

MyID MFA and PSM

Version 5.3.2

MyID Authentication Server Installation and Configuration 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

MyID Authentication Server Installation and Configuration Guide	1
Copyright	2
Conventions used in this document	3
Contents	4
1 Introduction	9
1.1 Considerations	9
1.1.1 System requirements	9
1.1.2 Rights and permissions	10
1.1.3 Password Breach Databases	10
1.1.4 High availability	11
1.1.5 Database backup and restoration	11
1.1.6 Developers	11
1.1.7 Language requirements	11
1.1.8 Internet Information Services requirements	12
1.2 Internet connectivity	12
1.2.1 Mobile Push Authentication	12
1.2.2 Password Breach Database	12
1.2.3 Licensing	13
1.3 Licensing	13
1.3.1 License functionality	13
1.3.2 Evaluation license	13
1.3.3 Free license	13
2 Design and deployment scenarios	14
2.1 Mobile push authentication	15
2.1.1 Overview	15
2.1.2 Public Push Networks	15
2.2 Passwordless MFA	15
2.2.1 Mobile Push	15
2.2.2 Passwordless for Windows	15
2.2.3 The MyID Server Password Vault	16
2.2.4 The Windows Desktop Agent	16
2.2.5 The Domain Controller Agent	18
2.3 Active Directory permissions	19
2.4 Integration with MyID CMS	20
2.4.1 Required information	21
2.4.2 High Availability integration	21
2.5 Deployment checklist	22
3 Multi-Factor Authentication technology	23
3.1 Mobile Push authentication technology	25
3.2 Grid Pattern technology	27
3.2.1 How it works – example	27
3.2.2 Grid sizes	28
3.3 Phrase authentication technology	31

3.3.1 Authentication scenario #1 – deviceless authentication	32
3.3.2 Authentication scenario #2 – multi-factor authentication	32
3.4 One Time Code technology	33
3.5 Standard OATH TOTP	34
3.6 YubiKey OTP	35
3.7 FIDO Passkeys for the Enterprise	36
3.7.1 Windows Managed Password for FIDO credentials	37
3.8 Authentication Technology against Factor type	38
3.9 Automatic MFA determination and SSO assurance levels	39
3.9.1 Hierarchy	39
3.10 Federation server	40
3.10.1 ADFS replacement	40
4 Deployment	41
4.1 High Availability and certificates	42
4.2 Installing the MyID Authentication Server	45
4.3 Uninstalling the MyID Authentication Server	49
4.3.1 Active Directory metadata	50
4.4 Updates and upgrades	50
4.5 Installing an update	51
4.6 Installing an upgrade	55
4.6.1 Upgrading from version 4.2	57
4.6.2 Windows Desktop Agent compatibility	57
4.7 Certificate export and import	58
4.7.1 Exporting a certificate from an existing MyID Authentication Server	58
4.7.2 Import a certificate to a new MyID Authentication Server	65
4.8 MyID Authentication Server Directory configuration	71
4.8.1 Directory Configuration Wizard	71
4.8.2 Add users to the MyID Administrators Group	74
4.9 MyID license configuration	75
4.9.1 Getting a free 10 user license or a 30-day trial license	75
4.9.2 Importing an offline license file	79
4.9.3 Entering an existing license key	82
4.10 MyID Password Security Management Wizard	84
4.10.1 Starting the Password Security Management Wizard	85
4.11 YubiKey OTP Configuration Wizard	93
4.11.1 Starting the YubiKey OTP Configuration Wizard	93
5 Administering the MyID Authentication Server	98
5.1 MyID Management Console views	98
5.1.1 OUs / Containers view	99
5.1.2 All Users view	99
5.1.3 Updating PSM users	100
5.2 MyID Authentication Server overview	105
5.2.1 Server details	105
5.2.2 Licensing information	106
5.2.3 Debugging tools	106

5.3 Global settings walkthrough	107
5.3.1 General tab	109
5.3.2 RADIUS tab	110
5.3.3 Alerts tab	112
5.3.4 Remediation tab	113
5.3.5 Schedule tab	115
5.3.6 SMTP Delivery tab	116
5.3.7 SMS Delivery tab	118
5.3.8 Licence tab	121
5.3.9 Authenticator App tab	123
5.3.10 Certificates tab	124
5.3.11 Grid Pattern Policy tab	125
5.3.12 Grid Options tab	127
5.3.13 Phrase tab	128
5.3.14 One Time Code tab	129
5.3.15 YubiKey OTP tab	130
5.3.16 FIDO2 tab	131
5.3.17 MyID CMS tab	133
5.4 Domain settings	134
5.4.1 Domain Properties dialog	135
5.5 Applications	138
5.5.1 Applications Properties	140
5.5.2 Self Service Portal Properties	147
5.5.3 Web Management Portal Properties	156
5.5.4 Windows Desktop Agent Properties	165
5.5.5 OpenID Connect application properties	172
5.5.6 Client Credential applications properties	184
5.5.7 SAML 2.0 application properties	192
5.5.8 Accessing applications through the IdP page	204
5.6 Adding new applications	205
5.6.1 Creating an OpenID Connect application	207
5.6.2 Creating a client credential application	212
5.6.3 Creating a SAML 2.0 application	216
5.7 Adding External Identities	223
5.7.1 Creating an OpenID Connect External Identity (Google)	225
5.7.2 Creating an OpenID Connect External Identity (Microsoft)	229
5.8 Adding users and user functionality	233
5.8.1 Adding a new realm	234
5.8.2 User account types – MFA or PSM	235
5.8.3 Adding a new MyID user account	236
5.8.4 Adding a new MyID PSM user account	244
5.8.5 Adding a new external MFA user account	249
5.8.6 Setting up a user for Grid Pattern Authentication	254
5.8.7 Setting up a user for Phrase authentication	262
5.8.8 Setting up a user for One Time Code	269

5.8.9 Setting up a user for YubiKey OTP	275
5.8.10 Adding a YubiKey device	281
5.9 Managing existing users	285
5.9.1 Managing a user's base settings	286
5.9.2 Multi-Factor devices assigned to a user account	293
5.9.3 Managing a user's Grid Patterns	294
5.9.4 Managing a user's Phrases	295
5.9.5 Managing a user's One Time Codes	296
5.9.6 Managing a user's YubiKey OTP	298
5.9.7 Managing user passwords	299
5.9.8 Assigning temporary access codes to a user	302
5.9.9 Revoking specific users' refresh tokens	304
5.10 Roles	306
5.10.1 Active Directory Group types for roles	307
5.10.2 Administrator role views	308
5.10.3 Managing administrative roles	310
5.10.4 Managing the Auditors role	313
5.10.5 Managing the Password Security Management Users role	314
5.10.6 Managing the Remediation and Alerts Exclusion role	316
5.11 Policies	319
5.11.1 Access control policies	319
5.12 Customizing the portal interfaces	325
5.12.1 Portal authentication type settings	325
5.12.2 Self Service Portal password tooltips	326
5.12.3 IdP Logon Page customization	330
5.12.4 SSP customization	331
5.12.5 Advanced Self Service Portal UI customization	334
5.13 RADIUS communication	336
5.13.1 Mobile Push MFA	337
5.13.2 2-step logons (Access-Challenge)	337
5.13.3 RADIUS extensions	337
5.13.4 RADIUS server ports and protocols	337
5.13.5 Adding a RADIUS client	338
5.13.6 RADIUS policies	341
6 Configuring MyID CMS settings	342
7 Configuring the PSM password policy	344
7.1 Configuring the MyID Password Policy settings	344
7.1.1 The PSM Users role	344
7.2 Main settings	345
7.2.1 Primary password policy	345
7.2.2 Exception password policy	359
7.3 Modifying the default domain policy	360
7.4 Security phrases	361
7.5 Configuring custom password blacklist checking	362
7.5.1 Wildcard usage within local blacklist	362

7.6 Advanced password checking	364
7.6.1 Heuristic scanning	364
7.6.2 Password stemming	365
7.6.3 Using both heuristic scanning and password stemming	366
8 Advanced configuration	367
8.1 Specifying Active Directory Domain Controllers	368
8.1.1 Specifying Global Catalog Servers	368
8.1.2 Specifying Domain Controllers	368
8.2 Adding a trusted SSL certificate for secure connections	369
8.3 Active Directory timing	369
8.3.1 Domain access timeout	369
8.3.2 Domain Controller refresh	369
8.4 Diagnostics logging	370
8.4.1 Enabling logging	370
8.4.2 Setting the logging location	370
8.4.3 Setting the retention time for rolling logs	370
8.4.4 Size limit of rolling log files	371
8.4.5 Example of rolling logs	372
8.4.6 Enabling verbose logging	373
9 Integration with external systems	375

1 Introduction

MyID Authentication Server is a multi-factor authentication system that provides:

- Token, tokenless, device, and deviceless Multi-Factor Authentication.
- Mobile Push Authentication.
- A NIST 800-63B compliant Password Security Management solution.
- Self-service password reset and unlocking.
- Web Service API and RADIUS interfaces for connectivity.
- Multiple Authentication technologies:
 - Grid Pattern – pattern-based authentication.
 - Phrase – random character authentication.
 - One Time Code – OATH (TOTP) compliant authentication.
 - YubiKey – Yubico YubiKey hardware token support.
 - FIDO2 / Passkey authentication.
 - Google / Microsoft Authenticators (OATH compliant).

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.

1.1 Considerations

1.1.1 System requirements

The supported operating systems for MyID Authentication Server are:

- Windows Server 2025
- Windows Server 2022

Note: The MyID Reporting Dashboard requires the Microsoft KB5023705 update, or the latest Windows Updates, on Windows Server 2022. This is due to a known OS issue listed by Microsoft as:

This update addresses an issue that affects the Get-WinEvent cmdlet. It fails. The system throws `InvalidOperationException`

- Windows Server 2019
- Windows Server 2016

Each machine running MyID Authentication Server requires .NET 8 Desktop Runtime; this is installed with the MyID Authentication Server.

The hardware requirements for MyID Authentication Server are:

	Minimum	Recommended
CPU	Dual Core 1.2 GHz	Quad Core 2.5 GHz
RAM	4Gb RAM	8Gb RAM
Disk	Single Disk	Dual Disk

1.1.2 Rights and permissions

Local administrator rights are required to perform the installation process of the MyID Authentication Server on a Windows Server.

The Directory Configuration Wizard requires either:

- Enterprise Admin rights, or:
- Domain Admin rights on the following:
 - The domain of which the Authentication server is a member.
 - Each domain containing user accounts that will be used with MyID.

Once the Directory Configuration Wizard is complete, administrators need to be a member of the MyID Administrators group and have local administration rights on the member server.

1.1.3 Password Breach Databases

Intercede has the following versions of its Password Breach Database:

- Offline Password Breach Database (Min)

This is the minimum offline database. It is included by default with MyID Authentication Server and contains the top one million breached passwords.

This is infrequently updated.

- Offline Password Breach Database (Full)

This is the full offline database. It is a separate download containing over 8 billion breached passwords.

This is infrequently updated.

If you have multiple authentication servers, you may want to install the Offline Password Breach Database to a shared location rather than duplicating the database on each authentication server. For information on setting this up, see the *Installing the Offline Password Breach Database to a shared location* section in the Offline Password Breach Database Guide.

- Cloud Password Breach Database

An Internet hosted database containing over eight billion breached credentials.

This is regularly updated.

The Offline Password Breach Database can reduce the reliance on Cloud Password Breach lookups.

If a password is not found in the minimum Offline Password Breach Database, then, unless disabled by policy, the MyID Cloud Password Breach Database is also checked.

The full Offline Password Breach Database containing over eight billion breached passwords is available on request from Intercede Support.

When the full database is installed, it may be possible to disable Cloud Password Breach Database lookups.

Note: The MyID Cloud Password Breach Database is regularly updated, but the Offline Password Breach Database is not. Unless a fully offline solution is required, Intercede recommends leaving Cloud Password Breach Database lookups enabled to ensure that the most recent entries are being checked.

1.1.4 High availability

MyID is designed for multiple deployment sizes, topologies, and configurations.

High availability is achieved by ensuring that there are multiple instances of the user database and the authentication server.

To ensure the user database is highly available, there must be multiple Domain Controllers in each domain. Active Directory automatically replicates the domain information to all Domain Controllers in the domain, including MyID data.

To ensure high availability of the MyID Authentication servers, simply install multiple instances on separate servers that are members of the same AD Forest. Each server uses standard Windows mechanisms to locate and work with the most appropriate Domain Controller, or Domain Controllers and Global Catalogs can be manually specified. Each server can be addressed separately as a Primary/Secondary configuration, for example RADIUS1 and RADIUS2, or they can be clustered through the built-in Windows Network Load Balancing and treated as a single entity.

1.1.5 Database backup and restoration

All user metadata is stored in Active Directory and no data is stored on the local server. When you perform a standard Active Directory backup, all MyID data is automatically backed up along with the Active Directory.

You can recover your MyID data by reinstalling MyID MFA and PSM from the ground up – the new installation is re-attached to the existing data in the Active Directory and continues functioning as before. Exceptions to this include any custom changes to the web UI and NPS (RADIUS) policy changes.

1.1.6 Developers

For developer-specific information regarding the Web Services Application Programming Interface (REST), see the [MyID Authentication Server Developers Guide](#).

1.1.7 Language requirements

The MyID Authentication Server is compatible with multilingual versions of Windows Server; however, it is only available in English. Product support and documentation are also available only in English.

Elements of the Microsoft Management Console (MMC) are shown in the language of the server, for example **OK** buttons, however, text specific to MyID is in English only.

1.1.8 Internet Information Services requirements

You must have the Internet Information Services (IIS) feature installed on your MyID Authentication Server.

Important: Make sure you do *not* have WebDAV Publishing installed, as this can cause issues with the operation of the MyID Authentication Server. To check whether you have this feature installed, in the Server Manager, select **Add roles and features**. In the **Server Roles** list, expand **Web Server (IIS) > Web Server > Common HTTP Features** and make sure **WebDAV Publishing** is not selected.

If you enable WebDAV Publishing, this may conflict with the MyID Authentication Server; for example, when attempting to remove an authentication device in the Self Service Portal, the system may stop responding, caused by the web server returning a 405 Method Not Allowed error.

1.2 Internet connectivity

The MyID Authentication Server requires Internet Access for certain functions. The majority of required connectivity is outbound to the Internet. All URLs are bound to the `authlogics.com` DNS domain for easier management.

You may not require all access, depending on your chosen product functionality.

1.2.1 Mobile Push Authentication

When using Mobile Push authentication for MFA, the MyID Authentication Server requires outbound Internet access to the following destination (depending on the capabilities of the network firewall):

Destination URL:

`https://*.ccp.authlogics.com/api/*`

Host:

`*.ccp.authlogics.com` on port 443

Note: Devices running the Authlogics Authenticator app also require access to the above URL. While this would normally be available when they are connected to GSM / public networks, they may require explicit access when on corporate Wi-Fi.

1.2.2 Password Breach Database

When using Password Security Management and the MyID Cloud Password Breach Database lookups are enabled, the MyID Authentication Server requires outbound Internet access to the following destination (depending on the capabilities of the network firewall):

Destination URL:

`https://passwordsecurityapi.authlogics.com/api/*`

Host:

`passwordsecurityapi.authlogics.com` on port 443

Note: Domain Controller Agents do not require direct access to the Internet as they perform lookups using the Authentication Server. However, there is a GPO setting to enable Internet access as a fallback and, if enabled, Internet access is required.

1.2.3 Licensing

Unless an offline license has been provided, the MyID Authentication Server requires outbound Internet access to the following destination (depending on the capabilities of the network firewall):

Destination URL:

`https://licencing.authlogics.com/api/*`

Host:

`licencing.authlogics.com` on port 443

Warning: If access to the licensing URL is not available the license may fail, and the Authentication Server may cease to function.

1.3 Licensing

MyID MFA and PSM solutions are licensed on a per-user basis with each user requiring a license. A license must be installed onto each instance of a MyID Directory. Contact sales@intercede.com for any licensing enquiries.

To install a MyID license, run the Licence Configuration Wizard within the MyID Authentication Server Management Console.

1.3.1 License functionality

The functionality available in the MyID Authentication Server depends on the types of license that you have installed. All solution features are broken down into two license types:

- Password Security Management (PSM)
- Multi-Factor Authentication (MFA)

A product key or license is issued for each license type.

Note: For detailed information on the license types please refer to the license agreement document embedded within the installation package.

1.3.2 Evaluation license

MyID is available for trial use for an unlimited number of users with a 30-day time-limit. You can request and instantly install an evaluation license through the Licence Configuration Wizard.

1.3.3 Free license

MyID MFA and PSM solutions are available free of charge for up to ten users with no time limit. You can request and instantly install a free license through the Licence Configuration Wizard.

2 Design and deployment scenarios

The MyID Authentication Server is an enterprise-class solution scaling from stand-alone single instance installations to highly availability multi-master Active Directory-integrated deployments. A single MyID server can support multiple Active Directory Domains in a single forest and the server can be a member of any domain within the forest. User accounts can be Active Directory user accounts or external accounts which do not have an Active Directory user account.

A variety of authentication tokens can be used with the MyID Authentication Server including SMS/Text message, email, offline OTP (pattern or OATH), Mobile Push, biometrics, FIDO2, Passkey, and YubiKey hardware tokens.

The MyID Authentication Server is designed to integrate with a multitude of remote access solutions and applications. The core of MyID is the Authentication Server, which is an IdP Server and also provides REST APIs and a RADIUS interface. MyID also provides agents for various third-party systems to allow for direct integration; for example, Windows Desktop, Remote Desktop Gateway, and Exchange Servers.

Any remote access concentrator or application that can interact with REST Services or RADIUS can communicate with the MyID Authentication Server. Integration guides and sample code are provided for common deployments to assist with the integration into third-party systems.

The MyID Authentication server is a Federated Identity Provider (IdP) capable of being used as a replacement for ADFS and supports standard protocols of SAML 2.0 and OpenID Connect.

The MyID Authentication Server is a complete NIST 800-63B compliant password policy and management solution for Active Directory. It can ensure that users are not using known breached or shared passwords in real-time, as well as with retrospective checking and automatic remediation.

The MyID Authentication Server Management console uses Microsoft Management Console technology. Administration rights are granted through roles that are typically mapped to Active Directory groups.

For high-availability deployment scenarios with numerous users, user information can be stored across multiple domains in an Active Directory Forest. Multiple MyID servers can be deployed within an Active Directory Forest for multiple points of presence, or in the same location with built-in Network Load Balancing for full High Availability.

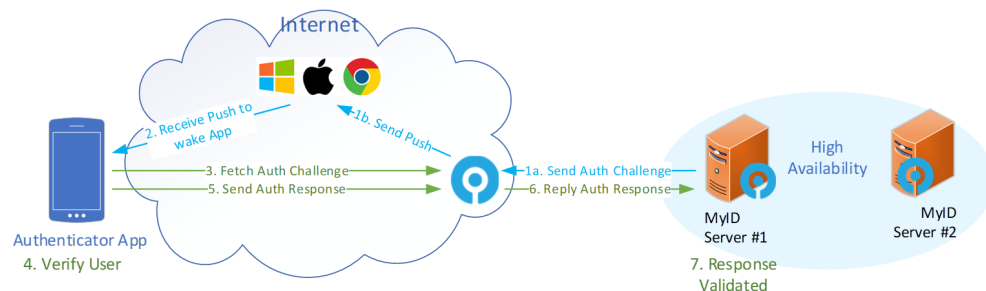
2.1 Mobile push authentication

2.1.1 Overview

MyID Mobile Push MFA is designed to work seamlessly when online or offline, and does not rely on Microsoft, Apple, or Google for timely delivery.

If the user is offline, they can enter a short alpha-numeric OTP generated by the same MyID Authenticator app they use when they are online.

MyID MFA Mobile Push MFA Logon Process Flow



2.1.2 Public Push Networks

App notifications through the Microsoft, Apple, and Google Public Push Networks can be unreliable and they are not a guaranteed delivery service. MyID does not rely on Public Push Networks for core functionality; therefore, no authentication data or sensitive information is contained within the Public Push Networks notification.

If the Public Push Networks are functioning as expected, it creates a better user experience, however, if not then the user can still load the Authenticator App themselves and log in as normal.

2.2 Passwordless MFA

2.2.1 Mobile Push

Mobile Push MFA is most commonly deployed as a passwordless authentication solution; however, it can be used in conjunction with a password if required.

This can be connected to applications through RADIUS, Web API, or various agents including for Windows Desktop Agent.

2.2.2 Passwordless for Windows

The MyID Windows Desktop Agent allows users to log on to Windows without having to enter their Windows password. This form of passwordless logon is achieved by storing the Active Directory Password in a secure password vault that is seamlessly delivered to the Windows desktop on the user's behalf when logging on.

Logging on to Windows in this way ensures compatibility with existing Windows applications that rely on Active Directory credentials. Passwordless logon is disabled by default and can be enabled by setting the **Enable Passwordless Logon** group policy option on the Windows Desktop Agent to remove the Active Directory password for logon.

2.2.3 The MyID Server Password Vault

The MyID Authentication Server uses Active Directory as a database. Therefore, all its data is physically stored on the Domain Controllers, including the Server Password Vault. The password vault is disabled by default and must be explicitly enabled before use.

During the MyID Authentication Server installation, a unique certificate is generated with an RSA 2048-bit key pair; this is used to encrypt the password data. This certificate can be replaced at any time by running the Certificate Configuration Wizard on the server, which re-encrypts the data with the new certificate key pair. The MyID Password Vault information can only be decrypted if the certificate's private key is available.

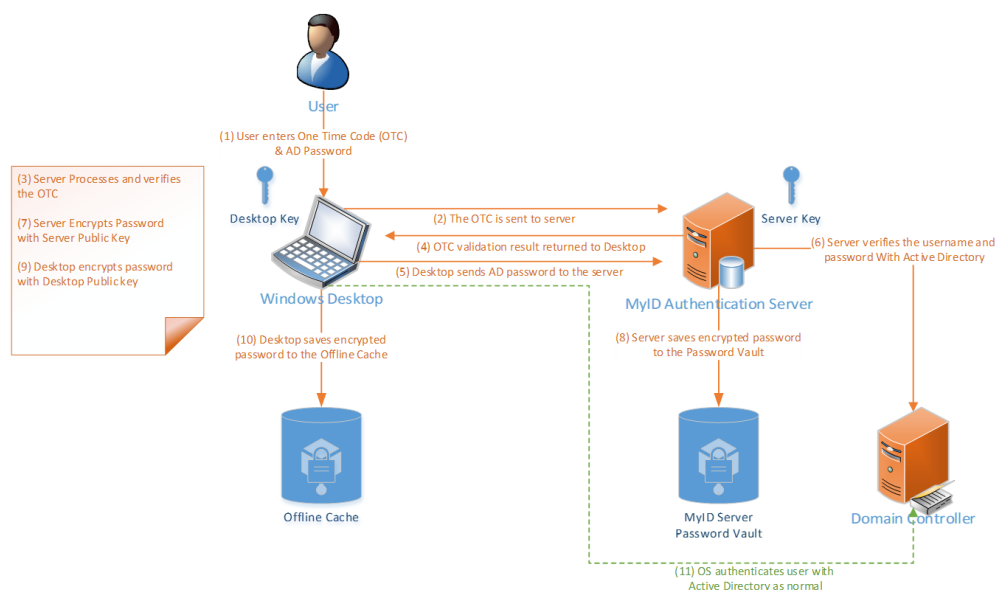
2.2.4 The Windows Desktop Agent

The Windows Desktop Agent is designed to run on a Windows desktop or Windows server machine to provide Multi-Factor Authentication security and Passwordless logons. The agent is fully managed and deployable through Active Directory group policy options for easy and granular administration.

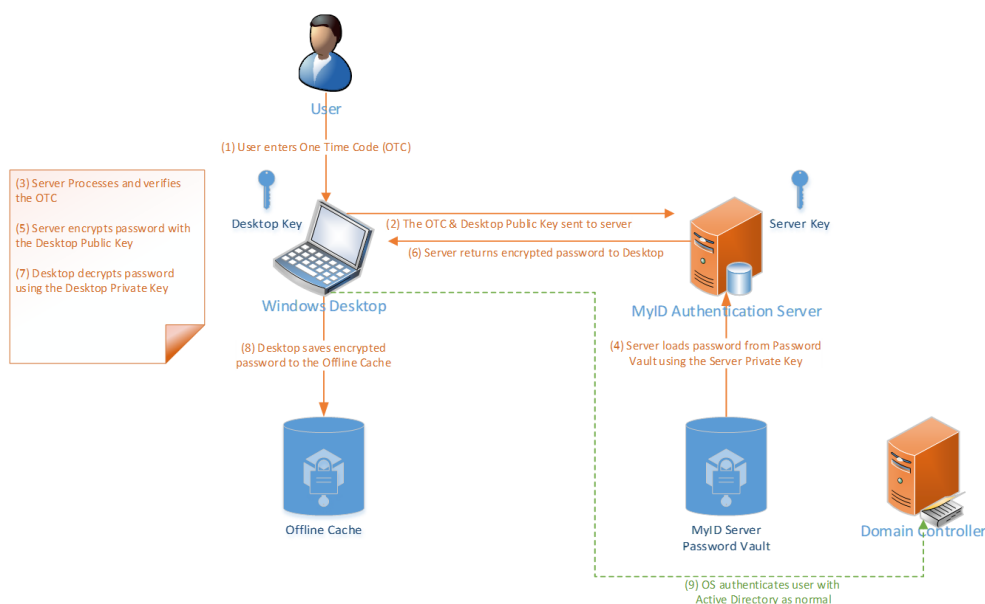
The agent can work in an offline scenario if there is no connection available to the MyID Authentication Server.

For more information, see the [Windows Desktop Agent Integration Guide](#).

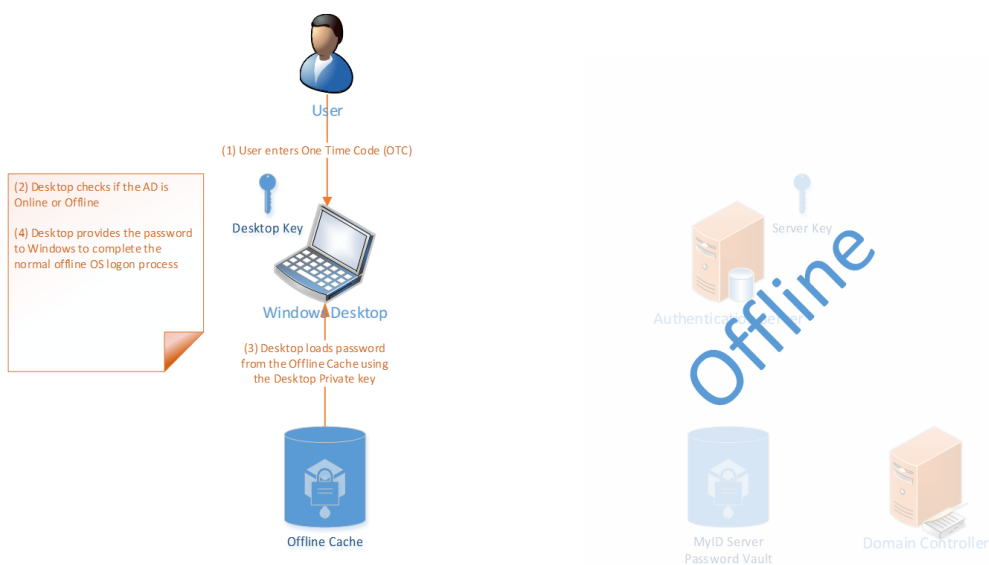
MyID MFA Windows Desktop Password-less logon process First Online Logon



MyID MFA Windows Desktop Password-less logon process Regular Online Logon



MyID MFA Windows Desktop Password-less logon process Regular Offline logon

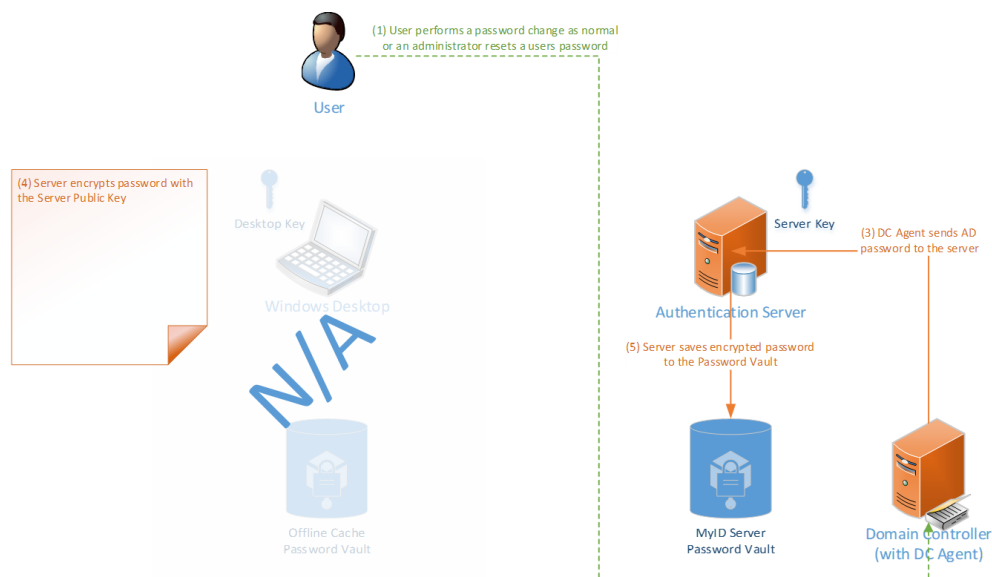


2.2.5 The Domain Controller Agent

The Domain Controller Agent is a lightweight service designed to capture password changes made on the Windows Domain, process them against policy to see if they comply, and store them securely in the MyID Server Password Vault. This ensures that all new passwords comply with the latest NIST SP 800-63B guidance.

The Domain Controller Agent also keeps the Active Directory password database and the MyID Server Password Vault synchronized at all times regardless of which mechanism is used to change or reset an Active Directory password. Administrators can use Domain Controller Agent to ensure that passwords used within the environment are unique and to prevent users from sharing passwords internally.

MyID MFA Active Directory Password-less AD password change capture



2.3 Active Directory permissions

The following groups are created in the Windows Domain that is selected when you first run the Directory Configuration Wizard. Members of the Enterprise Admins and Domain Admins group *always* have full access to MyID independently of these groups. This behavior cannot be changed due to the Active Directory security model that means that members of these groups always can take ownership of *any* object and change its permissions.

Group name	Type	Members	Member of	Provides access to
MyID Authentication Server Administrators	Universal Group	The installation user account.	Builtin Administrators.	Full admin access to the MMC and Web Management Portal.
MyID Authentication Server Operators	Universal Group	No members by default.	Not a member of any group.	Limited admin access only through the Web Management Portal.
MyID Authentication Servers	Universal Group	The Authlogics server account.	Builtin Administrators.	Full access to directory info.

If you are upgrading from V4.x Authentication Server deployments, the pre-existing Active Directory groups originally created remain. These Active Directory security groups are:

Group name	Type	Members	Member of	Provides access to
Authlogics Administrators	Universal Group	The installation user account.	Builtin Administrators.	Full admin access to the MMC and Web Management Portal.
Authlogics Operators	Universal Group	No members by default.	Not a member of any group.	Limited admin access only through the Web Management Portal.
Authlogics Servers	Universal Group	The Authlogics server account.	Builtin Administrators.	Full access to directory info.

Note: The Builtin Administrators group has full administrator access to the Domain Controllers and the Active Directory. Unlike the Domain Admins group, the Builtin Administrators group does not have administrator access to any member servers in the domain, as it is a Domain Local security group.

For information regarding granular application of rights within the Active Directory, contact Intercede customer support.

For further information about Active Directory groups and permissions, see:

docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/appendix-b--privileged-accounts-and-groups-in-active-directory

2.4 Integration with MyID CMS

MyID CMS can manage MyID Authentication Server user accounts.

The integration is performed through the MyID WebAPI which must be configured prior to use.

MyID CMS must be configured to connect to the MyID Authentication Server through the MFA Broker. This enables MyID CMS to create MyID Authentication Server users, provision MFA technologies, and change various account settings. For more information about the MFA Broker, contact your Intercede account manager.

The MyID Authentication Server can notify MyID CMS when an event occurs, such as a user completes setting up a new MFA device. To facilitate this configuration of MyID CMS, information is required in the MyID Authentication Server.

Note: MyID CMS version 12.9 or higher is required for integration.

2.4.1 Required information

The following information is required complete the integration:

- The MyID CMS Server URL

For example:

```
https://myid/web.oauth2
```

- The MyID CMS Callback URL

For example:

```
https://myid/MFABroker
```

- The MyID CMS Client ID used to authenticate

For example:

```
myid.notifications
```

- The MyID CMS Client Scope used to authenticate

For example:

```
myid.notifications.basic
```

- The MyID CMS Client Secret used to authenticate

For example:

```
4116e8f9-92e2-48b1-8616-5fb3d130b91d
```

See section [6, *Configuring MyID CMS settings*](#).

2.4.2 High Availability integration

You only need to configure your MyID CMS settings on *one* MyID Authentication Server and the settings are replicated to all the servers in the Active Directory Forest.

The MyID Authentication Server works on a multi-master High Availability model, not Active-Passive, therefore any MyID Authentication Server is able to update user account details.

Due to this, all MyID Authentication Servers must be able to access the **MyID CMS OAuth2 Authentication Service** and **MyID CMS MFA Broker Service** URLs.

MyID CMS can be configured to use any MyID Authentication Server for configuration changes. Specifying more than one server, or using a load balanced address, is recommended.

2.5 Deployment checklist

#	Item	Recommended	Check
1	A Physical or Virtual Machine to Operating System.	A Virtual Machine with 4 CPU cores and 8Gb RAM	
2	A Windows Server 2016 or higher OS on which to install MyID Authentication Server.	Windows Server 2019	
3	Internet Connectivity (HTTPS) from MyID Server for licensing and activation.	Allow the destination of: <code>https://*.authlogics.com</code>	
4	An administrative account with rights to install the software and configure the directory service on the Active Directory root domain.	An Enterprise Admin or Domain Admin account	
5	Server downtime authorization to reboot the server post-installation.		
6	Email / SMTP server settings and credentials (if required) to allow the server to send email tokens and provision emails.	Use an Exchange server with integrated authentication.	
7	Plan the DNS name to use in the URL for the Self Service Portal that users use to access their account.	Use: <code>ssp.<mycompany>.com</code>	
8	PSM only: Plan the deployment of the password policy. Must apply to all Domain Controllers and MyID Authentication Servers.	Use the policy defaults where possible.	
9	Plan which MFA technology to provision users for.	Grid Pattern Authentication suits most use cases and is the most secure.	
10	Plan if MFA devices are to be used or only deviceless authentication.	Use MFA where high security or compliance is required, otherwise use deviceless for convenience while improving security over passwords.	
11	Plan which MyID agents to deploy or how to integrate with third-party systems.	Use the industry-standard RADIUS for networking equipment and the WebAPI for application integration.	
12	Plan which applications can use SSO / Federation (for example, SAML 2.0, OpenID Connect, or WS-Fed).	Use MyID IdP services or Microsoft ADFS with the MyID ADFS Agent is still supported.	

3 Multi-Factor Authentication technology

As the usage of Information Technology has increased exponentially, the need for security of these systems has increased proportionately. Traditionally, authentication is solely performed by the user providing a valid username and password. This is known as single-factor authentication as the user *knows* all parts of the authentication process. Passwords have been proven to be insecure, therefore additional authentication factors are now required.

The increase of security provided by multi-factor (typically two-factor) authentication is that users must now both *have something* and *know something* in the authentication process.

The *something* that they *have* is usually a physical hardware device, like a key fob, that generates a specific unique One Time Pin (OTP). This OTP must also be entered as part of the authentication process.

Although these hardware token devices have improved security significantly, they do have certain limitations and incur a cost overhead in both implementation and on-going maintenance. Furthermore, they typically still need to be used together with a password and therefore do not provide a path towards Passwordless logons.

Intercede provides a multitude of hardware and software-based authentication technologies and delivery mechanisms to suit many scenarios, all while keeping down the logistical overhead of hardware tokens down.

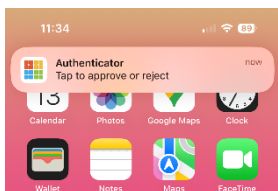
This chapter contains information on the following:

- Sending a notification to a user's phone to authenticate.
See section [3.1, Mobile Push authentication technology](#).
- Using a code derived from a grid of numbers or numbers and letters.
See section [3.2, Grid Pattern technology](#).
- Implementing a passphrase question and answer system.
Important: Phrase authentication technology is now deprecated for MFA. If you are currently using phrase authentication for MFA, you are recommended to migrate to a more secure type of authentication technology.
See section [3.3, Phrase authentication technology](#).
- Using an OATH RFC compliant two-factor authentication solution to deliver one-time codes through SMS or email.
See section [3.4, One Time Code technology](#).
- Using standard software OATH time-based one-time passwords (TOTPs) through tokens such as the Microsoft and Google Authenticator apps.
See section [3.5, Standard OATH TOTP](#).
- Using YubiKey USB tokens.
See section [3.6, YubiKey OTP](#).
- Using FIDO passkeys.
See section [3.7, FIDO Passkeys for the Enterprise](#).



- Information about how each authentication technology supports different authentication factors.
See section [3.8, *Authentication Technology against Factor type*](#).
- Automatically determining the most appropriate authentication technology for the user.
See section [3.9, *Automatic MFA determination and SSO assurance levels*](#).
- Using federation to share identity and authentication information between systems in a managed way.
See section [3.10, *Federation server*](#).

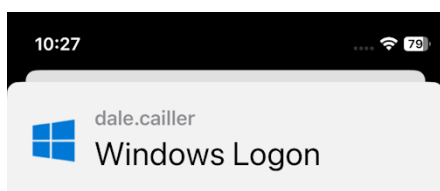
3.1 Mobile Push authentication technology

MyID Mobile Push is designed to simply send a notification to a user's phone to authenticate.



Once the notification is tapped, the MyID Authenticator app loads and the user may be required to authenticate with biometrics. The MyID Authenticator app was previously known as the Authlogics Authenticator app.


The user is presented with information about the logon and can choose to allow  or deny  the request.




Sign in request for Windows Desktop

Client: Windows Desktop
When: 30 June 2025 at 10:27:45
Where: Woking, United Kingdom



If the user taps the allow button , then the application they are trying to access completes its logon process.

However, if the user taps the deny button , they are asked why.

Why did you deny this request?

I did not make this request

I no longer want to logon

The answer is recorded on the MyID Authentication Server. If they stated they did not make this logon request, the server tracks future logon attempts and automatically throttles sending new Push requests to prevent MFA fatigue.

MyID Mobile Push helps to mitigate typical Push vulnerabilities:

- MFA fatigue protection:
 - Requires an initial offline logon for untrusted browser connections.
 - Dynamic throttling for legacy (for example, RADIUS) / non-browser channels when a logon attempt is **Denied** with a reason of `I did not make this request` recorded by the user.

If a user selects the `I no longer want to logon` reason, no throttling occurs.

For more information on Push authentication notification throttling, see section [5.9.1.4, Updating Push Authentication](#).

- Does not send any OTP or secret information through Apple or Google servers, so it therefore cannot be tampered with in transit.
- The MyID Authenticator App responds to a logon request when open, even if a network Push is not received through Apple or Google, to prevent denial of service attacks or network delays.

3.2 Grid Pattern technology

Grid Pattern authentication technology (formerly known as PINgrid) mitigates the security limitations of the traditional OTP tokens by generating a One Time Code derived from a grid of numbers or numbers and letters. These grids are specific to each user and change every minute, reflecting different characters. The additional security of Grid Pattern is that the user *also* needs to *know* a unique pattern to extrapolate an OTP.

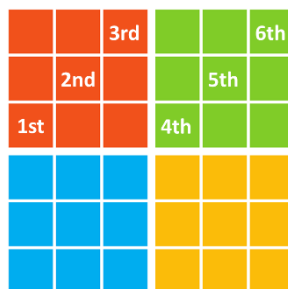
To protect against automated brute force attacks, MyID MFA includes **Account Lockout** functionality, where a user's account is locked out either indefinitely or for a pre-configured period when a passcode is entered incorrectly several times. Grid Pattern authentication mitigates even the threats of keylogging, screen scraping and shoulder surfing attacks.

Grid Pattern authentication is available in one, two, and three-factor authentication methodologies. You can view grids within an app, on a web page, sent via TEXT/SMS or email, or use them offline through the MyID Authenticator app in the App Store.

3.2.1 How it works – example

For simplicity, this example has a pattern of length 6. For better security, for a 6 x 6 grid, you are recommended to have a minimum pattern length of 8.

User pattern:



Pattern on a challenge grid:

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

One Time Code:

133125

In a 'Prove it!' situation the pattern is used with a challenge grid:

- A One Time Password (OTP) is hidden in the grid.
- Only the person who knows the secret pattern can find the OTP.

Grid Pattern authentication technology is a true One Time Pin authentication solution, as all valid passcodes entered can be used only once, even if the second authentication attempt occurs within the same period from the same device.

Note: Tokens can be sent only using email or SMS by clients that are *online*. No offline delivery is supported.

3.2.2 Grid sizes

4 x 4 and 5 x 5 grids display both numbers and letters for additional security. Characters that may cause confusion due to their similarities – for example 1 and i, 0 and o – are not used. Characters with descenders are also omitted; for example, y and p.

6 x 6 and 8 x 8 grids display numbers only.

You are recommended to use the 5 x 5 grid, as it is more secure. New installations of MyID CMS default to allowing 5 x 5 grids only.

3.2.2.1 4 x 4 grids

e	3	a	8
6	b	2	h
f	9	k	c
d	7	5	4

4 x 4 Grid Patterns have a default minimum length of 4.

3.2.2.2 5 x 5 grid

5	w	k	e	t
6	d	4	2	x
z	m	c	8	a
r	3	b	f	7
u	v	h	n	9

5 x 5 Grid Patterns have a default minimum length of 6.

3.2.2.3 6 x 6 grids

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

6 x 6 Grid Patterns have a default minimum length of 8.

3.2.2.4 8 x 8 grids

6	4	4	3	4	2	0	5
2	2	6	7	2	7	4	0
1	6	6	0	3	6	6	7
1	1	4	7	7	3	2	0
3	1	3	7	2	6	0	5
0	3	2	5	1	1	4	5
2	6	7	5	0	7	4	5
4	1	3	5	1	3	0	5

8 x 8 Grid Patterns have a default minimum length of 8.

3.3 Phrase authentication technology

Important: Phrase authentication technology is now deprecated for MFA. If you are currently using phrase authentication for MFA, you are recommended to migrate to a more secure type of authentication; see section 3, [Multi-Factor Authentication technology](#) for details of the available authentication technologies.

Phrase authentication (formerly known as PINphrase) uses some authentication methods that have become a generally accepted standard in the banking industry to provide a simple to use but efficient and cost-effective authentication solution.

Note: Multi-factor authentication Phrases are not the same as password security management security phrases. For information on security phrases, see section 7.4, [Security phrases](#).

Phrase authentication is based on a passphrase question and answer system that prompts the user to enter random characters from the answer to a randomly chosen question.

Unlike passwords, the answers to the questions are typically things that the user is unlikely to forget, which reduces helpdesk calls, limits resets, and further cuts costs. Since the user is only ever entering part of the answer, for example letters two, five and second last character, during each login the user is asked to enter different letters, and from different answers, making the response a One Time Code.

The full answer is not revealed during the login, which makes Phrase authentication ideal for both deviceless and Multi-Factor Authentication. Phrase authentication can also be configured to randomly select letters from different questions to further enhance security.

An administrator can configure multiple common questions for things that users generally know an answer for and can then specify how many of the questions a user must provide an answer for. For example, an administrator may set a scenario where the user must provide answers for at least four of the ten supplied questions.

By default, a user is assigned a Codeword – a randomly chosen dictionary word which can be used for first login.

Phrase authentication is based on a passphrase question and answer system that prompts the user to enter random characters from the answer to a randomly chosen question.

For example, a new user called Bob Jones is enabled and his mobile phone details are recorded. He provides answers to at least six questions from a pool. He chooses the following:

Question	Answer
Place of birth?	Seattle
Pet's name?	Tigger
Memorable place?	Springfield
Mother's maiden name?	Watson
Memorable date and time (YYYYMMDDHHMM)	201101021937
First school?	Winchester

3.3.1 Authentication scenario #1 – deviceless authentication

Bob wants to log on to an Internet banking site. He goes to the website and types in his username. He is then presented with a question from the answered pool. He is asked to enter specific characters from the answer.

Please provide the first, third, fourth and the last characters from your memorable place.

To authenticate, Bob enters: S R I D.

3.3.2 Authentication scenario #2 – multi-factor authentication

This requires a physical device that Bob receives the question and random positions (the soft token) on. Typically, this device is a mobile phone, as the mobile phone number is unique to the user.

Bob wants to log on to an Internet banking site. He goes to the website and types in his username. Once Bob enters his username, the Phrase authentication server detects that the logon process for Bob has started. A challenge is generated and sent as an SMS/Text message to Bob's mobile device as follows:

Phrase: Please provide the second, third, fifth, and penultimate characters from your place of birth.

To authenticate, Bob enters: A L S R.

A key part of MyID Phrase authentication is that both the deviceless and Multi-Factor methods have an identical look and feel to the user. The only difference is where the challenge message is displayed.

In cases where mobile phone reception cannot be guaranteed and instant message retrieval may not always be possible, Phrase authentication can pre-send tokens. Pre-sending tokens ensure that the user always has a token on their device prior to the authentication attempt. As soon as the token is used, the next token is sent to the user's mobile device ready to be used for the next login.

Note: Tokens can be sent only using email or SMS by clients that are *online*. No offline delivery is supported.

3.4 One Time Code technology

MyID One Time Code (formerly known as PINpass) is an OATH RFC compliant two-factor authentication solution which utilizes soft tokens to reduce the costs associated with hardware key fobs. One Time Code OTPs are delivered to mobile phones using SMS text messages or as an email for even more flexibility and cost savings.

One Time Codes give administrators the ability to pre-send one or more OTPs so that the user always has an OTP on their mobile device before logging on. As soon as the last OTP is used, then a new set of OTPs are sent to the user ready for future logon attempts.

Alternatively, a One Time Code can be used offline from the MyID Authenticator app in the App Store.

To increase security and convenience, administrators can configure users to provide an Active Directory password or static PIN with the One Time Pin. A static pin can be entered, before, after, or even in the middle of the OTP code making it more difficult for a key logger to differentiate between the OTC code and the user's static PIN.

When a user is configured with a real-time token and attempts to login, they enter their unique login name and One Time Code sends a six-to-eight-digit OTP to their mobile phone using SMS or an email address. The user then enters the OTC along with either their AD password or a static PIN, depending on the configuration.

