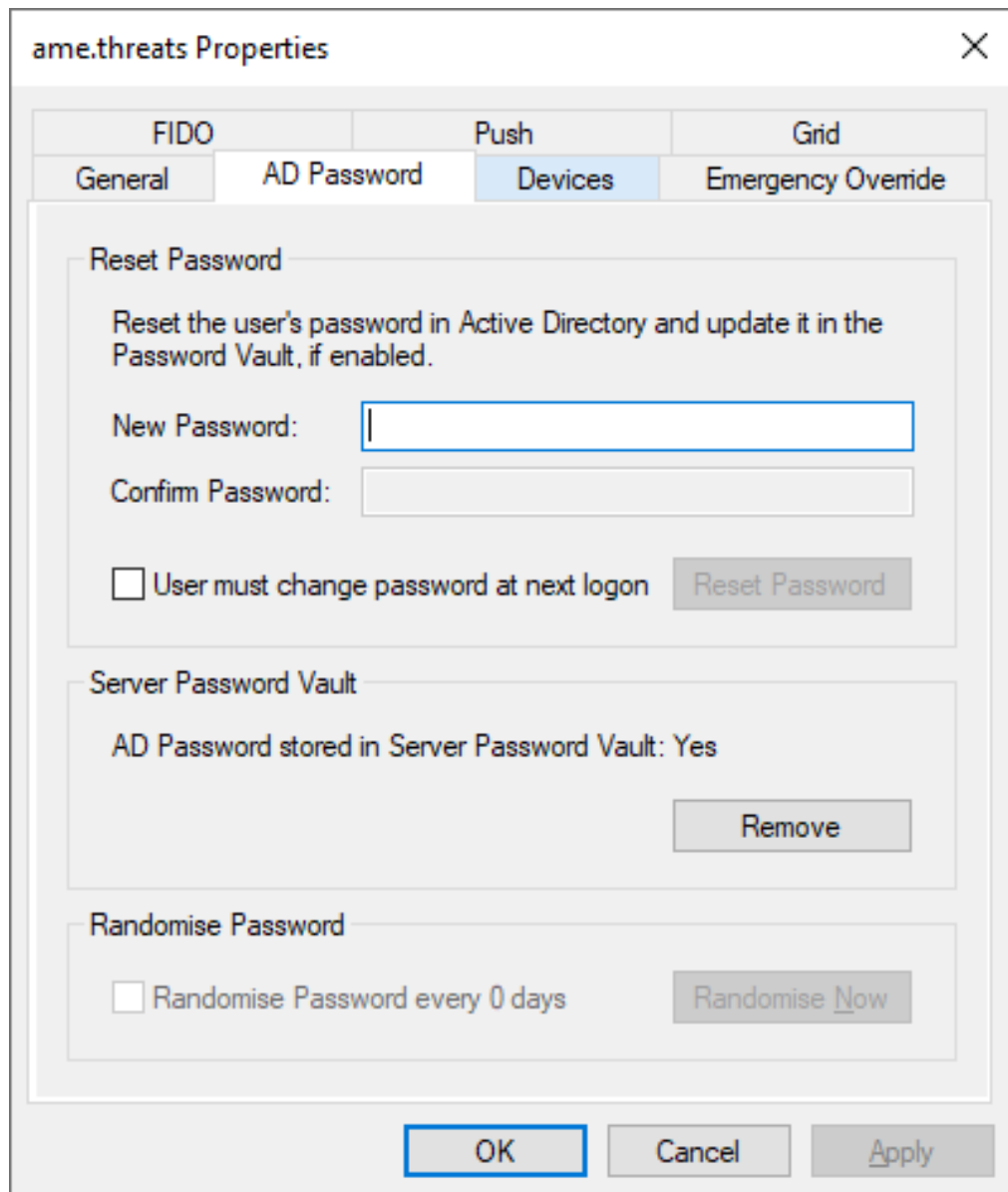
Note: There is no password option available:



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 image shows a screenshot of the 'ame.threats Properties' dialog box. The dialog has a title bar with a close button (X). Below the title bar is a tabbed interface with four tabs: 'FIDO', 'Push', 'Grid', and 'General'. The 'General' tab is selected. Inside the 'General' tab, there are three main sections: 'Reset Password', 'Server Password Vault', and 'Randomise Password'. The 'Reset Password' section contains a text box for 'New Password', a text box for 'Confirm Password', a checkbox for 'User must change password at next logon', and a 'Reset Password' button. The 'Server Password Vault' section contains a label 'AD Password stored in Server Password Vault: Yes' and a 'Remove' button. The 'Randomise Password' section contains a checkbox for 'Randomise Password every 0 days' and a 'Randomise Now' button. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

ame.threats Properties

General AD Password Push Grid

Reset Password

Reset the user's password in Active Directory and update it in the Password Vault, if enabled.