The login process is similar for a user who is configured with a pre-send token, except that a code is not sent to the user after they enter their username as they already have a code on their phone. Instead, a new code is only sent after they login for use during the next login.

Note: Tokens can be sent only using email or SMS by clients that are *online*. No offline delivery is supported.

3.5 Standard OATH TOTP

MyID MFA supports standard software OATH time-based one-time passwords (TOTPs) through tokens such as the Microsoft and Google Authenticator apps. With this, users are no longer required to download the MyID Authenticator app (previously known as the Authlogics Authenticator app) and can add MyID MFA to their Microsoft and Google Authenticator app profile.

As with the MyID OTC solution, standard OATH authenticators use soft tokens to reduce the costs associated with hardware key fobs. One Time Code OTPs are generated on the mobile phones out-of-band without the need for the mobile device to have signal or sufficient data.

As with other MyID MFA technologies, Standard OATH support extends to offline logins for our MyID Authentication agents.

3.6 YubiKey OTP

If hardware tokens are required, MyID supports YubiKey OTP tokens from Yubico. YubiKey OTP tokens are USB devices that do not have a battery, do not expire, and work with any OS.

To increase security and convenience, administrators can configure users to provide an Active Directory password or static PIN with the YubiKey OTP token. A static pin can be entered, before generating the YubiKey OTP code to ensure that the multi-factor requirements are satisfied as there is something they *have* (the YubiKey token) and something they *know* (the static PIN).

3.7 FIDO Passkeys for the Enterprise

Passkeys are based on the FIDO standard and enable cryptography-based phishing-resistant authentication. By combining high security with a passwordless user experience, Passkeys are revolutionizing the consumer authentication experience.

However, it is difficult for enterprises to gain the benefits Passkey-based authentication brings, as by design they do not enable the level of management and integration enterprises require.

By bringing enterprise managed FIDO passkeys into the MyID MFA product, organizations can now easily FIDO-enable multiple applications and deploy passkeys to end users, enhancing security and improving the user experience.

MyID MFA acts as both a FIDO authentication server and a passkey issuance solution. End users authenticate to MyID MFA with their passkey, and by support for standard federated identity protocols, MyID MFA provides authentication services to multiple applications including cloud, on-premise, and Windows desktop logon.

Note: The FIDO Credential Provider does not work over RDP; the device is not passed through. If you plug a FIDO token in on the client, the token does not show up in the RDP session. FIDO token Web Sign-On and browser authentication over RDP work on Windows Server 2022, but not on Windows Server 2019.

There are multiple types of Passkeys supported by MyID MFA, enabling customers to choose the best balance of security and costs that fits their particular needs:

- Synchronizable Passkeys

Synchronizable Passkeys use an existing mobile phone to protect the private key used in the authentication process.

Able to communicate over the FIDO protocol built into multiple devices and web browsers, the phone simply acts as the user's security token and the user accesses the protected private key using fingerprint, face ID or a PIN, delivering secure, passwordless authentication with a simple user experience.

Synch-able passkeys can be backed up and restored using the mobile operating system's built in mechanisms, for example iCloud. This effectively deals with lost or replacement devices without having to reissue credentials.

- Device Bound Passkeys

Device Bound Passkeys are useful for organizations that want higher levels of security and control over where passkeys are. MyID MFA also supports device-bound passkeys such as those stored on a USB authenticator, for example YubiKey. Device-bound passkeys never leave the device, resulting in the highest levels of phishing resistance.

MyID MFA supports the innovative YubiKey Bio device, which enables users to replace a PIN with a simple match of a fingerprint, delivering a seamless authentication experience while maintaining the highest level of security.

3.7.1 Windows Managed Password for FIDO credentials

You can allow MyID MFA to create a random, 32-byte token as the user's Windows password.

You can use this token to log in to or unlock your desktop, as well as during permission request events in Windows. This allows for a fully passwordless Windows experience.

The token is securely encrypted using a symmetric key derived using the FIDO HMAC secret. MyID MFA then secures and associates the Windows password token with a FIDO device-bound passkey. The Windows password therefore can be recovered only when a successful FIDO authentication takes place.

When a user authenticates with a different FIDO authentication device, a new Windows password token is created for that device.

For information on implementing this feature, see section [5.3.16, FIDO2 tab](#).

3.7.1.1 Known issues

- **IKB-440 - Offline logon caches only the last successful FIDO authentication method**

When the **Manage the Windows password** option is enabled on the **FIDO2** tab of the global settings, you can use only the last successful FIDO authentication method. If a user logs in with biometric FIDO before going offline, only biometric works offline, and similarly for non-biometric logon. Even if the user has previously logged in with both devices, only the most recent one is cached when working offline. This affects physical FIDO authentication devices only.

- **IKB-441 – Unable to carry out an offline logon after using a temporary access code**

When the **Manage the Windows password** option is enabled on the **FIDO2** tab of the global settings, if you use a temporary access code before going offline, all cached credentials are cleared, preventing you from carrying out an offline logon with either biometric or non-biometric FIDO devices, even if you have successfully logged in with FIDO devices before.

3.8 Authentication Technology against Factor type

Technology	Knowledge	Possession	Inherent
Password (NIST)	X		
Grid Authentication	X	X	X
Phrase Authentication	X	X	
One Time Code	X	X	X
Push		X	X
Standard OATH		X	
YubiKey OTP	X	X	
Passkey/FIDO2		X	X

3.9 Automatic MFA determination and SSO assurance levels

MyID MFA allows for users to be provisioned for multiple MFA technologies at once. Applications Logon Technology can be set to **Automatic** MFA; this determines the most appropriate technology that the user is capable of authenticating with.

Coupled to this, MyID MFA also provides Single Sign On (SSO) capabilities across applications. This means that a user can authenticate to one application and is then not required to re-authenticate to other applications.

As each application can be configured with its own MFA assurance level, users can authenticate to an application with a lower-level assurance level than another application.

MyID MFA provides conditional SSO where SSO is allowed, provided that the application being accessed has the same or lower assurance level than the application a user originally authenticated to, the user is not required to re-authenticate. If an application has a higher-level of assurance than the original authenticated to, then the user needs to re-authenticate to the application with the higher-level assurance MFA technology.

3.9.1 Hierarchy

This is the MyID MFA automatic logon technology and assurance levels hierarchy:

1. FIDO / Passkey
2. Grid Multi-Factor Authentication
3. Push
4. YubiKey One Time PIN
5. One Time Code
6. Phrase Multi-Factor Authentication
7. Grid Deviceless
8. Phrase Deviceless
9. AD Password (Not applicable to Realm users)

3.10 Federation server

Federation provides the ability to share identity and authentication information between systems in a managed way. By supporting standards-based protocols such as OpenID Connect and SAML, MyID MFA can easily add stronger authentication to a range of applications be they cloud based or on-premises.

By supporting the widest range of authentication options from OTP over SMS, through pass phrases, OTP generation using the MyID Authenticator app, push-notifications, and FIDO passkeys, you can introduce a single means of strong authentication to project multiple applications or mix and match technologies as best fits your security needs and deployment scenario.

Building Identity Provider capabilities into the MFA solution, not only supports federation, but also delivers a unified authentication experience across the entire application suite, including authentication to application, logging on to the windows desktop, accessing the self-service portal and resetting credentials such as passwords. A simplified and consistent authentication process improves the user experiences and reduces the likelihood of a call to the help desk.

3.10.1 ADFS replacement

Microsoft ADFS (Active Directory Federation Services) has been the mainstay of many organizations looking to add secure authentication to multiple applications in a Microsoft-centric environment. With the move to Microsoft Entra based solutions, a number of organizations are finding themselves looking for an alternative that is simpler to deploy and provides support for both cloud and legacy on-premises applications, as well as securing the Windows Desktop logon and Microsoft 365.

The federated Identity Provider (IdP) capabilities MyID MFA delivers provides a modern and easy to alternative to ADFS. By supporting a wide range of authenticators, including FIDO passkeys, and standard protocols such as OpenID Connect and SAML 2.0, MyID MFA is a natural successor to ADFS.

4 Deployment

The following deployment overview walks through the installation process for deploying a MyID Authentication Server.

To deploy a MyID Authentication Server fully, you must:

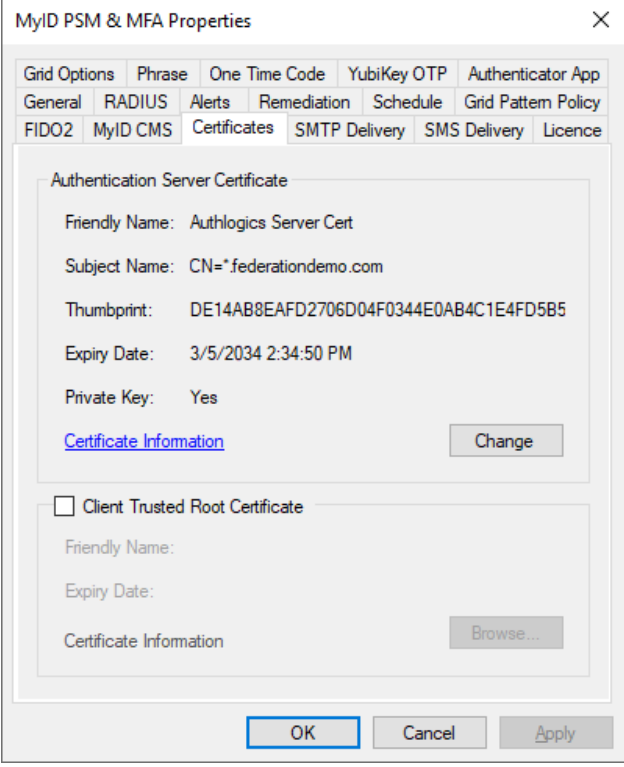
1. Install the MyID Authentication Server on a Windows Server.
2. Provision users in the MyID Directory.
3. Install the Plug-ins, configure the third-party integrations, or setup RADIUS clients.
MyID plug-ins have separate Integration guides which should be followed.
4. Create applications for Federated App support.
5. Optionally, you may choose to deploy additional MyID Authentication Servers to provide High Availability.

4.1 High Availability and certificates

The MyID Authentication Server installer automatically generates a MyID Server Certificate – this is used for encrypting data stored in the directory. In addition, the installer creates a MyID SSL Certificate that is used by IIS for encrypting web traffic in transit.

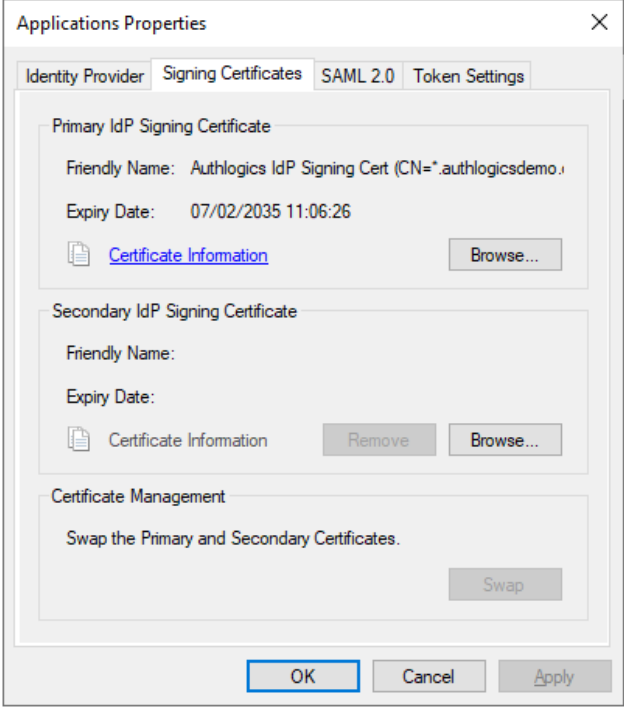
Before you install an additional MyID Authentication Server, you must export the MyID Server Certificate from the primary MyID Authentication Server with its private key and import it onto the additional server. Until you do this, the additional Authentication Server cannot access encrypted data stored in the directory.

To verify which certificate is being used on an existing Authentication Server, check the **Certificates** tab of the MyID PSM & MFA Properties dialog in the MyID Management Console:



The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'Certificates' tab selected. The dialog has a title bar with a close button (X). Below the title bar is a tabbed interface with the following tabs: Grid Options, Phrase, One Time Code, YubiKey OTP, Authenticator App, General, RADIUS, Alerts, Remediation, Schedule, Grid Pattern Policy, FIDO2, MyID CMS, Certificates (selected), SMTP Delivery, SMS Delivery, and Licence. The 'Certificates' tab contains two sections. The first section, 'Authentication Server Certificate', displays the following information: Friendly Name: Authlogics Server Cert, Subject Name: CN=*.federationdemo.com, Thumbprint: DE14AB8EAFD2706D04F0344E0AB4C1E4FD5B5, Expiry Date: 3/5/2034 2:34:50 PM, and Private Key: Yes. Below this information are a blue link 'Certificate Information' and a 'Change' button. The second section, 'Client Trusted Root Certificate', is currently unchecked and shows empty fields for Friendly Name and Expiry Date, with a 'Browse...' button and a 'Certificate Information' link. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

To verify which Identity Provider Signing certificates are being used, check the **Signing Certificates** tab of the Applications Properties dialog in the MyID Management Console.



The screenshot shows the 'Applications Properties' dialog box with the 'Signing Certificates' tab selected. The dialog has a title bar with a close button (X). Below the title bar is a tabbed interface with the following tabs: Identity Provider, Signing Certificates (selected), SAML 2.0, and Token Settings. The 'Signing Certificates' tab contains three sections. The first section, 'Primary IdP Signing Certificate', displays the following information: Friendly Name: Authlogics IdP Signing Cert (CN=*.authlogicsdemo.), Expiry Date: 07/02/2035 11:06:26, and a 'Browse...' button. Below this information are a blue link 'Certificate Information' and a 'Browse...' button. The second section, 'Secondary IdP Signing Certificate', displays the following information: Friendly Name: (empty), Expiry Date: (empty), and buttons for 'Certificate Information', 'Remove', and 'Browse...'. The third section, 'Certificate Management', contains the text 'Swap the Primary and Secondary Certificates.' and a 'Swap' button. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

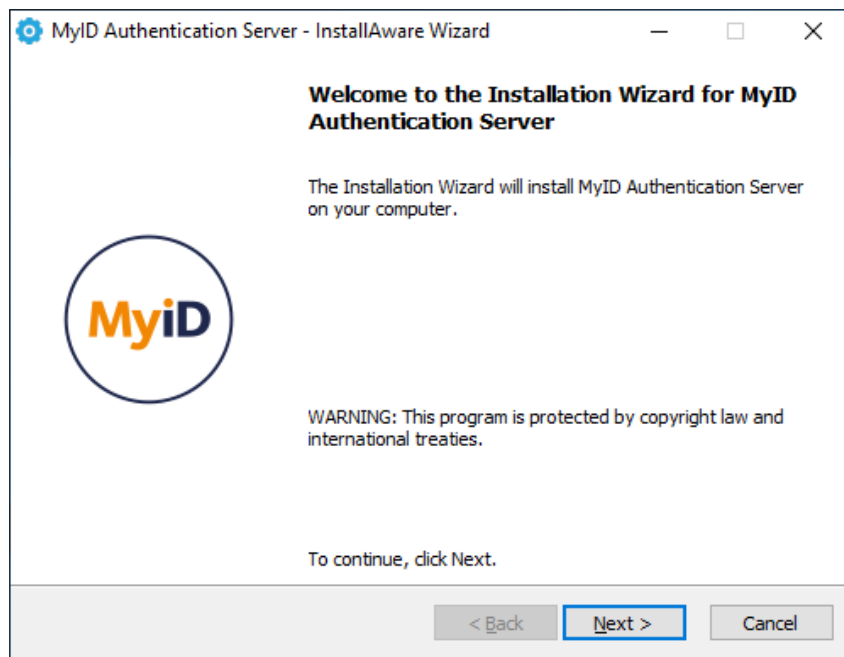
For information on exporting and importing certificates, see section [4.7](#), *Certificate export and import*.

4.2 Installing the MyID Authentication Server

The MyID Authentication Server is responsible for processing logon requests and other core activities. The MyID Authentication Server should be set up before any other MyID MFA or PSM component.

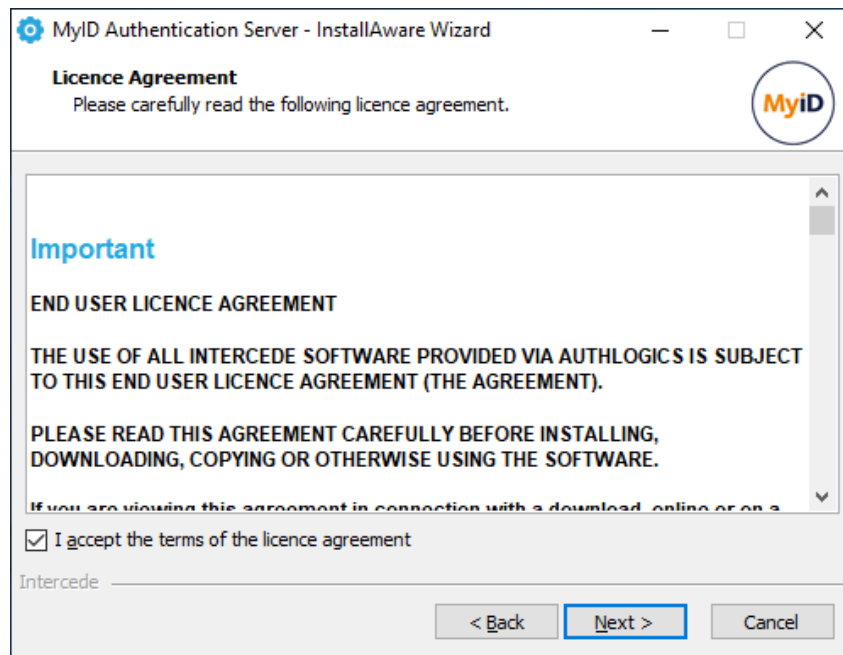
Note: This section of the installation process requires Local Administrator rights on the server. Domain rights are not required at this stage.

1. To start the MyID Authentication Server installation, run the MyID Authentication Server `xxxxx.exe` installer.
2. Click **Next** to automatically uninstall the previous version.

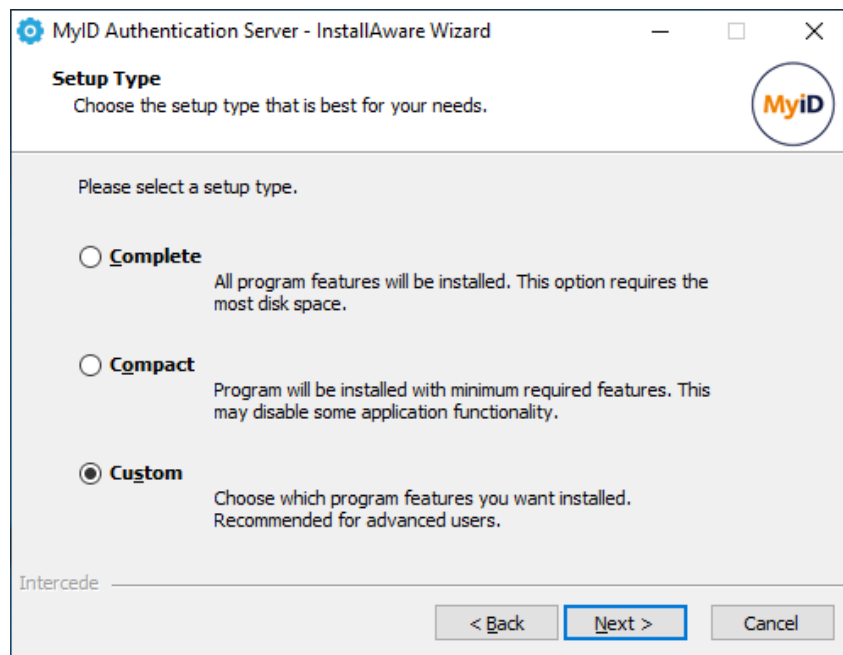


3. Click **Next**.

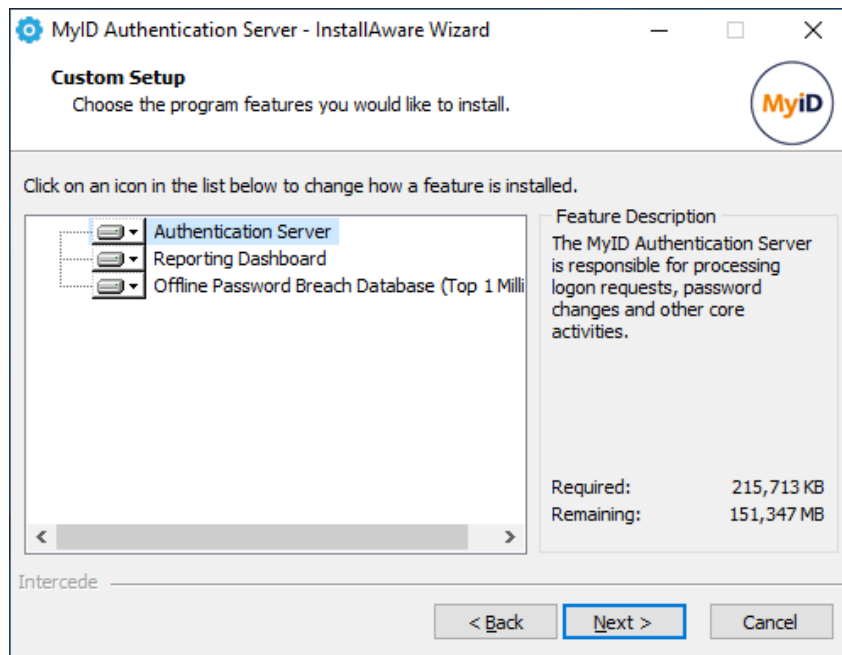
- Review the license agreement and check the **I accept the terms of the licence agreement** box.



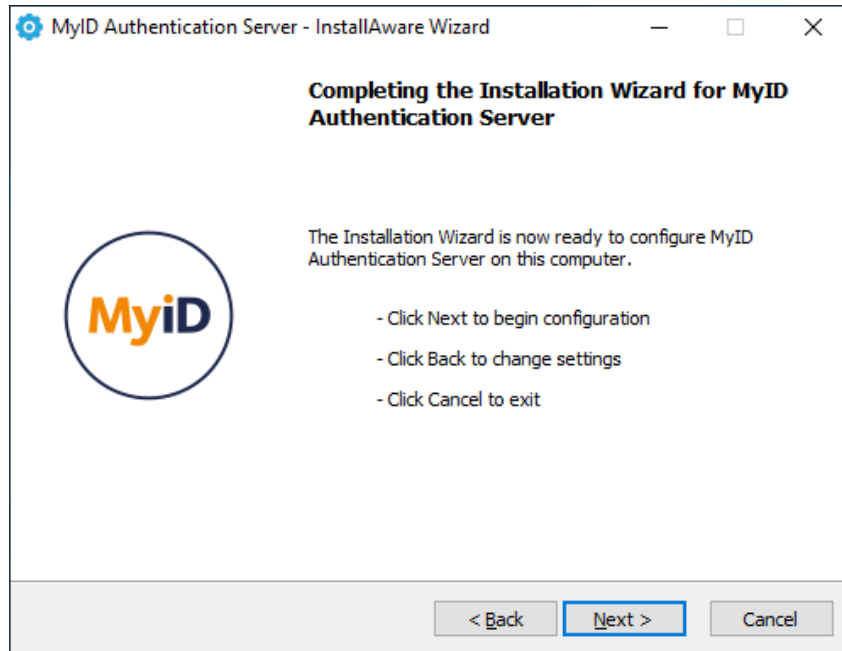
- Click **Next**.



6. Select the **Custom** setup type, and click **Next**.

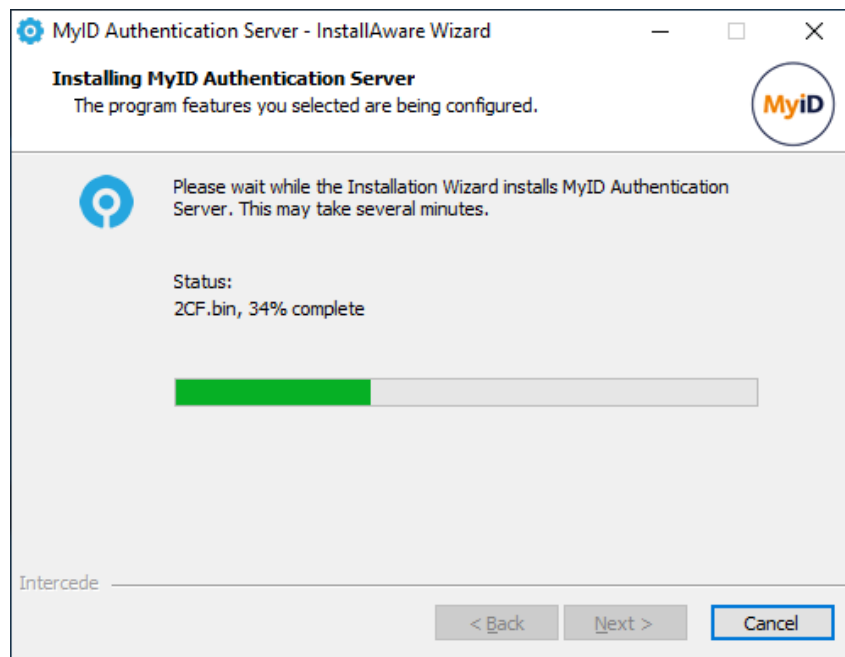


7. Select features to install.
At minimum, select the **Authentication Server** feature for installation.
8. Click **Next**.

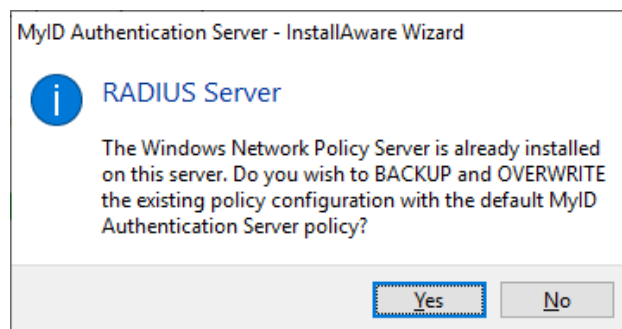


9. Click **Next**.

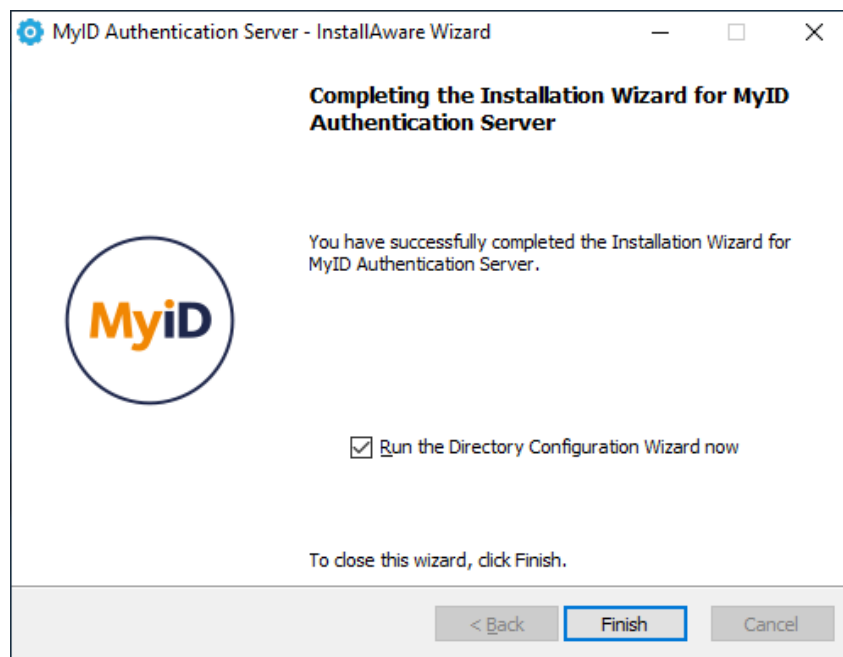
The installation is being performed.



10. You may be prompted to overwrite the existing NPS policy.



Click **Yes**.

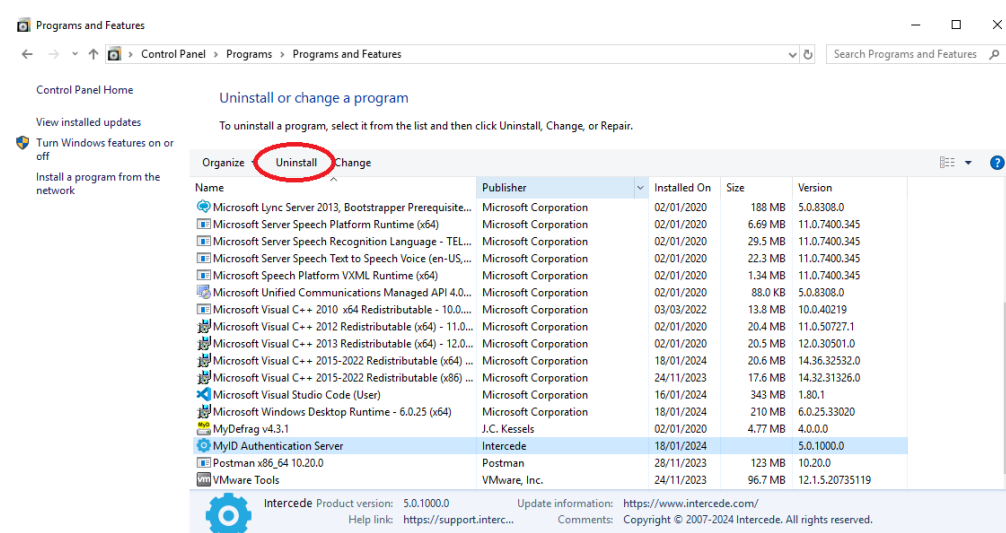


All necessary MyID Authentication Server files have been installed on your server.

11. If you want to set up your directory immediately, select **Run the Directory Configuration Wizard now**.
12. Click **Finish**.

4.3 Uninstalling the MyID Authentication Server

If you no longer require the MyID Authentication Server on a server, you can remove it by performing an uninstall from **Control Panel > Programs > Programs and Features**:



4.3.1 Active Directory metadata

Uninstalling the MyID Authentication Server does *not* remove the metadata from user accounts in the Active Directory. If you want to remove MyID MFA and PSM from your environment completely, delete all user accounts using the MMC before uninstalling. This does *not* delete the user accounts in the Active Directory; it just removes all MyID information from them.

For detailed information about MyID Active Directory metadata, see Authlogics KB207256965:

support.authlogics.com/hc/en-us/articles/207256965

4.4 Updates and upgrades

A product update is a minor new version designed to fix specific known issues in the product and introduce some new features. Updates are typically low risk to deploy and are designed to be a simple in-place update. Updates are released regularly and may be skipped if the changes in the update are not required. Check the `readme.txt` of the update to see the changelog.

Typically, updates can be performed in-place at your convenience allowing for differing versions for MyID Agents and Authentication servers operational within your environment.

For example, if you currently have V5.0.6947.0 deployed, an in-place update of all agents and servers to V5.0.6947.2 can be done sporadically in any order that fits your schedule.

Note: When updating or upgrading servers, you are recommended to perform the action one server at a time to update or upgrade additional servers only once the server you are currently performing update or upgrade action on is completed and fully tested to be operational.

A product upgrade is a major new version that includes fixes but is mainly designed to deliver new features and functionality. Upgrades are not released regularly. Upgrades may require additional planning before they are installed. For more information, see section 4.6, [Installing an upgrade](#). Always review the installation and configuration guide of the new version before upgrading.

4.5 Installing an update

You can use the installation program of an update for a full clean install, or to perform an in-place update of an existing installation.

The installation process is almost identical to performing a new installation. Once installed, you must run the Directory Configuration Wizard for the server to be used after the update.

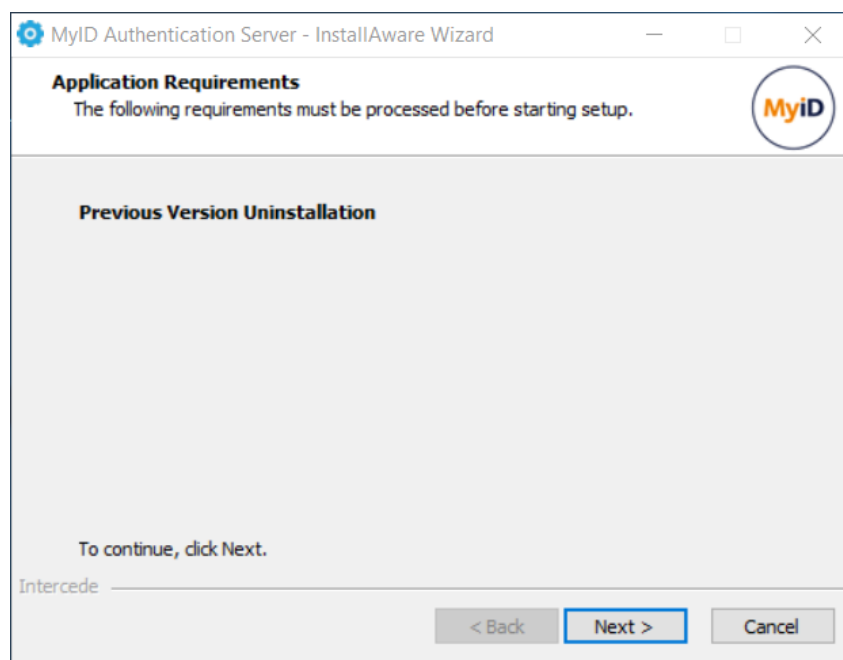
For PSM deployments, you must rerun the Password Security Management wizard after an upgrade.

All directory settings, registry settings, and supported web portal customizations are retained during an update.

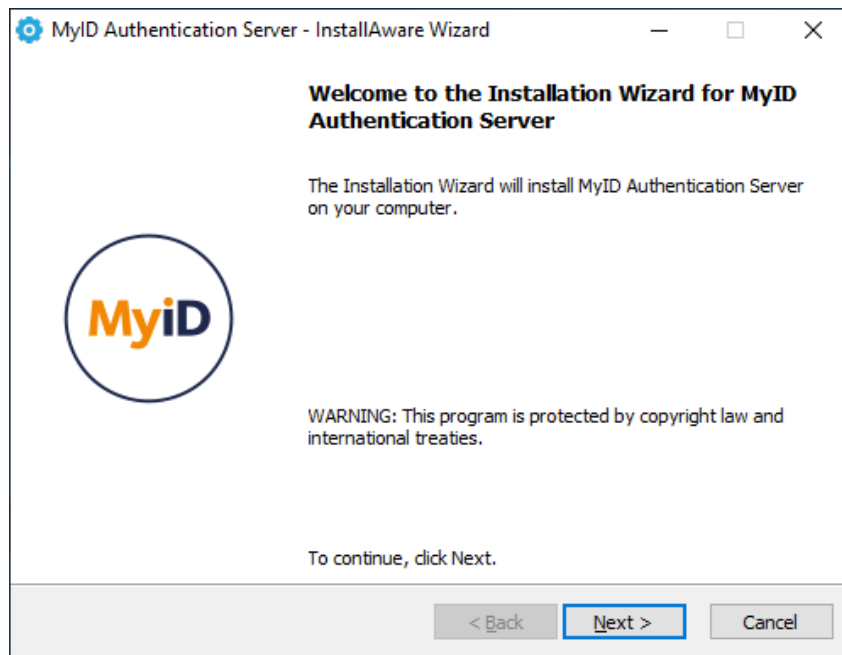
Note: If the latest version of MyID MFA and PSM is an upgrade to your current version, see section 4.5, *Installing an update*.

To perform an in-place update:

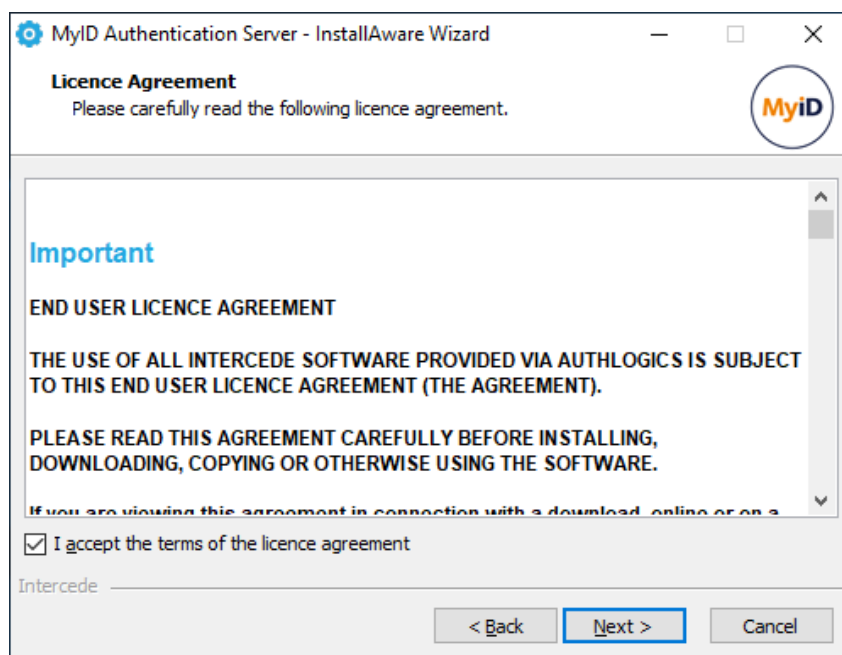
1. To start the MyID Authentication Server installation, run the MyID Authentication Server `xxxxx.exe` installer.



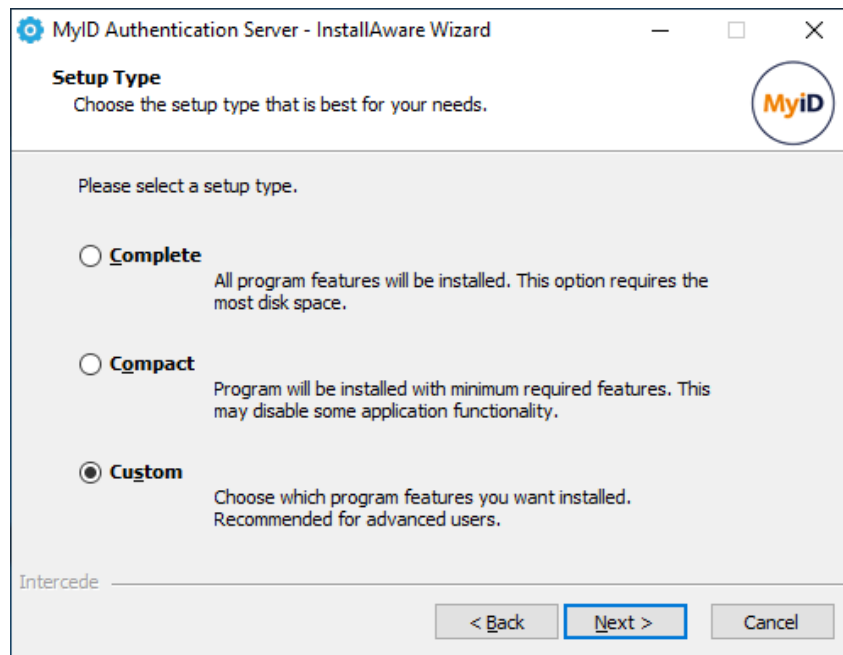
2. Click **Next** to automatically uninstall the previous version.



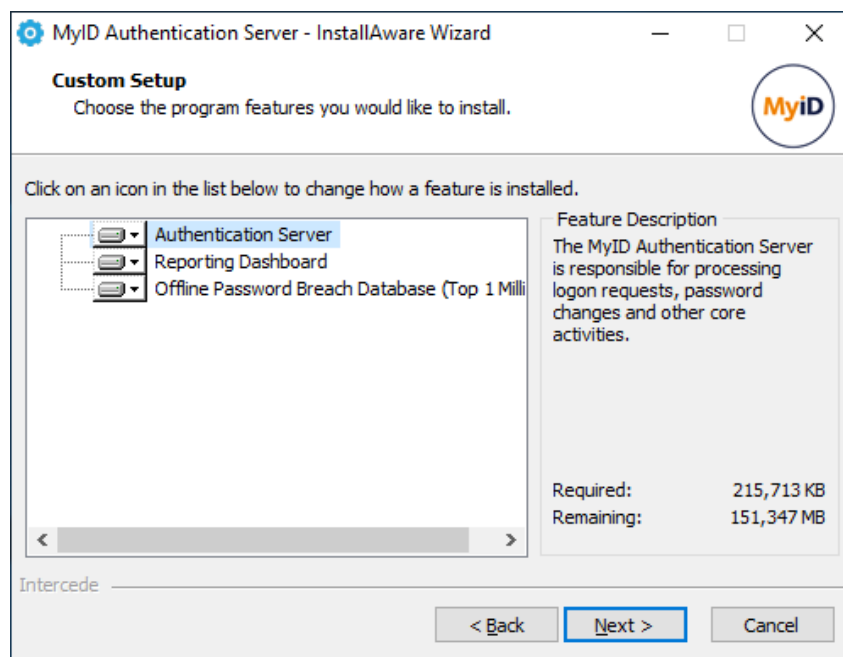
3. Click **Next**.
4. Review the license agreement and check the **I accept the terms of the licence agreement** box.



5. Click **Next**.



6. Select the **Custom** setup type, and click **Next**.



7. Select features to install.

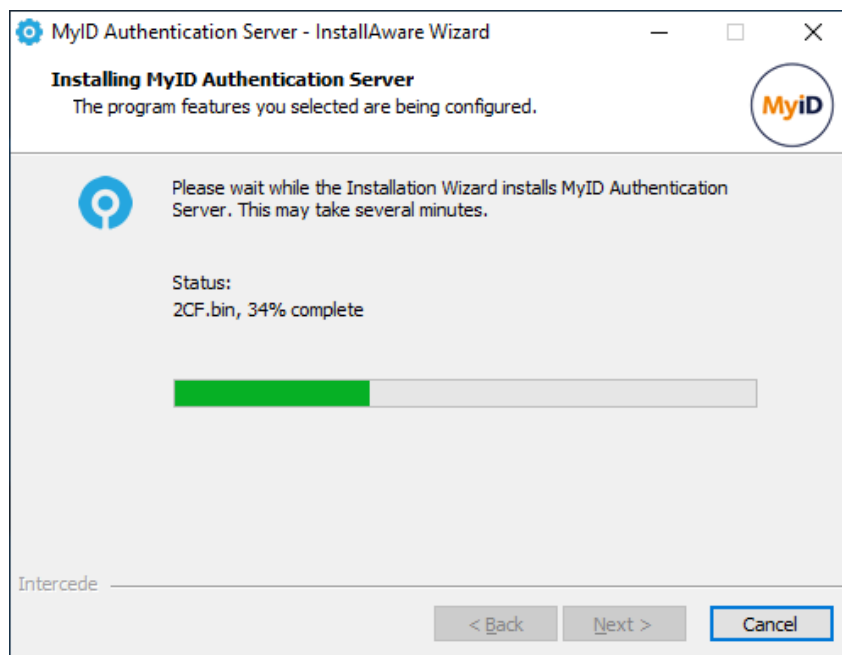
At minimum, select the **Authentication Server core** and the **Authentication Server Management Console** features for installation.

8. Click **Next**.

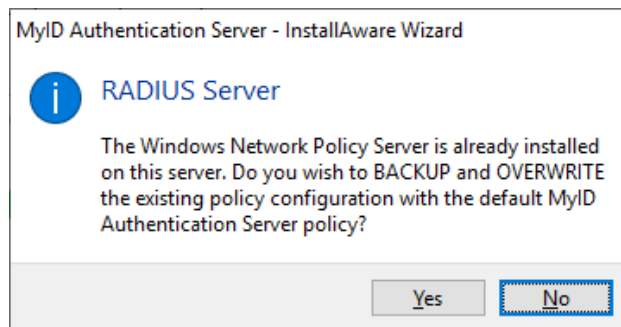


9. Click **Next**.

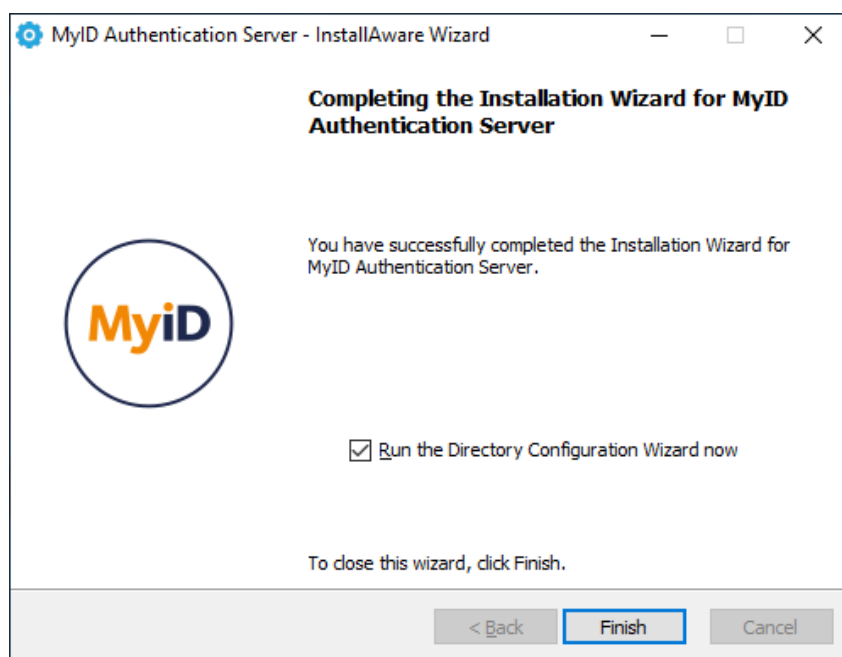
The installation is being performed.



10. You are prompted to overwrite the existing NPS policy.



Click **No** to preserve your preexisting Network Policy Server policy configurations.



All necessary MyID Authentication Server files have been installed on your server.

11. If you want to set up your directory immediately, select **Run the Directory Configuration Wizard now**.
12. Click **Finish**.

4.6 Installing an upgrade

To perform an Upgrade successfully (for example upgrading V4.1.xxxx.x deployments to V4.2.xxxx.x or V4.2.xxxx.x to V5.0.xxxx.x) without potentially impacting your environment, you must follow a step-by step process.

All MyID agents are designed to be backward compatible – a V5.x agent can communicate with a V4.2 Authentication Server; however, a V4.2 agent cannot communicate with a V5.0 Authentication server. Therefore, before you upgrade Authentication Servers, you must first upgrade the deployed agents.

Agents may have new Group Policy objects so, before deploying the new agent, you may need to push the Group Policy objects accordingly.

Once you have fully upgraded the agents, you can upgrade the Authentication servers.

Fully test each step of the recommended upgrade process before moving on to the next step. The recommended upgrade process is:

1. Push any new MyID MFA and PSM agent Group Policy Objects (GPO) to the servers and workstations where the agents are installed.
 - For more information on the Group Policy Objects relating to the Windows Desktop Agent, see the *Configuring the Windows Desktop Agent* section of the [Windows Desktop Agent Integration Guide](#).
 - For more information on the Group Policy Objects relating to the Domain Controller Agent, see the *Configuring the Domain Controller Agent Policy settings* section of the [Domain Controller Agent Integration Guide](#).
 - For more information on the Group Policy Objects relating to the ADFS Agent, see the *Configuring the MyID ADFS Agent* section of the [ADFS Agent Integration Guide](#).
 - For more information on the Group Policy Objects relating to the Exchange Agent, see the *Configuring the Exchange Agent* section of the [Exchange Agent Integration Guide](#).
2. Upgrade *all* MyID PSM and MFA agents.
 - For information on upgrading the Windows Desktop Agent, see the *Updating the MyID Windows Desktop Agent* section of the [Windows Desktop Agent Integration Guide](#).
 - For information on upgrading the Domain Controller Agent, see the *Updating the MyID Domain Controller Agent* section of the [Domain Controller Agent Integration Guide](#).
 - For information on upgrading the ADFS Agent, see the *Updating the MyID ADFS Agent* section of the [ADFS Agent Integration Guide](#).
 - For information on upgrading the Exchange Agent, see the *Updating the MyID Exchange Agent* section of the [Exchange Agent Integration Guide](#).

Ensure that the agents are all reading the GPOs that you configured and that they can communicate with the existing Authentication Servers.

3. Manually uninstall all but one Authentication Server.

You must ensure that you have only *one* Authentication Server remaining in your Active Directory forest.
4. Perform an in-place upgrade on the last remaining Authentication Server.

Ensure that the Internet Information Server Port bindings are the same as before, and that any NPS clients are not overwritten.

Performing an in-place upgrade of one Authentication Server has the same steps as performing an in-place update of one Authentication Server; see section [4.5, Installing an update](#).
5. After performing the in-place upgrade:
 - a. Run the Directory Configuration wizard with **Reprocess user data to latest storage version** enabled.

- b. Reboot.
 - c. If you are performing a PSM upgrade, run the Password Security Management wizard.
 - d. Use the on-server Self Service Portal to test the upgraded server. You are recommended to:
 - Test that you can log in with pre-existing MFA users.
 - Test that passwords that are valid according to PSM defined policies are accepted.
 - Test that passwords that are invalid according to PSM defined policies are rejected.
6. Install the latest Authentication Server version on the Authentication servers that you uninstalled.
- Before installing additional MyID Authentication servers, see section [4.7, Certificate export and import](#).
- After installing each in-place upgrade, carry out the previous step (performing the in-place upgrade) on each machine.
7. Review the MyID Authentication Server settings.
- Note the new features, and browse the documentation for more information on them.

4.6.1 Upgrading from version 4.2

The MyID Authentication Server 5.0 supports upgrading from version 4.0 and higher. To upgrade from version 3.x, you must first upgrade to version 4.1 (not version 4.2), and then to version 5.0; there is no direct upgrade path.

Important: If the Authlogics Desktop Logon Agent version 4.x is deployed, you *must* upgrade the Windows Desktop Agent to version 5.0 *before* you upgrade the MyID Authentication Server. The Windows Desktop Agent 5.0 is backward compatible with version 4.x Authentication servers. See the [Windows Desktop Agent Integration Guide](#) for further details.

4.6.2 Windows Desktop Agent compatibility

All Windows Desktop Agents are designed to be backward compatible; the latest version of the Desktop Agent works with the previous MyID Authentication Server version. However, the agent may not work with more recent MyID Authentication Server versions.

The following table details the MyID Authentication Server relative to the versions of Windows Desktop Agent supported:

MyID Authentication Server version	Minimum Desktop Agent version
5.0.6946.0 and lower	5.0.6946.0
5.0.6947.0	5.0.6947.0

When a Windows Desktop Agent falls out of compatibility, the agent can no longer communicate with the Authentication Server and therefore continues to operate in offline mode.

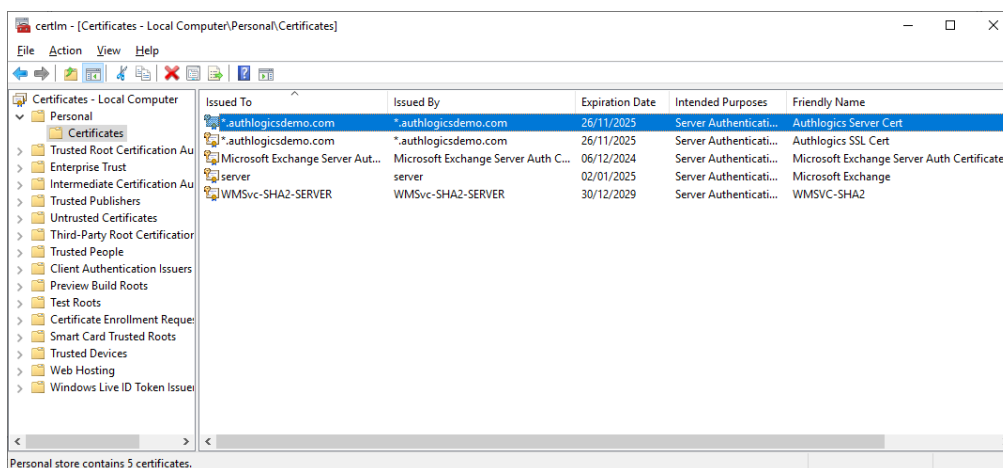
4.7 Certificate export and import

This section details the process of exporting the MyID Authentication Server directory encryption and Identity Provider certificates to a file so it can be imported onto another server where the MyID Authentication Server software will be installed.

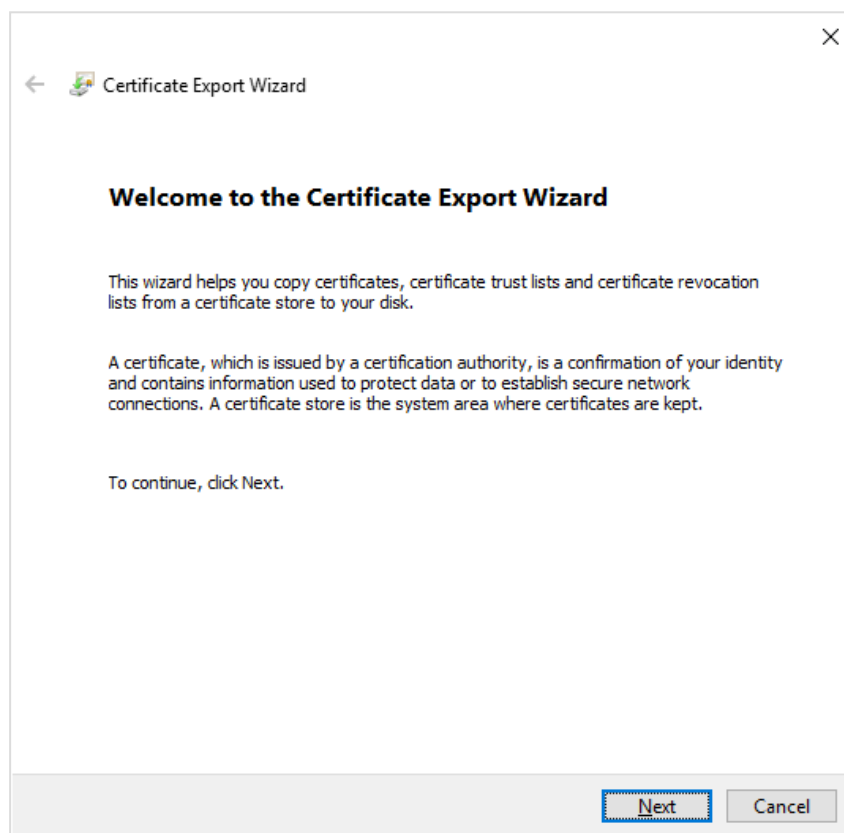
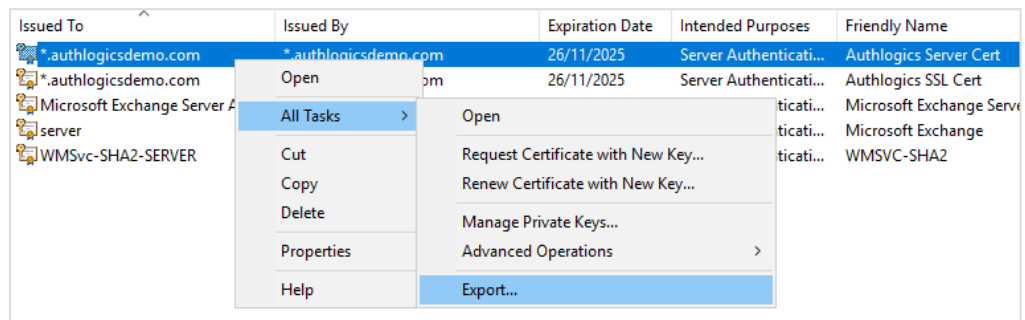
4.7.1 Exporting a certificate from an existing MyID Authentication Server

Note: The following documents the process to export the directory encryption certificate; this process must be repeated for the IdP Signing certificate.

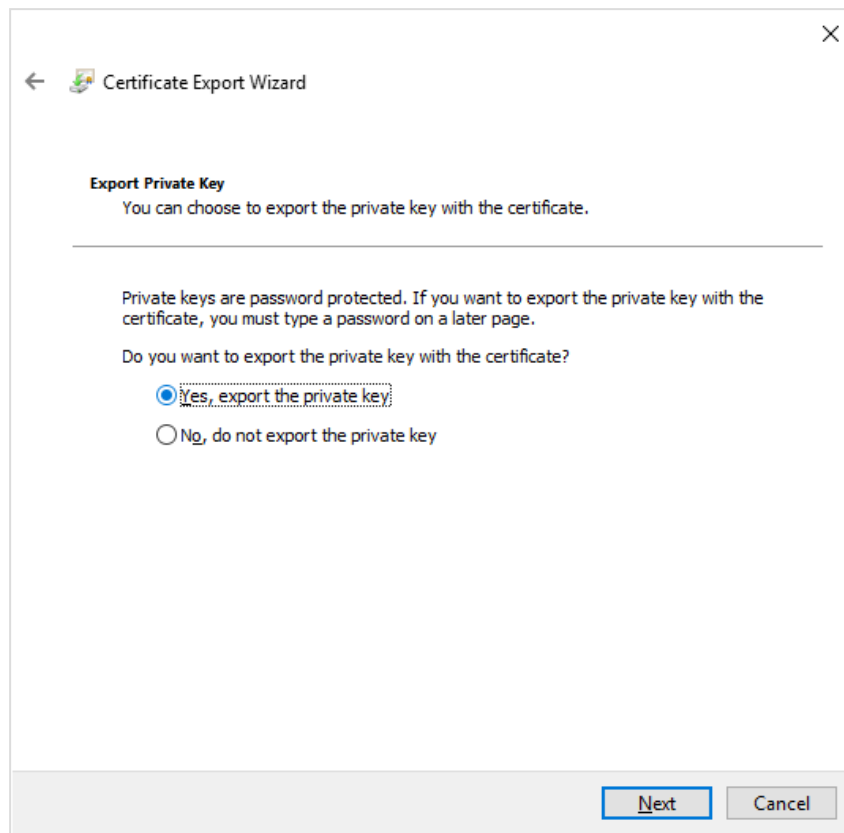
1. To start the Certificate MMC, run `certlm.msc`.



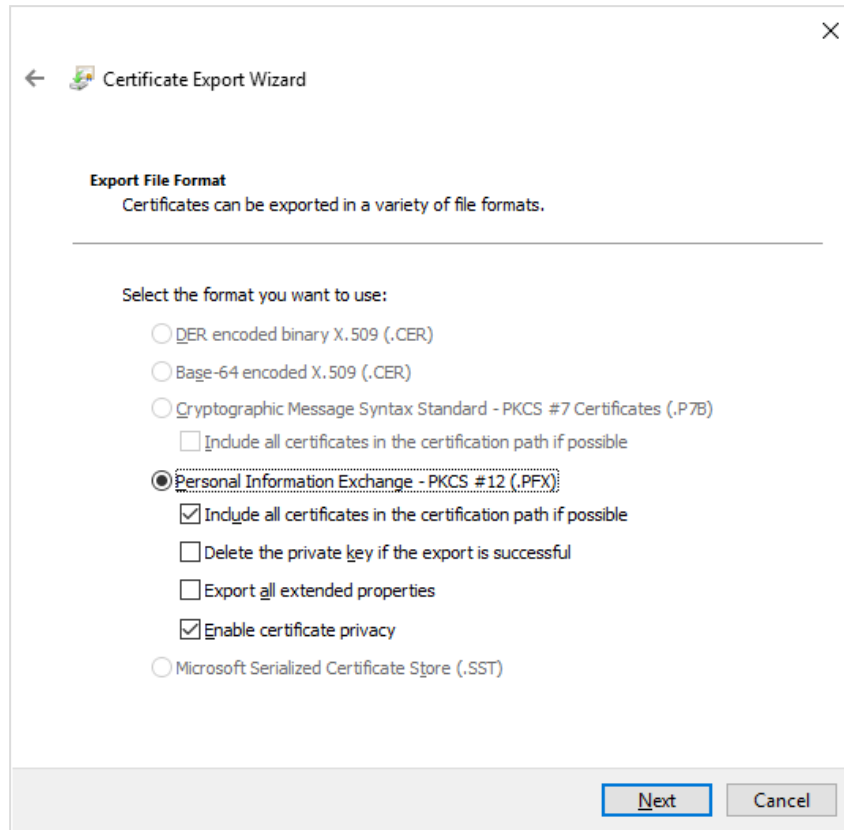
2. Right-click the MyID Server Certificate (or IdP Signing Certificate) being used, and select **All Tasks > Export**.



3. Click **Next**.

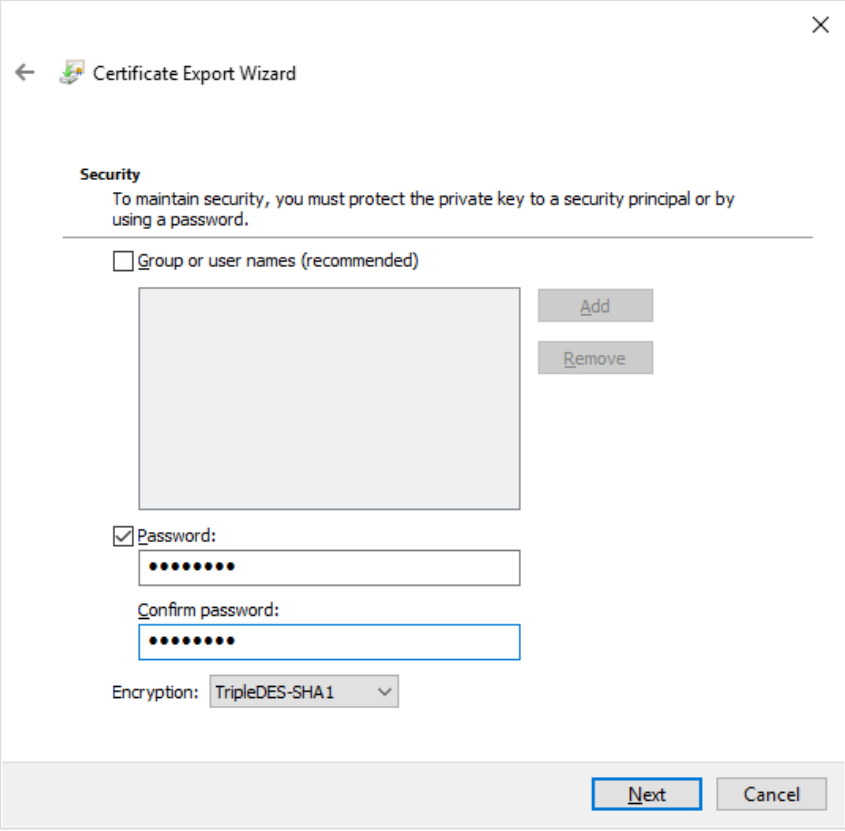


4. Select **Yes**, export the private key and click **Next**.



5. Click **Next**.

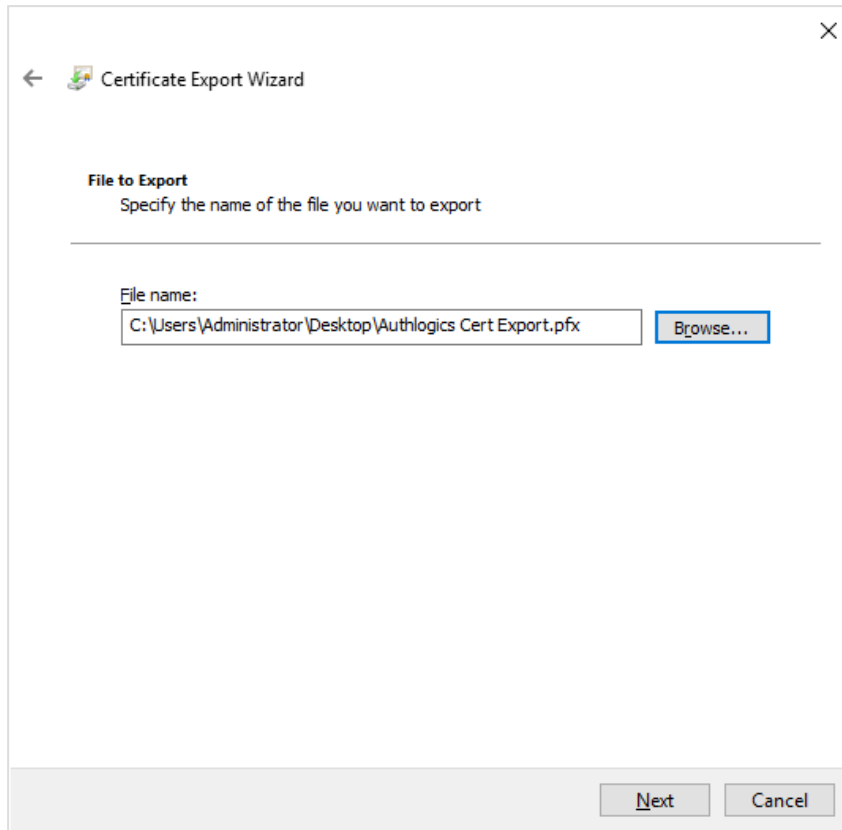
6. Select **Password** and enter your password twice to confirm.



The image shows a Windows-style dialog box titled "Certificate Export Wizard" with a close button (X) in the top right corner. The dialog has a back arrow icon and a small icon of a certificate. The main section is titled "Security" and contains the text: "To maintain security, you must protect the private key to a security principal or by using a password." Below this text is a horizontal line. Under the line, there is a checkbox labeled "Group or user names (recommended)" which is currently unchecked. To the right of this checkbox is a large empty rectangular box. To the right of this box are two buttons: "Add" and "Remove". Below the "Group or user names" section, there is a checkbox labeled "Password:" which is checked. To the right of this checkbox is a text input field containing eight dots. Below this field is another label "Confirm password:" followed by another text input field containing eight dots. At the bottom of the main section, there is a label "Encryption:" followed by a dropdown menu showing "TripleDES-SHA1". At the bottom right of the dialog, there are two buttons: "Next" and "Cancel".

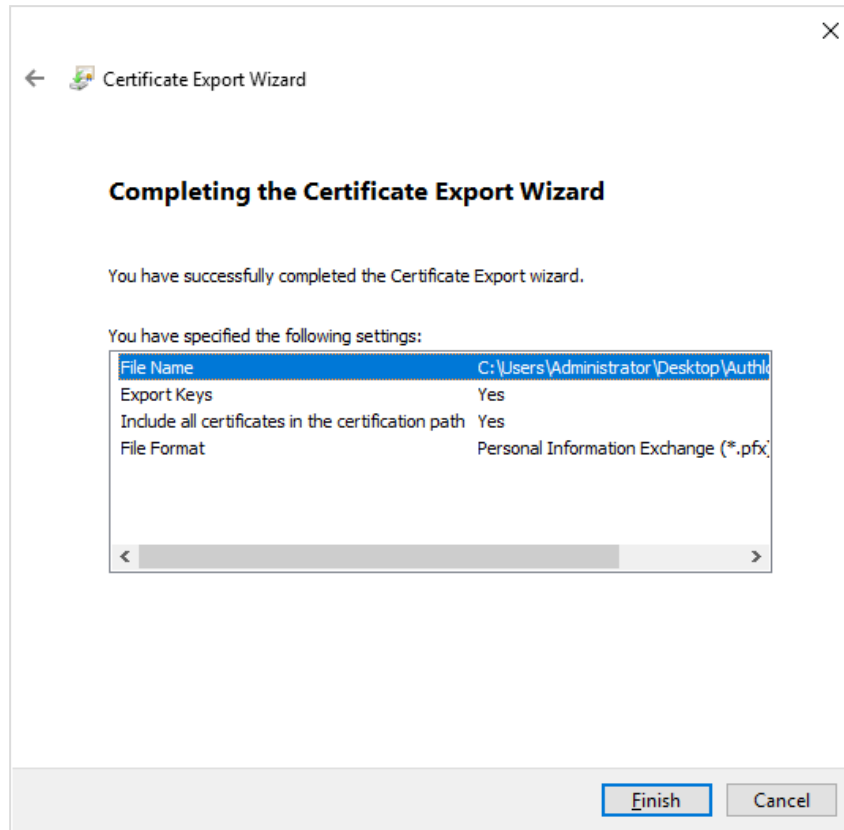
7. Click **Next**.

8. Enter allocation and **File name** to export to.

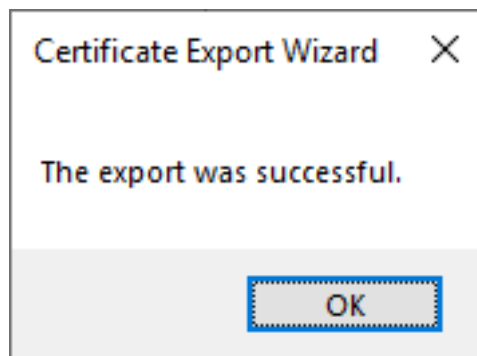


The image shows a Windows-style dialog box titled "Certificate Export Wizard". It has a back arrow icon and a close "X" button in the top-left corner. The main content area is titled "File to Export" and contains the instruction "Specify the name of the file you want to export". Below this is a horizontal line. Underneath the line, the text "File name:" is followed by a text input field containing the path "C:\Users\Administrator\Desktop\Authlogics Cert Export.pfx". To the right of the input field is a "Browse..." button. At the bottom of the dialog box, there are two buttons: "Next" and "Cancel".

9. Click **Next**.



10. Click **Finish**.

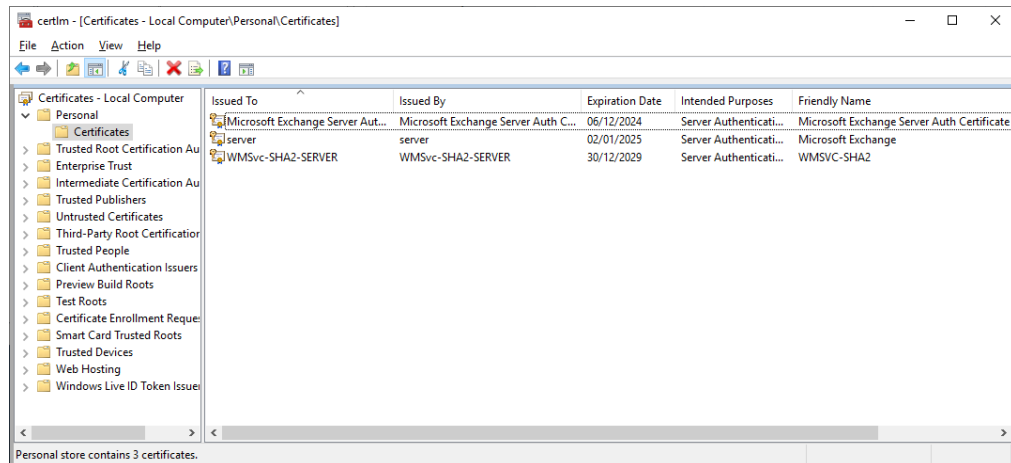


11. Click **OK**.
The wizard closes.

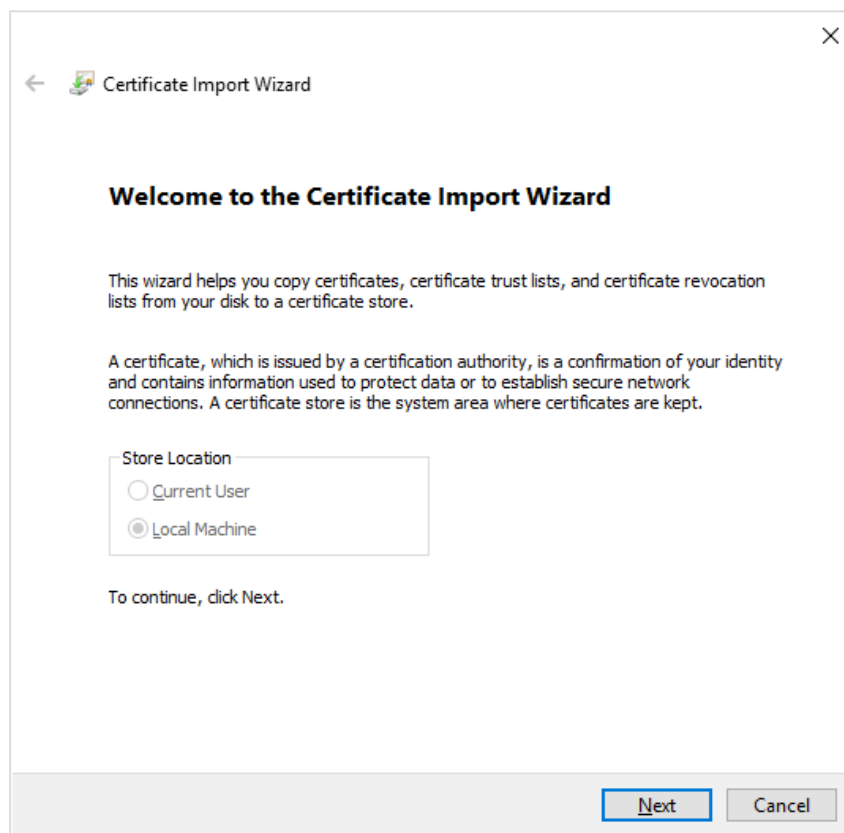
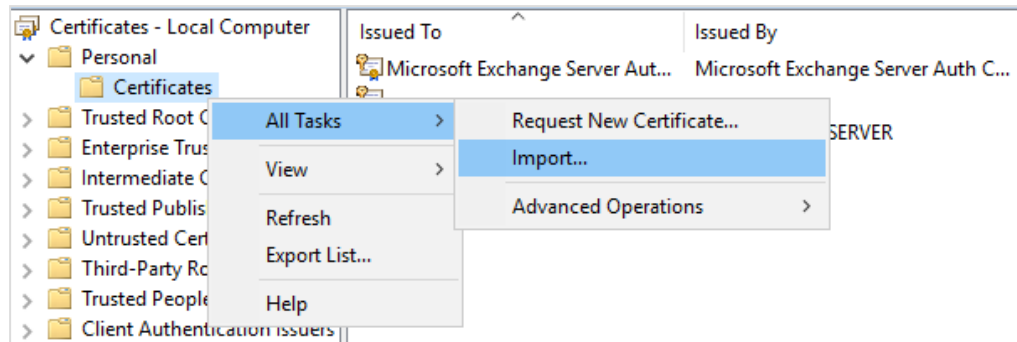
4.7.2 Import a certificate to a new MyID Authentication Server

Note: As with the export of the certificates, this process needs to be followed for both the Authenticate Server encryption and IdP Signing certificates.

1. To start the Certificate MMC, run `certlm.msc`.

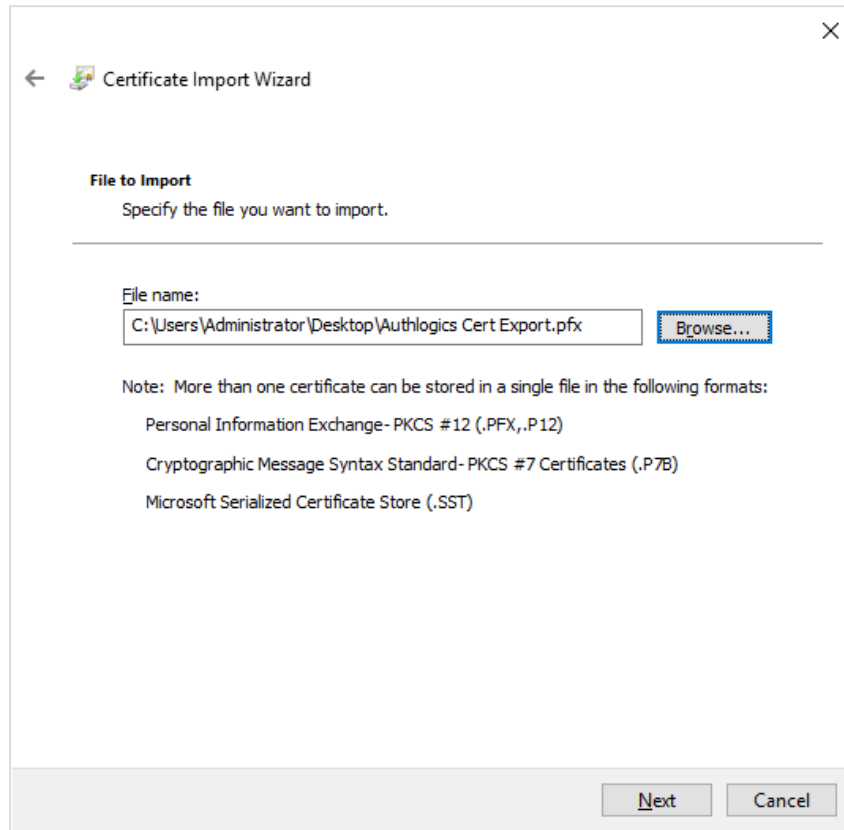


2. Right-click **Certificates** in the **Personal** store, select **All Tasks > Import**.



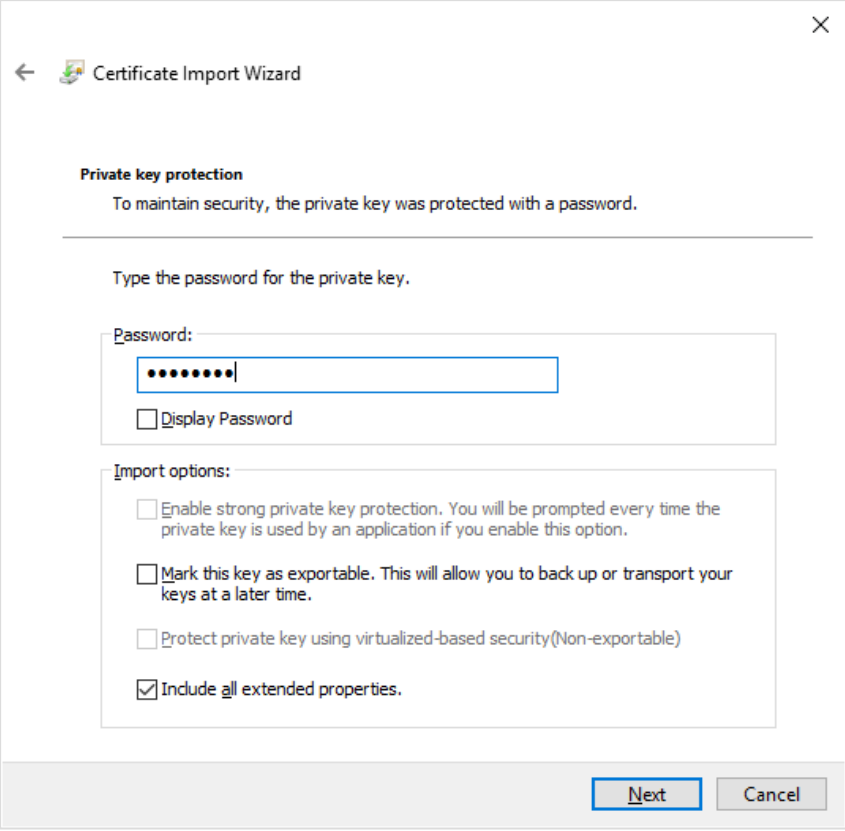
3. Click **Next**.

4. Enter the path to the file you previously exported.



5. Click **Next**.

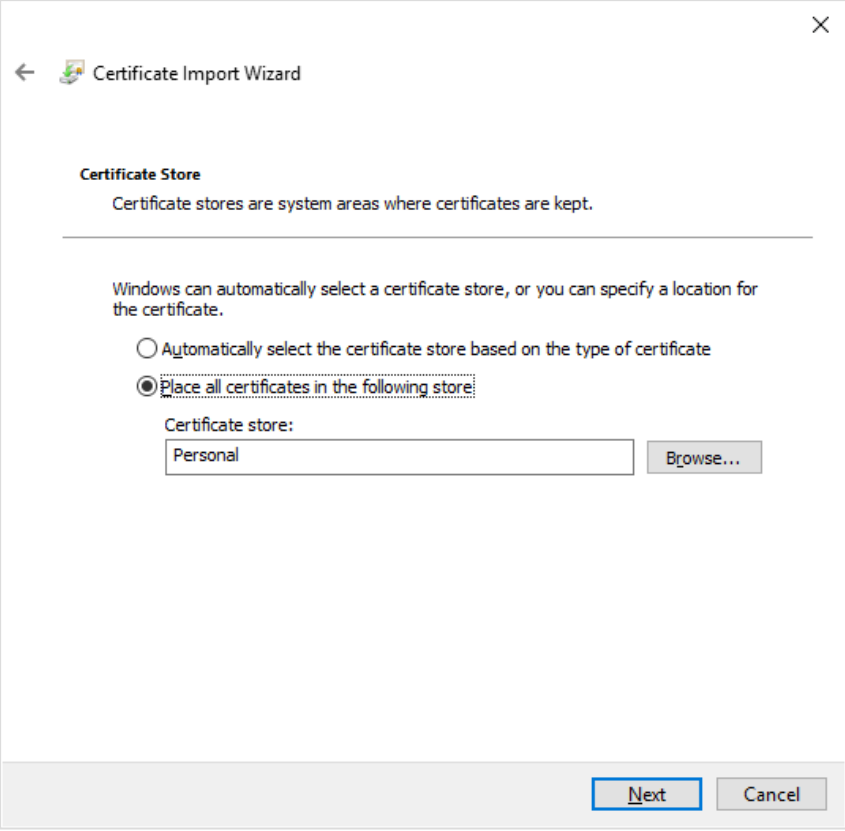
6. Enter the password that you used when exporting the certificate.



The image shows a 'Certificate Import Wizard' dialog box. It has a title bar with a back arrow, a forward arrow, and a close button. The main content area is titled 'Certificate Import Wizard' and contains the following sections:

- Private key protection**
To maintain security, the private key was protected with a password.
- Type the password for the private key.
- Password:**
A text box containing eight dots, indicating a password is entered.
- ☐ Display Password
- Import options:**
 - ☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
 - ☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
 - ☐ Protect private key using virtualized-based security (Non-exportable)
 - ☒ Include all extended properties.

At the bottom right, there are two buttons: 'Next' and 'Cancel'.

7. Click **Next**.

The image shows a Windows 'Certificate Import Wizard' dialog box. At the top, there is a title bar with a back arrow, a small icon, and the text 'Certificate Import Wizard', followed by a close button (X). Below the title bar, the section is titled 'Certificate Store'. Underneath, it says 'Certificate stores are system areas where certificates are kept.' A horizontal line separates this from the next section. The next section states 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' There are two radio button options: 'Automatically select the certificate store based on the type of certificate' (which is unselected) and 'Place all certificates in the following store:' (which is selected). Below the selected option, there is a text box labeled 'Certificate store:' containing the word 'Personal'. To the right of the text box is a 'Browse...' button. At the bottom right of the dialog, there are two buttons: 'Next' and 'Cancel'.

← Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store:

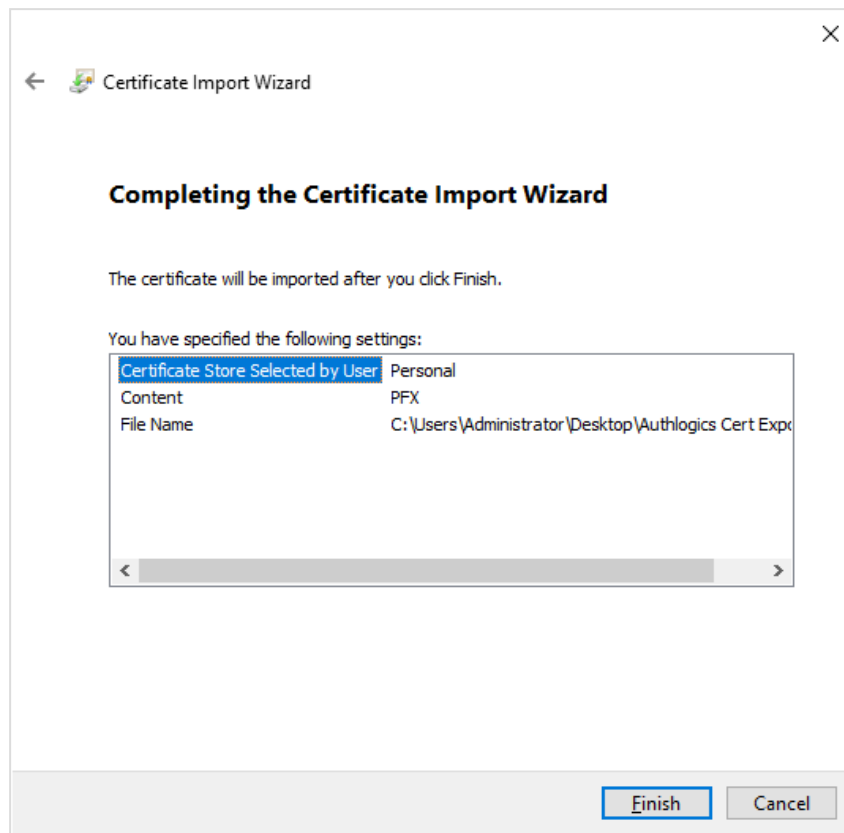
Certificate store:

Personal

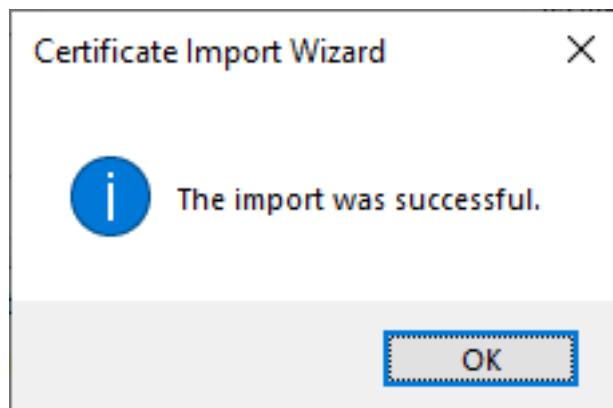
Browse...

Next Cancel

8. Click **Next**.



9. Click **Finish**.



10. Click **OK**.

4.8 MyID Authentication Server Directory configuration

MyID Authentication Server Directory must be configured before you can provision users for Multi-Factor Authentication or password policies created.

4.8.1 Directory Configuration Wizard

This section should be performed on the server running the MyID Authentication Server.

Note: This section of the installation process requires the logged-on user to have Domain Admin rights in the domain containing MyID Users and the domain containing the Authentication Server. Alternatively, an Enterprise Admin account can be used.

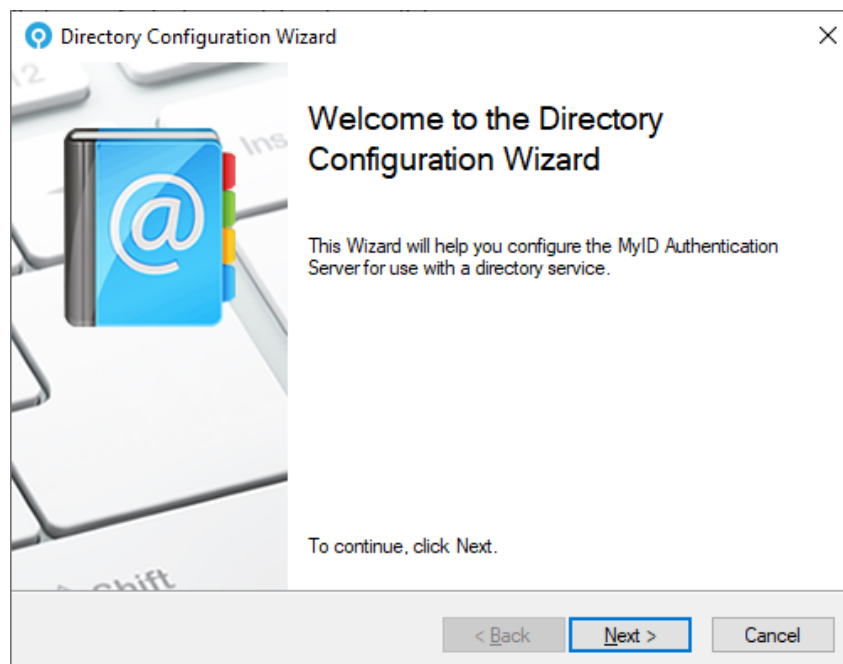
1. Start the MyID Directory Configuration Wizard.

The MyID Directory Configuration Wizard starts automatically when the MyID Management Console is first loaded. It can also be started from the **Directory Configuration Wizard** action from the **Actions** of the MMC.

Start the MyID Management Console from the Windows Start menu:

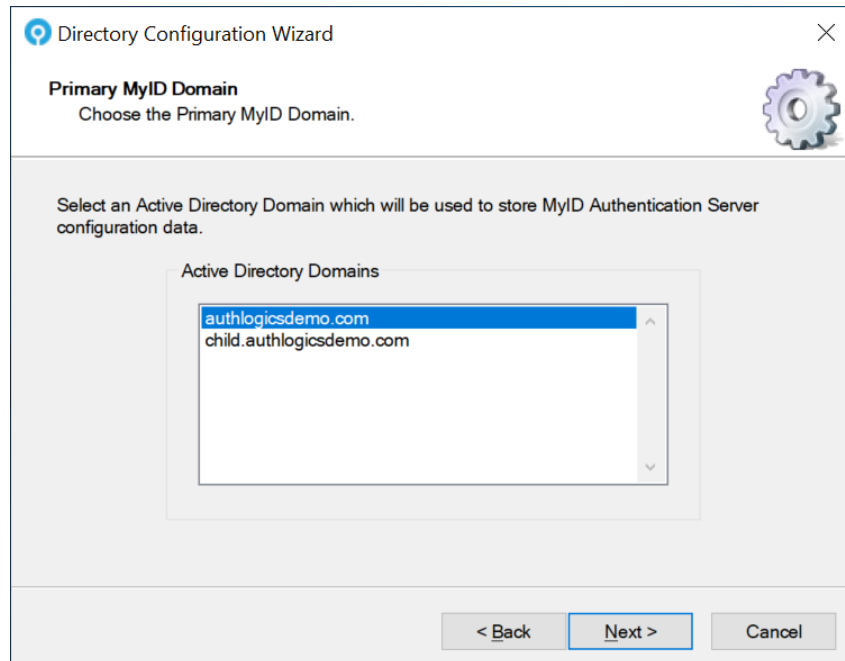
Start > All Programs > MyID Authentication Server Management Console

Note: Ensure that you are logged on with domain administrator account and not a local administrator account.

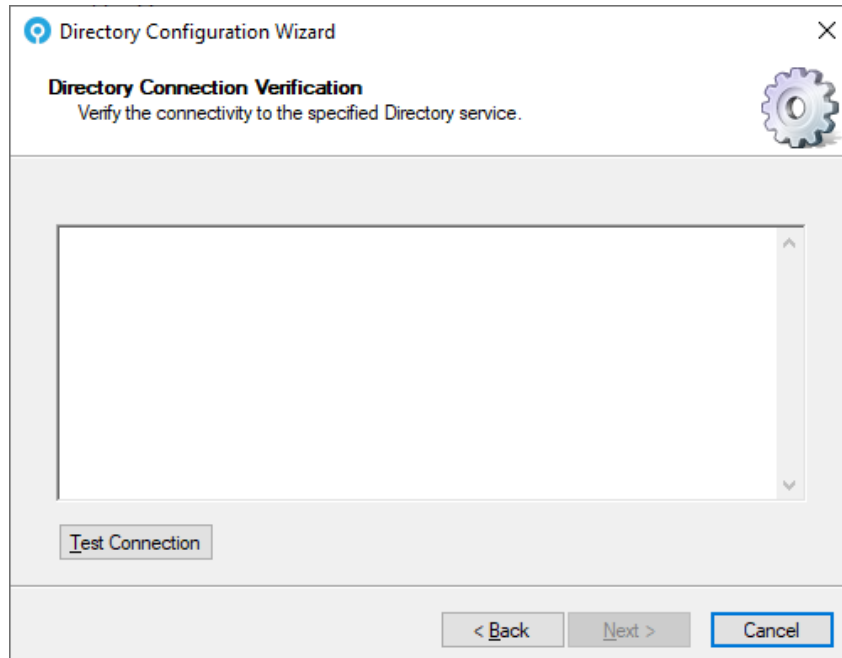


2. Click **Next**.

3. If the Active Directory Forest contains more than one domain and this is the first time the directory is being configured:
 - a. Select the Active Directory Domain you want to use to store MyID configuration data.