New Password:

Confirm Password:

☐ User must change password at next logon

Server Password Vault

AD Password stored in Server Password Vault: Yes

Randomise Password

☐ Randomise Password every 0 days

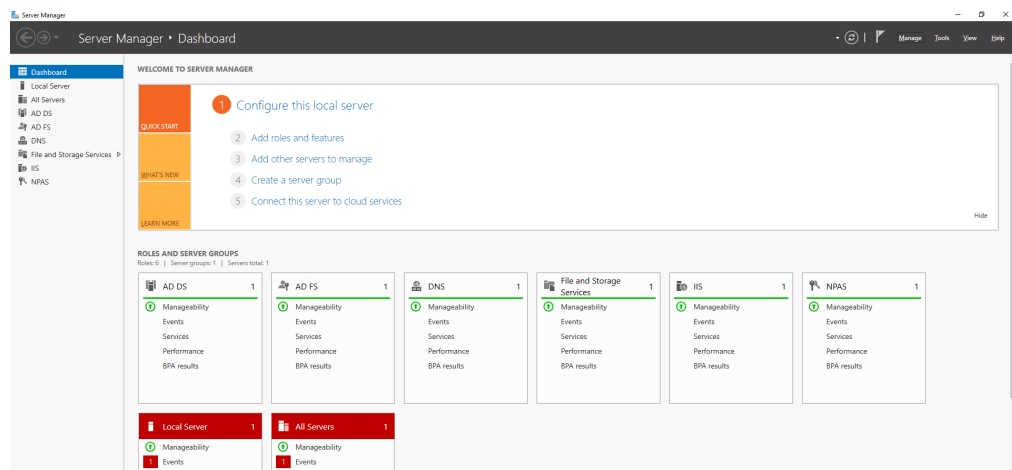
4 Configuring a Certificate Authority

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.

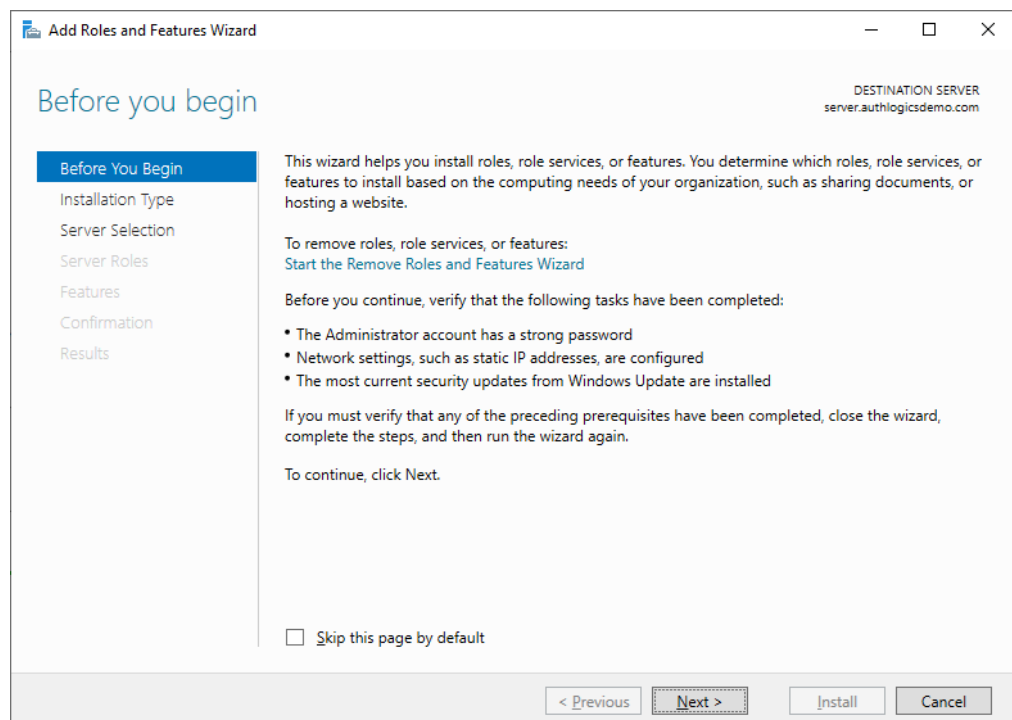
4.1 Installing the Certificate Authority

Perform these actions on the server:

1. Open Server Manager.



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



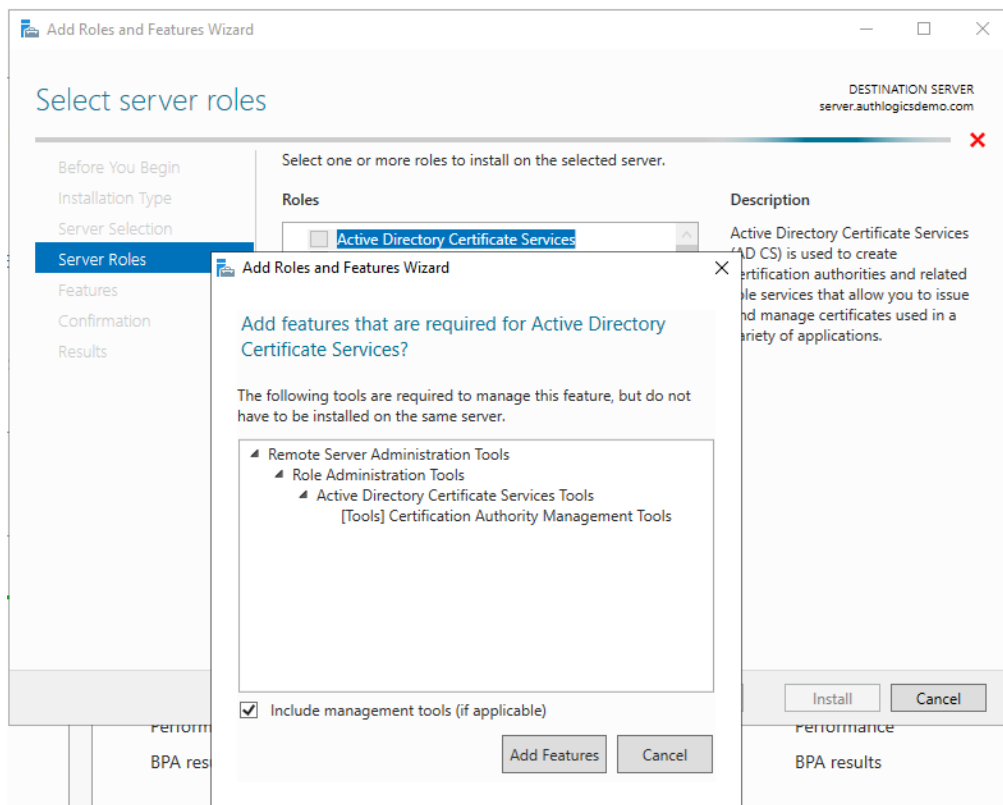
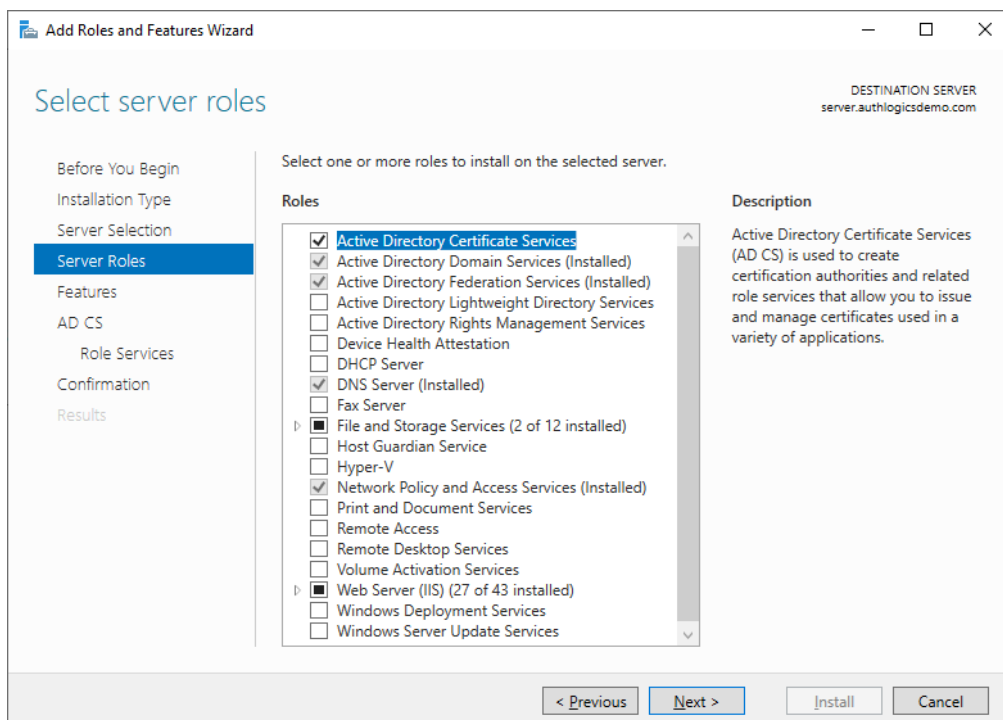
3. Click **Next**.