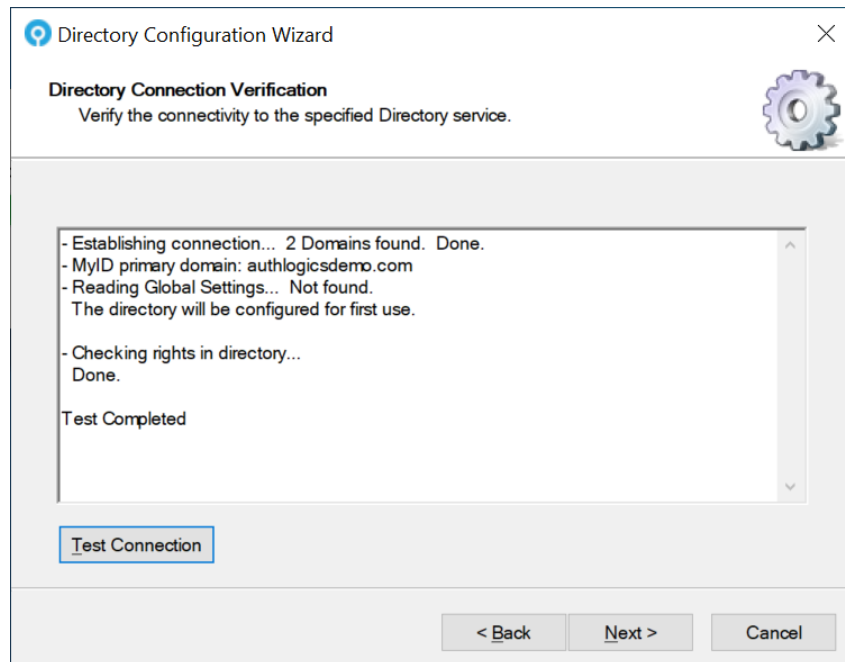


- b. Click **Next**.

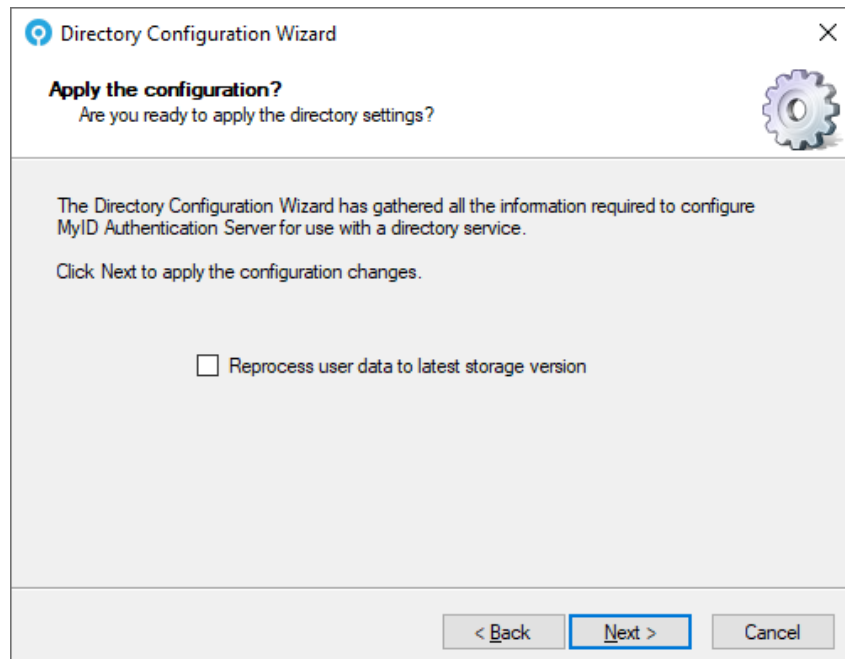


- Click the Test Connection button.

This ensures that the MyID Authentication Server can access the specified directory.



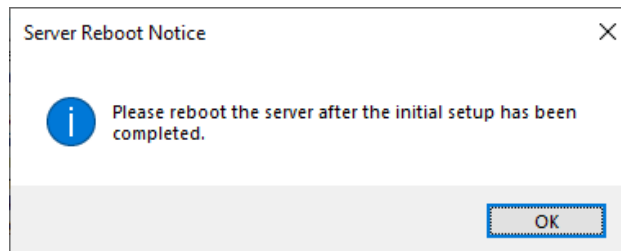
- If the test is successful and all the necessary information has been collected, click **Next**, otherwise correct the issue, and try again.



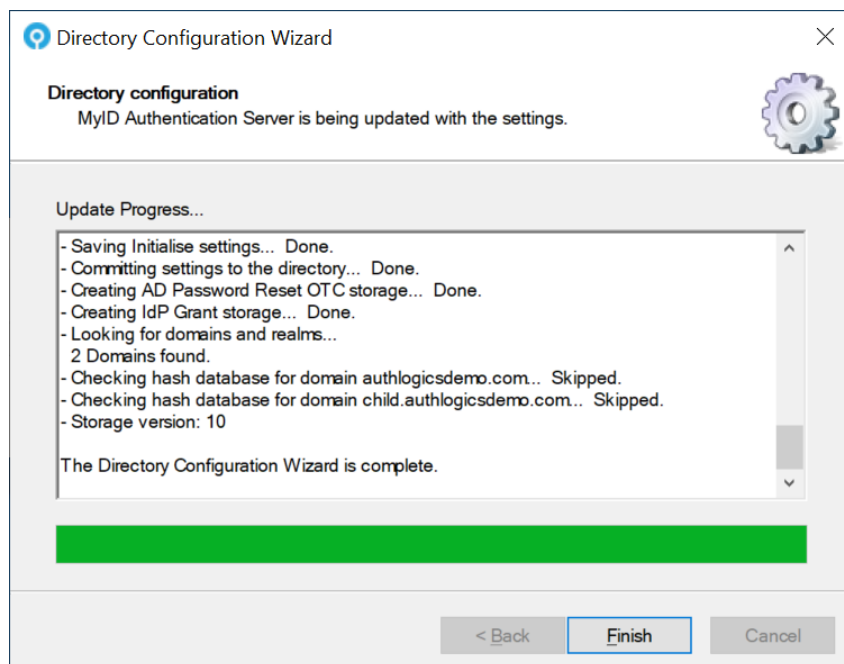
- Click the **Reprocess user data to latest storage version** to upgrade the user information from a version 4 schema to the latest schema. For clean installations or native MyID version 5 deployment, this is not necessary.

7. Click Next.

This applies any configuration changes.



8. Click **OK**.



9. Examine the update progress information for any unexpected errors that may have occurred during the AD configuration.

This information is also logged in the Windows Application Event Log with Information Event ID 1719.

10. Click **Finish**.

11. Reboot your server.

Important: This is not optional – if you do not reboot the server authentication services fail. These failures are reflected in the Windows Events – Application logs.

4.8.2 Add users to the MyID Administrators Group

The MyID Directory Configuration wizard automatically adds the currently logged in user account to the MyID Administrators Active Directory security group. User accounts for the administrators of MyID must also be *manually* added to the MyID Administrators Active Directory security group.

4.9 MyID license configuration

The License Configuration Wizard is responsible for adding all license types to the Authentication Server.

Intercede supplies a unique license key for each product (PSM and MFA) specific to each Active Directory. The license key is entered in the Licence Configuration Wizard through the MMC. The license requires product activation, and the server periodically updates Intercede with license usage information - this requires Internet connectivity to

<https://licencing.authlogics.com/> * which must be maintained for the server to continue functioning.

In certain circumstances, Intercede may supply an offline license file. These digitally signed license files do not require product activation or any Internet connectivity. You must not modify or tamper with them – if you do, they are rendered inoperable. For more information contact Intercede Support.

4.9.1 Getting a free 10 user license or a 30-day trial license

Intercede provides a free MFA and PSM license for up to ten users. The free license does not include our standard product support and assistance and Intercede provides only email assistance on a best-effort basis. However, access to our knowledge base and community site is freely available, see:

support.authlogics.com

If you require additional users in the future, we can easily upgrade your existing license.

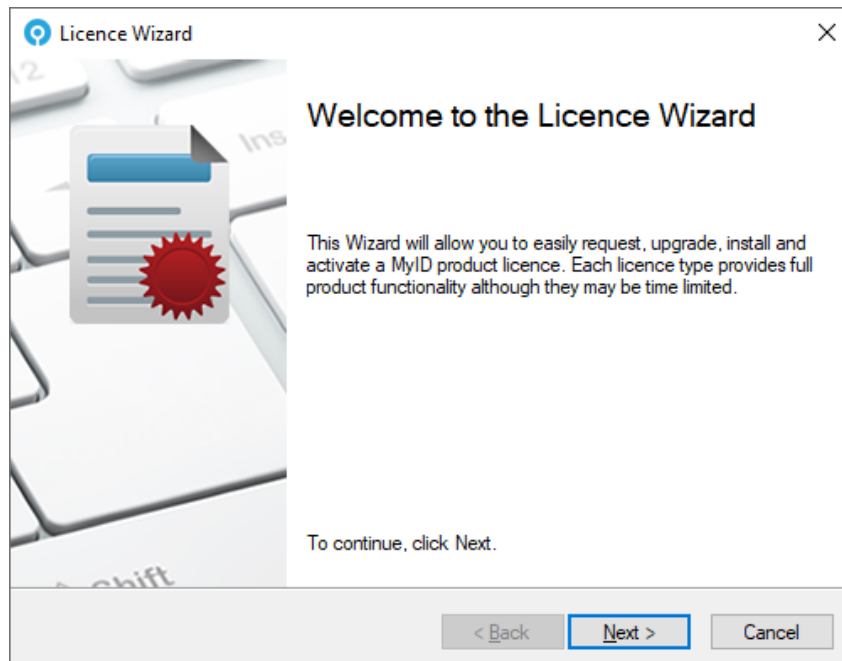
To test the MyID Authentication Server before you buy, you can get a free 30-day trial at any time, and when you decide MyID is for you we can update your license to a full one when you purchase, no reinstall is required.

A free or trial license is installed instantly so you can evaluate at your own pace, however, it does require Internet connectivity (HTTPS) to be installed and activated. If Internet connectivity is not available on the authentication server, please contact Intercede Support.

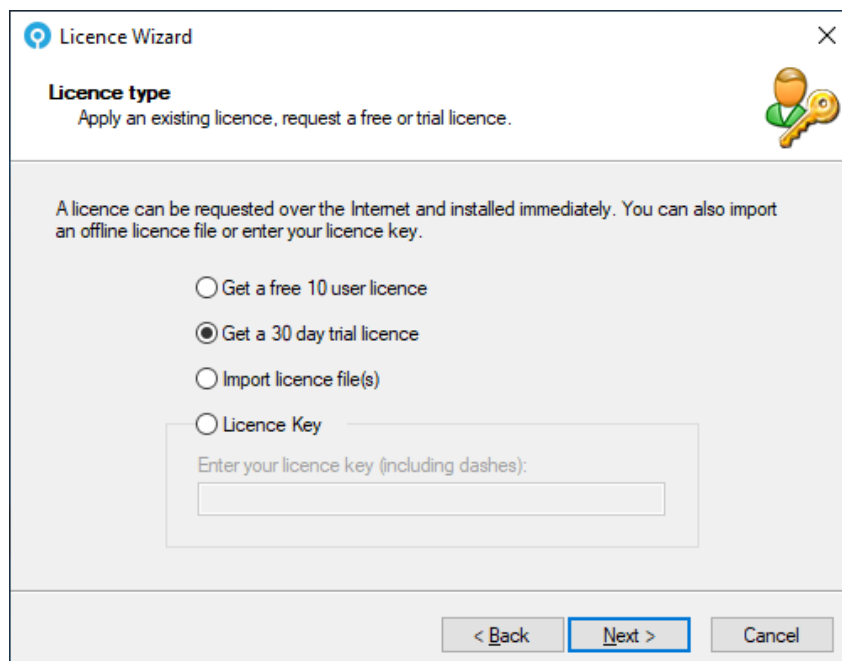
To obtain a license:

1. Start the Licence Wizard.

The Licence Wizard starts automatically when the MyID Management Console is first loaded. You can also start the wizard by clicking **Licence Wizard**, under **Actions** in the MMC.

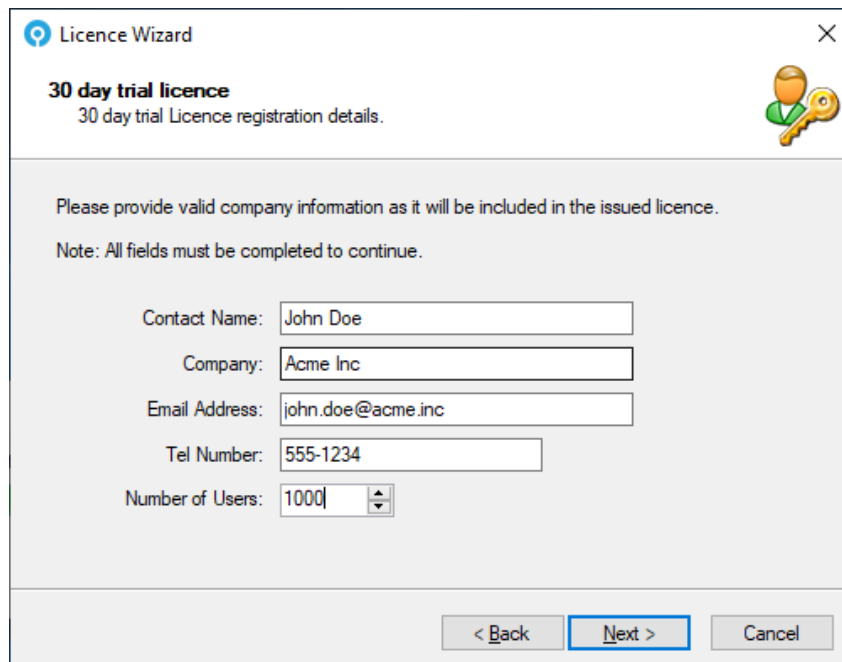


2. Click **Next**.



3. Select **Get a free 10 user license** or **Get a 30-day trial license**.
4. Click **Next**.

5. Complete your details.



Licence Wizard ✕

30 day trial licence
30 day trial Licence registration details.

Please provide valid company information as it will be included in the issued licence.
Note: All fields must be completed to continue.

Contact Name:

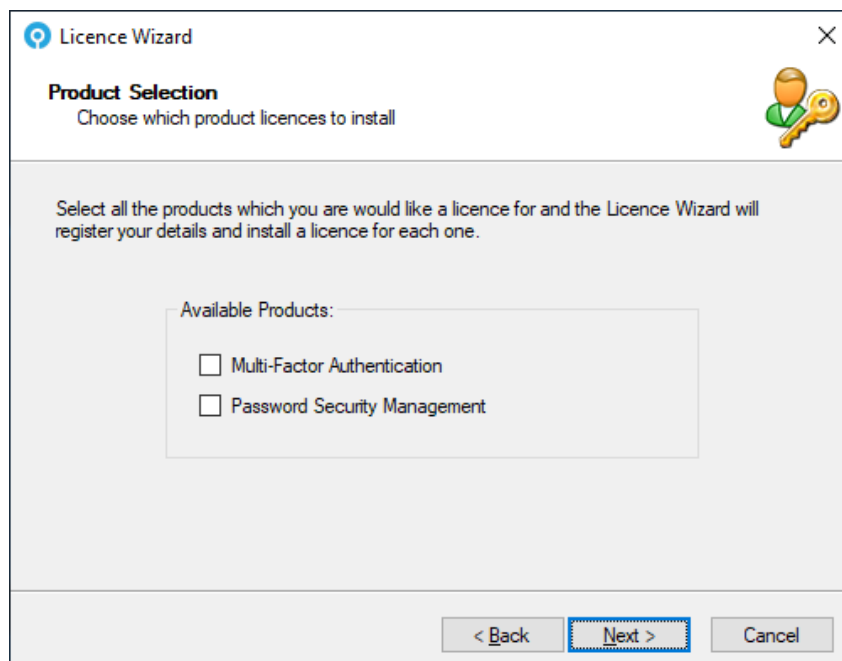
Company:

Email Address:

Tel Number:

Number of Users:

< Back **Next >** Cancel

6. Click **Next**.

Licence Wizard ✕

Product Selection
Choose which product licences to install

Select all the products which you would like a licence for and the Licence Wizard will register your details and install a licence for each one.

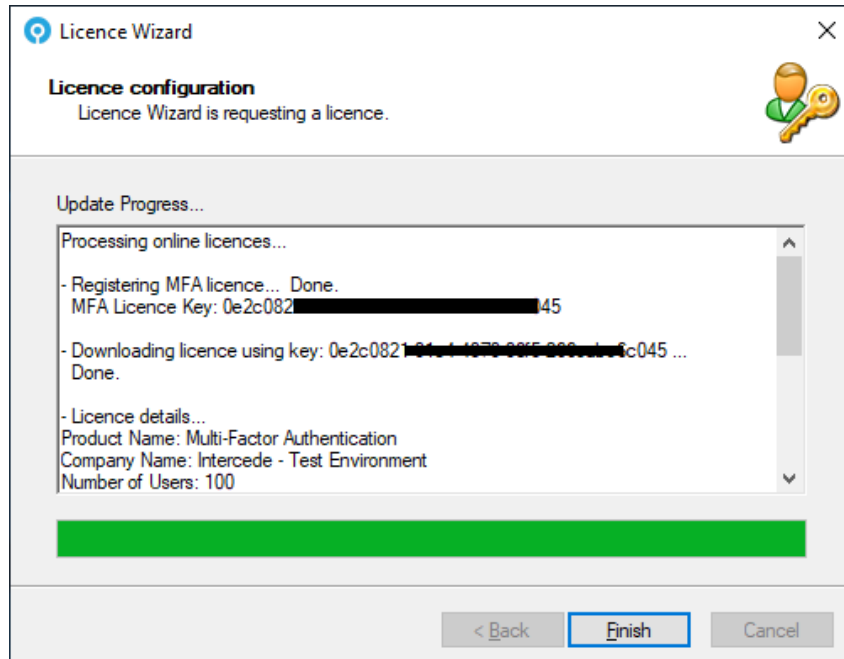
Available Products:

- ☐ Multi-Factor Authentication
- ☐ Password Security Management

< Back **Next >** Cancel

7. Select the product or products that you would like the licenses for.

8. Click **Next**.



The licenses are requested over the Internet and are activated.

9. Click **Finish**.

4.9.2 Importing an offline license file

An offline license file may be issued by Intercede in certain circumstances. Please contact Intercede Support for eligibility. These licenses *do not* require Internet connectivity or activation.

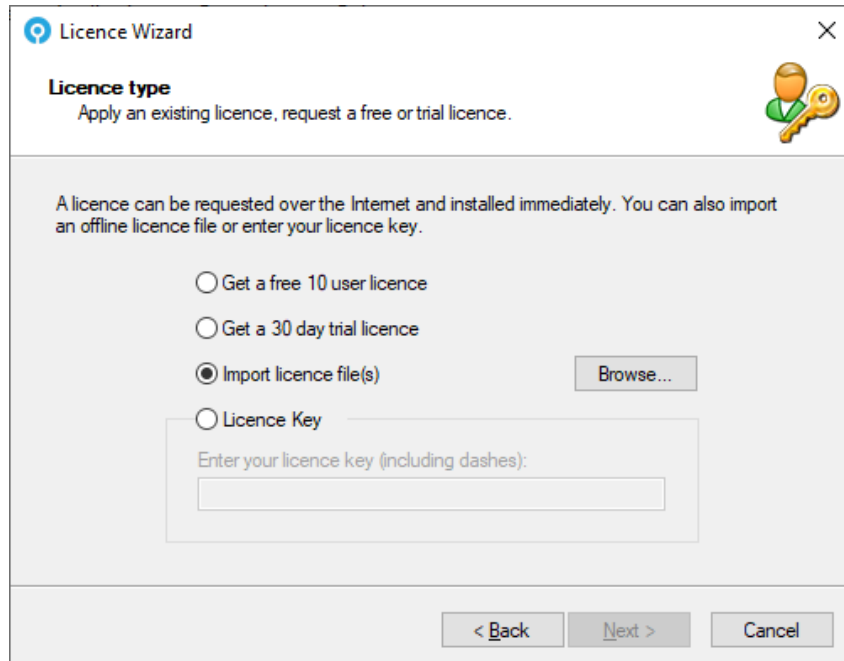
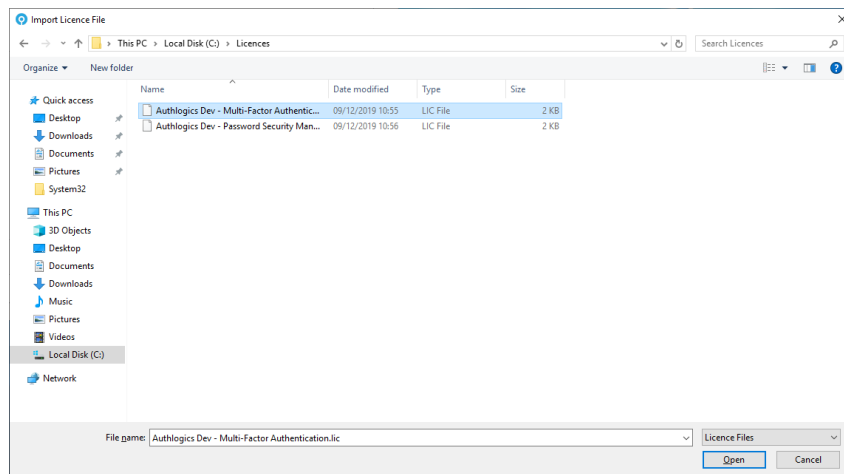
If you have multiple license files, you must add them one at a time. Run the Licence Wizard again to add the second license file.

To import an offline license, you must use the Licence Wizard.

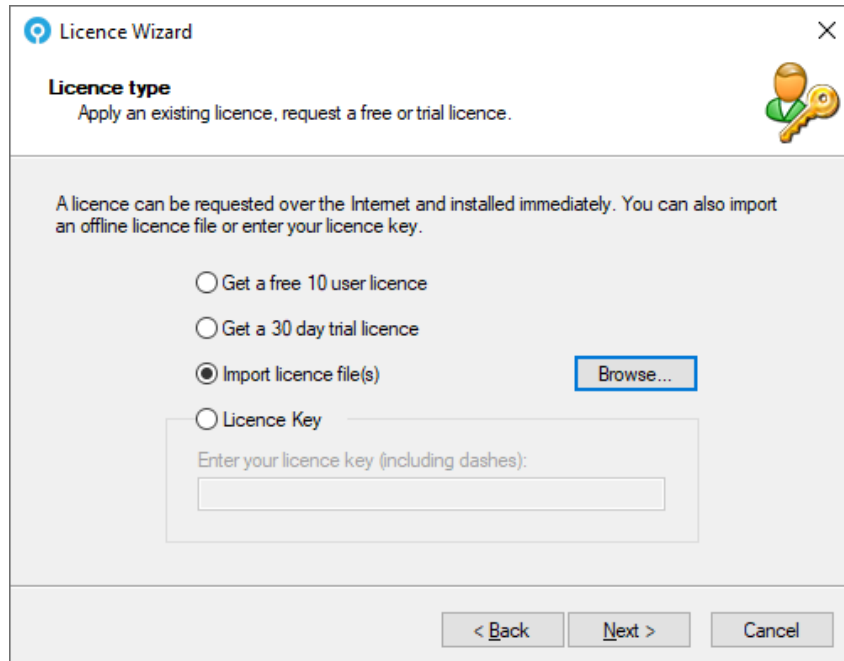
1. Start the Licence Wizard.

The Licence Wizard starts automatically when the MyID Management Console is first loaded. You can also start the wizard by clicking **Licence Wizard**, under **Actions** in the MMC.



2. Click **Next**.3. Select **Import licence file(s)**, and click **Browse**.

4. Select one or more of your license files (ending in .LIC) and click **Open**.



The image shows a 'Licence Wizard' dialog box. At the top, it says 'Licence type' and 'Apply an existing licence, request a free or trial licence.' Below this, there is a text box explaining that a licence can be requested over the Internet or imported from an offline file. There are four radio button options: 'Get a free 10 user licence', 'Get a 30 day trial licence', 'Import licence file(s)' (which is selected), and 'Licence Key'. A 'Browse...' button is next to the 'Import licence file(s)' option. Below the 'Licence Key' option, there is a text input field with the placeholder 'Enter your licence key (including dashes):'. At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'.

5. Click **Next**.
The license or licenses are installed, and activation is skipped.
6. Click **Finish**.

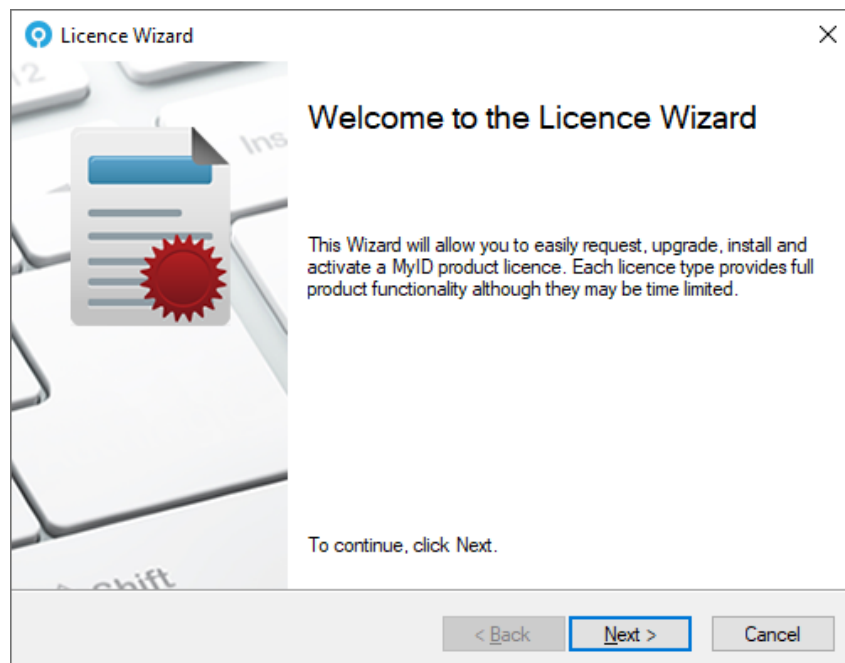
4.9.3 Entering an existing license key

A license key is issued by Intercede at the point of purchase. License keys *do* require Internet connectivity for installation, activation, and ongoing license reporting metrics. No private or confidential information is reported back to Intercede.

If you have multiple license keys, you must add them one at a time. Run the wizard again to add the second license key.

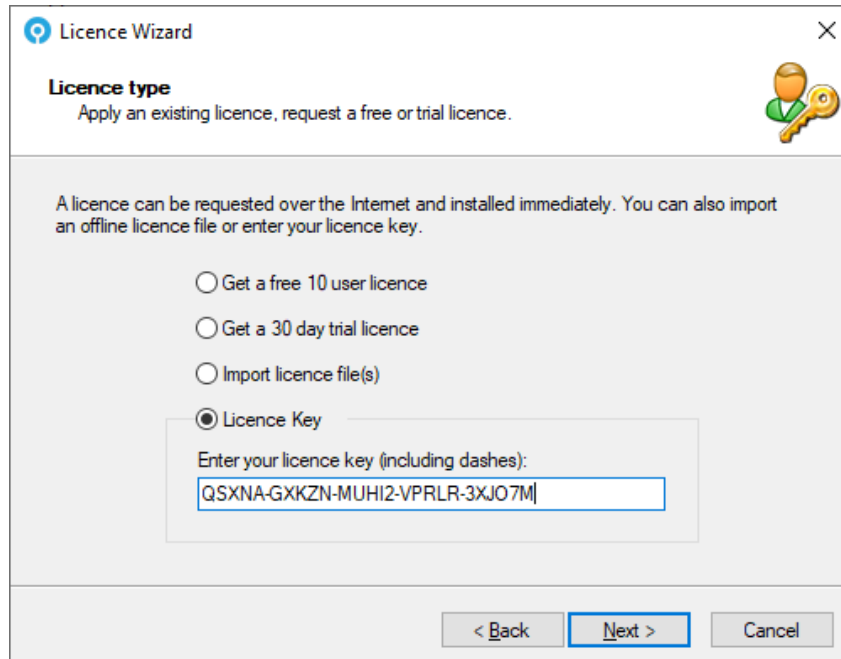
1. Start the Licence Wizard.

The Licence Wizard starts automatically when the MyID Management Console is first loaded. You can also start the wizard by clicking **Licence Wizard**, under **Actions** in the MMC.



2. Click **Next**.

3. Select **Licence Key** and enter the license key that Intercede sent you.



Licence Wizard

Licence type
Apply an existing licence, request a free or trial licence.

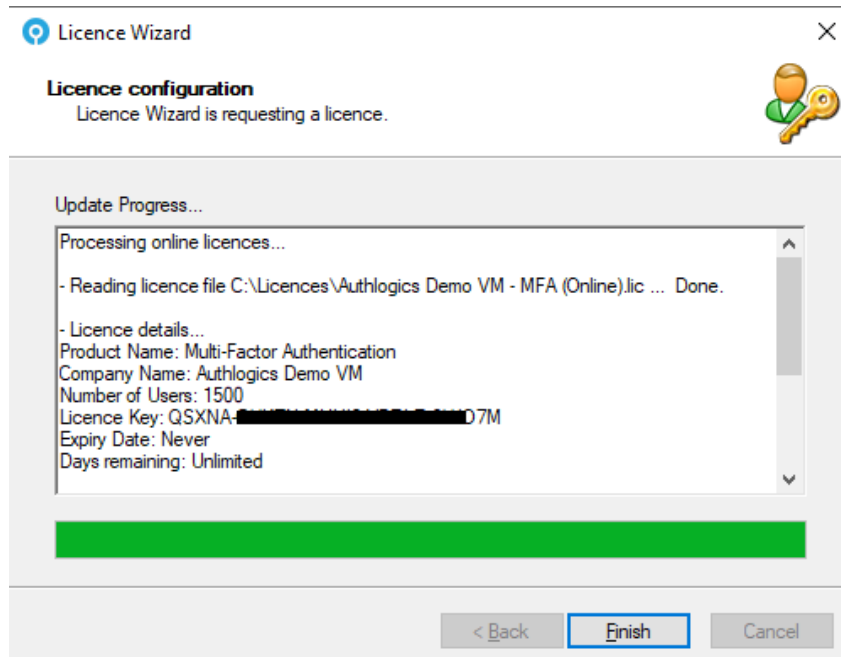
A licence can be requested over the Internet and installed immediately. You can also import an offline licence file or enter your licence key.

☐ Get a free 10 user licence
☐ Get a 30 day trial licence
☐ Import licence file(s)
☒ Licence Key

Enter your licence key (including dashes):
Q SXNA-GXKZN-MUHI2-VPRLR-3XJO7M

< Back Next > Cancel

4. Click **Next**.



Licence Wizard

Licence configuration
Licence Wizard is requesting a licence.

Update Progress...

Processing online licences...

- Reading licence file C:\Licences\Authlogics Demo VM - MFA (Online).lic ... Done.

- Licence details...

Product Name: Multi-Factor Authentication
Company Name: Authlogics Demo VM
Number of Users: 1500
Licence Key: Q SXNA-XXXXXXXXXXXX-07M
Expiry Date: Never
Days remaining: Unlimited

Finish

The license is installed and activated.

5. Click **Finish**.

4.10 MyID Password Security Management Wizard

The Password Security Management Wizard (PSM) is responsible for configuring domains in the Active Directory Forest for real-time and retrospective protection against known breached and shared passwords, as well as dormant accounts. This includes:

- Analyzing existing password hashes in AD.
- Setting a remediation protection schedule.
- Setting the account remediation policy.
- Setting the alerting actions and recipients.

Retrospective Protection: The MyID Authentication Server is responsible for doing all retrospective protection, remediation, and alerting work required by the schedule.

Real-Time Protection: The MyID Authentication Server works in conjunction with the MyID Domain Controller Agent (DCA) to provide real-time protection of Active Directory passwords. The Domain Controller Agent intercepts password changes at the Domain Controller as they happen and queries the MyID Authentication Server to check if the password should be accepted.

Note: A PSM Password Policy must be configured, enabled, and applied through Group Policy to the Domain Controllers as well as the MyID Authentication Servers for the policy to take effect. For more information, see section [7.1, Configuring the MyID Password Policy settings](#).

The MyID Authentication Server requires Internet access to query the MyID Password Breach Database in the Cloud.

A fully offline copy of the MyID Password Breach Database can be installed on the MyID Authentication Server; you can download this from:

www.intercede.com/support/downloads

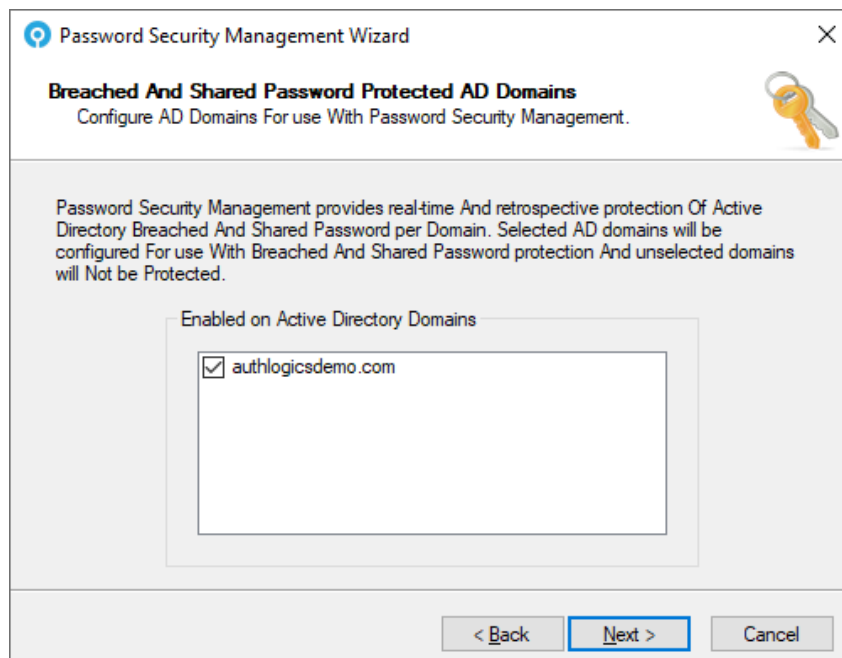
4.10.1 Starting the Password Security Management Wizard

1. Start the Password Security Management Wizard.

You can start the Password Security Management Wizard by clicking **Password Security Management Wizard**, under **Actions** in the MMC.

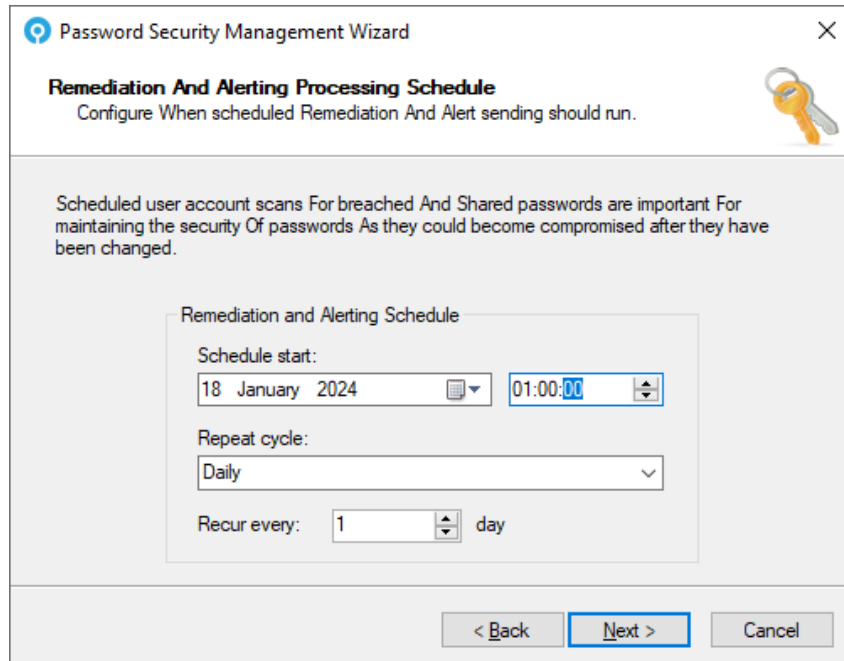


2. Click **Next**.



3. Select the domain or domains that you want to enable MyID PSM password protection on.

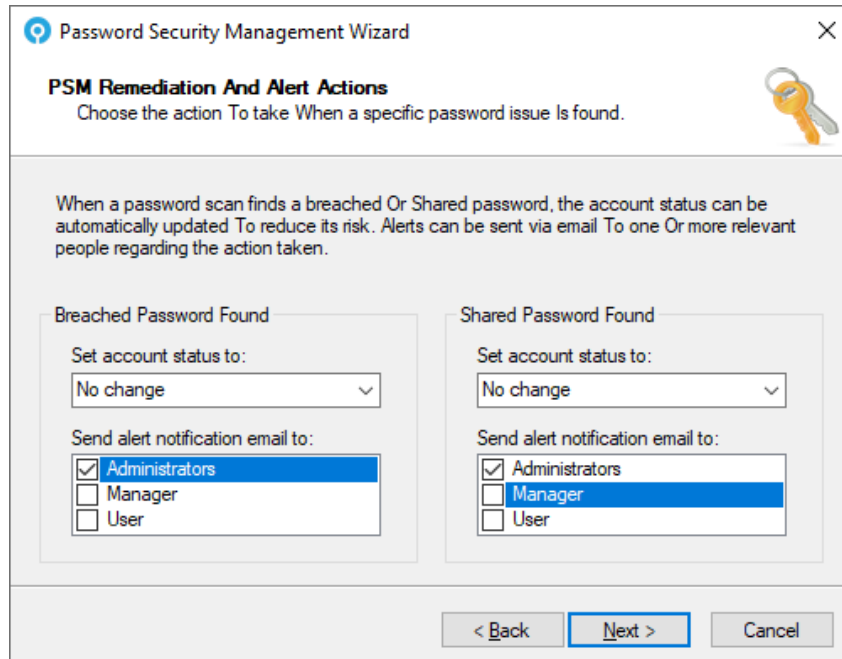
4. Click **Next**.



The MyID Authentication Server provides the ability to run Password Security Management remediation and alerting on a scheduled basis.

5. Select the **Schedule start** date and time.
This is when you want to schedule to start.
6. Select the Repeat cycle and recurrence cycle. The available options are:
 - Run Once
 - Hourly
 - Daily
 - Weekly
 - Monthly

7. Click **Next**.



8. Select what you want to happen when breached or shared passwords are found.

Password Security Management can alert Administrators, Managers or Users for newly detected breached or shared passwords.

PSM also includes auto-remediation functionality where accounts can be disabled or users can be forced to change their password at next logon for breached or shared passwords.

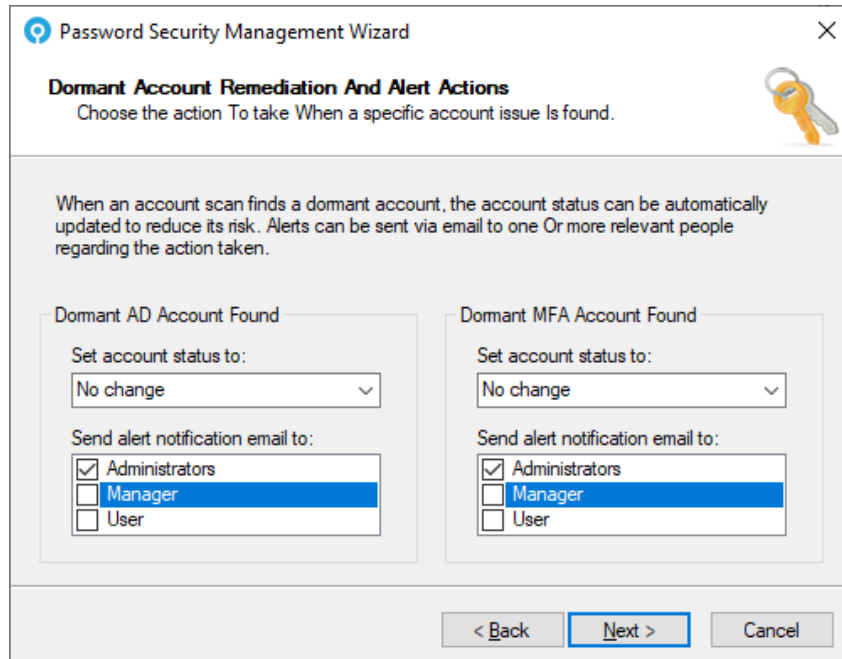
You must set the account status for detected breached passwords and shared passwords to one of the following:

- No change.
- Must change password at next logon.
- Account is disabled.

You can also select who receives an alert about the breached or shared password.

- Administrators.
- Managers.
- Users.

9. Click **Next**.



The screenshot shows the 'Password Security Management Wizard' window, specifically the 'Dormant Account Remediation And Alert Actions' step. The window title is 'Password Security Management Wizard' with a close button (X) in the top right corner. Below the title bar, the section header is 'Dormant Account Remediation And Alert Actions' with a subtitle 'Choose the action To take When a specific account issue Is found.' and a key icon. The main content area explains: 'When an account scan finds a dormant account, the account status can be automatically updated to reduce its risk. Alerts can be sent via email to one Or more relevant people regarding the action taken.' There are two side-by-side configuration panels. The left panel is titled 'Dormant AD Account Found' and the right panel is titled 'Dormant MFA Account Found'. Both panels have a 'Set account status to:' dropdown menu with 'No change' selected. Below each dropdown is a 'Send alert notification email to:' section with three checkboxes: 'Administrators' (checked), 'Manager' (selected/highlighted), and 'User' (unchecked). At the bottom of the wizard, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

10. Select what happens when dormant Active Directory or MFA accounts are found.

Password Security Management can alert Administrators, Managers or Users for newly detected dormant Active Directory or MFA accounts.

PSM also includes auto-remediation functionality that can disable accounts or force users to change their password at their next logon for breached or shared passwords.

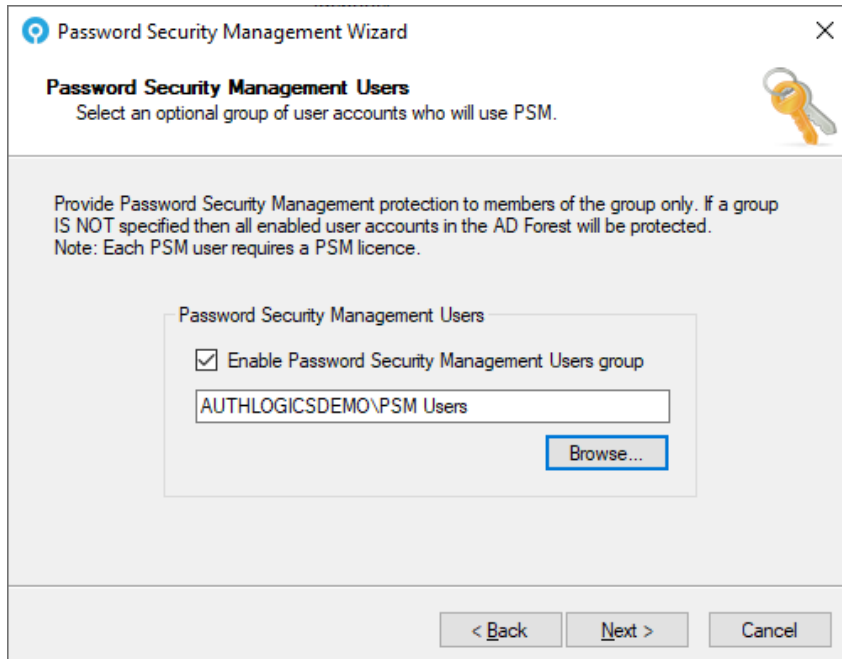
You must set the account status for detected dormant Active Directory or MFA accounts to one of the following:

- No change.
- Must change password at next logon.
- Account is disabled.

You can also select who receives an alert about the detected dormant Active Directory or MFA accounts.

- Administrators.
- Managers.
- Users.

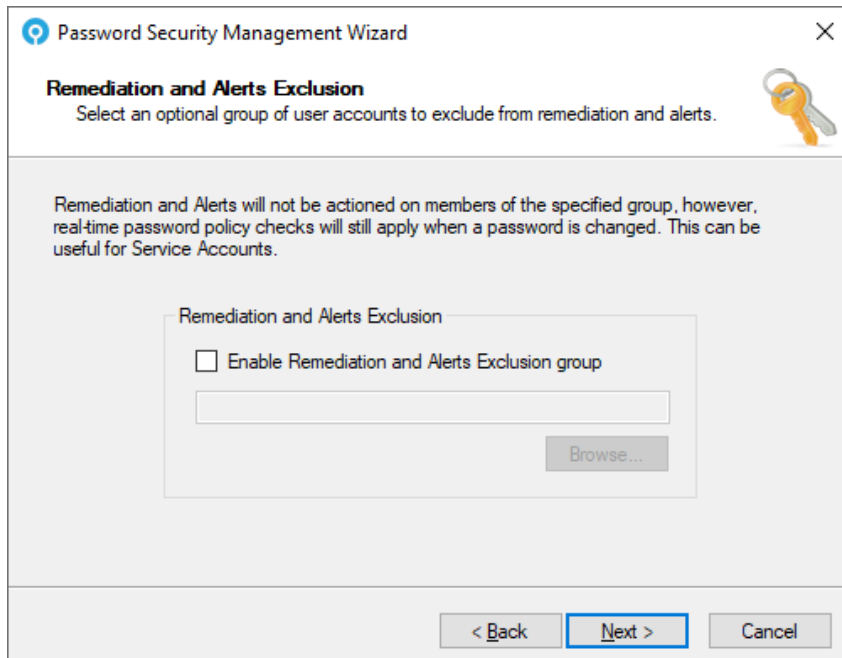
11. Click **Next**.



The screenshot shows the 'Password Security Management Wizard' window. The title bar says 'Password Security Management Wizard'. The main heading is 'Password Security Management Users' with a sub-instruction: 'Select an optional group of user accounts who will use PSM.' Below this, a text box explains: 'Provide Password Security Management protection to members of the group only. If a group IS NOT specified then all enabled user accounts in the AD Forest will be protected. Note: Each PSM user requires a PSM licence.' There is a checkbox labeled 'Enable Password Security Management Users group' which is checked. Below the checkbox is a text field containing 'AUTHLOGICSDemo\PSM Users' and a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

To limit which users can use PSM (and therefore require a license), select **Enable Password Security Management Users group** and then click **Browse** to select an Active Directory Group containing the user accounts to include.

12. Click **Next**.



The screenshot shows the 'Password Security Management Wizard' window. The title bar says 'Password Security Management Wizard'. The main heading is 'Remediation and Alerts Exclusion' with a sub-instruction: 'Select an optional group of user accounts to exclude from remediation and alerts.' Below this, a text box explains: 'Remediation and Alerts will not be actioned on members of the specified group, however, real-time password policy checks will still apply when a password is changed. This can be useful for Service Accounts.' There is an unchecked checkbox labeled 'Enable Remediation and Alerts Exclusion group'. Below the checkbox is an empty text field and a 'Browse...' button. At the bottom are three buttons: '< Back', 'Next >', and 'Cancel'.