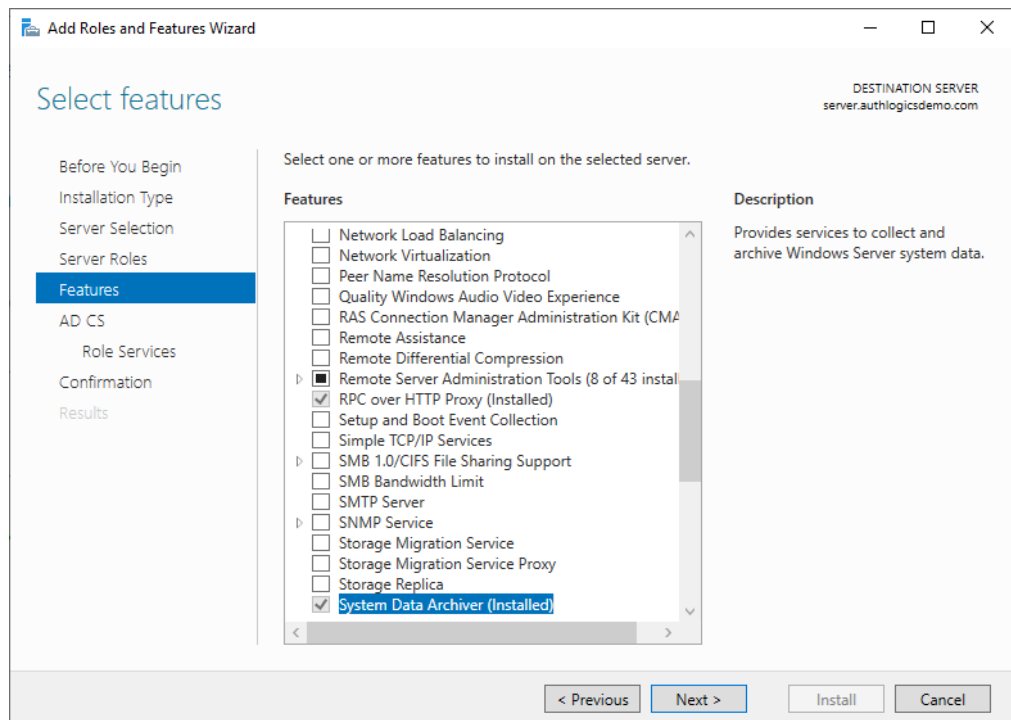
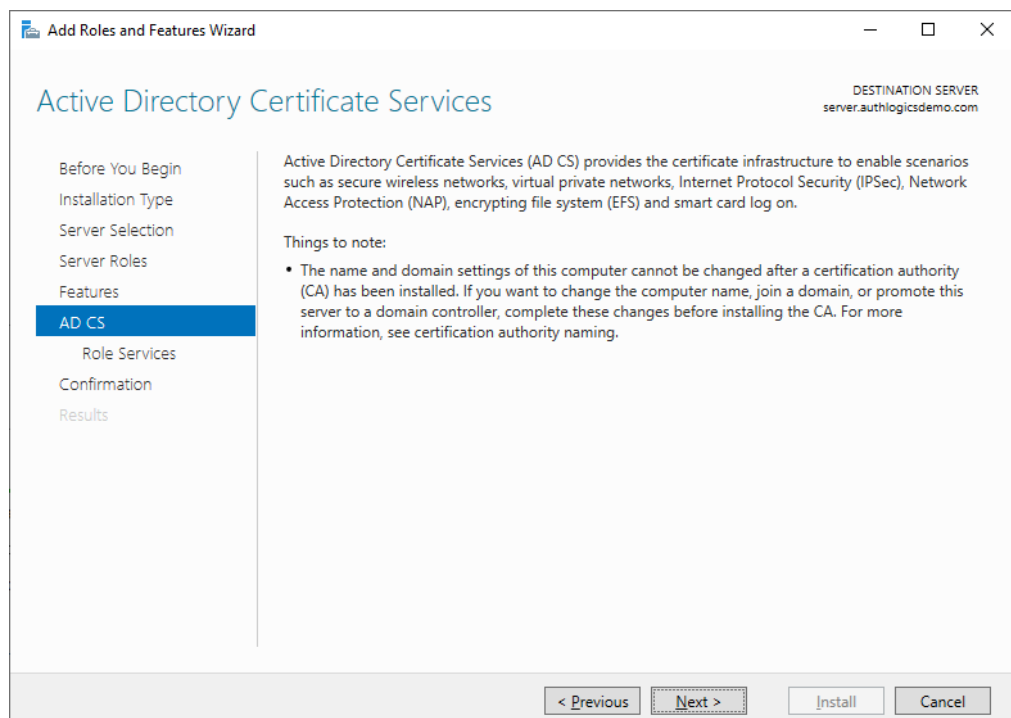
The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select installation type'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type' (highlighted), 'Server Selection', 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main content area has the text: 'Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD)'. There are two radio button options: 'Role-based or feature-based installation' (selected) and 'Remote Desktop Services installation'. Below the first option is the text: 'Configure a single server by adding roles, role services, and features.' Below the second option is the text: 'Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.' At the bottom right, there is a 'DESTINATION SERVER' label with the value 'server.authlogicsdemo.com'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

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

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection' (highlighted), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main content area has the text: 'Select a server or a virtual hard disk on which to install roles and features.' There are two radio button options: 'Select a server from the server pool' (selected) and 'Select a virtual hard disk'. Below the first option is a 'Server Pool' section. It contains a 'Filter:' label and a text input field. Below the input field is a table with the following columns: 'Name', 'IP Address', and 'Operating System'. The table has one row with the following data: 'server.authlogicsdemo.com', '192.168.255.1...', and 'Microsoft Windows Server 2019 Standard'. Below the table, it says '1 Computer(s) found'. At the bottom, there is a paragraph of text: 'This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.' At the bottom right, there is a 'DESTINATION SERVER' label with the value 'server.authlogicsdemo.com'. At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

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**.

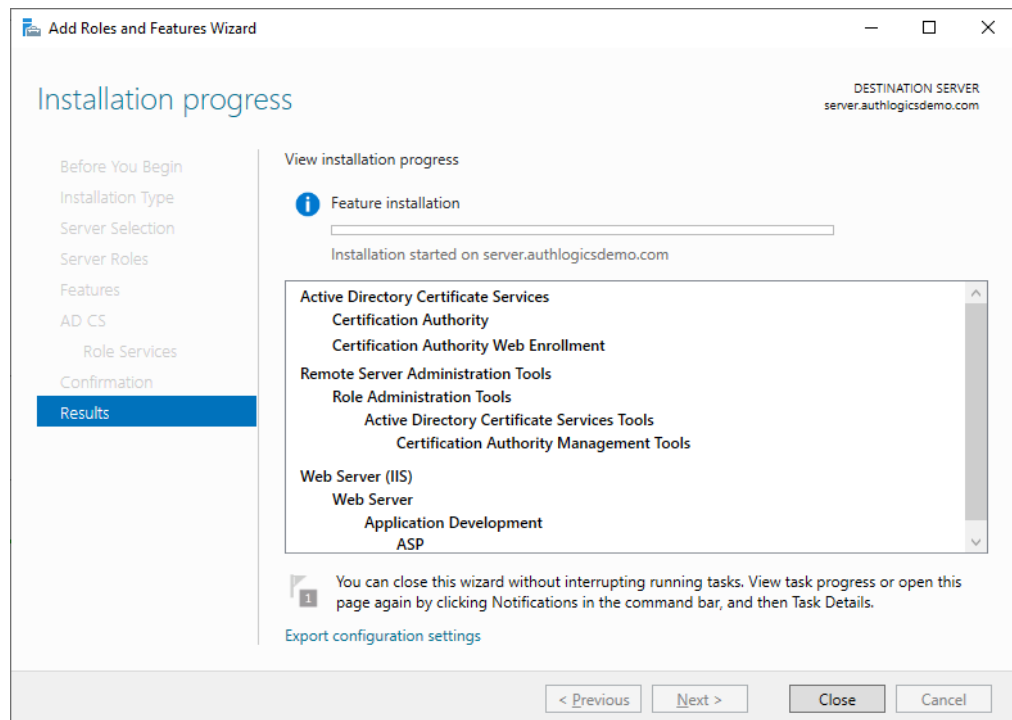
10. Click **Next**.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select role services'. On the right, it says 'DESTINATION SERVER server.authlogicsdemo.com'. On the left, a navigation pane shows steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services' (highlighted), 'Confirmation', and 'Results'. The main area is titled 'Select the role services to install for Active Directory Certificate Services'. It contains a table with two columns: 'Role services' and 'Description'. The 'Role services' column has a list of services with checkboxes: 'Certification Authority' (checked), 'Certificate Enrollment Policy Web Service' (unchecked), 'Certificate Enrollment Web Service' (unchecked), 'Certification Authority Web Enrollment' (checked and highlighted), 'Network Device Enrollment Service' (unchecked), and 'Online Responder' (unchecked). The 'Description' column for 'Certification Authority Web Enrollment' says: 'Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.' At the bottom, there are buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