13. Click **Next**.

The screenshot shows a window titled "Password Security Management Wizard" with a close button (X) in the top right corner. Below the title bar, the text "Public Email Domain Breach Monitoring" is displayed, followed by the instruction "Configure the list of email domain names to monitor for public breaches." To the right of this text is a key icon. Below this, a paragraph states: "If an email address at one of the specified domains is found in a public breach then PSM will display the information on the dashboard." Underneath this text is a section titled "Public Email Domains" containing a text area with the domains "authlogicsdemo.com" and "intercede.com". To the right of the text area are "Import" and "Clear" buttons. At the bottom of the window are "< Back", "Next >" (highlighted with a blue border), and "Cancel" buttons.

14. List the email domains that you want to monitor for password breaches. These do not have to be local domains.

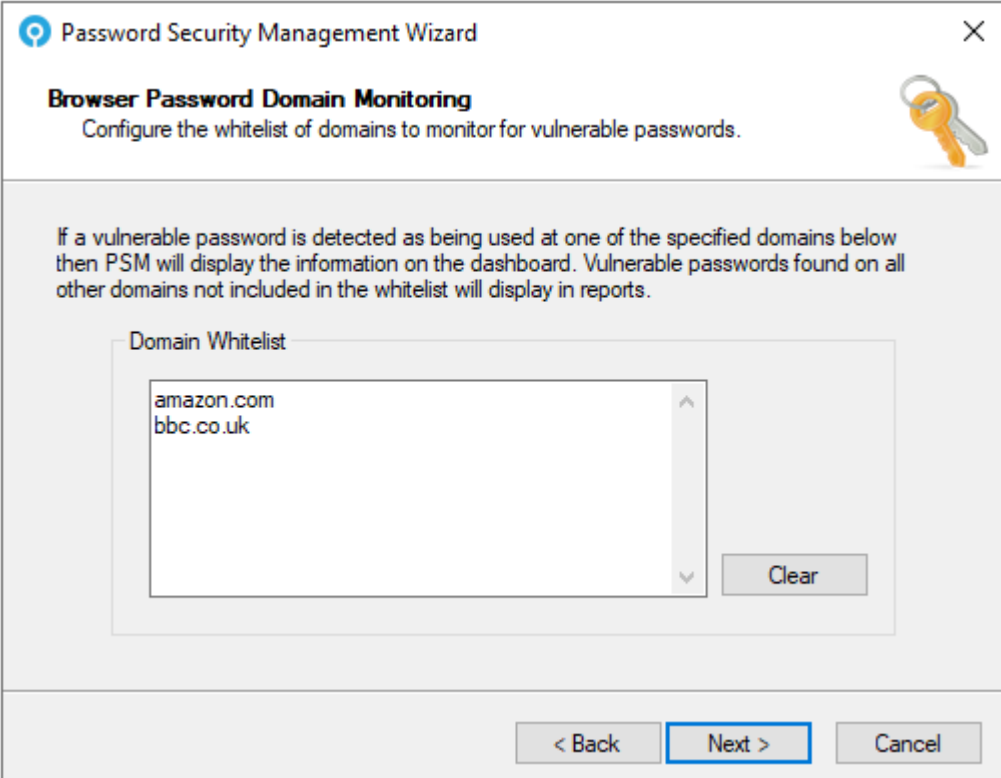
To manually add domains, enter each domain on a new line.

To import all accepted domains from any Microsoft Exchange servers in your Active Directory, click **Import**.

The screenshot shows a small dialog box titled "Password Security Management Wizard" with a close button (X) in the top right corner. Inside the dialog, there is a question mark icon followed by the text: "Are you sure you want to import all of the 'Accepted Domains' from Microsoft Exchange?". At the bottom of the dialog are "Yes" and "No" buttons, with the "No" button highlighted with a blue border.

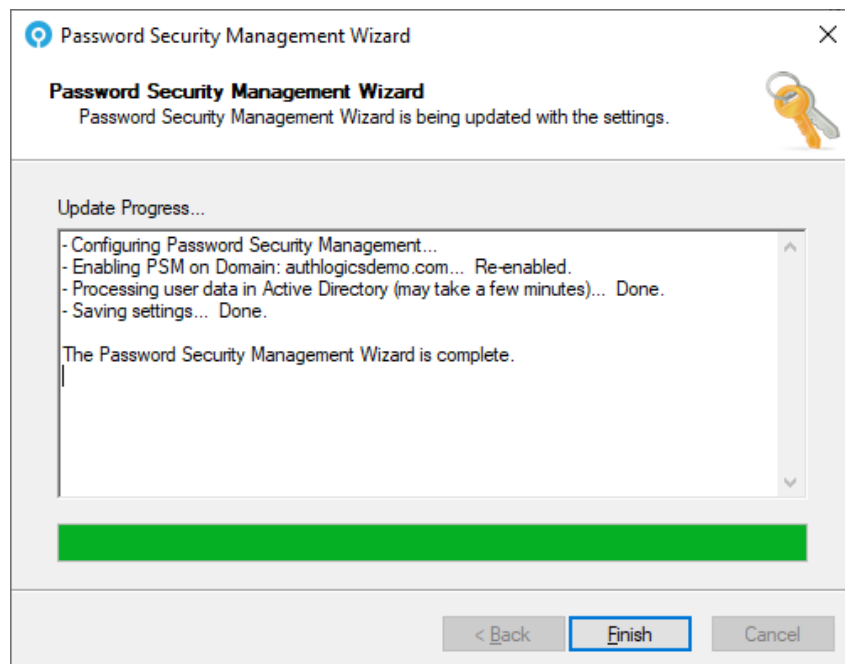
Click **Yes**.

15. Click **Next**.



The screenshot shows a window titled "Password Security Management Wizard" with a close button (X) in the top right corner. Below the title bar, the section is "Browser Password Domain Monitoring" with a subtitle "Configure the whitelist of domains to monitor for vulnerable passwords." and a key icon. A text block explains: "If a vulnerable password is detected as being used at one of the specified domains below then PSM will display the information on the dashboard. Vulnerable passwords found on all other domains not included in the whitelist will display in reports." Below this is a "Domain Whitelist" section containing a text area with "amazon.com" and "bbc.co.uk" on separate lines, a "Clear" button, and scroll arrows. At the bottom are "< Back", "Next >" (highlighted with a blue border), and "Cancel" buttons.

16. In the **Domain Whitelist** box, list the website domains for which you want to view the password breach information in Web Management Portal dashboards. These do not have to be local domains.
- Enter each domain on a new line.
- For more information on the browser password breach Web Management Portal dashboards, see the *Password Security* section of the [Web Management Portal User Guide](#).
17. Click **Next**.
- Password Security Management is configured.



18. Click **Finish**.

4.11 YubiKey OTP Configuration Wizard

The YubiKey OTP Configuration Wizard is responsible for managing reprogrammed YubiKey tokens; this means that YubiKey OTPs are processed by the MyID Authentication Server and that access to the Internet-based YubiKey servers is *not* required for validation.

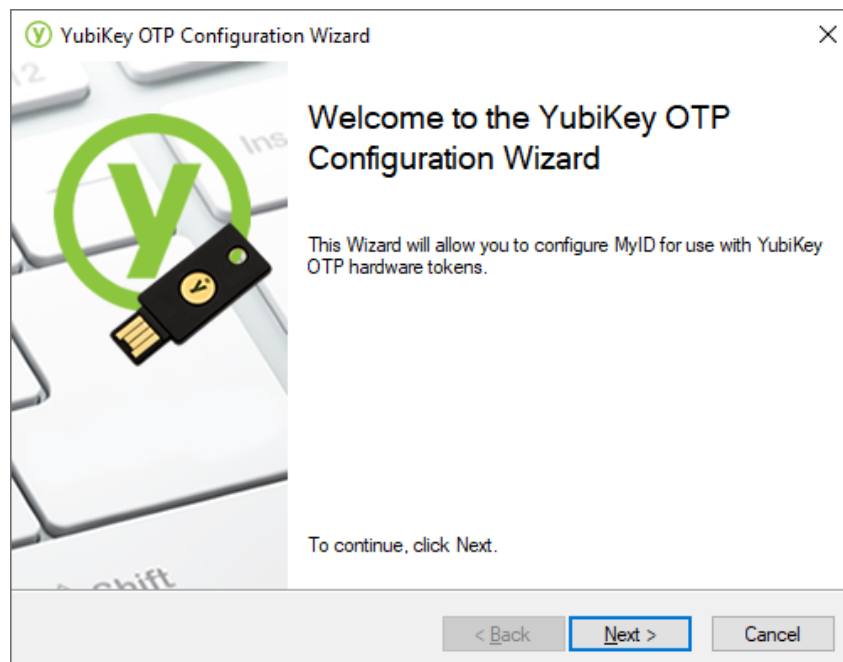
If you want to validate YubiKey OTPs using the Internet-based YubiKey servers for tokens that have not been reprogrammed, the MyID Authentication Server still requires Internet access.

For information on how to reprogram YubiKey tokens and create a YubiKey Personalization CSV file, see the *Configuring YubiKey devices* section of the [YubiKey Reprogramming Guide](#).

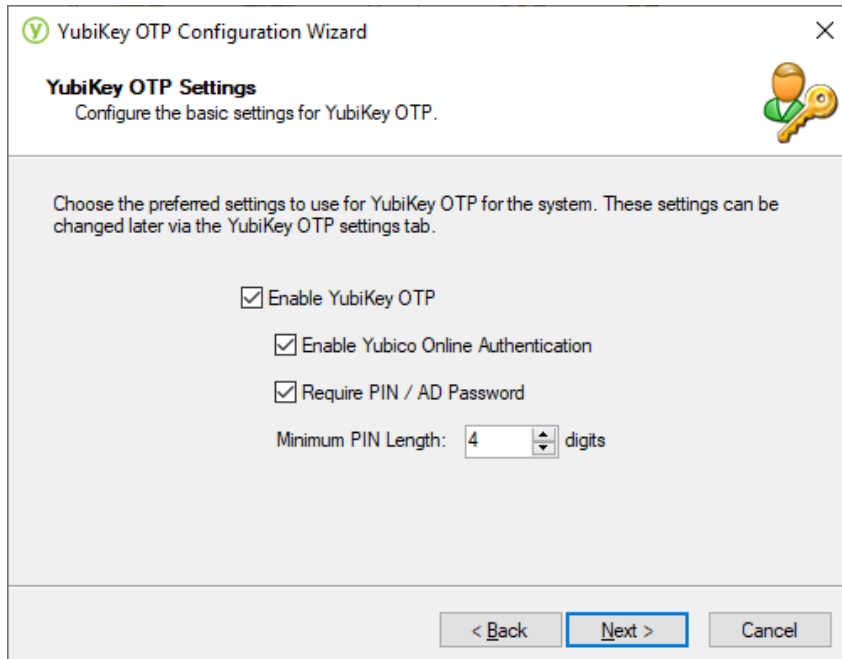
4.11.1 Starting the YubiKey OTP Configuration Wizard

1. Start the YubiKey OTP Configuration Wizard.

You can start the YubiKey OTP Configuration Wizard by clicking **YubiKey OTP Configuration Wizard**, under **Actions** in the MMC.



2. Click **Next**.



The image shows a 'YubiKey OTP Configuration Wizard' dialog box. It has a title bar with a green 'Y' icon and a close button. The main content area is titled 'YubiKey OTP Settings' and includes a subtitle 'Configure the basic settings for YubiKey OTP.' Below this, there is a paragraph: 'Choose the preferred settings to use for YubiKey OTP for the system. These settings can be changed later via the YubiKey OTP settings tab.' There are three checked checkboxes: 'Enable YubiKey OTP', 'Enable Yubico Online Authentication', and 'Require PIN / AD Password'. Below these is a 'Minimum PIN Length' field with a value of '4' and a unit of 'digits'. At the bottom, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

YubiKey OTP Configuration Wizard

YubiKey OTP Settings
Configure the basic settings for YubiKey OTP.

Choose the preferred settings to use for YubiKey OTP for the system. These settings can be changed later via the YubiKey OTP settings tab.

☒ Enable YubiKey OTP

☒ Enable Yubico Online Authentication

☒ Require PIN / AD Password

Minimum PIN Length: 4 digits

< Back Next > Cancel

3. Configure YubiKey OTP options.

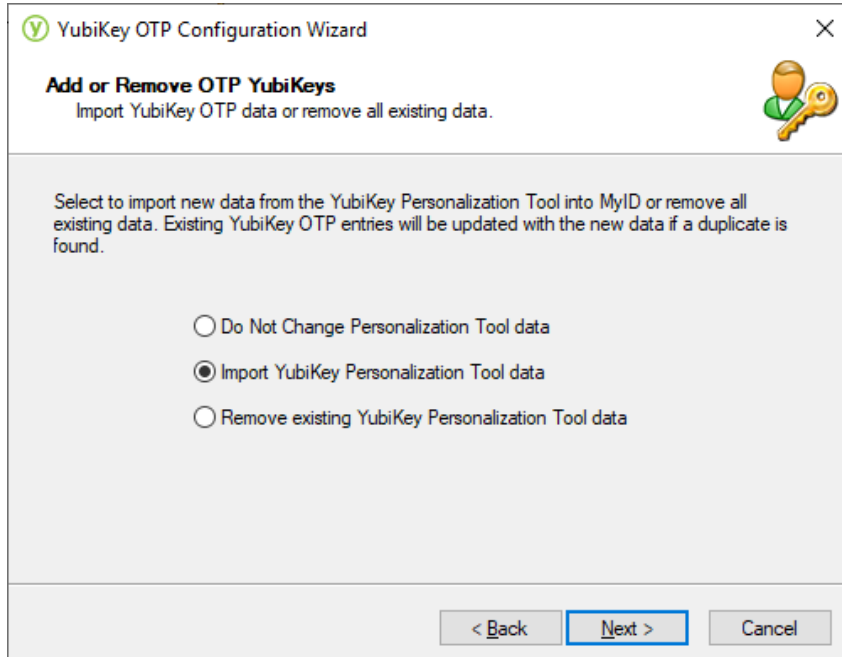
Select **Enable Yubico Online Authentication** to send YubiKey OTPs to Yubico's servers to verify the validity of the YubiKey token.

Choose if you want the user to require knowledge as well as the YubiKey when logging in. Knowledge adds a factor to the authentication. For the knowledge, the user's Active Directory password can be used instead of a PIN, or the user can select a PIN.

Alternatively, a PIN can be automatically generated, or not required at all for OTP-only validation. To require knowledge, select the **Require PIN / AD Password** option.

If you have enabled knowledge, choose the **Minimum PIN Length**.

4. Click **Next**.



YubiKey OTP Configuration Wizard

Add or Remove OTP YubiKeys
Import YubiKey OTP data or remove all existing data.

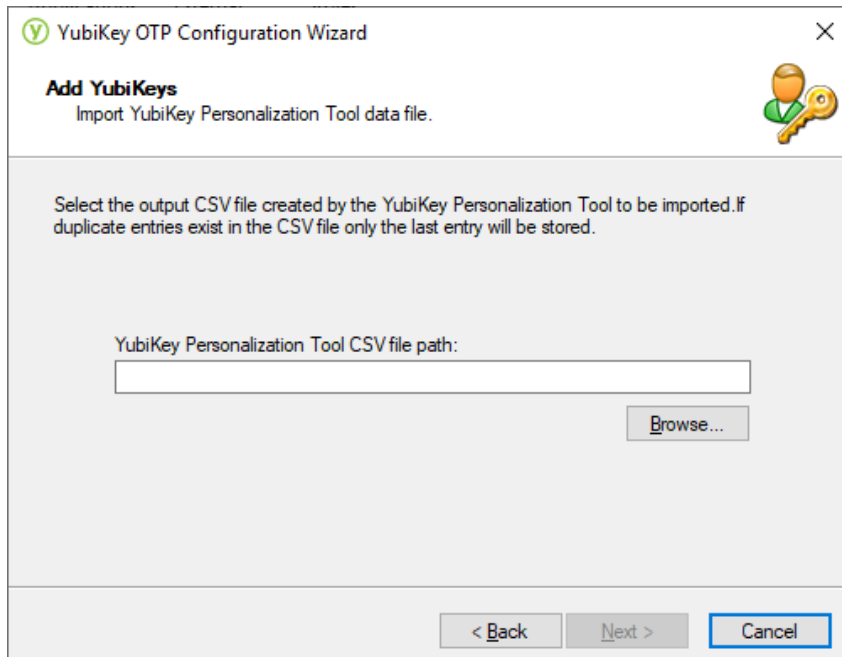
Select to import new data from the YubiKey Personalization Tool into MyID or remove all existing data. Existing YubiKey OTP entries will be updated with the new data if a duplicate is found.

☐ Do Not Change Personalization Tool data
☒ Import YubiKey Personalization Tool data
☐ Remove existing YubiKey Personalization Tool data

< Back **Next >** Cancel

5. Select **Import YubiKey Personalization Tool data**.

6. Click **Next**.



YubiKey OTP Configuration Wizard

Add YubiKeys
Import YubiKey Personalization Tool data file.

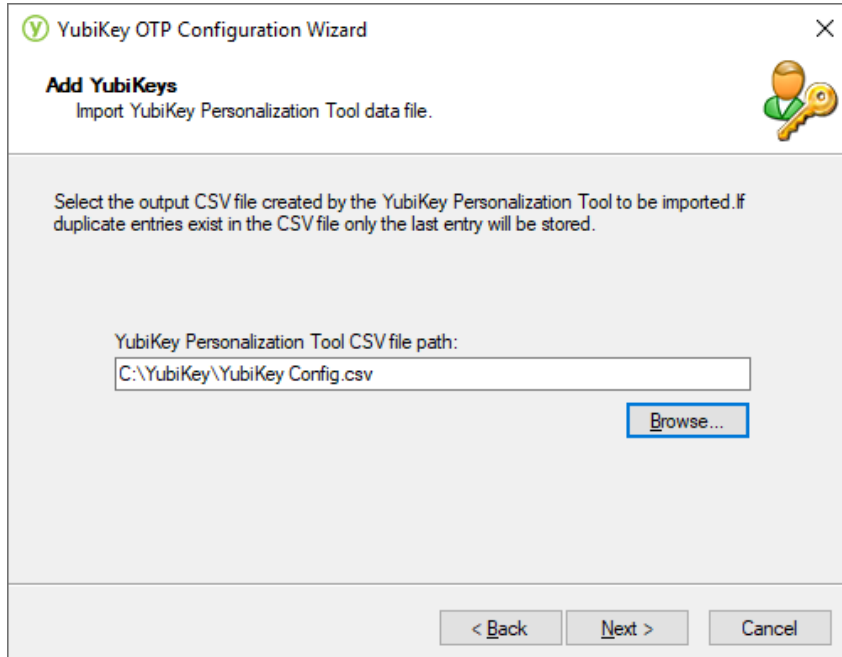
Select the output CSV file created by the YubiKey Personalization Tool to be imported. If duplicate entries exist in the CSV file only the last entry will be stored.

YubiKey Personalization Tool CSV file path:

Browse...

< Back Next > **Cancel**

- Click **Browse** and select the YubiKey Personalization Tool generated CSV file.



YubiKey OTP Configuration Wizard

Add YubiKeys
Import YubiKey Personalization Tool data file.

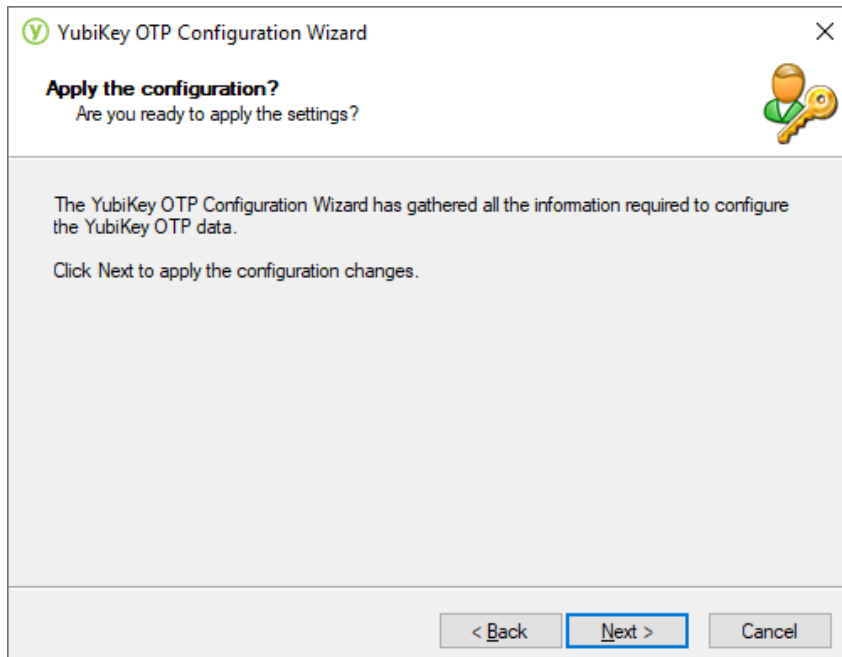
Select the output CSV file created by the YubiKey Personalization Tool to be imported. If duplicate entries exist in the CSV file only the last entry will be stored.

YubiKey Personalization Tool CSV file path:

Browse...

< Back Next > Cancel

- Click **Next**.



YubiKey OTP Configuration Wizard

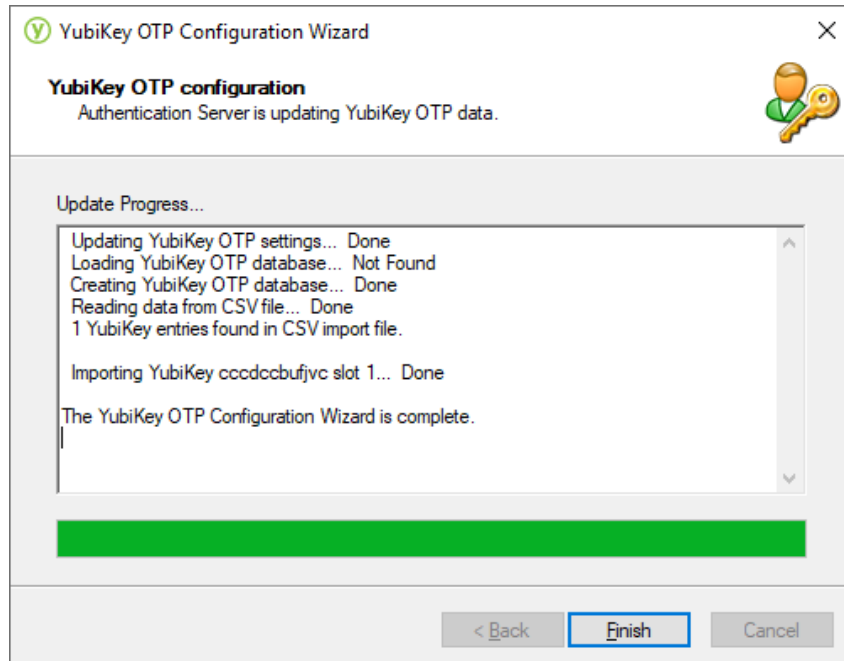
Apply the configuration?
Are you ready to apply the settings?

The YubiKey OTP Configuration Wizard has gathered all the information required to configure the YubiKey OTP data.

Click Next to apply the configuration changes.

< Back **Next >** Cancel

9. Click **Next**.

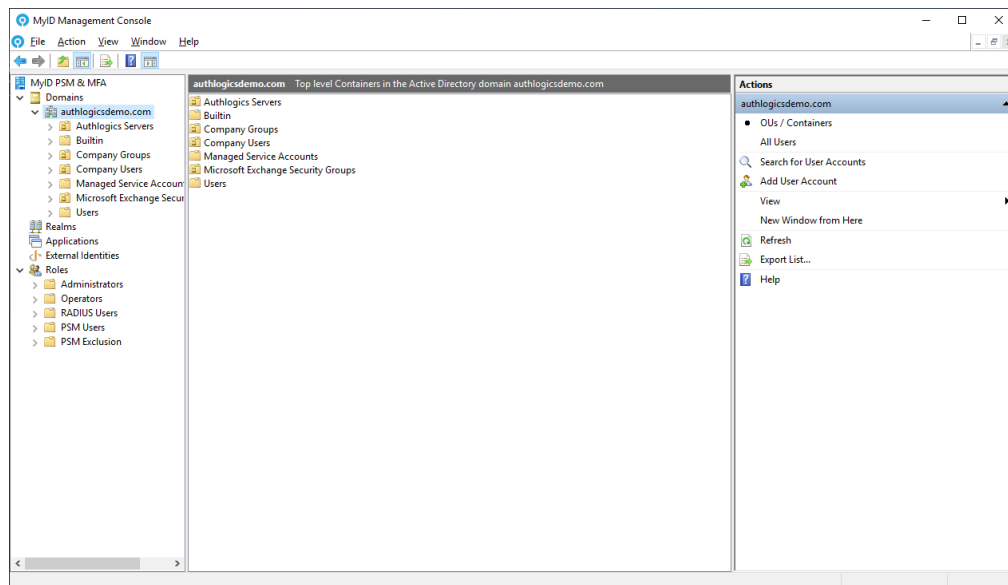


The configuration is applied and the YubiKey database is imported.

10. Click **Finish**.

5 Administering the MyID Authentication Server

The MyID Management Console provides administrators with the ability to configure MyID settings and administer users. Functionality and options may differ depending on the product license installed.



The MyID Management Console provides Administrators with the ability to manage the following:

- Directory Configuration
- MyID Global Settings
- MyID Users in Domains or Realms
- Applications
- External Identities
- User Roles

5.1 MyID Management Console views

The MyID Management Console displays both the MFA and PSM users.



PSM only users.



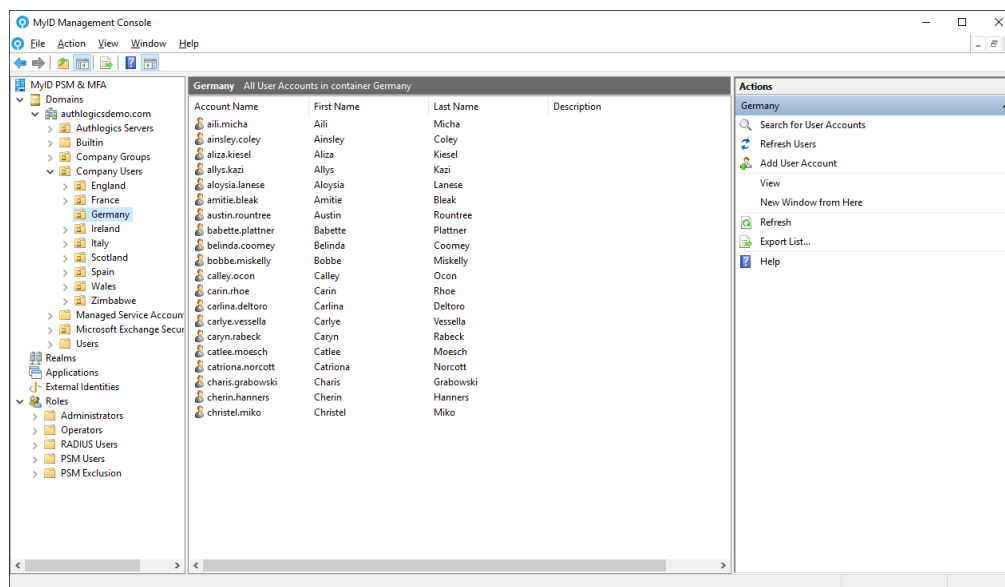
MFA only users.

The MyID Management Console is suited to small deployments and also scales to very large Active Directory environments. This is achieved by utilizing the **OUs / Containers** and the **All Users** view for Active Directory Domains, and a Realms view for External users.

The Active Directory view can be chosen by selecting the domain and toggling between the two options.

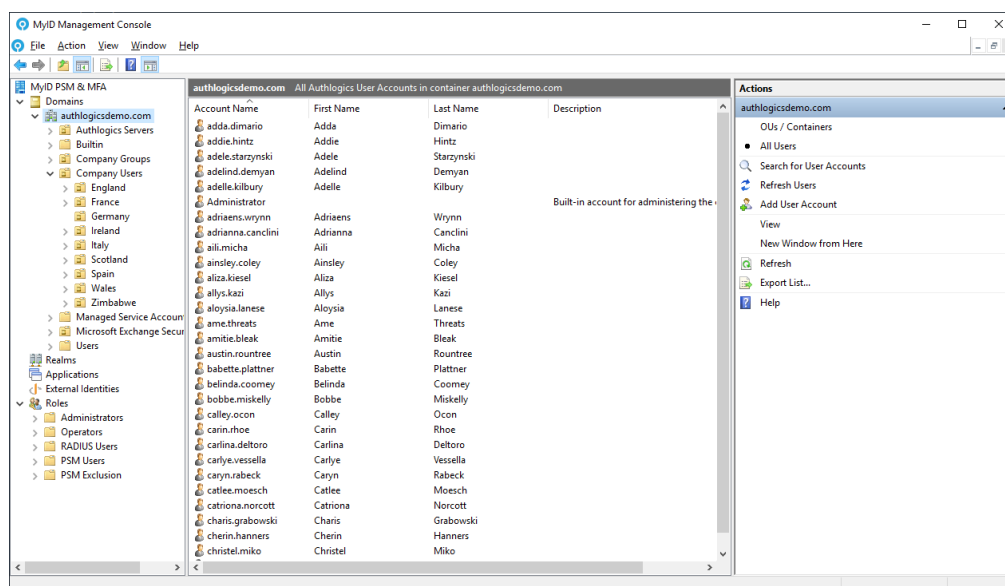
5.1.1 OUs / Containers view

The OUs / Containers view is the default view that allows the Active Directory OU structure to be traversed. You can search for user accounts from the domain level or an OU or Container. All users in an OU tree can be found for by searching for the wildcard “*”.



5.1.2 All Users view

The **All Users** view is a single view that lists all users for the entire domain. Since all users are loaded for the domain at once this view may be slower to load on large domains.

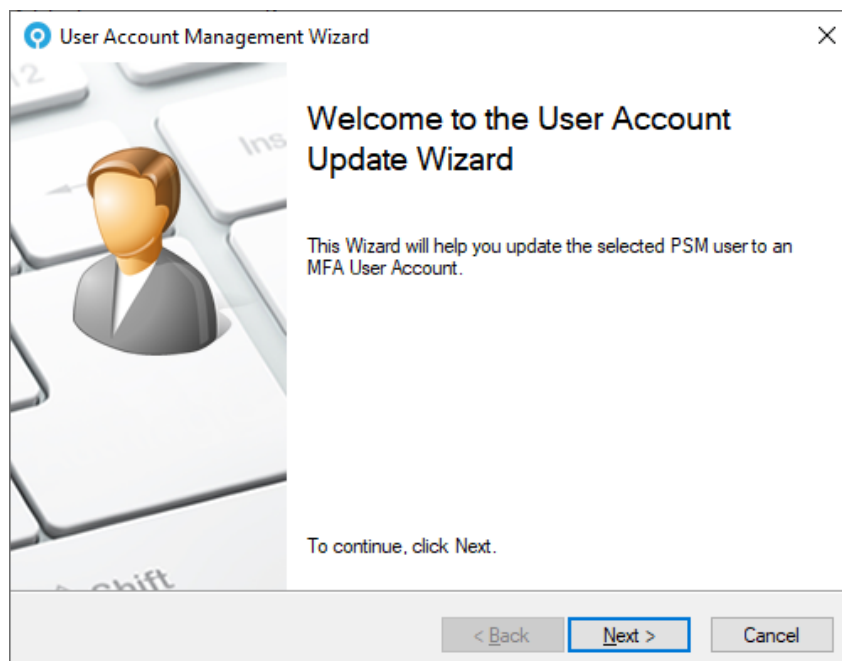
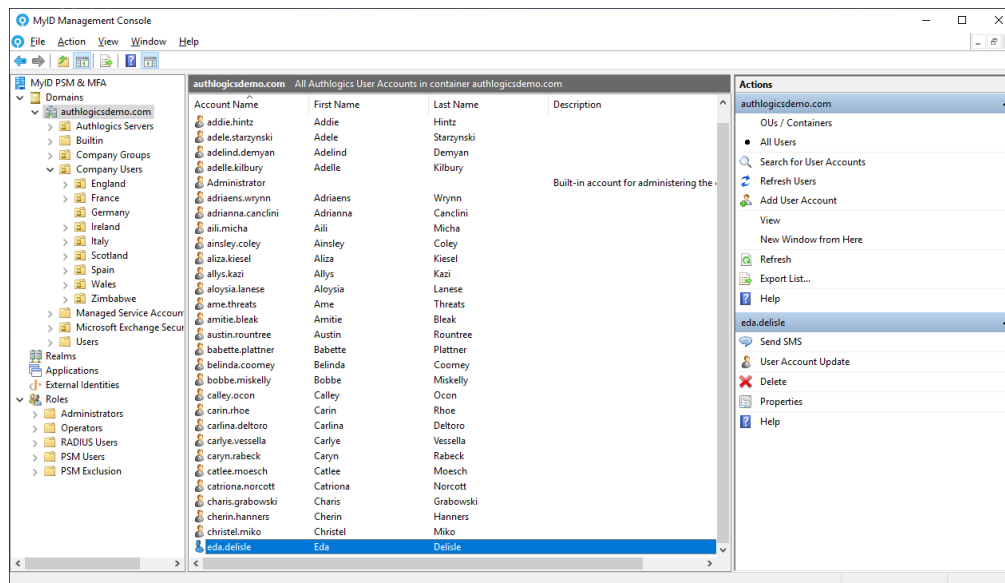


5.1.3 Updating PSM users

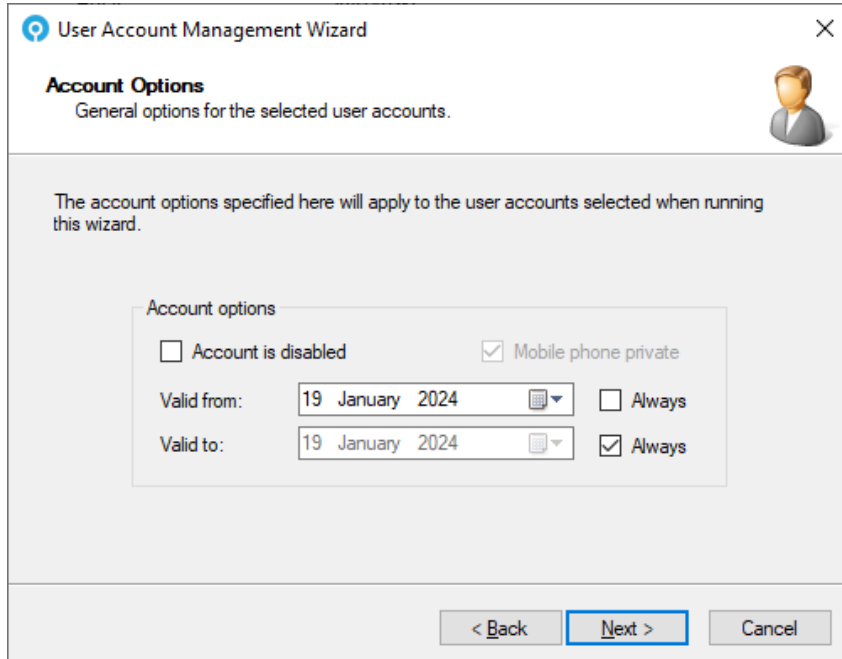
PSM users are automatically added to the MyID Management Console when the user interacts with MyID using either an Active Directory password change or a Self-service portal login. These users can be made into MFA users (provided a valid MFA license exists) by running the **User Account Update** user action.

1. Start the User Account Update Wizard.

You can start the User Account Update Wizard for a user from the MMC by clicking on a user and then clicking **User Account Update**, under their username in **Actions**.



2. Click **Next**.

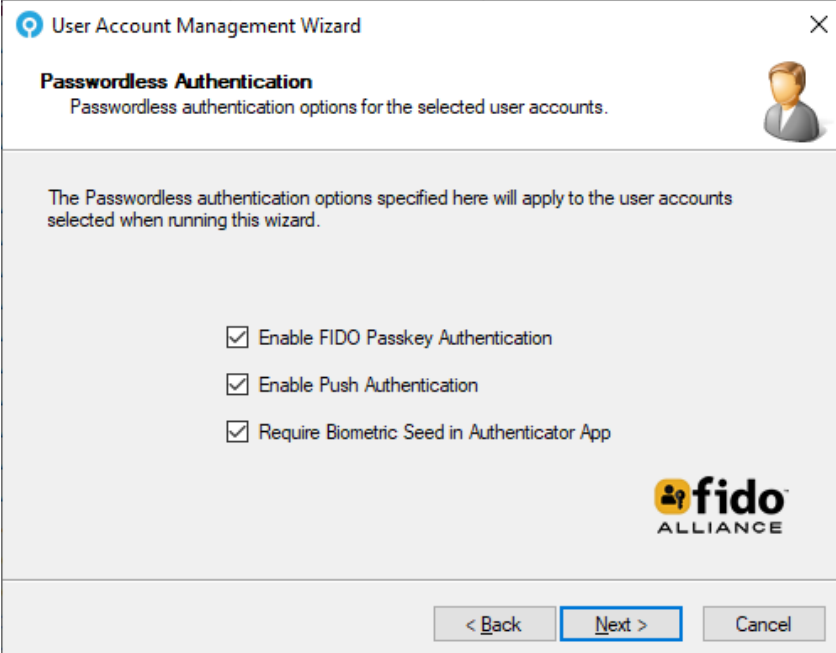


The screenshot shows the 'User Account Management Wizard' window, specifically the 'Account Options' step. The window title is 'User Account Management Wizard' with a close button (X) in the top right corner. Below the title bar, the section is titled 'Account Options' with a subtitle 'General options for the selected user accounts.' and a user icon. A message states: 'The account options specified here will apply to the user accounts selected when running this wizard.' The main area contains a box titled 'Account options' with the following settings: 'Account is disabled' is unchecked, 'Mobile phone private' is checked, 'Valid from:' is set to '19 January 2024', 'Valid to:' is set to '19 January 2024', 'Always' (for valid from) is unchecked, and 'Always' (for valid to) is checked. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

3. Set the **Account options**.

Account options determine the user's initial state. You can give accounts start and end validity dates and create them as disabled accounts for later use. You can also specify the mobile phone privacy setting.

4. Click **Next**.



The screenshot shows a 'User Account Management Wizard' window. The title bar says 'User Account Management Wizard' with a close button. Below the title bar, the section is 'Passwordless Authentication' with a subtitle 'Passwordless authentication options for the selected user accounts.' and a user icon. The main content area states: 'The Passwordless authentication options specified here will apply to the user accounts selected when running this wizard.' Below this, there are three checked checkboxes: 'Enable FIDO Passkey Authentication', 'Enable Push Authentication', and 'Require Biometric Seed in Authenticator App'. The FIDO Alliance logo is in the bottom right of the content area. At the bottom of the window, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

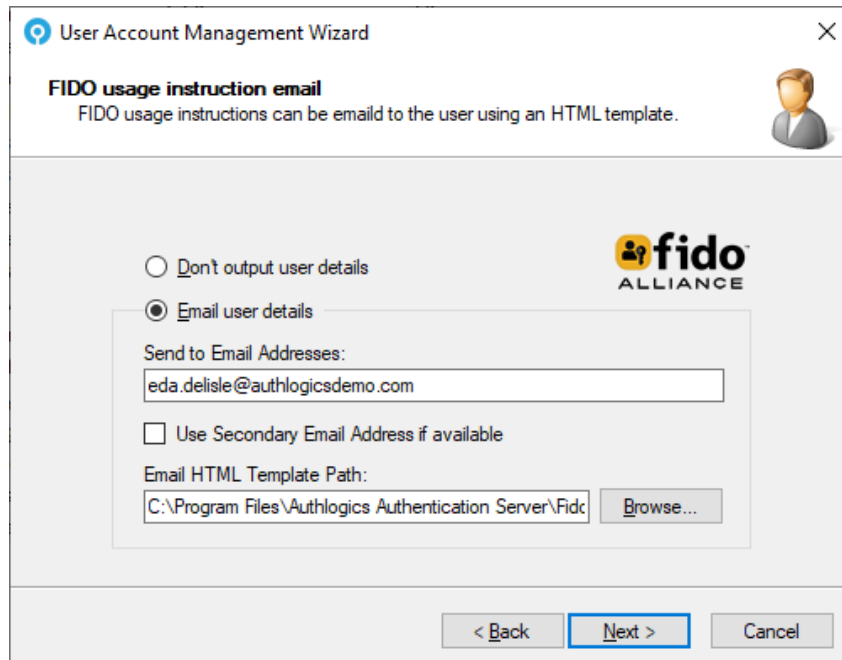
Choose if you want to:

- **Enable FIDO Passkey Authentication.**
- **Enable Push Authentication.**
- **Require Biometric Seed in Authenticator App.**

This option makes the user required to provide valid biometrics when accessing the Authenticator App.

5. Click **Next**.

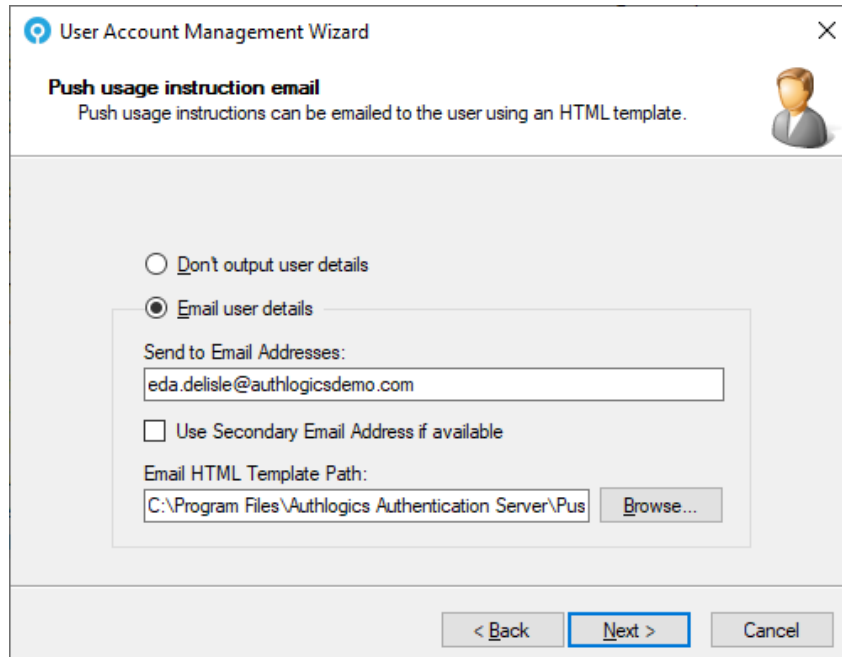
6. If you chose to **Enable FIDO Passkey Authentication** for this user, the FIDO instruction letter can be emailed to the user.



The screenshot shows the 'User Account Management Wizard' window. The title bar says 'User Account Management Wizard'. The main heading is 'FIDO usage instruction email'. Below it, a subtitle says 'FIDO usage instructions can be emailed to the user using an HTML template.' There is a small icon of a person in a suit. The main content area has two radio buttons: 'Don't output user details' (unselected) and 'Email user details' (selected). Below the radio buttons is a text box labeled 'Send to Email Addresses:' containing the email address 'eda.delisle@authlogicsdemo.com'. There is a checkbox labeled 'Use Secondary Email Address if available' which is unchecked. Below that is a text box labeled 'Email HTML Template Path:' containing the path 'C:\Program Files\Authlogics Authentication Server\Fido'. To the right of the text box is a 'Browse...' button. At the bottom right are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'. The FIDO Alliance logo is visible in the top right corner of the main content area.

If a secondary email address is configured, the email can be sent to the alternate address.

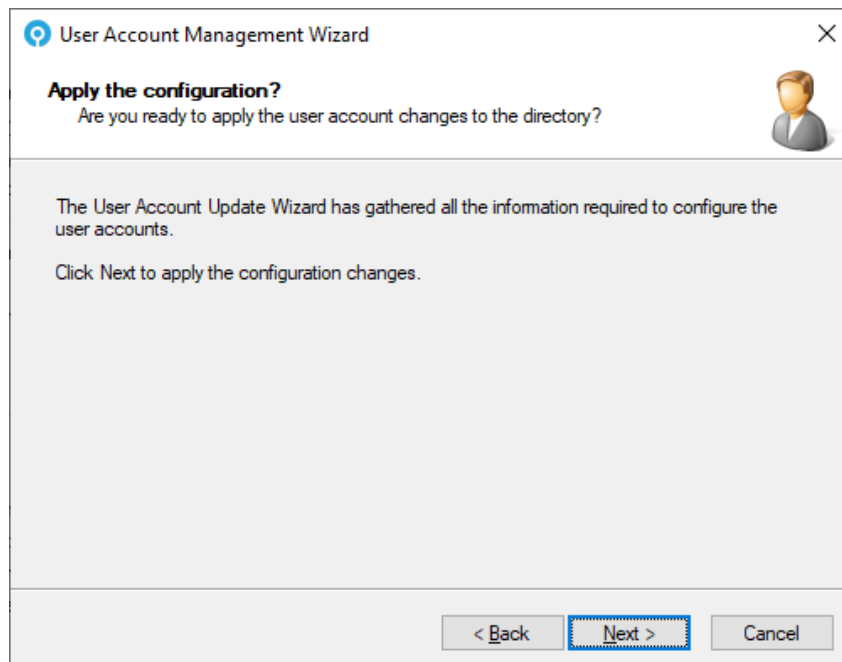
7. Click **Next**.
8. If you chose to **Enable Push Authentication** for this user, a PUSH instruction letter can be emailed to the user.