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

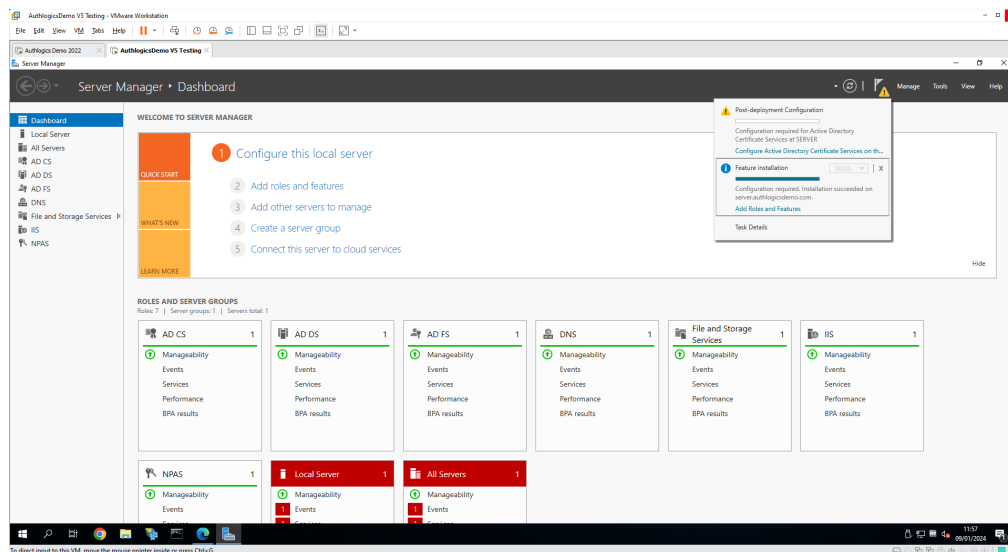
The screenshot shows the 'Add Roles and Features Wizard' window at the 'Confirm installation selections' step. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Confirm installation selections'. On the right, it says 'DESTINATION SERVER server.authlogicsdemo.com'. On the left, the navigation pane shows steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services', 'Confirmation' (highlighted), and 'Results'. The main area has the text: 'To install the following roles, role services, or features on selected server, click Install.' Below this is a checkbox labeled 'Restart the destination server automatically if required' which is checked. A note says: 'Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.' Below the note is a list box containing the following items: 'Active Directory Certificate Services' (with sub-items 'Certification Authority' and 'Certification Authority Web Enrollment'), 'Remote Server Administration Tools' (with sub-items 'Role Administration Tools', 'Active Directory Certificate Services Tools', and 'Certification Authority Management Tools'), 'Web Server (IIS)' (with sub-items 'Web Server' and 'Application Development'), and 'AD CS' (partially visible). At the bottom, there are buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. There are also links for 'Export configuration settings' and 'Specify an alternate source path'.

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

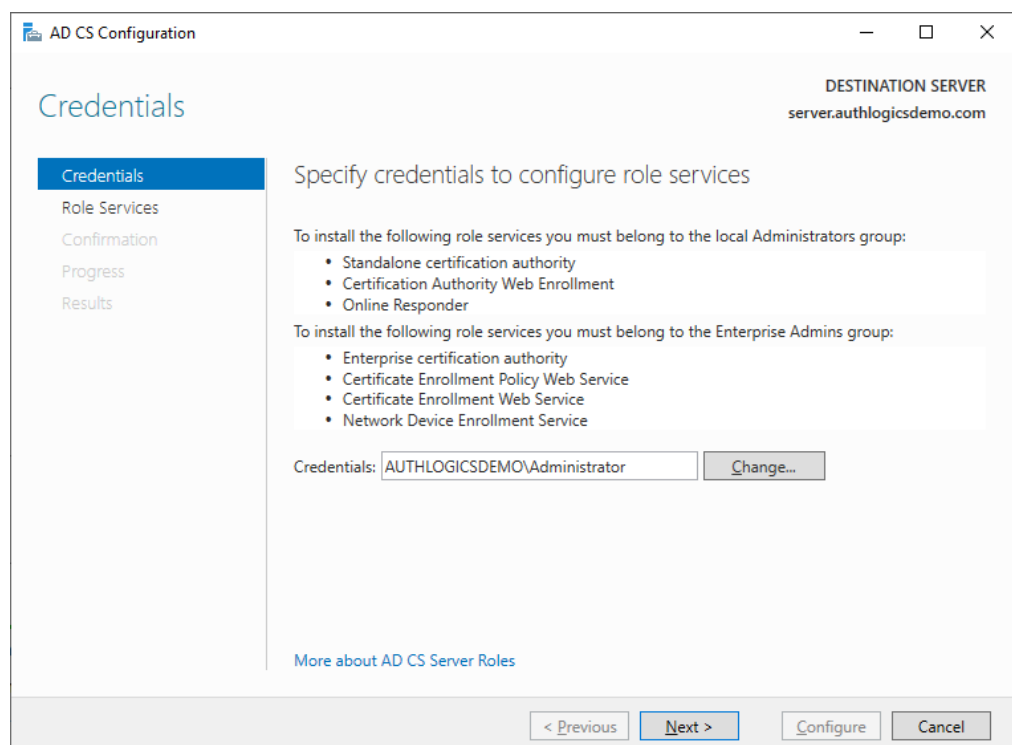


13. When the installation is complete, click **Close**.

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.

The screenshot shows the 'AD CS Configuration' wizard at the 'Role Services' step. The left sidebar lists steps: Credentials, Role Services (selected), Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Select Role Services to configure'. It lists several services with checkboxes: 'Certification Authority' (checked), 'Certification Authority Web Enrollment' (checked and highlighted with a dashed border), 'Online Responder' (unchecked), 'Network Device Enrollment Service' (unchecked), 'Certificate Enrollment Web Service' (unchecked), and 'Certificate Enrollment Policy Web Service' (unchecked). At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The top right corner indicates the 'DESTINATION SERVER' as 'server.authlogicsdemo.com'.

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

The screenshot shows the 'AD CS Configuration' wizard at the 'Setup Type' step. The left sidebar lists steps: Credentials, Role Services, Setup Type (selected), CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the setup type of the CA'. It explains that Enterprise CAs use Active Directory Domain Services (AD DS) to simplify certificate management, while Standalone CAs do not. There are two radio button options: 'Enterprise CA' (selected and highlighted with a dashed border) and 'Standalone CA'. Below 'Enterprise CA', it states 'Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.' Below 'Standalone CA', it states '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).' At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The top right corner indicates the 'DESTINATION SERVER' as 'server.authlogicsdemo.com'.

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

The screenshot shows the 'AD CS Configuration' wizard window. The title bar includes standard window controls and the text 'AD CS Configuration'. The 'DESTINATION SERVER' is listed as 'server.authlogicsdemo.com'. On the left, a navigation pane lists steps: Credentials, Role Services, Setup Type, CA Type (highlighted), Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'CA Type' and contains the text: '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.' There are two radio button options: 'Root CA' (selected) and 'Subordinate CA'. Below the 'Root CA' option is a note: 'Root CAs are the first and may be the only CAs configured in a PKI hierarchy.' Below the 'Subordinate CA' option is a note: 'Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.' A link 'More about CA Type' is at the bottom left of the main area. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

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

The screenshot shows the 'AD CS Configuration' wizard window at the 'Private Key' step. The title bar includes standard window controls and the text 'AD CS Configuration'. The 'DESTINATION SERVER' is listed as 'server.authlogicsdemo.com'. On the left, a navigation pane lists steps: Credentials, Role Services, Setup Type, CA Type, Private Key (highlighted), Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Private Key' and contains the text: 'Specify the type of the private key. To generate and issue certificates to clients, a certification authority (CA) must have a private key.' There are two radio button options: 'Create a new private key' (selected) and 'Use existing private key'. Below 'Create a new private key' is a note: 'Use this option if you do not have a private key or want to create a new private key.' Below 'Use existing private key' are three sub-options: 'Select a certificate and use its associated private key' (with a note: 'Use this option to ensure continuity with previously issued certificates when reinstalling a CA. 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' (with a note: 'Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.'), and 'Select an existing private key on this computer' (with a note: 'Select this option if you have retained private keys from a previous installation or want to use a private key from an alternate source.'). A link 'More about Private Key' is at the bottom left of the main area. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

6. Click **Next**.

The screenshot shows the 'Cryptography for CA' step in the 'AD CS Configuration' wizard. The left sidebar lists the steps: Credentials, Role Services, Setup Type, CA Type, Private Key, **Cryptography**, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the cryptographic options'. It includes a 'Select a cryptographic provider:' dropdown set to 'RSA#Microsoft Software Key Storage Provider' and a 'Key length:' dropdown set to '2048'. Below this is a 'Select the hash algorithm for signing certificates issued by this CA:' list box with options: SHA256 (selected), SHA384, SHA512, SHA1, and MD5. There is an unchecked checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' and a link 'More about Cryptography'. At the bottom are buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed as 'server.authlogicsdemo.com'.

7. Click **Next**.

The screenshot shows the 'CA Name' step in the 'AD CS Configuration' wizard. The left sidebar lists the steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, **CA Name**, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the name of the CA'. It includes a text box for 'Common name for this CA:' with the value 'authlogicsdemo-SERVER-CA'. Below it is a text box for 'Distinguished name suffix:' with the value 'DC=authlogicsdemo,DC=com'. A 'Preview of distinguished name:' text box shows 'CN=authlogicsdemo-SERVER-CA,DC=authlogicsdemo,DC=com'. There is a link 'More about CA Name'. At the bottom are buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed as 'server.authlogicsdemo.com'.