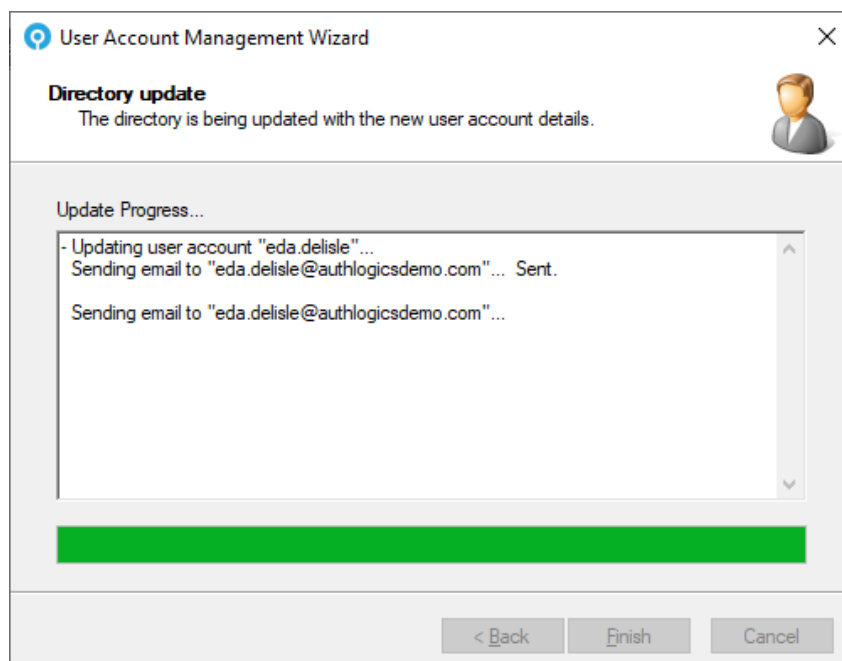
The screenshot shows the 'User Account Management Wizard' window. The title bar says 'User Account Management Wizard'. The main heading is 'Push usage instruction email'. Below it, a subtitle says 'Push usage instructions can be emailed to the user using an HTML template.' There is a small icon of a person in a suit. The main content area has two radio buttons: 'Don't output user details' (unselected) and 'Email user details' (selected). Below the radio buttons is a text box labeled 'Send to Email Addresses:' containing the email address 'eda.delisle@authlogicsdemo.com'. There is a checkbox labeled 'Use Secondary Email Address if available' which is unchecked. Below that is a text box labeled 'Email HTML Template Path:' containing the path 'C:\Program Files\Authlogics Authentication Server\Pus'. To the right of the text box is a 'Browse...' button. At the bottom right are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

If a secondary email address is configured, the email can be sent to the alternate address.

9. Click **Next**.



10. Click **Next**.
This applies the configuration changes.

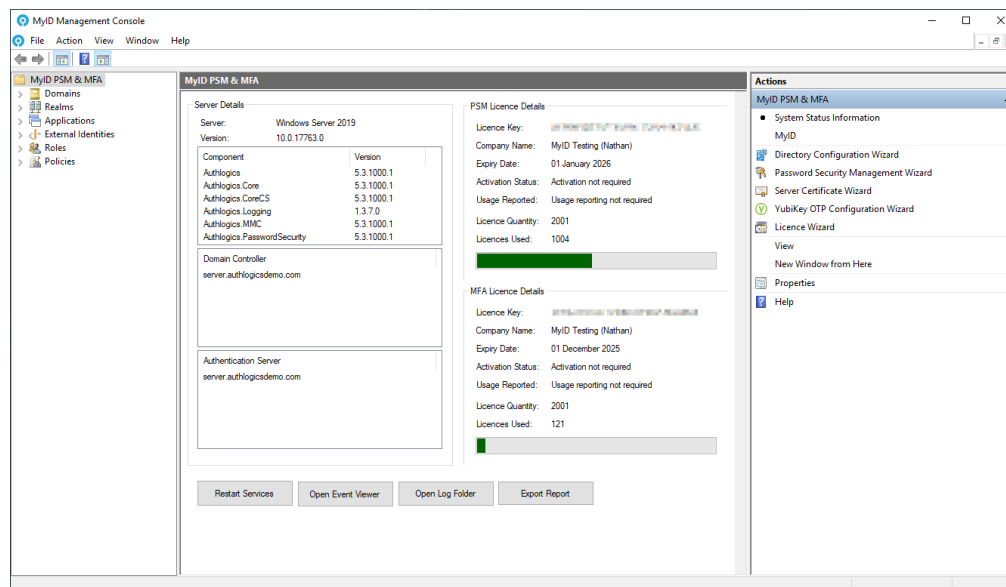


The user account is updated.

11. Click **Finish**.

5.2 MyID Authentication Server overview

When you open the MyID Management Console or click the high-level **MyID** node, you can see your MyID Authentication Server overview.



This shows your server details and licensing information, and several tools to help you debug:

- For information on viewing your server details, see section [5.2.1, *Server details*](#).
- For information on viewing your licensing information, see section [5.2.2, *Licensing information*](#).
- For information on the debugging tools, see section [5.2.3, *Debugging tools*](#).

5.2.1 Server details

You can view the version of your server and the version of each MyID component on your server.

You can also view the address or addresses of your domain controllers, as well as the address or addresses of your MyID Authentication Server.

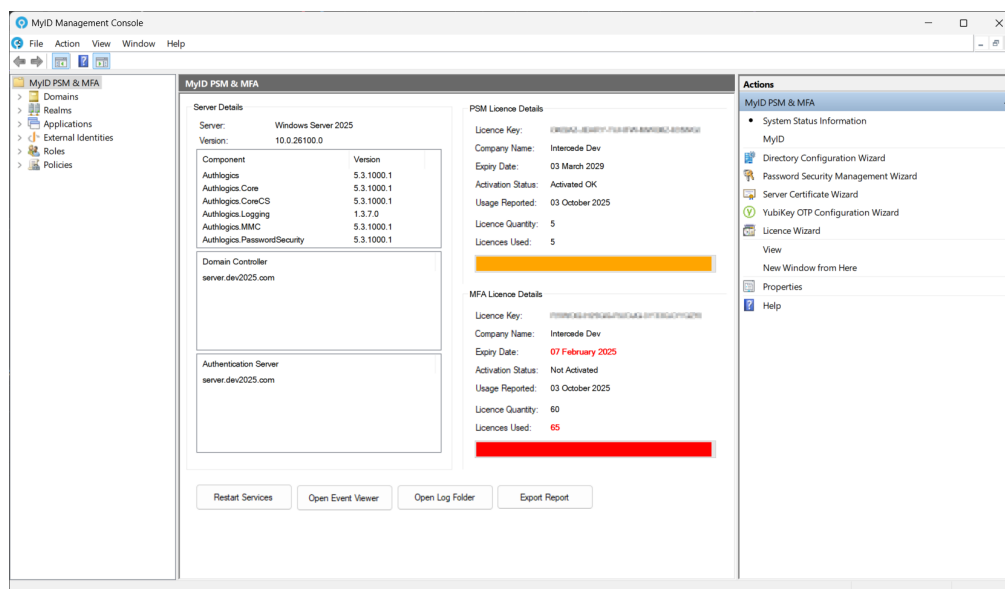
5.2.2 Licensing information

Details of your licenses are displayed for your information, including the number of licenses supported and the dates during which they are valid.

If you have used 90% or more of your licenses, the bar displaying the number of licenses is orange.

If you have used more licenses than you have available, the bar displaying the percentage of licenses used is red, and the number of **Licences Used** is red and bold.

If your license has expired, the expiry date is red and bold.



You can update or remove your licenses on the Licence tab in the global settings; for more information, see section [5.3.8, Licence tab](#).

5.2.3 Debugging tools

If you are experiencing issues with MyID MFA or PSM, you may need to speak to Intercede Support. If you do, they may ask you to provide information regarding your issue or to restart your MyID applications. The buttons at the bottom of your MyID Authentication Server overview can help with these initial activities.

The **Restart Services** button restarts the MyID web services and the MyID web applications from your application pool.

The following buttons can help you provide the correct information to Intercede Support:

- **Open Event Viewer** – Opens the Event Viewer on a custom view for MyID events.
- **Open Log Folder** – Opens the folder containing your MyID logs.
- **Export Report** – Bundles your server information into a file for Intercede Support. It opens the location of the report; you must send the report to support yourself.

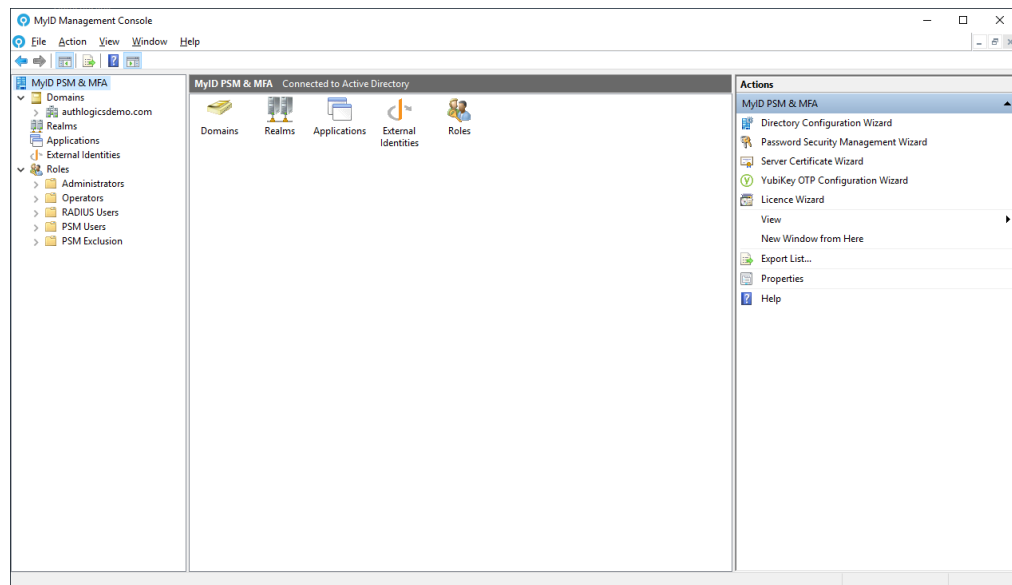
5.3 Global settings walkthrough

The MyID global settings are a group of directory configuration options that apply to *all* MyID servers in the forest; they are not per-user settings.

To access the global settings:

1. In the MyID Management Console, click the high-level **MyID** node. The name of this node includes the product name of the installed licenses.

For example, it may be called **MyID PSM & MFA**.



2. Click **Properties**, in the **Actions** pane.

This opens the global MyID Properties dialog.

You can also right-click the **MyID** node and click **Properties** from that menu.

You can access the following tabs in the Properties dialog:

- General tab
- RADIUS tab
- Alerts tab
- Remediation tab
- Schedule tab
- SMTP Delivery tab
- SMS Delivery tab
- Licence tab
- Authenticator App tab
- Certificates tab
- Grid Pattern Policy tab
- Grid Options tab

- Phrase tab
- One Time Code tab
- YubiKey OTP tab
- FIDO2 tab
- MyID CMS tab

5.3.1 General tab

The General tab contains the **Account Lockout Policy**, **Multi-Factor Factor Timing**, and **Temporary Access** options.

The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'General' tab selected. The dialog has a title bar with a close button (X). Below the title bar is a tabbed interface with the following tabs: Grid Options, Phrase, One Time Code, YubiKey OTP, Authenticator App, FIDO2, MyID CMS, Certificates, SMTP Delivery, SMS Delivery, Licence, General (selected), RADIUS, Alerts, Remediation, Schedule, and Grid Pattern Policy. The 'General' tab contains three sections: 'Account Lockout Policy' with settings for 'Account lockout duration' (240 minutes), 'Account lockout threshold' (5 attempts), and 'Reset account lockout counter after' (15 minutes); 'Multi-Factor Timing' with settings for 'Allowed soft token time delta' (3 minutes) and 'Real-Time Token Lifespan' (15 minutes); and 'Temporary Access Codes' with a checked 'Allow Temporary Access Codes' checkbox, 'Maximum usage time permitted' (24 hours), and 'Maximum number of uses' (3 logons). At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

The **Account Lockout Policy** settings take effect when a user logs on incorrectly after the amount of invalid logon attempts specified in the **Account lockout threshold** setting within the lockout counter period. The lockout counter period is set in the **Reset lockout counter after** setting. Accounts that are attempted to be logged onto in an invalid manner that many times are locked out for the **Account lockout duration**.

Allowed soft token time delta allows you to configure how many minutes difference are allowed between the clock of a two-factor device compared to the clock of the MyID server.

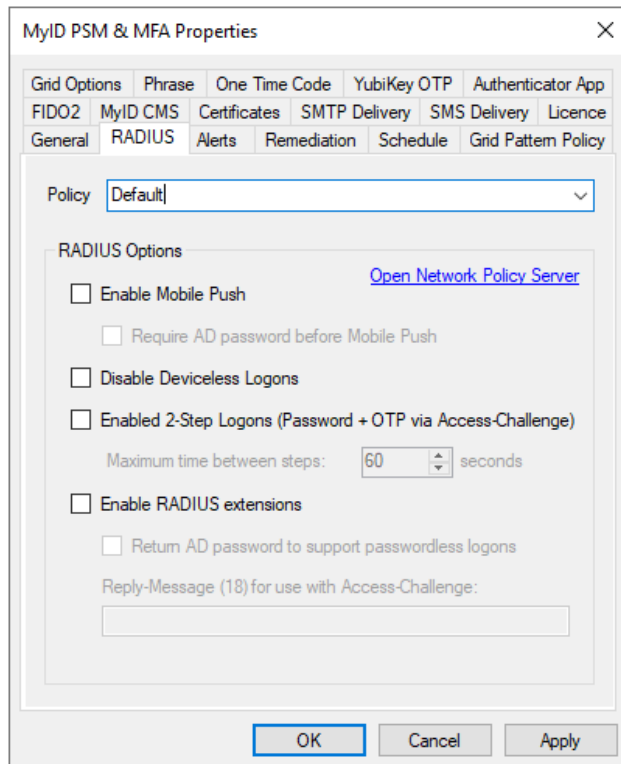
Real-time Token Lifespan allows you to configure how many minutes after being provided that a Real-Time token can be used for before it expires. After this period has exceeded, the token can no longer be used.

Temporary access codes are a feature that allows a user to log in with a temporary PIN or password in an emergency or as a first usage code. The user is provided with a PIN or password and the usage of the password is limited by time, or by the number of uses. Unlike a standard password, the temporary access code or password is self-managed and expires automatically.

The default time limit for temporary access code is 24 hours and three logons. Once these limits are reached, or the user logs on using Multi-Factor Authentication and the temporary access requirements have ended, the user's temporary access is automatically removed.

5.3.2 RADIUS tab

The RADIUS tab allows you to configure RADIUS options that are not available within Microsoft NPS.



The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'RADIUS' tab selected. The 'Policy' dropdown is set to 'Default'. The 'RADIUS Options' section contains several checkboxes: 'Enable Mobile Push' (unchecked), 'Require AD password before Mobile Push' (unchecked), 'Disable Deviceless Logons' (unchecked), 'Enabled 2-Step Logons (Password + OTP via Access-Challenge)' (unchecked), 'Maximum time between steps' (60 seconds), 'Enable RADIUS extensions' (unchecked), and 'Return AD password to support passwordless logons' (unchecked). There is also a text field for 'Reply-Message (18) for use with Access-Challenge:'. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

Using the drop-down list, specify the **Policy** for which you want to configure the **RADIUS Options**.

You can select a level of access control over which users are allowed to use RADIUS authentication through specifying the IP addresses and groups that are allowed to access the policy. Users must fit the criteria for at least one RADIUS enabled access control policy to prevent them from failing the RADIUS logon request. For information on setting up access control policies, see section [5.11.1, Access control policies](#).

MyID RADIUS supports Mobile Push authentication over RADIUS; to enable this, select the **Enable Mobile Push** option.

If you want a Push to be sent after a password has been successfully verified, select **Require AD password before Mobile Push**. This is performed in a single RADIUS request. When disabled, a Push is sent to the user with only a username being received over RADIUS.

If you enable the **Disable Deviceless Logons** option, users are prevented from using Grid Pattern and Phrase OTPs generated in deviceless mode and are forced to use a two-factor generated OTP for RADIUS connections.

You can configure a two-step logon process using the RADIUS Access-Challenge attribute by setting the **Enable 2-Step Logons** option.

Step 1: If the Active Directory username and password is valid, then the Access-Challenge is returned, which tells the RADIUS client to request an OTP. If the Active Directory password is invalid, then an Access-Reject is returned.

Step 2: If the OTP is received within the allowed time (60 seconds by default) and it is valid, an Access-Accept is returned. If the OTP is invalid another Access-Challenge is returned to prompt the RADIUS client to request a new OTP. An Access-Reject is returned for any OTP received after the allowed time.

You can select **Enable RADIUS extensions** to send additional metadata about the user to the RADIUS client. Additionally, the user's password can be returned to the RADIUS client to support Single Sign-On (for example, on Citrix Access Gateways). The password is returned as clear text over RADIUS; however, it is encrypted in transit using the RADIUS shared secret. Returning the password requires the MyID Password Vault to be enabled on the Active Directory tab.

5.3.3 Alerts tab

The Alerts tab allows you to configure multiple alerting options based on the type of event and the recipient.

The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'Alerts' tab selected. The dialog has a tabbed interface with the following tabs: Grid Options, Phrase, One Time Code, YubiKey OTP, Authenticator App, Certificates, SMTP Delivery, SMS Delivery, Licence, FIDO2, MyID CMS, General, RADIUS, Alerts (selected), Remediation, Schedule, and Grid Pattern Policy.

Active Directory Password Alerts

	Admin	User	Manager
Breached password found:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Shared password found:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Password expires within 10 days:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Account and Licence Alerts

	Admin	User	Manager
AD account dormant for 120 days:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MFA account dormant for 110 days:	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
MFA account locked out:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
MFA device change on user account:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Licence events:	<input checked="" type="checkbox"/>		

Buttons: OK, Cancel, Apply

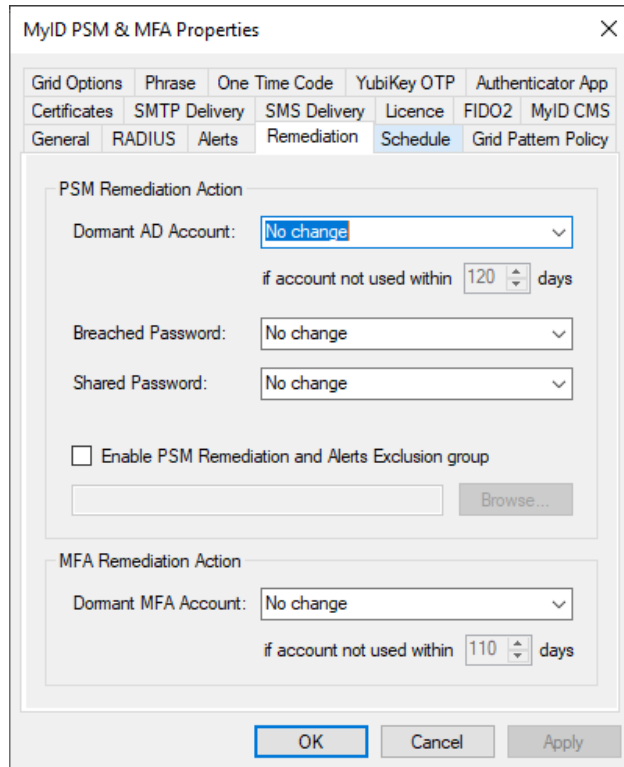
Note: Alerts are sent through SMTP and cannot be configured unless an SMTP server is configured first. The options available are dependent on what license types are installed and which PSM policies are configured.

Administrators receive a summary email instead of individual emails for each user whenever possible. Administrator emails are sent to the email address of all the accounts in the Authlogics Administrators role, if any.

If **Manager** is selected, an alert is sent to the email address of the user account specified as the **Manager** for the user account within Active Directory. If no manager has been specified, then the alert is not sent.

5.3.4 Remediation tab

The Remediation tab allows you to configure an automatic resolution based on the type of condition found.



The image shows a screenshot of the 'MyID PSM & MFA Properties' dialog box, specifically the 'Remediation' tab. The dialog has a title bar with a close button (X). Below the title bar is a tabbed interface with the following tabs: Grid Options, Phrase, One Time Code, YubiKey OTP, Authenticator App, Certificates, SMTP Delivery, SMS Delivery, Licence, FIDO2, MyID CMS, General, RADIUS, Alerts, Remediation (selected), Schedule, and Grid Pattern Policy. The 'Remediation' tab contains two main sections: 'PSM Remediation Action' and 'MFA Remediation Action'. In the 'PSM Remediation Action' section, there are three dropdown menus: 'Domant AD Account' (set to 'No change'), 'Breached Password' (set to 'No change'), and 'Shared Password' (set to 'No change'). Below these is a checkbox labeled 'Enable PSM Remediation and Alerts Exclusion group' which is unchecked. To the right of the checkbox is a 'Browse...' button. In the 'MFA Remediation Action' section, there is a dropdown menu for 'Domant MFA Account' (set to 'No change') and a text field for 'if account not used within' set to '120' days. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

MyID PSM & MFA Properties

Grid Options | Phrase | One Time Code | YubiKey OTP | Authenticator App
Certificates | SMTP Delivery | SMS Delivery | Licence | FIDO2 | MyID CMS
General | RADIUS | Alerts | Remediation | Schedule | Grid Pattern Policy

PSM Remediation Action

Domant AD Account: No change

if account not used within 120 days

Breached Password: No change

Shared Password: No change

☐ Enable PSM Remediation and Alerts Exclusion group

Browse...

MFA Remediation Action

Domant MFA Account: No change

if account not used within 110 days

OK Cancel Apply

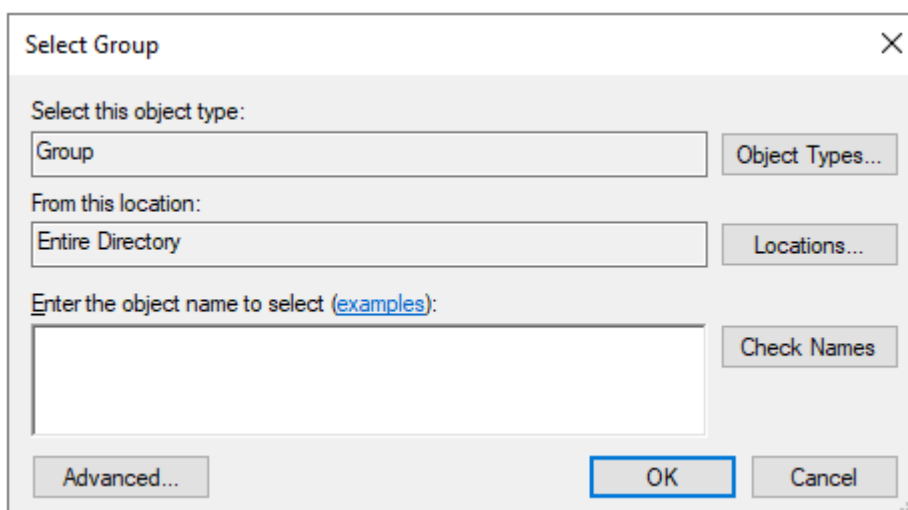
Remediation provides an automated way to fix common user account issues to prevent security breaches. Automating these fixes is important as they are time-sensitive and often overlooked by manual processes.

If an account is found that has a breached or shared password, or is dormant, then the account can be set to:

- **No change** – the default. You are initially recommended to leave this and analyze the administrator alerts before you enable remediation to allow you to assess the impact of enabling it.
- **Must change at next logon** – once you have analyzed the impact of remediation, you are recommended to set this for accounts with breached or shared passwords.
- **Account is disabled** – once you have analyzed the impact of remediation, you are recommended to set this for dormant accounts and dormant MFA accounts.

You can create a group that does not get affected by alert or remediation policies; administrators do not get alerts regarding the members of this group, and the members of this group do not have to do remediation actions. To enable the Remediation and Alerts Exclusion role and assign an Active Directory group to the role:

1. Select the **Enable Remediation and Alerts Exclusion group** option.
2. Click **Browse**.

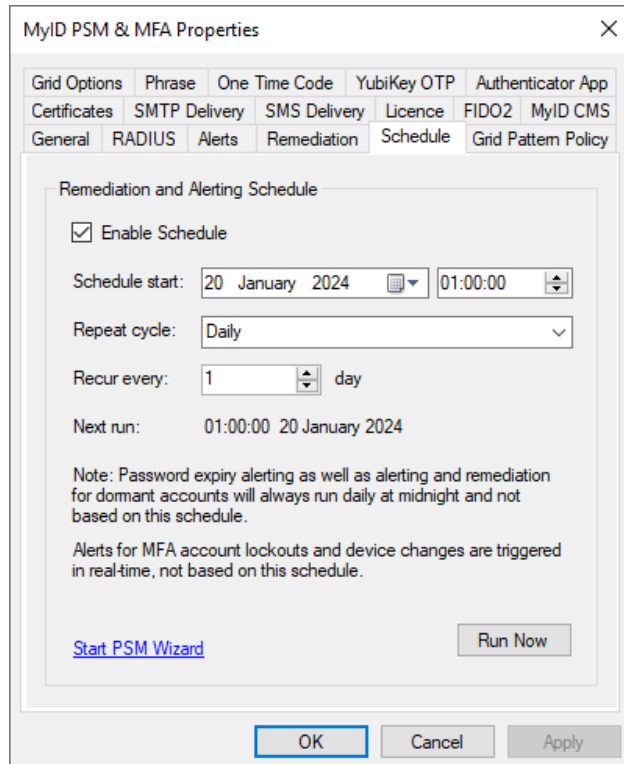


3. Locate the Active Directory Password Policy group that you created.
4. Click **OK**.

You can also enable the Remediation and Alerts Exclusion role and assign an Active Directory group to the role from the Roles Properties dialog, for more information, see section [5.10.6, Managing the Remediation and Alerts Exclusion role](#).

5.3.5 Schedule tab

The Schedule tab allows you to configure when breached and shared password remediation and alerting takes place.



The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'Schedule' tab selected. The 'Remediation and Alerting Schedule' section is active, showing the following configuration:

- ☒ Enable Schedule
- Schedule start: 20 January 2024, 01:00:00
- Repeat cycle: Daily
- Recur every: 1 day
- Next run: 01:00:00 20 January 2024

Below the schedule settings, there is a note: "Note: Password expiry alerting as well as alerting and remediation for dormant accounts will always run daily at midnight and not based on this schedule. Alerts for MFA account lockouts and device changes are triggered in real-time, not based on this schedule."

At the bottom of the dialog, there are buttons for 'OK', 'Cancel', and 'Apply'. A 'Run Now' button is also present in the bottom right corner of the 'Remediation and Alerting Schedule' section.

It is recommended to run the schedule daily and out of hours; however, this can be customized as required. The processing work is only performed on the primary MyID Server.

To run a check as soon as possible without waiting for the schedule click **Run Now**. This will begin the process within the next 15 minutes.

Note: Password expiry alerting and alerting and remediation for dormant accounts always runs daily at midnight and not based on this schedule. Also, alerts for MFA account lockouts and device changes are triggered in real-time, not based on this schedule.

5.3.6 SMTP Delivery tab

When you provision users using the MyID Management Console, they can be sent an email with details of how to access the Self Service Portal, their initial pattern, PINs, and other necessary logon information. Alerts are also sent to administrators using email. The SMTP Delivery tab allows administrators to set the SMTP host and port for the email server for email message delivery.

The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'SMTP Delivery' tab selected. The 'Email delivery options' section contains the following fields: 'From address' (administrator@authlogicsdemo.com), 'SMTP server 1' (server.authlogicsdemo.com, port 25), and 'SMTP server 2' (server2.authlogicsdemo.com, port 587). There is a checkbox for 'Use SSL/TLS Encryption' and a 'Send Test Email' button. The 'Email authentication options' section has three radio buttons: 'Anonymous (No authentication)', 'Windows Integrated (Computer account credentials)', and 'Specify Credentials' (which is selected). Below the 'Specify Credentials' option are fields for 'Username' (authlogicsdemo\administrator) and 'Password' (masked with dots). At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

The **From address** setting specifies the email address that delivered mail is received from.

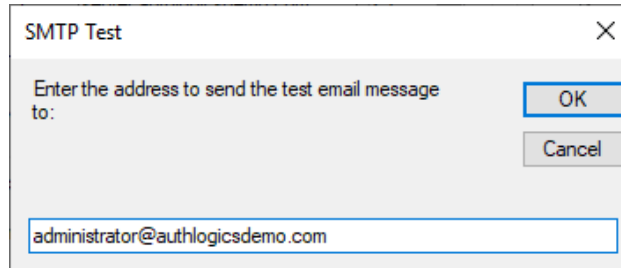
Note: Ensure that the **From** address can deliver emails to users through any anti-spam filters.

A primary SMTP must be specified to send an email. A secondary SMTP may be specified for redundancy purposes. The secondary server is only used if the sending fails when using the primary server. Enter the **SMTP server 1** and **SMTP server 2** DNS names or IP addresses and corresponding port numbers. If the servers require an encrypted connection, enable the **Use SSL/TLS Encryption** option.

If your email server requires authentication, select either **Use default Integrated credentials** or **Specify Credentials** and provide a username and password of an account with credentials to authenticate to the email server. These credentials are stored with 256bit AES asymmetric encryption.

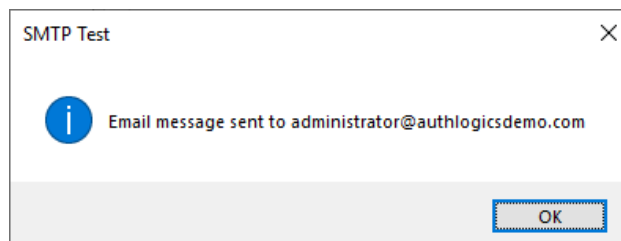
To ensure that the SMTP details are valid:

1. Click **Send Test Email**.
2. Enter a test email.



The dialog box is titled "SMTP Test" and has a close button (X) in the top right corner. It contains a text input field with the placeholder text "Enter the address to send the test email message to:". Below the input field is a text box containing the email address "administrator@authlogicsdemo.com". To the right of the input field are two buttons: "OK" and "Cancel".

3. Click **OK**.



The dialog box is titled "SMTP Test" and has a close button (X) in the top right corner. It contains a blue information icon (i) followed by the text "Email message sent to administrator@authlogicsdemo.com". At the bottom right of the dialog box is an "OK" button.

A confirmation that the message has been sent is displayed if the send was successful; if the test email is not sent correctly, an error stating the SMTP issue is displayed.

5.3.7 SMS Delivery tab

The SMS Delivery tab allows administrators to set the SMS/Text delivery providers for SMS/Text message delivery and the **Message options**. MyID can use SMS messages for delivery of two-factor tokens to mobile devices that do not have soft-tokens.

The administrator can also send notification or broadcast messages to one or many users through the MMC by right-clicking an account and selecting the **Send SMS** option.

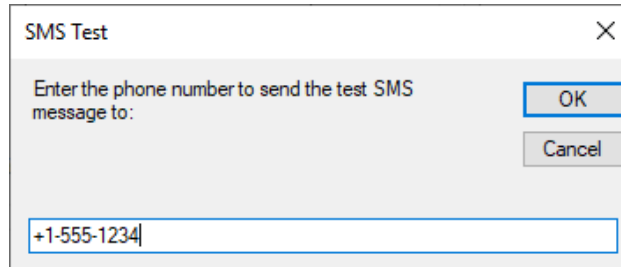
The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'SMS Delivery' tab selected. The 'SMS / Text delivery provider' section includes a 'Provider' dropdown menu set to 'Disabled', a 'Web Site' link, 'Username' (AQL), 'Password' (masked with dots), and a 'Send Test SMS' button. The 'Message Options' section includes checkboxes for 'Overwrite previous message' and 'Enable SMS Flash', a 'From Info' field (SMS IN), a 'Retry Send Limit' of 6 Messages / hour / user, and a 'Default Country Code' dropdown set to 'Zimbabwe (+263)'. The dialog has 'OK', 'Cancel', and 'Apply' buttons at the bottom.

The **Provider** list is preconfigured with some commonly used Internet-based SMS providers from around the globe; see section [5.3.7.1, List of supported SMS providers](#). If you do not have an account with an SMS provider, you can choose one from the list and click the **Web Site** link; this takes you to the provider's sign up page where you typically sign up for a free trial account.

Select your SMS provider and enter the **Username** and **Password** details for it.

To ensure that the SMS provider credentials are valid:

1. Click **Send Test SMS**.
2. Enter a test mobile number.

A dialog box titled "SMS Test" with a close button (X) in the top right corner. Inside the dialog, there is a text prompt "Enter the phone number to send the test SMS message to:" followed by a text input field containing the number "+1-555-1234". To the right of the input field are two buttons: "OK" and "Cancel".

SMS Test

Enter the phone number to send the test SMS message to:

OK

Cancel

+1-555-1234

3. Click **OK**.

If you receive a text message on the specified mobile device, then the provider details are correct.

Some providers allow SMS messages from the same source to overwrite previous SMS messages. To allow this, enable **Select Overwrite previous message**. For SMS messages to be delivered as a Flash SMS, select **Enable SMS Flash**.

The **From Info** setting specifies the number that all messages appear to be delivered from.

The **Retry Send Limit** setting prevents more than the specified number of text messages to be delivered to a specific user per hour.

The **Default Country Code** prefixes mobile phone numbers with the selected dialing code for all mobile numbers that do not have an international dialing code.

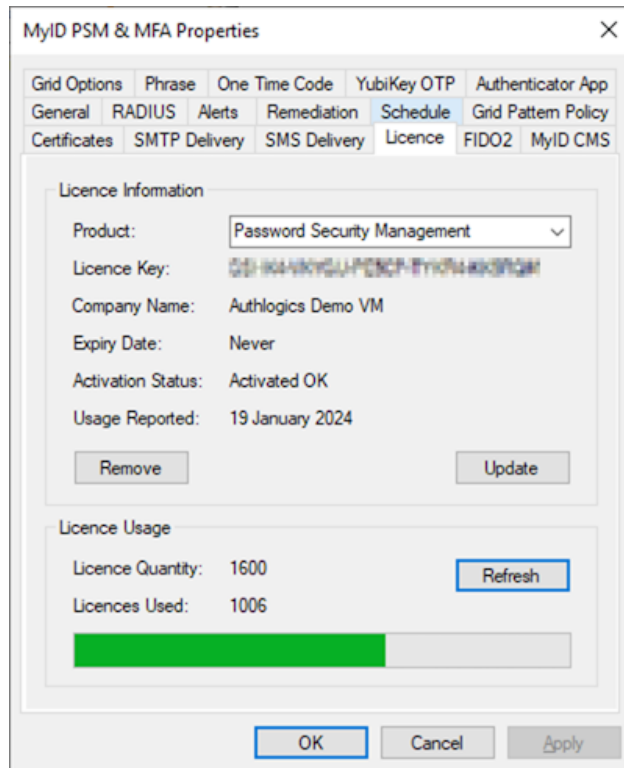
5.3.7.1 List of supported SMS providers

The following SMS providers are supported:

- AQL
- Bulk SMS International
- Bulk SMS South Africa
- Bulk SMS UK
- Bulk SMS USA
- Clickatell
- Clickatell (Legacy)
- EE UK Enterprise Messaging
- Infobip
- Inforelics (Turkey)
- Jawal B SMS (STC)
- Mediaburst Clockwork
- Mobile Sasa
- MobiShastra
- MobiWeb
- Notisify
- Omantel iSmart SMS
- Sidpec
- T2 (KSA)
- Unifonic (Legacy)
- Unifonic NextGen
- Yamamah

5.3.8 Licence tab

The Licence tab displays the loaded license information.



The screenshot shows the 'MyID PSM & MFA Properties' window with the 'Licence' tab selected. The 'Licence Information' section displays the following details:

Field	Value
Product:	Password Security Management
Licence Key:	001-00000000000000000000000000000000
Company Name:	Authlogics Demo VM
Expiry Date:	Never
Activation Status:	Activated OK
Usage Reported:	19 January 2024

Buttons: Remove, Update

The 'Licence Usage' section displays the following details:

Field	Value
Licence Quantity:	1600
Licences Used:	1006

Buttons: Refresh

A green progress bar is shown below the usage information, representing the ratio of used licenses to total quantity.

Buttons: OK, Cancel, Apply

Details of the selected license are displayed for your information, including the number of licenses supported and the dates during which they are valid. Details of your Multi-Factor Authentication and Password Security Management licenses can be viewed and modified by selecting the **Product** from the drop-down list.

You can remove licenses by selecting the **Product** that the license is for, and clicking the **Remove** button. If you have removed a license, the Remove button is replaced by the **Add** button. If you click the **Add** button, the Licence Configuration Wizard starts.

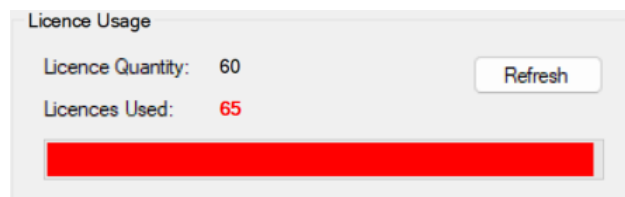
The license is automatically refreshed periodically but *must* be updated at least every 60 days. If your license details change, for example if you renew your subscription or purchase more user licenses, or you want to manually update the usage reporting, click the **Update** button to get the latest license version from Intercede.

If your license has expired, the **Expiry Date** is bold.

The number of used licenses is updated periodically; however, you can update it as needed by clicking the **Refresh** button.

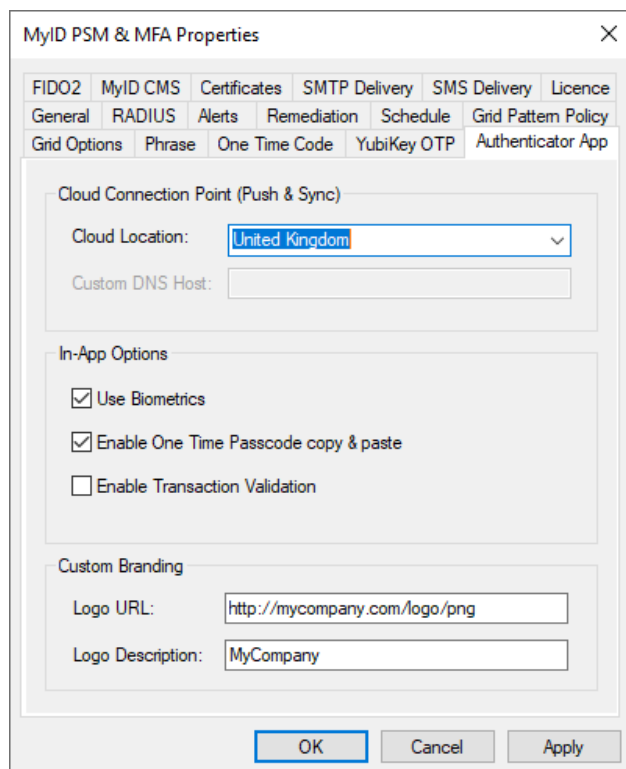
If you have used 90% or more of your licenses, the bar displaying the number of licenses is orange.

If you have used more licenses than you have available, the bar displaying the percentage of licenses used is red, and the number of **Licences Used** is red and bold.



5.3.9 Authenticator App tab

The Authenticator App tab allows you to customize the appearance and functionality of the MyID Authenticator app that is installed on mobile devices from popular App Stores.



The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'Authenticator App' tab selected. The dialog has a tabbed interface with the following tabs: FIDO2, MyID CMS, Certificates, SMTP Delivery, SMS Delivery, Licence, General, RADIUS, Alerts, Remediation, Schedule, Grid Pattern Policy, Grid Options, Phrase, One Time Code, YubiKey OTP, and Authenticator App. The 'Authenticator App' tab is active, showing three sections: 'Cloud Connection Point (Push & Sync)' with a 'Cloud Location' dropdown set to 'United Kingdom' and a 'Custom DNS Host' text field; 'In-App Options' with checkboxes for 'Use Biometrics' (checked), 'Enable One Time Passcode copy & paste' (checked), and 'Enable Transaction Validation' (unchecked); and 'Custom Branding' with a 'Logo URL' text field containing 'http://mycompany.com/logo/png' and a 'Logo Description' text field containing 'MyCompany'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

To allow the Authenticator App to perform an online pairing and Mobile Push authentication, select a **Cloud Location** region. Once you have registered a mobile device, the device keeps the cloud location under which it was registered. If you change the **Cloud Location**, this does not affect any existing devices, but any devices registered after the change use the new value. If you want an existing device to reflect the new location, you must re-register the device. You can view the location associated with a device on the associated user's Devices tab; for more information, see section 5.9.2, *Multi-Factor devices assigned to a user account*.

Note: The **Cloud Location** option replaces the **Enable Online Device access** option. On a clean installation, or during an upgrade from an installation with **Enable Online Device access** enabled, the **Cloud Location** is set to **United Kingdom**. During an upgrade from an installation with **Enable Online Device access** disabled, the **Cloud Location** is set to **None**.

To host your own instance of the web service and to set your own URL, contact Intercede customer support.

The in-app Authenticator App options can also be customized. Once these are set, they cannot be changed by the user.

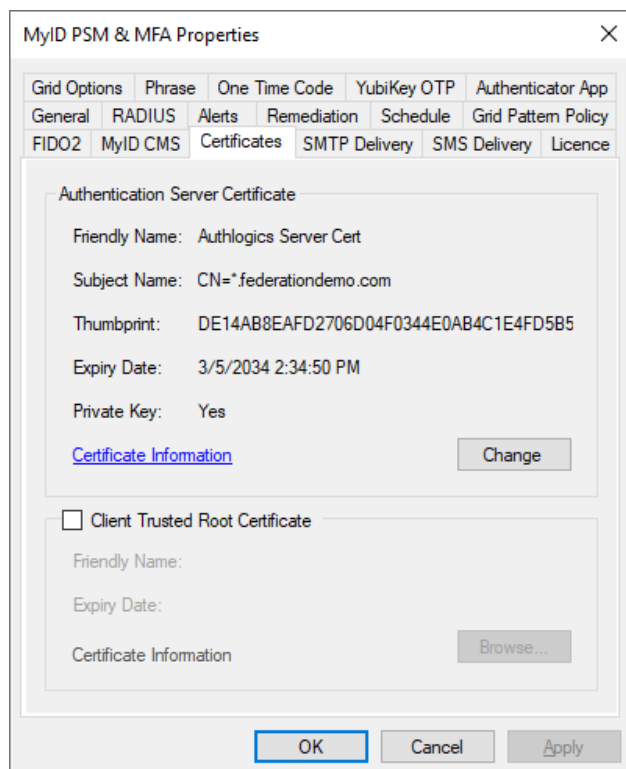
To show a custom logo at the top of the Authenticator App, enter a public URL to a graphic file that the mobile device can access. When provisioned, the Authenticator App accesses the URL and downloads and stores the graphic within the Authenticator App. The graphic should be a 900 x 210 transparent PNG image. For accessibility purposes. You are recommended to enter a description for the logo. This may just be the company name.

5.3.10 Certificates tab

The Certificates tab allows you to change the MyID Server signing certificate. This certificate is used to secure the MyID data stored in Active Directory and the Server Password Vault.

By default, the installation program generates a self-signed certificate.

This is *not* the certificate used by IIS for HTTPS (SSL) connections to the server.



The Authentication Server Certificate contains the public and private keys used to carry out asymmetric encryption and decryption of the stored data. An instance of the certificate, along with its private key, must be installed on each MyID Server in the Windows Computer certificate store. If the private key is not available, the Authentication Server cannot operate.

Warning: If the private key is lost it is not possible to recover the MyID data stored in Active Directory.

If you are using the Windows Desktop Agent, you can select a MyID Server Certificate Trusted Root certificate. If there is an enterprise CA available, you can specify a CA root certificate. This requires that all MyID Desktop Agent machines have a certificate installed on them that was issued from the specified root. If such a certificate is unavailable, some of the agent's features are not available, for example, offline and passwordless logons. If a MyID Server Certificate Trusted Root certificate is not configured, the default Self Signed Certificates are used.

All Windows Desktop Agents connecting to the MyID Authentication Server using the External Access Server role must have a trusted certificate installed on it so that it can be validated by the MyID Authentication Server.

5.3.11 Grid Pattern Policy tab

This tab configures the pattern policy and complexity settings.

The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'Grid Pattern Policy' tab selected. The dialog has a close button (X) in the top right corner. Below the title bar is a tabbed interface with the following tabs: Grid Options, Phrase, One Time Code, YubiKey OTP, Authenticator App, FIDO2, MyID CMS, Certificates, SMTP Delivery, SMS Delivery, Licence, General, RADIUS, Alerts, Remediation, Schedule, and Grid Pattern Policy. The 'Grid Pattern Policy' tab is active and contains two main sections: 'Pattern Policy' and 'Pattern Complexity'. The 'Pattern Policy' section includes: 'Minimum Length' with a dropdown set to '4x4' and a numeric spinner set to '4'; 'Pattern age in days' with a numeric spinner set to '2' and a label 'min', and another numeric spinner set to '42' and a label 'max'; and 'Enforce pattern history' with a numeric spinner set to '24' and the text 'patterns remembered'. The 'Pattern Complexity' section includes: 'Enforce complexity' with four checked checkboxes: 'Block sequential straight lines', 'Block single plane', 'Restrict sequential linear adjacencies', and 'Restrict cell instance usage'; 'Maximum sequential linear adjacencies' with a numeric spinner set to '3'; 'Maximum cell usage instances' with a numeric spinner set to '2'; and 'Minimum quadrant number' with a numeric spinner set to '2'. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

The **Minimum Length** setting determines the least number of characters allowed for a pattern for each size of grid. The larger the number, the more secure the patterns are, but the more complex they are for users to manage. Select the size of grid from the drop-down list, and input the minimum length of pattern for that size.

The minimum and maximum **Pattern age in days**, prevents users from excessive changes of patterns within a short period and forces users to change their pattern regularly.

By enabling **Enforce pattern history**, an administrator can prevent users from re-using previously used patterns. Specify how many previous patterns are remembered.

Enforcing complexity ensures that users do not choose simple patterns that could be easily guessed. Administrators can enforce the following complexity checks:

- Block sequential straight lines.

Blocks the use of a straight line in any direction in a contiguous chain and sequence.

- Block single plane.

Blocks the usability to select all positions in a pattern that are on the same plane in any orientation, regardless of spacing or sequence. This includes straight lines.

- Restrict sequential linear adjacencies.

Restricts the maximum number of allowed positions that are sequential and in a straight line before a gap and change of direction is required.

- Restrict cell instance usage.

Restricts the number of times the same cell can be selected when choosing a pattern.

For example, if the **Maximum cell usage instances** is two then a maximum of two cells, within the selected pattern, can be re-used.

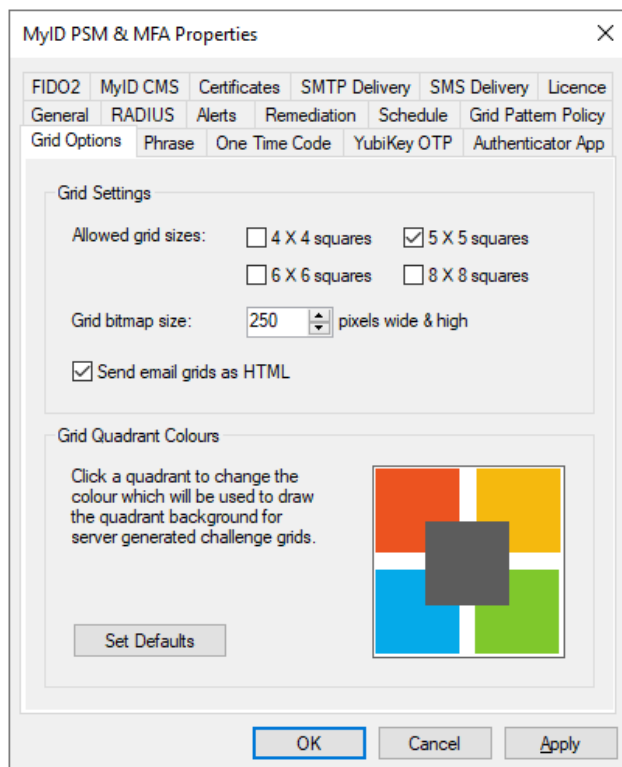
- Restrict number of quadrants.