8. Click **Next**.

The screenshot shows the 'AD CS Configuration' wizard window. The title bar says 'AD CS Configuration'. The main heading is 'Validity Period'. On the right, it says 'DESTINATION SERVER server.authlogicsdemo.com'. On the left, there is a list of steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, **Validity Period** (highlighted), Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the validity period'. It contains the text 'Select the validity period for the certificate generated for this certification authority (CA):'. Below this is a text box with '5' and a dropdown menu with 'Years'. Below that is 'CA expiration Date: 09/01/2029 12:00:00'. Further down is a note: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' At the bottom right, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. At the bottom left, there is a link 'More about Validity Period'.

9. Click **Next**.

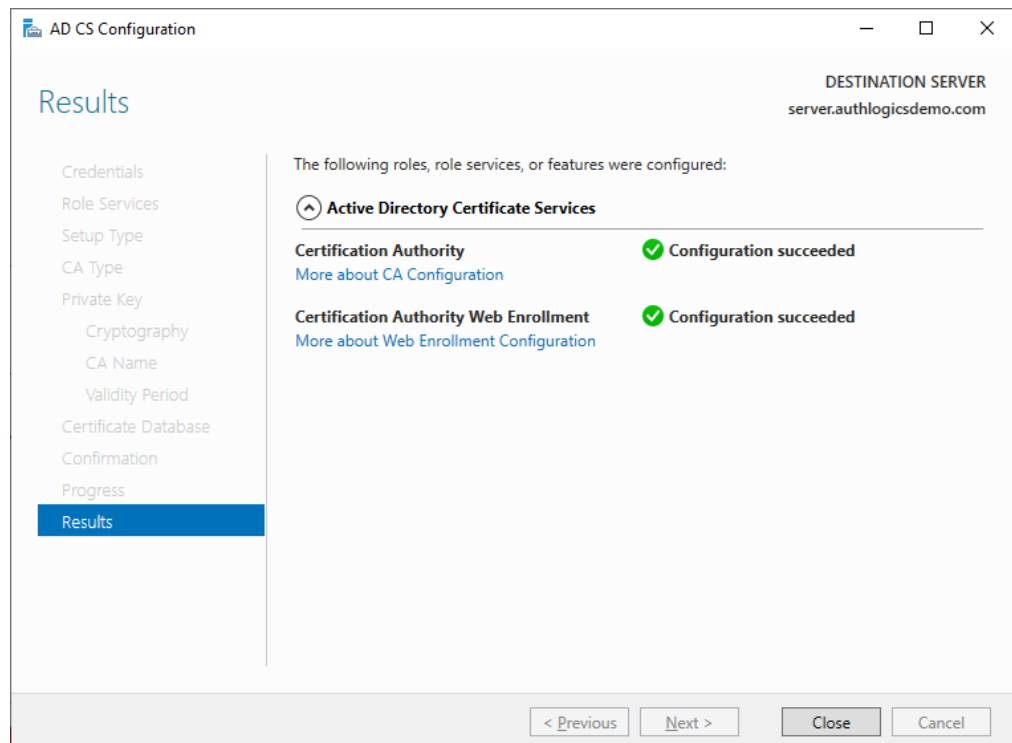
The screenshot shows the 'AD CS Configuration' wizard window. The title bar says 'AD CS Configuration'. The main heading is 'CA Database'. On the right, it says 'DESTINATION SERVER server.authlogicsdemo.com'. On the left, there is a list of steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, **Certificate Database** (highlighted), Confirmation, Progress, and Results. The main area is titled 'Specify the database locations'. It contains two text boxes. The first is labeled 'Certificate database location:' and contains 'C:\Windows\system32\CertLog'. The second is labeled 'Certificate database log location:' and contains 'C:\Windows\system32\CertLog'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. At the bottom left, there is a link 'More about CA Database'.

10. Click **Configure**.

The screenshot shows the 'AD CS Configuration' window in the 'Confirmation' step. The left sidebar lists the configuration steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation (highlighted), Progress, and Results. The main area is titled 'Confirmation' and shows the 'DESTINATION SERVER' as 'server.authlogicsdemo.com'. Below this, it says 'To configure the following roles, role services, or features, click Configure.' A dashed box highlights 'Active Directory Certificate Services'. The 'Certification Authority' section lists the following details: 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. The 'Certification Authority Web Enrollment' section is also listed. At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

The screenshot shows the 'AD CS Configuration' window in the 'Progress' step. The left sidebar lists the configuration steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress (highlighted), and Results. The main area is titled 'Progress' and shows the 'DESTINATION SERVER' as 'server.authlogicsdemo.com'. Below this, it says 'The following roles, role services, or features are being configured:'. A progress bar is shown with the text 'Configuring...'. The 'Active Directory Certificate Services' section lists the following details: Certification Authority and Certification Authority Web Enrollment. At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

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.