Restricts the minimum number of quadrants a chosen pattern must use.

For example, if the **Minimum quadrant number** is two, then a pattern must use at least two of the four quadrants. While this encourages a user to choose a pattern that is well spread out, it also limits the number of possible pattern combinations available.

5.3.12 Grid Options tab

This tab configures generic and visual elements of MyID Grid authentication.



The **Allowed grid sizes** option defines the sizes of grids that users can have. The default for new installations is for only 5 x 5 grids to be allowed, as this is the most secure option; 6 x 6 and 8 x 8 grids are larger, but allow only numeric characters, while 4 x 4 and 5 x 5 grids allow alphanumeric characters.

If you are using the MyID Authentication Server for deviceless logons through an API, you can use the **Grid bitmap size** option to specify the default dimensions of the PNG image that is displayed on the client to suit the location you are displaying the image.

Note: The **Grid bitmap size** option is relevant only if you are using an API call to get the grid; for example, using `GetPinGridToken`. If you are instead using the MyID Authentication Server for deviceless logons through the IdP, the IdP manages the rendering size of the grid to ensure that it fits well within the overall layout of the page, overriding any user-defined bitmap size.

When challenge grids are delivered using email, the **Send email grids as HTML** option defines whether challenge grids are generated in plain text or as HTML.

You can also customize the grid colors used to display the squares in each quadrant of the grid. The middle section is available only in 5 x 5 grids, and is not visible in other dimensions of grids.

To return the **Grid Quadrant Colours** to the default colors, click the **Set Defaults** button.

5.3.13 Phrase tab

This tab configures the standard Phrase policy settings.

The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'Phrase' tab selected. The 'Policy Settings' section includes:

- Minimum Length:** A spinner box set to 6, followed by the text 'chars per answer'.
- Minimum Questions:** A spinner box set to 2.
- Message prefix text:** A text box containing 'Phrase question'.
- Question List:** A table with 5 rows. The 4th row is selected.

#	Question - What is...
1	your Codeword
2	your mother maiden
3	your favourite sports teams
4	your favourite subject at school
5	your spouses middle name

At the bottom of the 'Policy Settings' section, there is a checkbox labeled 'Use multiple questions per login' which is checked, and an 'Add' button. The main dialog box has 'OK', 'Cancel', and 'Apply' buttons at the bottom.

The **Minimum Length** sets the minimum number of characters that a user must enter for each answer.

The **Minimum Questions** setting allows an administrator to specify the minimum number of questions that a user must answer to be fully provisioned for phrase authentication. Phrase authentication allows administrators to create multiple questions and allow a user to select a subset of those questions to answer.

The **Message prefix text** precedes all Phrase challenges which are sent to mobile devices.

By default, the only question is `your Codeword`; this is to cater for auto-provisioning where a user is provided with a random dictionary word to get them started. It is not recommended to change the first challenge question. To modify and add new Phrase challenge questions, click **Add**.

Enable the **Use multiple questions per login** option to make Phrase randomly ask for letters from answers to multiple questions instead of picking random letters from a single answer. This option can increase security but may make it harder for users to login.

5.3.14 One Time Code tab

This tab configures the standard One Time Code policy settings.

The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'One Time Code' tab selected. The 'Policy Settings' section contains the following options:

- ☒ **Require static PIN / AD Password**
- Minimum OTP Length: 6 digits
- Minimum PIN Length: 4 digits
- PIN / Password Position: Any
- Message prefix text: OTC

Below these settings, a note states: 'The Message prefix text is placed at the beginning of the SMS / Text / Email message and can be used as an introduction to the user or an indication of what the PINpass code is for. e.g. "Acme Inc. remote access." or "Secure website login code."'

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

One Time Code (OTC) can be used as a single or Multi-Factor Authentication solution. To enforce two-factor authentication with OTC, enable the **Require PIN / AD Password** option; if this option is enabled, the user must enter a PIN code or Password along with a One Time PIN (OTP) when authenticating. This option is typically disabled when OTC is only being used to validate OTPs and static data such as passwords are being verified elsewhere, or not at all.

The **Minimum OTP Length** option sets the minimum number of digits allowed in an OTP code generated. The actual number of digits is set on a per-user basis but cannot be lower than this number.

The **Minimum PIN Length** option allows an administrator to specify the minimum number of digits in a user's static PIN code. This length is ignored when using Active Directory passwords in place of a PIN code.

The **PIN / Password position** option dictates where users must enter the static PIN / Password in relation to the OTP. The default setting is *Any*.

The **Message prefix text** that precedes all OTC token challenges.

5.3.15 YubiKey OTP tab

This tab configures the YubiKey One Time PIN policy settings.

The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'YubiKey OTP' tab selected. The 'Policy Settings' section contains the following options:

- ☒ Enable YubiKey OTP
- ☒ Enable Yubico Online Authentication
- ☒ Require PIN / AD Password
- Minimum PIN Length: 4 digits

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

MyID MFA supports both programmed and native (non-reprogrammed) YubiKey devices. In order to validate non-reprogrammed YubiKey devices, the MyID Server requires access to the Yubico servers hosted in the cloud. **Enable Yubico Online Authentication** to pass non-reprogrammed YubiKey OTPs to the Yubico servers in the cloud.

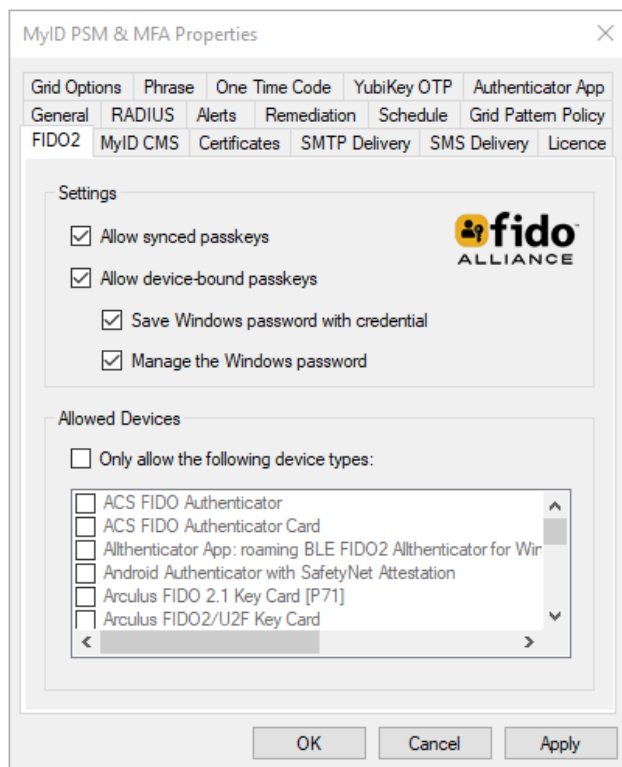
YubiKey OTPs can be used as a single or Multi-Factor Authentication solution. To enforce two-factor authentication with your YubiKey OTP, enable the **Require PIN / AD Password** option; when this is enabled, the user must enter a PIN code or Password along with their YubiKey One Time PIN (OTP) when authenticating. This option is typically disabled when OTC is only being used to validate OTPs and static data such as a password is being verified elsewhere, or not at all.

The **Minimum PIN Length** option allows an administrator to specify the minimum number of digits in a user's static PIN code. This length is ignored when using Active Directory passwords in place of a PIN code.

The **PIN / Password position** option dictates where users must enter the static PIN / Password in relation to the OTP. The default setting is *Any*.

5.3.16 FIDO2 tab

This tab configures the FIDO2 Passkey settings.



MyID MFA supports both FIDO2 synced and device-bound passkeys. Users need to be provisioned and enabled for FIDO2 support individually.

Enable the **Allow synced passkeys** option to enable support for synced passkeys. Synced passkeys are typically installed on mobile devices.

Enable the **Allow device-bound passkeys** option to enable support for device-bound passkeys. Device-bound passkeys are typically separate hardware tokens such as those provided by Yubico.

Enable the **Save Windows password with credential** option to bind the user's Active Directory password with the user's FIDO credential for passwordless login. This password is not stored with the MyID MFA password vault.

Enable the **Manage the Windows password** option to allow MyID MFA to create a random, 32-byte token as the user's Windows password, and then secure and associate the Windows password token with a FIDO device-bound passkey. The Windows password therefore can be recovered only when a successful FIDO authentication takes place. If you enable this option, do not set the **Randomise AD Passwords every x days** setting in the Domain Properties dialog.

Note: If you have applications that requires the user to input their Windows password manually, do not enable this option as the Windows password token is never visible to the user.

For more information on managing Windows passwords using FIDO, see section [3.7.1, Windows Managed Password for FIDO credentials](#).

5.3.16.1 Known issues

- **IKB-440 - Offline logon caches only the last successful FIDO authentication method**

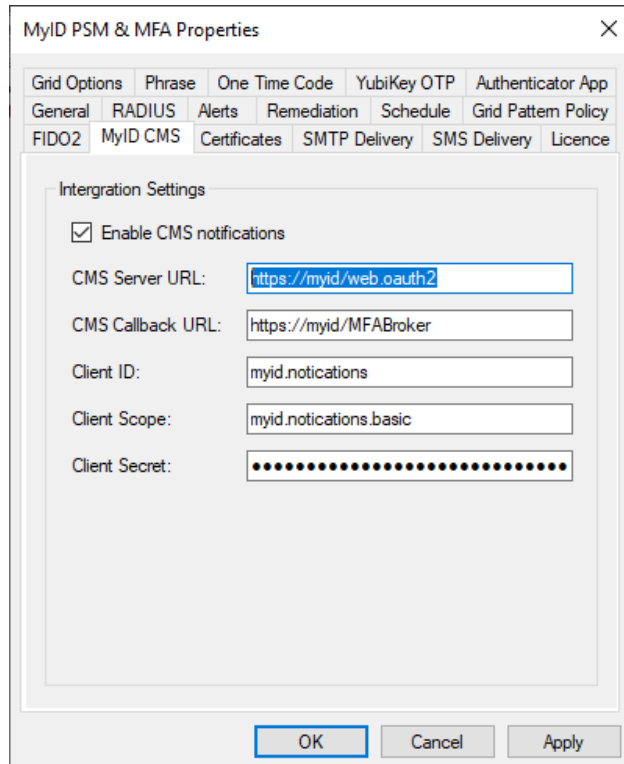
When the **Manage the Windows password** option is enabled on the **FIDO2** tab of the global settings, you can use only the last successful FIDO authentication method. If a user logs in with biometric FIDO before going offline, only biometric works offline, and similarly for non-biometric logon. Even if the user has previously logged in with both devices, only the most recent one is cached when working offline. This affects physical FIDO authentication devices only.

- **IKB-441 – Unable to carry out an offline logon after using a temporary access code**

When the **Manage the Windows password** option is enabled on the **FIDO2** tab of the global settings, if you use a temporary access code before going offline, all cached credentials are cleared, preventing you from carrying out an offline logon with either biometric or non-biometric FIDO devices, even if you have successfully logged in with FIDO devices before.

5.3.17 MyID CMS tab

This tab configures the MyID CMS settings to allow for integration between the MyID MFA/PSM Server and the MyID CMS Server.



The screenshot shows the 'MyID PSM & MFA Properties' dialog box with the 'MyID CMS' tab selected. The 'Integration Settings' section is visible, containing the following fields:

- ☒ Enable CMS notifications
- CMS Server URL:
- CMS Callback URL:
- Client ID:
- Client Scope:
- Client Secret:

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

You require the following information to complete the configuration:

- **CMS Server URL** – the MyID CMS OAuth2 Authentication Service URL.

For example:

`https://myid/web.oauth2`

- **CMS Callback URL** – the MyID CMS MFA Broker Service URL.

For example:

`https://myid/MFABroker`

- **Client ID** – the MyID CMS Client ID used to authenticate.

For example:

`myid.notifications`

- **Client Scope** – the MyID CMS Client Scope used to authenticate.

For example:

`myid.notifications.basic`

- **Client Secret** – the MyID CMS Client Secret used to authenticate.

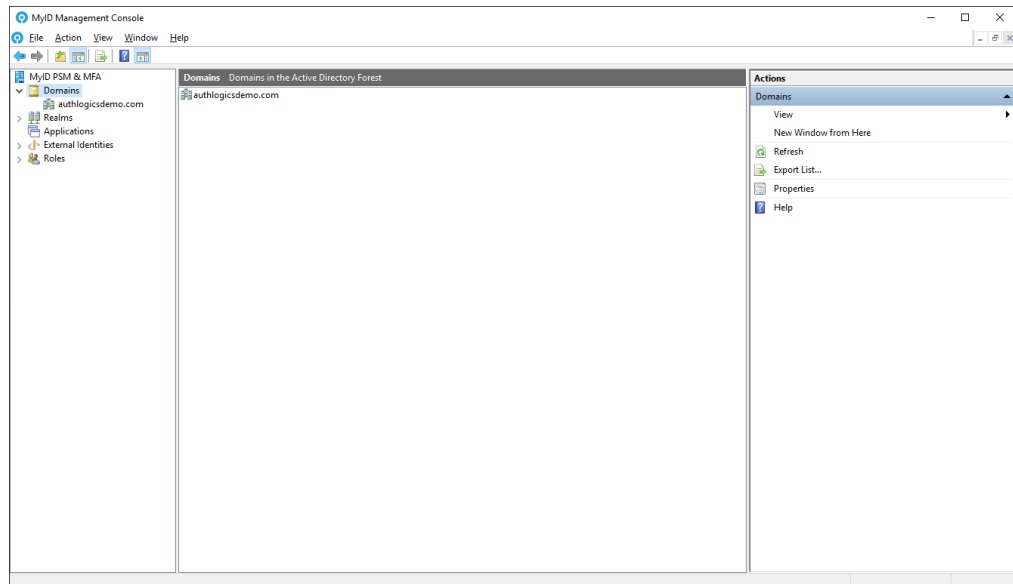
For example:

`4116e8f9-92e2-48b1-8616-5fb3d130b91d`

5.4 Domain settings

The MyiD Domain settings are a set of domain specific configuration options that apply to all MyiD servers in the forest and are not per-user settings. To access the domain settings:

1. In the MyiD Management Console, highlight the **Domains** node.
2. Click **Properties**, in the **Actions** pane.

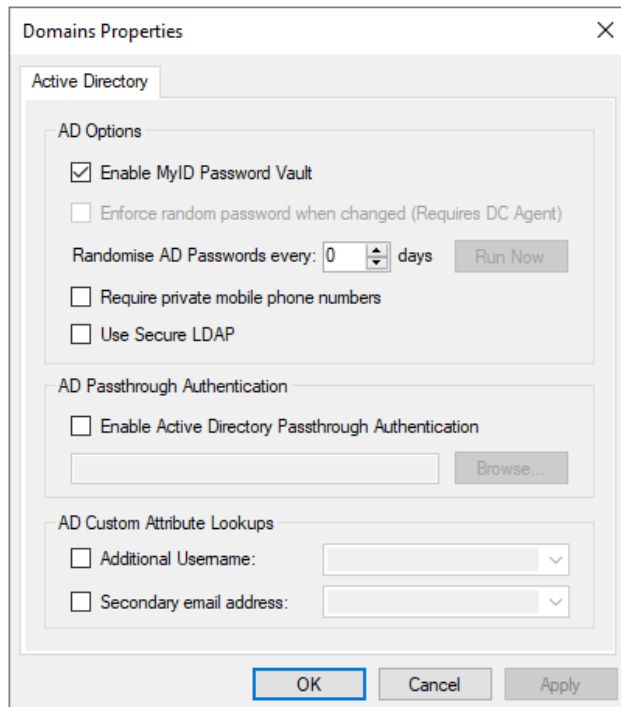


The Domain Properties dialog opens.

See section [5.4.1, Domain Properties dialog](#) for details.

5.4.1 Domain Properties dialog

The Domain Properties dialog allows administrators to control various Active Directory specific options.



Enable MyID Password Vault enables the MyID Password Vault. The MyID Password Vault is a secure storage location protected with AES 256-bit asymmetric encryption with certificates. The password vault stores user passwords to allow for Passwordless logons to Windows and other applications. This feature can be used in conjunction with the Windows Desktop Agent with Passwordless logons enabled. The Password Vault is disabled by default and must be explicitly enabled.

Randomise AD Passwords every x days enables the MyID Server to manage user passwords automatically by regularly setting them to a highly secure random value. The random passwords are kept secure because the users never know what they are, and they constantly change. This feature must be used only in conjunction with MyID agents that support Passwordless logons, such as the Windows Desktop Agent with Passwordless logons enabled.

To enable this feature, specify the number of days until the passwords must be randomly changed. If you set this value to 0, the feature is disabled.

Note: If you set this option, do not set the **Manage the Windows password** option in the global settings.

Note: To enable this option for individual users, you must either enable the **Randomise AD Passwords every x days** option as you add them, or manually enable the **Randomise AD Passwords every x days** option for each user in the user properties dialog. See section [5.8.3, Adding a new MyID user account](#) and section [5.9.7.4, Managing an Active Directory user's password randomization](#).

You can also enable **Enforce random password when changed**, which prevents a user's password from being reset/changed to a non-random password. If it is not enforced, the password reset is allowed, and the new password can be used until the next randomization schedule. The block is done directly at the Domain Controller by the Domain Controller Agent which must be installed separately on all Domain Controllers.

To force password randomization of all accounts, click **Run Now**. This causes the Password Policy Agent to run the password randomization task within the next 15 minutes.

To ensure that all user mobile phone numbers are kept private, enable **Require private mobile phone numbers**. This setting ensures that mobile numbers are encrypted instead of using the clear text default mobile phone Active Directory field.

To connect to the directory using the secure LDAP port, 636, instead of the standard LDAP port, 389, when validating a user's password, enable the **Use Secure LDAP** option.

Important: You must use the secure LDAP port if you are using a Windows Server 2025 Active Directory.

AD Passthrough Authentication allows logon attempts to be passed directly to Active Directory for logon processing if a user has not been provisioned for MFA. AD Passthrough Authentication is only permitted for user accounts that are a member of a specified AD group and is disabled by default. To enable AD Passthrough Authentication:

1. Enable the **Enable Active Directory Passthrough Authentication** option.
2. Click **Browse**.
3. Select the Active Directory group that contains the user accounts which are permitted to use AD Passthrough Authentication.

AD Custom Attribute Lookups enables MyID to use custom LDAP attributes on a user account when looking up a user account name or secondary email address.

The **Additional Username** option may be useful to locate a user account using an employee number instead of an Active Directory account name. If the employee number is stored in **extensionAttribute1** in Active Directory, you can configure MyID to also look in the specified attribute. The custom field is used as a secondary addition to the standard Username or UPN, if an account match is found using the standard **Username**, the custom LDAP field is not searched.

The **Secondary email address** option can be used to locate a secondary email address for a user account. The secondary email address can be used in the authentication provisioning wizards for sending welcome emails to.

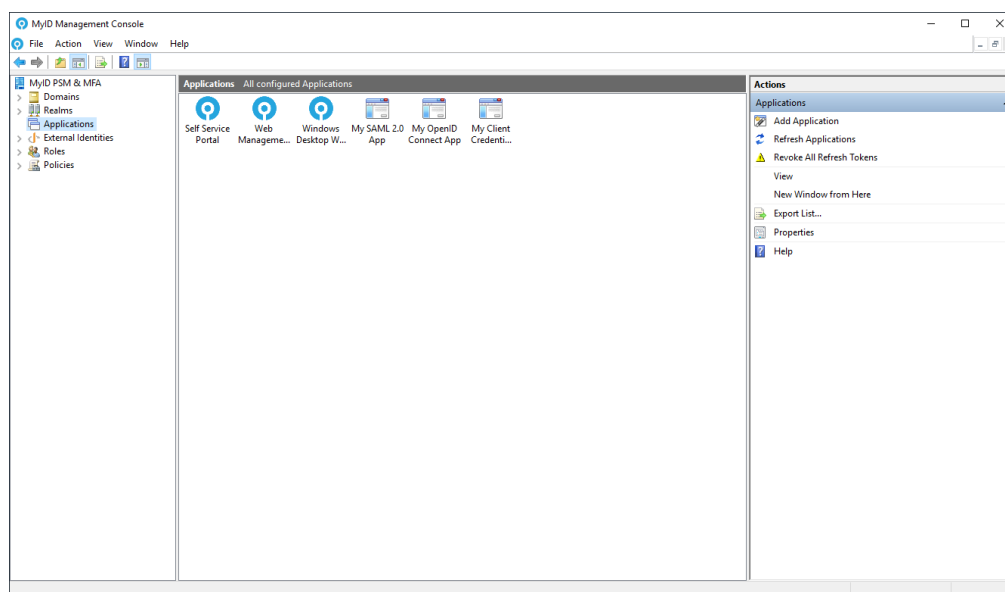
To enable a custom attribute lookup, enable **Additional Username** or **Secondary email address**, and select an LDAP attribute from the list that MyID should search.

5.5 Applications

Applications are all IdP published services and websites that require authentication. MyID includes three preconfigured applications: the Self Service Portal, the Web Management Portal, and the Windows Desktop agent service.

To access the Applications Properties:

1. In the MyID Management Console, highlight the **Applications** node.



2. Click **Properties**, in the **Actions** pane.

To access a specific application's properties:

1. In the MyID Management Console, highlight the **Applications** node.
2. Double-click on the application for which you want to access the properties.

You can access the following properties dialogs:

- Applications Properties.
See section [5.5.1, Applications Properties](#).
- Self Service Portal Properties.
See section [5.5.2, Self Service Portal Properties](#).
- Web Management Portal Properties.
See section [5.5.3, Web Management Portal Properties](#).
- Windows Desktop Agent Properties.
See section [5.5.4, Windows Desktop Agent Properties](#).
- OpenID Connect application properties.
See section [5.5.5, OpenID Connect application properties](#).
- Client Credential applications properties.
See section [5.5.6, Client Credential applications properties](#).

- SAML 2.0 application properties.

See section [5.5.7, SAML 2.0 application properties](#).

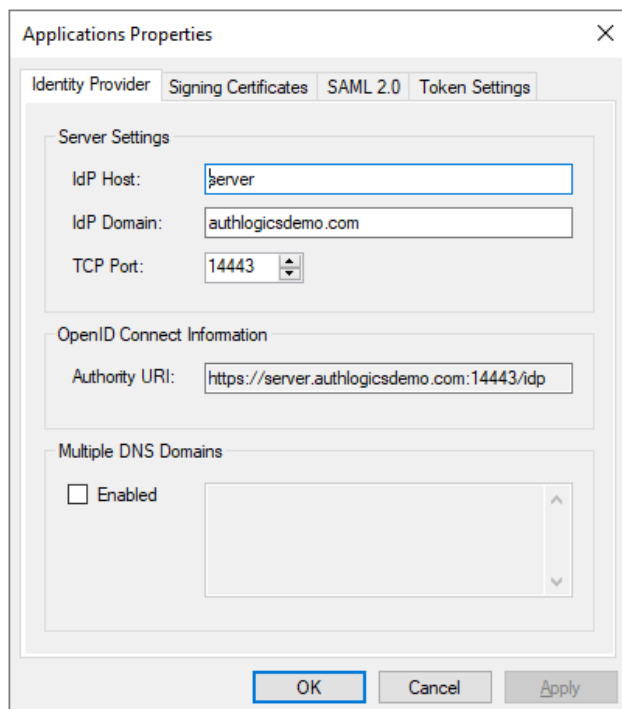
You can also click **Revoke All Refresh Tokens** in the **Actions** pane for the **Applications** node to revoke all refresh tokens. For more information on refresh tokens, see section [5.5.1.4, Token Settings tab](#).

For information on accessing applications through the IdP web page, see section [5.5.8, Accessing applications through the IdP page](#).

5.5.1 Applications Properties

The Applications Properties dialog allows administrators to control the Identity Provider (IdP) server options. These properties apply to all MyID IdP servers in the forest and are not per-user settings.

5.5.1.1 Identity Provider tab



The **IdP Host** is the DNS name of the MyID Authentication Server (or servers).

The **IdP Domain** is the domain name of the MyID Authentication Server.

The **IdP Host** and **IdP Domain** are combined to create the DNS Fully Qualified Domain Name (FQDN) for accessing the MyID Authentication Server from web based clients.

While the DNS FQDN must resolve to the IP address of the MyID Authentication Server, it does not have to be the actual name of the MyID Authentication Server. If you have multiple authentication servers for high availability, you must set the **IdP Host** and **IdP Domain** to create a virtual name that either resolves to all authentication servers, or to a network load balancer virtual IP address.

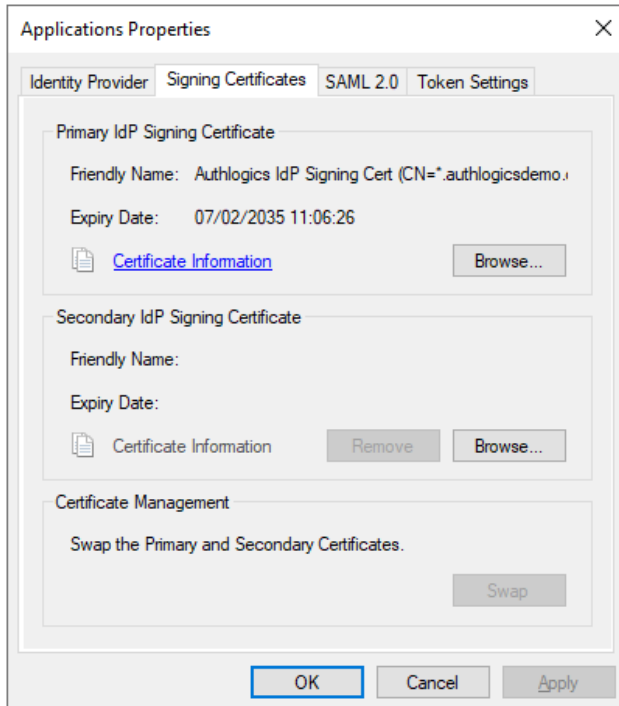
The MyID Authentication Server operates on the HTTPs protocol and is bound to the port specified within the **TCP Port** option. By default, the **TCP Port** is 14443; however, you are recommended to use port 443 with a matching trusted SSL certificate. You must configure the certificate and TCP binding separately on each authentication server in your IIS.

In the **OpenID Connect Information** section, the **Authority URI** is dynamically built based on the **IdP Host**, **IdP Domain**, and **TCP Port** settings.

If the same IdP is used with multiple DNS domains, for example if there are multiple DNS domain names associated with a Microsoft Azure tenant, you must enable **Multiple DNS Domains**, and list the domains.

If you are using only one domain, you are not required to add it to the list.


5.5.1.2 Signing Certificates tab



The screenshot shows the 'Applications Properties' dialog box with the 'Signing Certificates' tab selected. The dialog has four tabs: 'Identity Provider', 'Signing Certificates', 'SAML 2.0', and 'Token Settings'. The 'Signing Certificates' tab contains three sections: 'Primary IdP Signing Certificate', 'Secondary IdP Signing Certificate', and 'Certificate Management'. The 'Primary IdP Signing Certificate' section shows a 'Friendly Name' of 'Authlogics IdP Signing Cert (CN=*.authlogicsdemo.)' and an 'Expiry Date' of '07/02/2035 11:06:26'. It includes a 'Certificate Information' link with a document icon and a 'Browse...' button. The 'Secondary IdP Signing Certificate' section has empty fields for 'Friendly Name' and 'Expiry Date', a 'Certificate Information' link with a document icon, a 'Remove' button, and a 'Browse...' button. The 'Certificate Management' section has a 'Swap the Primary and Secondary Certificates.' label and a 'Swap' button. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

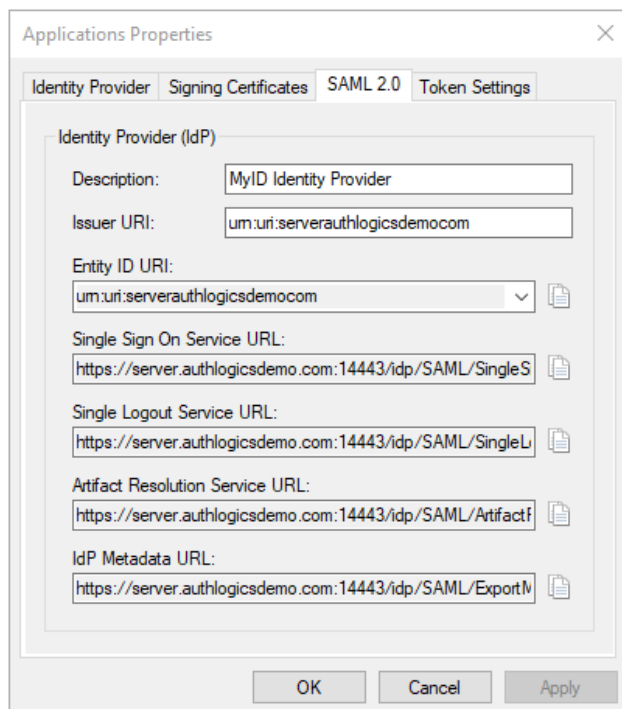
You must have at least one IdP signing certificate. You can configure a Secondary IdP Signing Certificate with a different expiry date to the Primary IdP Signing Certificate to allow for certificate rollover without service interruption.

IdP signing certificates do not have to be publicly trusted as they are not SSL certs; they are shared with application service providers during app setup.

To obtain the Base 64 formatted copy of the certificate, click the copy icon .

To view information about a certificate, click **Certificate Information**.

5.5.1.3 SAML 2.0 tab



On the **SAML 2.0** tab, you can enter a **Description** for your MyID IdP Server.

The **Issuer Uri** must be a unique value. By default it is configured in the following format:

```
urn:uri:<server-host><server-domain-with-no-dots>
```

Where:

- <server-host> is the IdP Host.
- <server-domain-with-no-dots> is the IdP Domain without dots.

For information on setting the IdP Host and IdP Domain, see section [5.5.1.1, Identity Provider tab](#).

If you have configured multiple domains, multiple **Entity ID URI** values are dynamically created; you can view these in the drop-down list. For each domain, a unique Issuer URI is created in the following format:

```
urn:uri:{server-host}{server-domain-with-no-dots}:{mult-domain-name-with-no-dots}
```

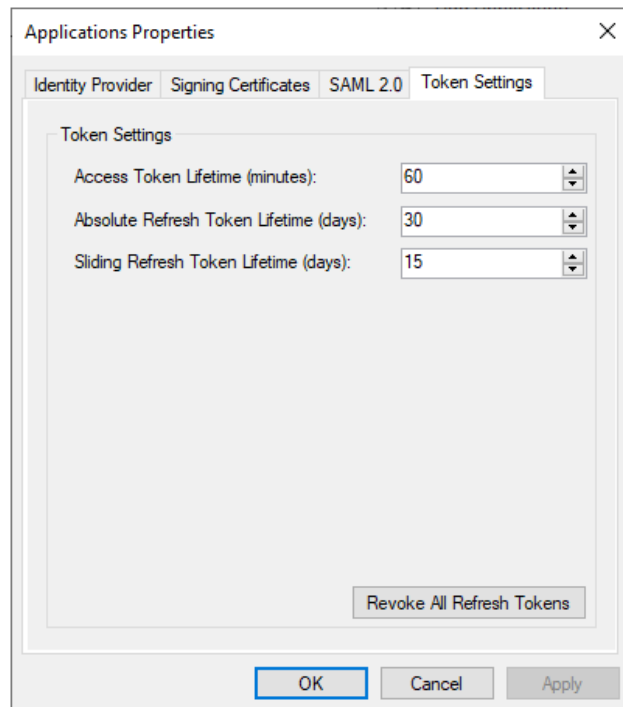
Where:

- <server-host> is the IdP Host.
- <server-domain-with-no-dots> is the IdP Domain without dots.
- <mult-domain-name-with-no-dots> is a domain from your Multiple DNS Domains list.

For information on setting the IdP Host, IdP Domain, and multiple DNS domains, see section [5.5.1.1, Identity Provider tab](#).

The URLs to access the Single Sign On Service, Single Logout Service, Artifact Resolution Service, and the IdP Metadata are displayed for your information. You can click the button next to each URL to copy it to your clipboard.

5.5.1.4 Token Settings tab



Users can remain logged in to multiple sessions. The user logs in by acquiring an access token. Access tokens are either acquired by the user when they authenticate themselves, or are automatically acquired for a user when they attempt to access a session for which they have previously authenticated.

When a user authenticates to a session, they acquire an access token with a lifetime set by the **Access Token Lifetime** setting, a fresh refresh token with a lifetime set by the **Absolute Refresh Token Lifetime** setting, and a fresh sliding refresh time, set by the **Sliding Refresh Token Lifetime** setting.

A new access token can be automatically acquired for a user as long as there is still time remaining in both the absolute refresh token's lifetime and the sliding refresh time. When a new access token is requested, the session's sliding refresh time is reset.

If the user logs out of a session, all tokens related to that session are revoked.

The user must reauthenticate if a new access token cannot be acquired for the user for a session. This may happen for the following reasons:

- The user has not authenticated to that session before.
- The user last authenticated to that session longer than the absolute refresh token's lifetime ago.
- The user logged out of the session.
- The user has not attempted to authenticate to that session for longer than the duration of the sliding refresh time.
- An administrator has revoked the user's refresh tokens.

You can set the lifetimes of the various tokens relating to how often a user must authenticate to a session:

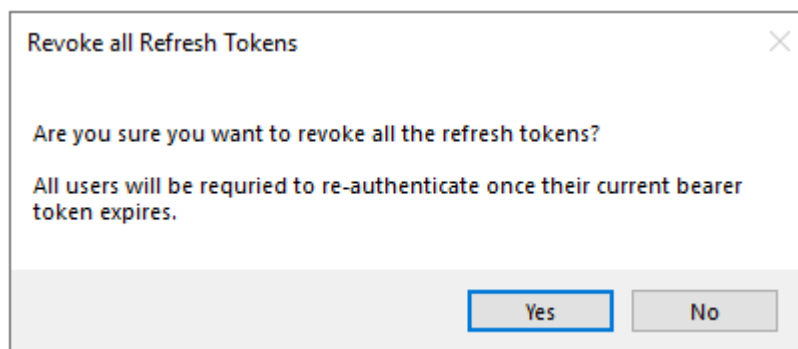
- **Access Token Lifetime** – the lifetime of access tokens; access tokens cannot be revoked and once issued work for their full lifetime. This is measured in minutes and has a default value of 60.
- **Absolute Refresh Token Lifetime** – the maximum lifetime of an absolute refresh token. After this time, tokens can no longer be refreshed and the user must re-authenticate. This is measured in days and has a default value of 30.
- **Sliding Refresh Token Lifetime** – the sliding refresh time, that is, the time since the last access token was made in which a session can be refreshed. This is the window in which a token can be refreshed – this applies to the original token and any subsequent tokens that have been refreshed from that one.

You may want to revoke a user's access tokens if you believe that they have not logged out of their session on an insecure machine, or that a malicious actor has accessed their session.

To prevent all issued access tokens from being refreshed, you can revoke the refresh tokens of all users:

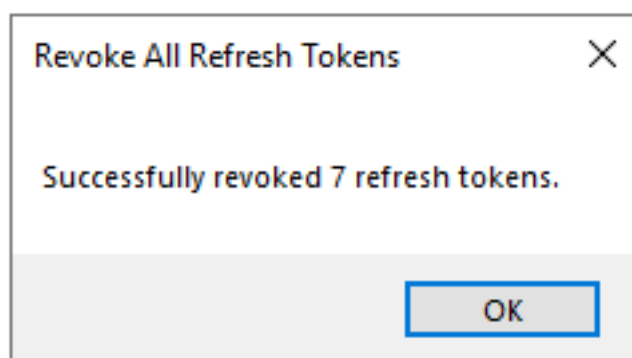
1. Click **Revoke All Refresh Tokens**.

A pop-up appears to confirm that you want to revoke refresh tokens for all users.



2. Click **Yes**.

A pop-up appears to confirm how many refresh tokens have been revoked.



You can also revoke all refresh tokens from the **Actions** pane for the **Applications** node.

You can also revoke the refresh tokens of a specific user or selected group of users. For more information, see section [5.9.9, Revoking specific users' refresh tokens](#).

When you revoke a user's refresh tokens:

- Their access tokens expire based on the set **Access Token Lifetime**; when the access tokens expire, the users with those tokens must reauthenticate.
- They cannot change their mobile phone number or password in the Self Service Portal until they reauthenticate.

Users with revoked refresh tokens regain full functionality when they reauthenticate.

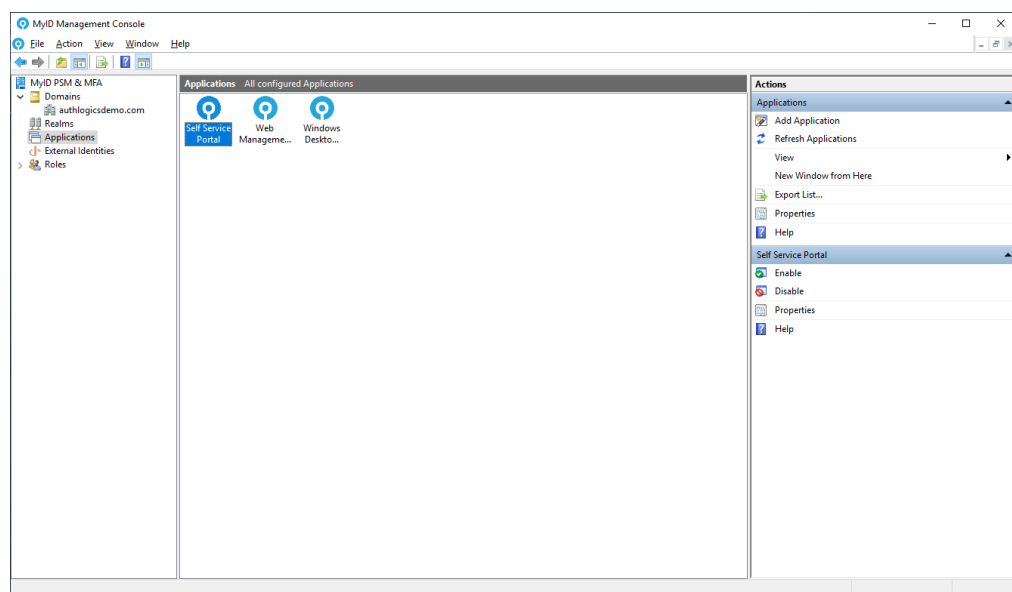
5.5.2 Self Service Portal Properties

The Self Service Portals properties dialog contains the customization options for the Self Service Portal. The MyID Authentication Server includes a user Self Service Portal where users can perform various common administrative tasks themselves such as register a new MFA device, change their Grid pattern, Phrase answers, static YubiKey and OTC PINs and reset their Active Directory password and update their mobile/cellular phone number. The Web Management Portal provides basic administration and operational capabilities suited to helpdesk personnel.

The portal is designed to be compatible with desktop and mobile browsers.

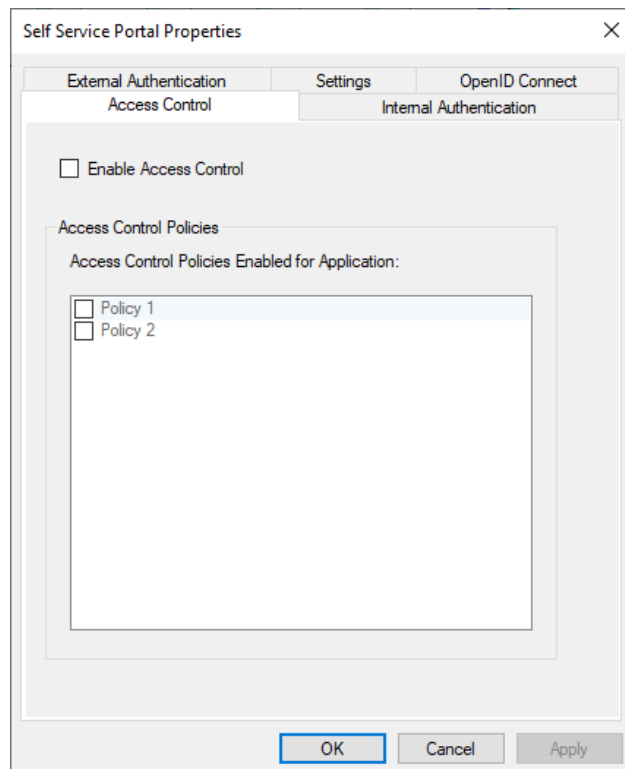
To access the Self Service Portal application properties:

1. In the MyID Management Console, enter the **Applications** node.
2. Highlight the **Self Service Portal**.



3. Click **Properties**, in the **Actions** pane.

5.5.2.1 Access Control tab



The **Access Control** tab allows you to apply access control policies to the current application. For each policy that you have enabled for the application, you can configure unique settings for the internal and external authentication.

Important: If you enable access control, the only policies that apply are those that are configured; if you do not configure any policies, no users can access the application.

To apply access control policies to the application:

1. On the **Access Control** tab, select the **Enable Access Control** option.
2. In the **Access Control Policies Enabled for Application** list, select the access control policies you want to use for the current application.

For information on creating access control policies, see section [5.11.1, Access control policies](#).

3. Click **Apply**.

Note: You must click **Apply** before changing to a different tab to ensure that you have saved the changes to the list of enabled policies.

4. On the **Internal Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.

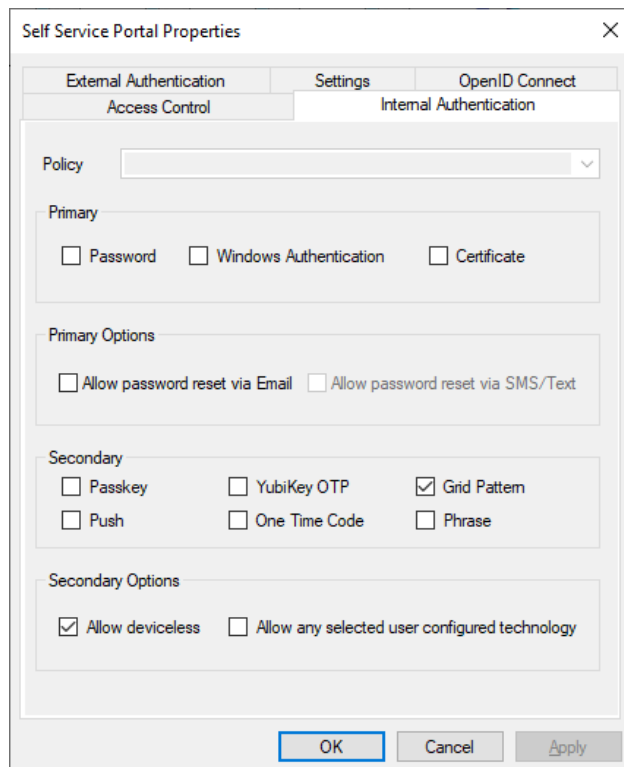
You can configure the settings for each access control policy, so that different configurations apply to different sets of users.

5. Configure the internal authentication settings for the policy.
6. Click **Apply**.

Note: You must click **Apply** before changing to a different policy to ensure that you have saved the changes for the current policy.

7. On the **External Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.
8. Configure the external authentication settings for the policy.
9. Click **Apply**.
10. Click **OK**.

5.5.2.2 Internal Authentication tab



The image shows a screenshot of the 'Self Service Portal Properties' dialog box, specifically the 'Internal Authentication' tab. The dialog has a title bar with a close button (X). Below the title bar are three tabs: 'External Authentication', 'Settings', and 'OpenID Connect'. The 'Settings' tab is selected, and within it, the 'Internal Authentication' sub-tab is active. The main content area is divided into several sections: 'Policy' with a drop-down menu; 'Primary' with three checkboxes: 'Password', 'Windows Authentication', and 'Certificate'; 'Primary Options' with two checkboxes: 'Allow password reset via Email' and 'Allow password reset via SMS/Text'; 'Secondary' with six checkboxes: 'Passkey', 'YubiKey OTP', 'Grid Pattern' (checked), 'Push', 'One Time Code', and 'Phrase'; and 'Secondary Options' with two checkboxes: 'Allow deviceless' (checked) and 'Allow any selected user configured technology'. At the bottom right are three buttons: 'OK', 'Cancel', and 'Apply'.

If you have enabled access control for this application, select a **Policy** from the drop-down list and configure the internal authentication settings for each policy. See section [5.5.2.1, Access Control tab](#) for details.

You can specify the logon technology users must use to authenticate to the portal.

You can choose one logon technology from the options in the **Primary** section.

If only a PSM license is installed, the options are limited to **Password** and **Windows Authentication**.

For new installations, for applications of this type, the primary logon technology defaults to **Password** only. However, if you have an MFA license, you are recommended to update this to use more secure technologies. If you are upgrading from a version earlier than 5.1.0 and **Enable Passwordless MFA** was not selected, **Password** is automatically selected as the primary logon technology.

If you select **Password**, users are required to enter a valid Active Directory password as well as their MFA credentials. If you do not select **Password**, passwordless logins are enabled.

If you select **Windows Authentication** or **Certificate**, the **Primary Options**, **Secondary**, and **Secondary Options** sections are disabled, as these technologies do not require further configuration.

Note: If you select **Windows Authentication**, you must configure IIS to use Windows Authentication – this disables multi-factor authentication for this application. If you enable Windows Authentication in the MyID Management Console without configuring Windows Authentication in IIS, the user is shown the standard Windows prompt to enter their Username and Password.

Similarly, if you select **Certificate** authentication, you must configure IIS to handle the certificate, at which point all other MFA options are no longer valid for this application, and you cannot select them in the MyID Management Console.

You can choose as many or as few **Secondary** logon technologies as you want.

If you select only one secondary option, the user must have that logon technology.

If you select multiple secondary options, the type of technology used is determined after the user has entered their account name and, if required, password. The type of logon technology used is determined based on the selected options and which technologies the user has configured. The priority order for the secondary logon technologies is:

- **Passkey**
- **Grid Pattern** (if **Allow deviceless** is not selected)
- **Push**
- **YubiKey OTP**
- **One Time Code**
- **Phrase** (if **Allow deviceless** is not selected)
- **Grid Pattern** (if **Allow deviceless** is selected)
- **Phrase** (if **Allow deviceless** is selected)

If **Password** is selected as the primary logon technology, and no secondary logon technology is selected, the user requires only a password to log in.

If a user does not have access to any of the secondary logon technologies selected, they cannot log in to the application, unless all of the following are true:

- No primary logon technology is selected.
- All secondary logon technologies selected require devices.
- The user has no device registered.

In that case, fallback password authentication occurs, and the user can log in with just their username and password.

If no logon technologies are selected, no-one can log in.

If the user has a device registered, the technologies that require a device (**Passkey**, and, if **Allow deviceless** is not selected, **Grid Pattern** and **Phrase**) can be selected, whether or not the device is enabled.

For example, if a user has a FIDO token registered but the device has been disabled, the user is still prompted to authenticate with their FIDO token. This is so that temporarily displaced devices do not allow users to fall back on lesser authentication methods.

If a user temporarily loses their FIDO device, you can give them a temporary access code – by default, this only lasts 24 hours or three logons, whichever comes first. For information on changing temporary access code limitations, see section [5.3.1, General tab](#). If the user finds their FIDO token, you can re-enable it, and if they cannot find it, you can remove the device from their account and issue a new one. For information on assigning temporary access codes, see section [5.9.8, Assigning temporary access codes to a user](#) or the *Assigning a temporary access code to a user* section of the [Web Management Portal User Guide](#).

If you select the **Allow any selected user configured technology** option, users are allowed to authenticate using any MFA technology for which they are provisioned. If this option is not selected, the user can enter only the valid authentication credentials that are shown by the application.

Grid Pattern and Phrase authentication technologies both support deviceless authentication; select the **Allow Deviceless** option to enable this support. If this is selected, you cannot use these technologies with a device, which is less secure. If this is not selected, then multi-factor authentication is always required.

If you have only a PSM license installed, the Self Service Portal can still issue One Time Codes using SMS/Text or Email for Active Directory Password reset purposes. To use this feature, the **Password** must be set as the **Primary** logon technology, and either **Allow password reset via Email** or **Allow password reset via SMS/Text** must be enabled.

5.5.2.3 External Authentication tab

The screenshot shows a dialog box titled "Self Service Portal Properties" with a close button (X) in the top right corner. The dialog has two main tabs: "Access Control" and "Internal Authentication". Under "Access Control", there are sub-tabs: "External Authentication" (which is selected), "Settings", and "OpenID Connect". In the "External Authentication" sub-tab, there is a "Policy" dropdown menu. Below this, there is a section titled "External Authentication" containing a box labeled "External Identities linked with this Application:". At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

If you have enabled access control for this application, you can select the **Policy** from the drop-down list and configure the external authentication settings for each policy. See section [5.5.2.1, Access Control tab](#) for details.

The External Identities linked with this application allow users to authenticate to the website or service using a preconfigured external identity provider; for information on adding an external identity, see section [5.7, Adding External Identities](#).

5.5.2.4 Settings tab

The screenshot shows the 'Self Service Portal Properties' dialog box with the 'Settings' tab selected. The 'General Settings' section contains an 'Email URL' field with the value 'https://server.authlogicsdemo.com:14443/'. Below this is a descriptive text block. The 'Allowed User Actions' section contains several checkboxes: 'Unlock AD Account', 'Reset AD Password', 'Auto unlock AD Account on password reset', 'Change Mobile / Cellular phone number', 'Add Token devices', and 'Remove Token devices'. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

Self Service Portal Properties

Access Control Internal Authentication

External Authentication Settings OpenID Connect

General Settings

Email URL:

The Email URL is the address that is embedded into onboarding welcome emails which are sent to users when they are provisioned for a new account or MFA technology. This URL should resolve to the Authentication Server and must match the port, DNS name and SSL certificate details in IIS.

Allowed User Actions

☒ Unlock AD Account

☒ Reset AD Password

☒ Auto unlock AD Account on password reset

☒ Change Mobile / Cellular phone number

☒ Add Token devices ☐ Remove Token devices

OK Cancel Apply

The **Email URL** must be an accessible and resolvable web-based address that provides users access to the Self Service Portal hosted on the Authentication Server. The default HTTPS port (SSL) for the SSP is TCP:14443, although additional ports can be configured within IIS. A reverse proxy or SSL VPN device may be used to provide connectivity to the portal if required.

Administrators can enable or disable the user's ability to perform the following actions through the Self Service Portal (depending on the installed product license):

- **Unlock AD Account** – Allows users to unlock their Active Directory Account.
- **Reset AD Password** – Allows users to reset their Active Directory Password.
 - **Auto unlock AD Account on password reset** – Auto unlocks the user's Active Directory Account when their password is reset.
- **Change Mobile / Cellular phone number** – Allows users to change their mobile/cellular phone number.
- **Add Token devices** – Allows users to add token devices.
- **Remove Token devices** – Allows users to remove token devices.

5.5.2.5 OpenID Connect tab

The OpenID Connect tab details the IdP Server and Relying Party trust settings.

The screenshot shows the 'Self Service Portal Properties' dialog box with the 'OpenID Connect' tab selected. The dialog is divided into two main sections: 'Identity Provider (IdP)' and 'Relying Party (RP)'. In the 'Identity Provider (IdP)' section, the 'Client ID' is set to 'internal.selfservice' and the 'Client Secret' is masked with dots. In the 'Relying Party (RP)' section, the 'Grant Type' is set to 'Code'. The 'Scopes' section has three checkboxes: 'profile' (checked), 'email' (unchecked), and 'phone' (unchecked). The 'Redirect URI' and 'Logout URI' are both set to 'https://server.authlogicsdemo.com:14443/ssp/si'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

Access Control		Internal Authentication	
External Authentication		Settings	OpenID Connect
Identity Provider (IdP)			
Client ID:	internal.selfservice		
Client Secret:		
Relying Party (RP)			
Grant Type:	Code		
Scopes:	<input checked="" type="checkbox"/> profile <input type="checkbox"/> email <input type="checkbox"/> phone		
Redirect URI:	https://server.authlogicsdemo.com:14443/ssp/si		
Logout URI:	https://server.authlogicsdemo.com:14443/ssp/si		
OK		Cancel	Apply

Through this, you can specify the Self Service Portal's **Grant Type**, **Redirect** and **Logout URIs** and the scope for the relying party trust.

5.5.3 Web Management Portal Properties

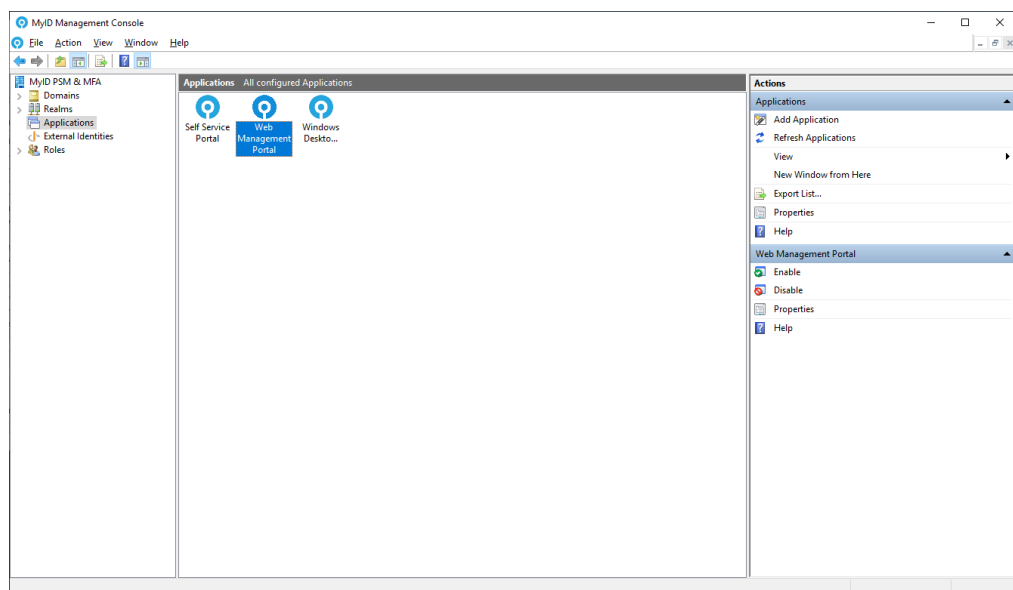
The MyID Authentication Server includes a user Web Management Portal where administrators and web operators can perform basic administration and operational capabilities suited to helpdesk personnel.

The Web Management Portal application properties contain the customization options for the Web Management Portal.

The portal is designed to be compatible with desktop and mobile browsers.

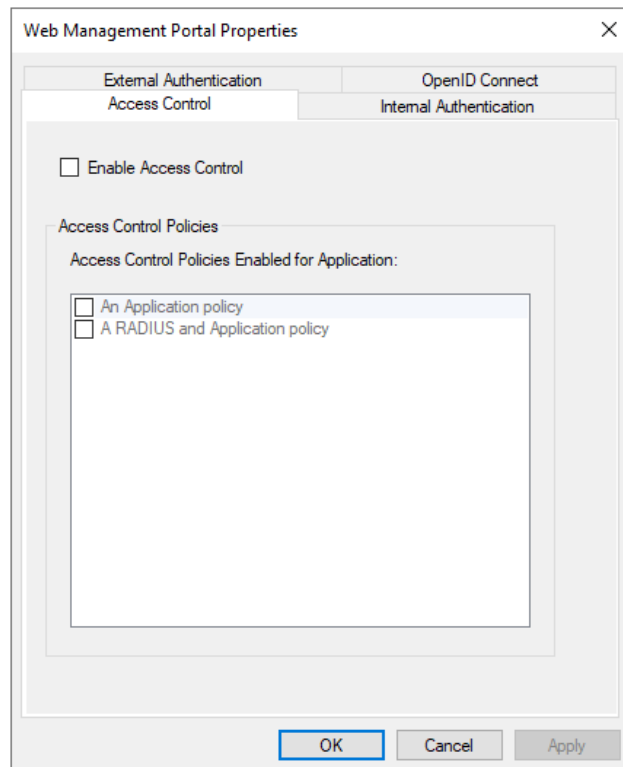
To access the Web Management Portal application properties:

1. In the MyID Management Console, enter the **Applications** node.
2. Highlight the **Web Management Portal**.



3. Click **Properties**, in the **Actions** pane.

5.5.3.1 Access Control tab



The **Access Control** tab allows you to apply access control policies to the current application. For each policy that you have enabled for the application, you can configure unique settings for the internal and external authentication.

Important: If you enable access control, the only policies that apply are those that are configured; if you do not configure any policies, no users can access the application.

To apply access control policies to the application:

1. On the Access Control tab, select the **Enable Access Control** option.
2. In the **Access Control Policies Enabled for Application** list, select the access control policies you want to use for the current application.

For information on creating access control policies, see section [5.11.1, Access control policies](#).

3. Click **Apply**.

Note: You must click **Apply** before changing to a different tab to ensure that you have saved the changes to the list of enabled policies.

4. On the **Internal Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.

You can configure the settings for each access control policy, so that different configurations apply to different sets of users.

5. Configure the internal authentication settings for the policy.
6. Click **Apply**.

Note: You must click **Apply** before changing to a different policy to ensure that you have saved the changes for the current policy.

7. On the **External Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.
8. Configure the external authentication settings for the policy.
9. Click **Apply**.
10. Click **OK**.

5.5.3.2 Internal Authentication tab

The screenshot shows the 'Web Management Portal Properties' dialog box with the 'Internal Authentication' tab selected. The 'Access Control' sub-tab is also active. A 'Policy' dropdown menu is at the top. Below it, the 'Primary' section contains three unchecked checkboxes: 'Password', 'Windows Authentication', and 'Certificate'. The 'Primary Options' section contains two unchecked checkboxes: 'Allow password reset via Email' and 'Allow password reset via SMS/Text'. The 'Secondary' section contains six checked checkboxes: 'Passkey', 'YubiKey OTP', 'Grid Pattern', 'Push', 'One Time Code', and 'Phrase'. The 'Secondary Options' section contains two unchecked checkboxes: 'Allow deviceless' and 'Allow any selected user configured technology'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

If you have enabled access control for this application, you can select a **Policy** from the drop-down list and configure the internal authentication settings for each policy. See section [5.5.3.1, Access Control tab](#) for details.

You can specify the logon technology users must use to authenticate to the portal.

You can choose one logon technology from the options in the **Primary** section.

If only a PSM license is installed, the options are limited to **Password** and **Windows Authentication**.

For new installations, for applications of this type, the primary logon technology defaults to **Password** only. However, if you have an MFA license, you are recommended to update this to use more secure technologies. If you are upgrading from a version earlier than 5.1.0 and **Enable Passwordless MFA** was not selected, **Password** is automatically selected as the primary logon technology.

If you select **Password**, users are required to enter a valid Active Directory password as well as their MFA credentials. If you do not select **Password**, passwordless logins are enabled.

If you select **Windows Authentication** or **Certificate**, the **Primary Options**, **Secondary**, and **Secondary Options** sections are disabled, as these technologies do not require further configuration.

Note: If you select **Windows Authentication**, you must configure IIS to use Windows Authentication – this disables multi-factor authentication for this application. If you enable Windows Authentication in the MyID Management Console without configuring Windows Authentication in IIS, the user is shown the standard Windows prompt to enter their Username and Password.

Similarly, if you select **Certificate** authentication, you must configure IIS to handle the certificate, at which point all other MFA options are no longer valid for this application, and you cannot select them in the MyID Management Console.

You can choose as many or as few **Secondary** logon technologies as you want.

If you select only one secondary option, the user must have that logon technology.

If you select multiple secondary options, the type of technology used is determined after the user has entered their account name and, if required, password. The type of logon technology used is determined based on the selected options and which technologies the user has configured. The priority order for the secondary logon technologies is:

- **Passkey**
- **Grid Pattern** (if **Allow deviceless** is not selected)
- **Push**
- **YubiKey OTP**
- **One Time Code**
- **Phrase** (if **Allow deviceless** is not selected)
- **Grid Pattern** (if **Allow deviceless** is selected)
- **Phrase** (if **Allow deviceless** is selected)

If **Password** is selected as the primary logon technology, and no secondary logon technology is selected, the user requires only a password to log in.

If a user does not have access to any of the secondary logon technologies selected, they cannot log in to the application, unless all of the following are true:

- No primary logon technology is selected.
- All secondary logon technologies selected require devices.
- The user has no device registered.

In that case, fallback password authentication occurs, and the user can log in with just their username and password.

If no logon technologies are selected, no-one can log in.

If the user has a device registered, the technologies that require a device (**Passkey**, and, if **Allow deviceless** is not selected, **Grid Pattern** and **Phrase**) can be selected, whether or not the device is enabled.

For example, if a user has a FIDO token registered but the device has been disabled, the user is still prompted to authenticate with their FIDO token. This is so that temporarily displaced devices do not allow users to fall back on lesser authentication methods.

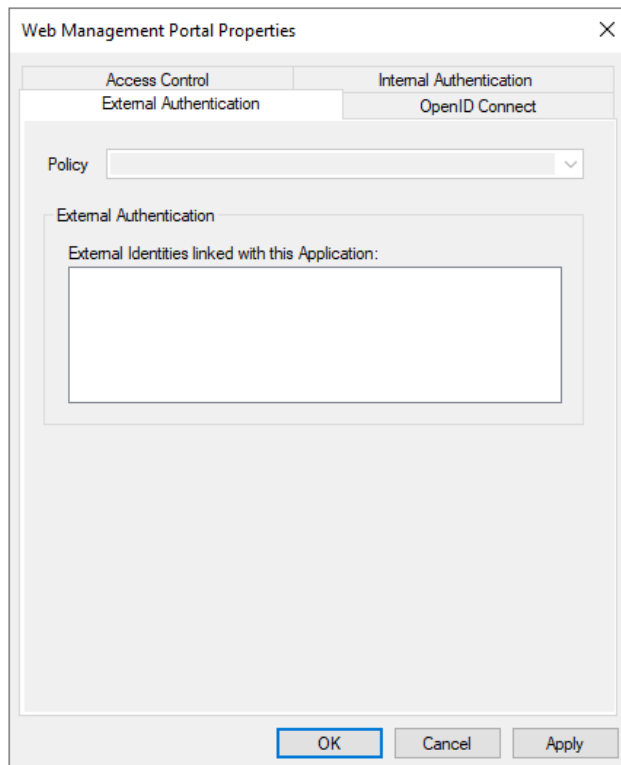
If a user temporarily loses their FIDO device, you can give them a temporary access code – by default, this only lasts 24 hours or three logons, whichever comes first. For information on changing temporary access code limitations, see section [5.3.1, General tab](#). If the user finds their FIDO token, you can re-enable it, and if they cannot find it, you can remove the device from their account and issue a new one. For information on assigning temporary access codes, see section [5.9.8, Assigning temporary access codes to a user](#) or the *Assigning a temporary access code to a user* section of the [Web Management Portal User Guide](#).

If you select the **Allow any selected user configured technology** option, users are allowed to authenticate using any MFA technology for which they are provisioned. If this option is not selected, the user can enter only the valid authentication credentials that are shown by the application.

Grid Pattern and Phrase authentication technologies both support deviceless authentication; select the **Allow Deviceless** option to enable this support. If this is selected, you cannot use these technologies with a device, which is less secure. If this is not selected, then multi-factor authentication is always required.

If you have only a PSM license installed, the Web Management Portal can still issue One Time Codes using SMS/Text or Email for Active Directory Password reset purposes. To use this feature, the **Password** must be set as the **Primary** logon technology, and either **Allow password reset via Email** or **Allow password reset via SMS/Text** must be enabled.

5.5.3.3 External Authentication tab



The image shows a screenshot of the 'Web Management Portal Properties' dialog box, specifically the 'External Authentication' tab. The dialog has a title bar with a close button (X). Inside, there are two sub-tabs: 'Access Control' and 'Internal Authentication'. The 'Access Control' sub-tab is active, showing a 'Policy' dropdown menu. Below this, there is a section titled 'External Authentication' which contains a label 'External Identities linked with this Application:' followed by an empty rectangular box for listing identities. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

If you have enabled access control for this application, you can select the **Policy** from the drop-down list and configure the external authentication settings for each policy. See section [5.5.3.1, Access Control tab](#) for details.

The External Identities linked with this application allows users to authenticate to the website or service using a preconfigured external identity provider; for information on adding an external identity, see section [5.7, Adding External Identities](#).

5.5.3.4 OpenID Connect tab

The OpenID Connect tab details the IdP Server and Relying Party trust settings.

The screenshot shows the 'Web Management Portal Properties' dialog box with the 'OpenID Connect' tab selected. The dialog has three tabs: 'Access Control', 'External Authentication', and 'Internal Authentication'. The 'OpenID Connect' tab is active, showing settings for the Identity Provider (IdP) and the Relying Party (RP).

Identity Provider (IdP)

- Client ID: `internal.webmanagement`
- Client Secret: `.....`

Relying Party (RP)

- Grant Type: `Code` (dropdown menu)
- Scopes: ☒ profile, ☐ email, ☐ phone
- Redirect URI: `https://server.authlogicsdemo.com:14443/admin`
- Logout URI: `https://server.authlogicsdemo.com:14443/admin`

Buttons at the bottom: OK, Cancel, Apply.

Through this, you can specify the Web Management Portal's **Grant Type**, **Redirect** and **Logout URIs** and the scope for the relying party trust.

5.5.3.5 Disabling password changing

To stop administrators and operators from being able to change user passwords through the Web Management Portal:

1. If you do not have an `appsettings.Production.json` file for the Web Management Portal, create it in the Web Management Portal settings folder. By default this is the following location:

`C:\Program Files\Authlogics Authentication Server\Web\Admin`

Note: Do not use the `appsettings.json` file – that file can be overwritten when you update or upgrade MyID MFA and PSM.

2. In a text editor, open the `appsettings.Production.json` file for the Web Management Portal.
3. Create a `Customisation` section, and within it set the `DisablePasswordReset` option to `True`.

```
{
  "Customisation": {
    "DisablePasswordReset": "True"
  }
}
```

Note: Due to the limitations of PDFs, some whitespace characters may not come across cleanly. You are recommended to validate and sanitize your JSON; for example, you can use a JSON reformatter.

4. Save the `appsettings.Production.json` file.
5. To ensure that this change is immediately enforced, you must refresh the application pool. To recycle the Web Management Portal application pool:
 - a. On the MyID Authentication Server, in Internet Information Services (IIS) Manager, select **Application Pools**.
 - b. Right-click the **Authlogics Authentication Server WMP** application pool, then from the pop-up menu click **Recycle**.
6. Check that the changes are successful by logging in to the Web Management Portal and seeing if you can change a user's password.

To re-enable changing passwords in the Web Management Portal, set `DisablePasswordReset` to `False` in the Web Management Portal `appsettings.Production.json`, or delete the Web Management Portal `appsettings.Production.json`.

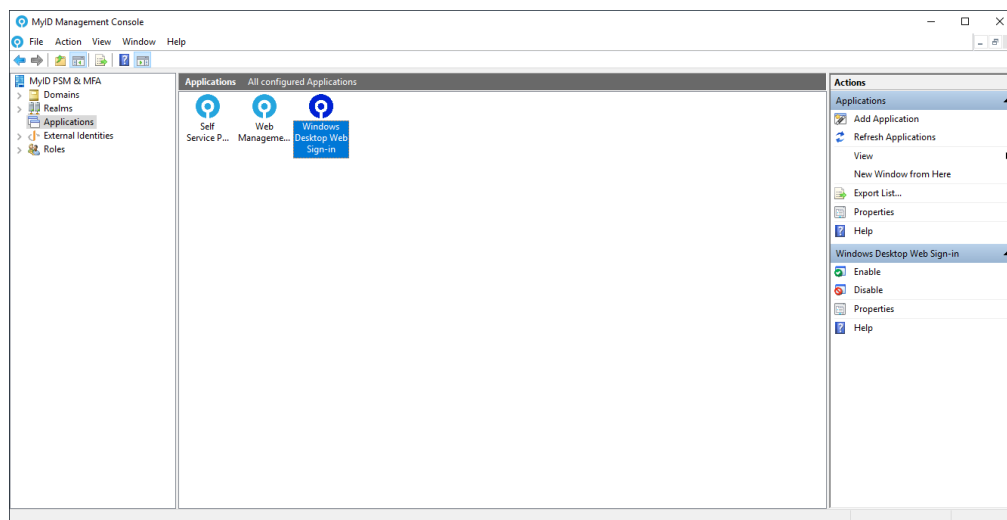
5.5.4 Windows Desktop Agent Properties

The MFA Windows Desktop Agent tabs contain the customization options for the MyID MFA Windows Desktop Agent.

The portal is designed to be compatible with desktop and mobile browsers.

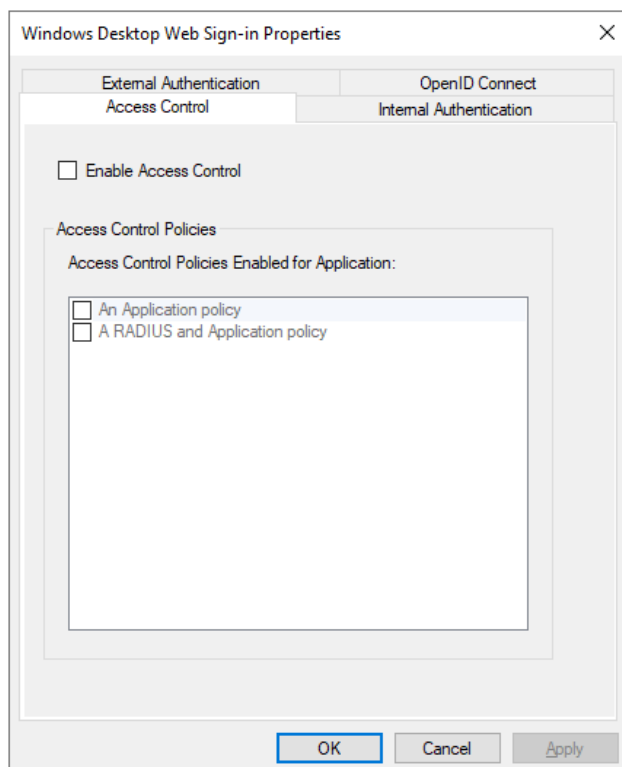
To access the Windows Desktop Agent application properties:

1. In the MyID Management Console, enter the **Applications** node.
2. Highlight the **Windows Desktop Web Sign-in**.



3. Click **Properties**, in the **Actions** pane.

5.5.4.1 Access Control tab



The **Access Control** tab allows you to apply access control policies to the current application. For each policy that you have enabled for the application, you can configure unique settings for the internal and external authentication.

Important: If you enable access control, the only policies that apply are those that are configured; if you do not configure any policies, no users can access the application.

To apply access control policies to the application:

1. On the Access Control tab, select the **Enable Access Control** option.
2. In the **Access Control Policies Enabled for Application** list, select the access control policies you want to use for the current application.

For information on creating access control policies, see section [5.11.1, Access control policies](#).

3. Click **Apply**.

Note: You must click **Apply** before changing to a different tab to ensure that you have saved the changes to the list of enabled policies.

4. On the **Internal Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.

You can configure the settings for each access control policy, so that different configurations apply to different sets of users.

5. Configure the internal authentication settings for the policy.
6. Click **Apply**.

Note: You must click **Apply** before changing to a different policy to ensure that you have saved the changes for the current policy.

7. On the **External Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.
8. Configure the external authentication settings for the policy.
9. Click **Apply**.
10. Click **OK**.

5.5.4.2 Internal Authentication tab

The screenshot shows the 'Windows Desktop Web Sign-in Properties' dialog box with the 'Internal Authentication' tab selected. The 'Access Control' sub-tab is also visible. The 'Policy' dropdown is empty. Under 'Primary', 'Password' is checked. Under 'Primary Options', 'Allow password reset via Email' and 'Allow password reset via SMS/Text' are unchecked. Under 'Secondary', 'Grid Pattern' is checked. Under 'Secondary Options', 'Allow deviceless' and 'Allow any selected user configured technology' are unchecked. The 'OK', 'Cancel', and 'Apply' buttons are at the bottom.

External Authentication	OpenID Connect
Access Control	Internal Authentication

Policy: []

Primary

☒ Password ☐ Windows Authentication ☐ Certificate

Primary Options

☐ Allow password reset via Email ☐ Allow password reset via SMS/Text

Secondary

☐ Passkey ☐ YubiKey OTP ☒ Grid Pattern

☐ Push ☐ One Time Code ☐ Phrase

Secondary Options

☐ Allow deviceless ☐ Allow any selected user configured technology

OK Cancel Apply

If you have enabled access control for this application, you can select a **Policy** from the drop-down list and configure the internal authentication settings for each policy. See section [5.5.4.1, Access Control tab](#) for details.

You can specify the logon technology users must use to authenticate to the portal.

You can choose one logon technology from the options in the **Primary** section.

If only a PSM license is installed, the options are limited to **Password** and **Windows Authentication**.

For new installations, for applications of this type, the primary logon technology defaults to **Password** only. However, if you have an MFA license, you are recommended to update this to use more secure technologies. If you are upgrading from a version earlier than 5.1.0 and **Enable Passwordless MFA** was not selected, **Password** is automatically selected as the primary logon technology.

If you select **Password**, users are required to enter a valid Active Directory password as well as their MFA credentials. If you do not select **Password**, passwordless logins are enabled.

If you select **Windows Authentication** or **Certificate**, the **Primary Options**, **Secondary**, and **Secondary Options** sections are disabled, as these technologies do not require further configuration.

Note: If you select **Windows Authentication**, you must configure IIS to use Windows Authentication – this disables multi-factor authentication for this application. If you enable Windows Authentication in the MyID Management Console without configuring Windows Authentication in IIS, the user is shown the standard Windows prompt to enter their Username and Password.

Similarly, if you select **Certificate** authentication, you must configure IIS to handle the certificate, at which point all other MFA options are no longer valid for this application, and you cannot select them in the MyID Management Console.

You can choose as many or as few **Secondary** logon technologies as you want.

If you select only one secondary option, the user must have that logon technology.

If you select multiple secondary options, the type of technology used is determined after the user has entered their account name and, if required, password. The type of logon technology used is determined based on the selected options and which technologies the user has configured. The priority order for the secondary logon technologies is:

- **Passkey**
- **Grid Pattern** (if **Allow deviceless** is not selected)
- **Push**
- **YubiKey OTP**
- **One Time Code**
- **Phrase** (if **Allow deviceless** is not selected)
- **Grid Pattern** (if **Allow deviceless** is selected)
- **Phrase** (if **Allow deviceless** is selected)

If **Password** is selected as the primary logon technology, and no secondary logon technology is selected, the user requires only a password to log in.

If a user does not have access to any of the secondary logon technologies selected, they cannot log in to the application, unless all of the following are true:

- No primary logon technology is selected.
- All secondary logon technologies selected require devices.
- The user has no device registered.

In that case, fallback password authentication occurs, and the user can log in with just their username and password.

If no logon technologies are selected, no-one can log in.

If the user has a device registered, the technologies that require a device (**Passkey**, and, if **Allow deviceless** is not selected, **Grid Pattern** and **Phrase**) can be selected, whether or not the device is enabled.

For example, if a user has a FIDO token registered but the device has been disabled, the user is still prompted to authenticate with their FIDO token. This is so that temporarily displaced devices do not allow users to fall back on lesser authentication methods.

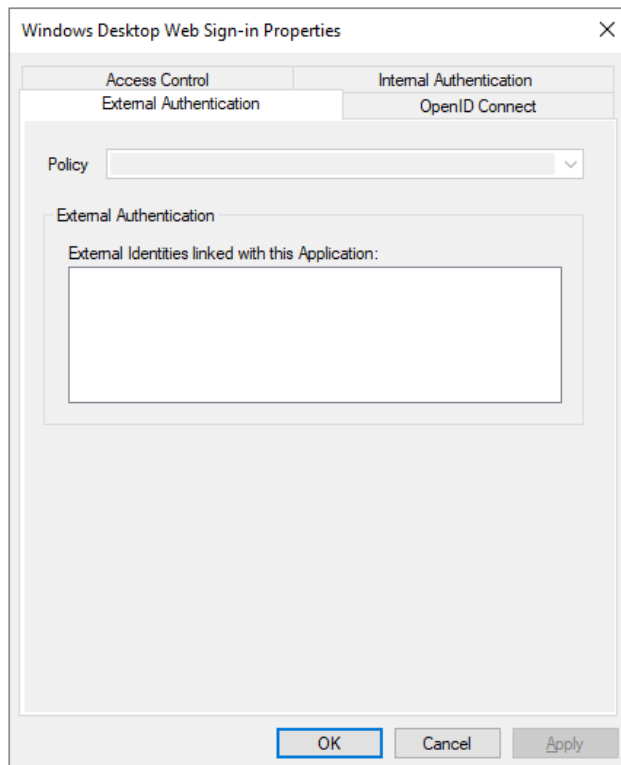
If a user temporarily loses their FIDO device, you can give them a temporary access code – by default, this only lasts 24 hours or three logons, whichever comes first. For information on changing temporary access code limitations, see section [5.3.1, General tab](#). If the user finds their FIDO token, you can re-enable it, and if they cannot find it, you can remove the device from their account and issue a new one. For information on assigning temporary access codes, see section [5.9.8, Assigning temporary access codes to a user](#) or the *Assigning a temporary access code to a user* section of the [Web Management Portal User Guide](#).

If you select the **Allow any selected user configured technology** option, users are allowed to authenticate using any MFA technology for which they are provisioned. If this option is not selected, the user can enter only the valid authentication credentials that are shown by the application.

Grid Pattern and Phrase authentication technologies both support deviceless authentication; select the **Allow Deviceless** option to enable this support. If this is selected, you cannot use these technologies with a device, which is less secure. If this is not selected, then multi-factor authentication is always required.

If you have only a PSM license installed, you can use the Window Desktop Agent to issue One Time Codes using SMS/Text or Email for Active Directory Password reset purposes. To use this feature, the **Password** must be set as the **Primary** logon technology, and either **Allow password reset via Email** or **Allow password reset via SMS/Text** must be enabled.

5.5.4.3 External Authentication tab



If you have enabled access control for this application, you can select the **Policy** from the drop-down list and configure the external authentication settings for each policy. See section [5.5.4.1, Access Control tab](#) for details.

The **External Identities linked with this application** option allows users to authenticate to the website or service using a preconfigured external identity provider; for information on adding an external identity, see section [5.7, Adding External Identities](#).

5.5.4.4 OpenID Connect tab

The OpenID Connect tab details the IdP Server and Relying Party trust settings.

The screenshot shows the 'Windows Desktop Web Sign-in Properties' dialog box with the 'OpenID Connect' tab selected. The dialog is divided into two main sections: 'Identity Provider (IdP)' and 'Relying Party (RP)'. In the 'Identity Provider (IdP)' section, the 'Client ID' is set to 'internal.desktop' and the 'Client Secret' is masked with dots. In the 'Relying Party (RP)' section, the 'Grant Type' is set to 'Code'. Under 'Scopes', the 'profile' checkbox is checked, while 'email' and 'phone' are unchecked. Both the 'Redirect URI' and 'Logout URI' are set to 'http://127.0.0.1/pkce'. At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

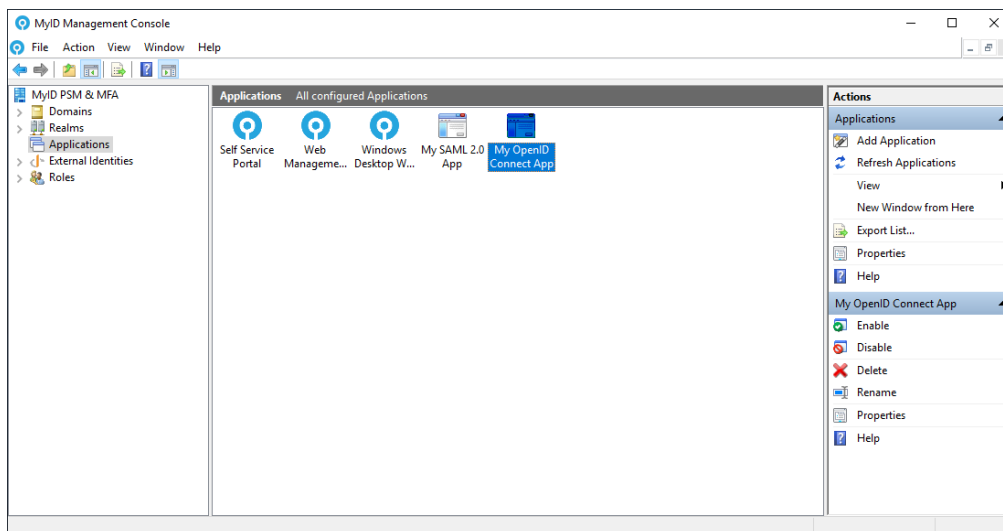
Through this, you can specify the Windows Desktop Agent's **Grant Type**, **Redirect** and **Logout URIs** and the scope for the relying party trust.

5.5.5 OpenID Connect application properties

The applications properties dialog of an OpenID Connect application allows administrators to control the OpenID Connect application. For more information on adding a OpenID Connect application, see section [5.6.1, *Creating an OpenID Connect application*](#).

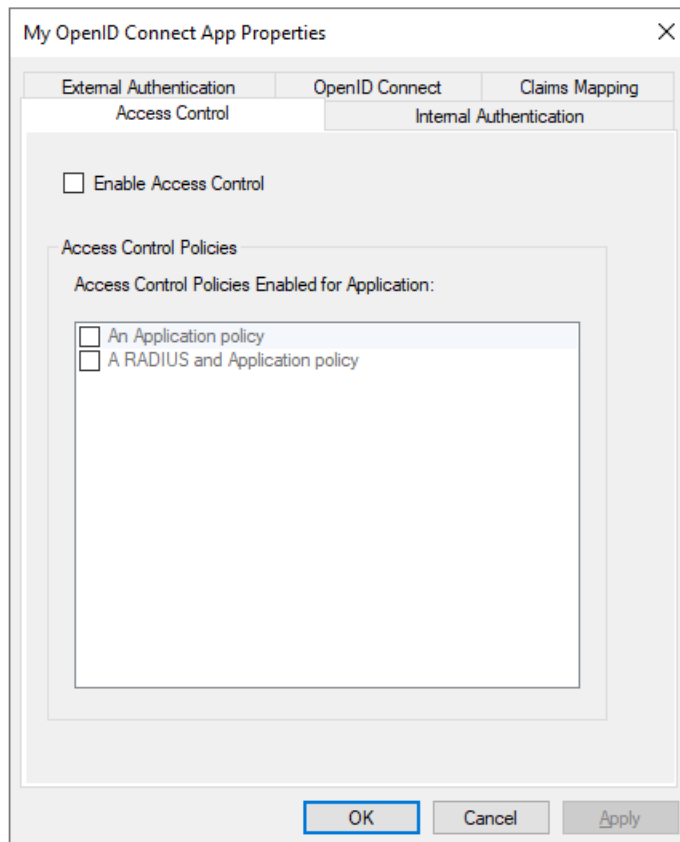
To access the application properties of an OpenID Connect application:

1. In the MyID Management Console, enter the **Applications** node.
2. Highlight your OpenID Connect application.



3. Click **Properties**, in the **Actions** pane.

5.5.5.1 Access Control tab



The **Access Control** tab allows you to apply access control policies to the current application. For each policy that you have enabled for the application, you can configure unique settings for the internal and external authentication.

Important: If you enable access control, the only policies that apply are those that are configured; if you do not configure any policies, no users can access the application.

To apply access control policies to the application:

1. On the Access Control tab, select the **Enable Access Control** option.
2. In the **Access Control Policies Enabled for Application** list, select the access control policies you want to use for the current application.

For information on creating access control policies, see section [5.11.1, Access control policies](#).

3. Click **Apply**.

Note: You must click **Apply** before changing to a different tab to ensure that you have saved the changes to the list of enabled policies.

4. On the **Internal Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.

You can configure the settings for each access control policy, so that different configurations apply to different sets of users.

5. Configure the internal authentication settings for the policy.

6. Click **Apply**.
Note: You must click **Apply** before changing to a different policy to ensure that you have saved the changes for the current policy.
7. On the **External Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.
8. Configure the external authentication settings for the policy.
9. Click **Apply**.
10. Click **OK**.

5.5.5.2 Internal Authentication tab

The screenshot shows the 'My OpenID Connect App Properties' dialog box with the 'Internal Authentication' tab selected. The 'Access Control' sub-tab is also active. A 'Policy' dropdown menu is visible. Below it, the 'Primary' section has three checkboxes: 'Password' (checked), 'Windows Authentication', and 'Certificate'. The 'Primary Options' section has two checkboxes: 'Allow password reset via Email' and 'Allow password reset via SMS/Text'. The 'Secondary' section has six checkboxes: 'Passkey', 'YubiKey OTP', 'Grid Pattern', 'Push', 'One Time Code', and 'Phrase'. The 'Secondary Options' section has two checkboxes: 'Allow deviceless' and 'Allow any selected user configured technology'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

If you have enabled access control for this application, you can select the **Policy** from the drop-down list and configure the internal authentication settings for each policy. See section [5.5.5.1, Access Control tab](#) for details.

You can specify the logon technology users must use to authenticate to the portal.

You can choose one logon technology from the options in the **Primary** section.

If only a PSM license is installed, the options are limited to **Password** and **Windows Authentication**.

New applications of this type, by default, have no primary technology selected. If you are upgrading from a version earlier than 5.1.0 and **Enable Passwordless MFA** was not selected, **Password** is automatically selected as the primary logon technology.

If you select **Password**, users are required to enter a valid Active Directory password as well as their MFA credentials. If you do not select **Password**, passwordless logins are enabled.

If you select **Windows Authentication** or **Certificate**, the **Primary Options**, **Secondary**, and **Secondary Options** sections are disabled, as these technologies do not require further configuration.

Note: If you select **Windows Authentication**, you must configure IIS to use Windows Authentication – this disables multi-factor authentication for this application. If you enable Windows Authentication in the MyID Management Console without configuring Windows Authentication in IIS, the user is shown the standard Windows prompt to enter their Username and Password.

Similarly, if you select **Certificate** authentication, you must configure IIS to handle the certificate, at which point all other MFA options are no longer valid for this application, and you cannot select them in the MyID Management Console.

You can choose as many or as few **Secondary** logon technologies as you want.

If you select only one secondary option, the user must have that logon technology.

If you select multiple secondary options, the type of technology used is determined after the user has entered their account name and, if required, password. The type of logon technology used is determined based on the selected options and which technologies the user has configured. The priority order for the secondary logon technologies is:

- **Passkey**
- **Grid Pattern** (if **Allow deviceless** is not selected)
- **Push**
- **YubiKey OTP**
- **One Time Code**
- **Phrase** (if **Allow deviceless** is not selected)
- **Grid Pattern** (if **Allow deviceless** is selected)
- **Phrase** (if **Allow deviceless** is selected)

If **Password** is selected as the primary logon technology, and no secondary logon technology is selected, the user requires only a password to log in.

If a user does not have access to any of the secondary logon technologies selected, they cannot log in to the application, unless all of the following are true:

- No primary logon technology is selected.
- All secondary logon technologies selected require devices.
- The user has no device registered.

In that case, fallback password authentication occurs, and the user can log in with just their username and password.

If no logon technologies are selected, no-one can log in.

If the user has a device registered, the technologies that require a device (**Passkey**, and, if **Allow deviceless** is not selected, **Grid Pattern** and **Phrase**) can be selected, whether or not the device is enabled.

For example, if a user has a FIDO token registered but the device has been disabled, the user is still prompted to authenticate with their FIDO token. This is so that temporarily displaced devices do not allow users to fall back on lesser authentication methods.

If a user temporarily loses their FIDO device, you can give them a temporary access code – by default, this only lasts 24 hours or three logons, whichever comes first. For information on changing temporary access code limitations, see section [5.3.1, General tab](#). If the user finds their FIDO token, you can re-enable it, and if they cannot find it, you can remove the device from their account and issue a new one. For information on assigning temporary access codes, see section [5.9.8, Assigning temporary access codes to a user](#) or the *Assigning a temporary access code to a user* section of the [Web Management Portal User Guide](#).

If you select the **Allow any selected user configured technology** option, users are allowed to authenticate using any MFA technology for which they are provisioned. If this option is not selected, the user can enter only the valid authentication credentials that are shown by the application.

Grid Pattern and Phrase authentication technologies both support deviceless authentication; select the **Allow Deviceless** option to enable this support. If this is selected, you cannot use these technologies with a device, which is less secure. If this is not selected, then multi-factor authentication is always required.

5.5.5.3 External Authentication tab

My OpenID Connect App Properties

Access Control Internal Authentication

External Authentication OpenID Connect Claims Mapping

Policy

External Authentication

External Identities linked with this Application:

OK Cancel Apply

If you have enabled access control for this application, you can select the **Policy** from the drop-down list and configure the external authentication settings for each policy. See section [5.5.5.1, Access Control tab](#) for details.

The **External Identities linked with this application** option allows users to authenticate to the website or service using a preconfigured external identity provider; for information on adding an external identity, see section [5.7, Adding External Identities](#).

5.5.5.4 OpenID Connect tab

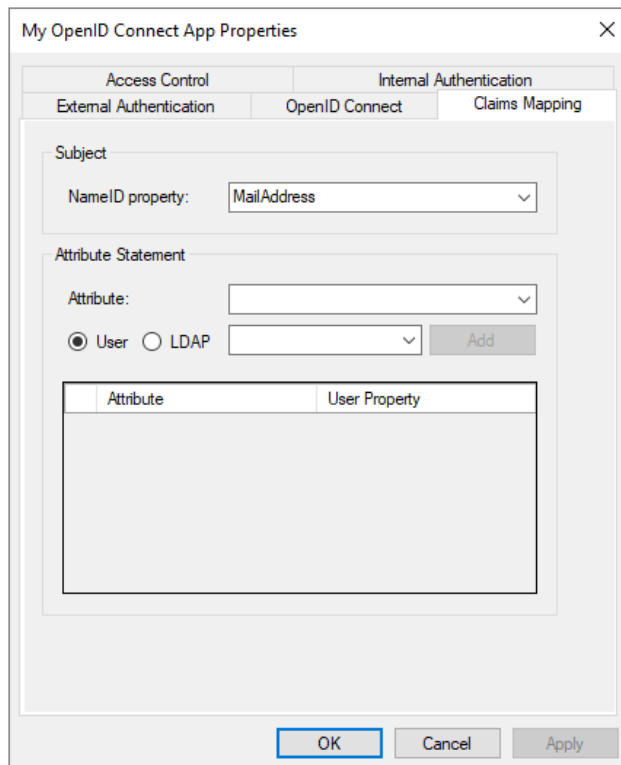
The OpenID Connect tab details the IdP Server and Relying Party trust settings.

The screenshot shows a dialog box titled "My OpenID Connect App Properties" with a close button (X) in the top right corner. The dialog has three tabs: "Access Control", "Internal Authentication", and "Claims Mapping". The "OpenID Connect" tab is selected. Under the "Identity Provider (IdP)" section, there is a "Client ID" field with the value "MyOpenIDConnectApp" and a "Client Secret" field with a masked password (dots). Under the "Relying Party (RP)" section, there is a "Grant Type" dropdown menu set to "Code", a "Scopes" section with checkboxes for "profile" (checked), "email", and "phone", a "Redirect URI" field with the value "https://myapp.server.com/redirecturi", and a "Logout URI" field with the value "https://myapp.server.com/logout". At the bottom of the dialog are "OK", "Cancel", and "Apply" buttons.

Through this, you can change the OpenID Connect application's **Client Secret**.

You can also specify the OpenID Connect application's **Grant Type**, the **Scopes** for the relying party trust, the **Redirect URI**, and the **Logout URI**.

5.5.5.5 Claims Mapping tab



The dialog box is titled "My OpenID Connect App Properties" and has a close button (X) in the top right corner. It contains three tabs: "Access Control", "OpenID Connect", and "Claims Mapping". The "Claims Mapping" tab is selected. Inside the tab, there are two main sections: "Subject" and "Attribute Statement".

Subject Section:

NameID property: MailAddress (dropdown menu)

Attribute Statement Section:

Attribute: (dropdown menu)

☒ User ☐ LDAP (dropdown menu) [Add button]

Below the Attribute Statement section is a table with two columns: "Attribute" and "User Property". The table is currently empty.

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

The **NameID** is mapped during the application creation.

You can add any other claims required by the application on this tab.

To add a claims sample mapping:

1. Select an **Attribute** from the list, or type in a value for a custom attribute.

My OpenID Connect App Properties

Access Control Internal Authentication

External Authentication OpenID Connect Claims Mapping

Subject

NameID property: MailAddress

Attribute Statement

Attribute:

☒ User ☐ LDAP

Attribute
Actor
Anonymous
Authentication
AuthenticationInstant
AuthenticationMethod
AuthorizationDecision
CookiePath
Country
DateOfBirth
DenyOnlyPrimaryGroupSid
DenyOnlyPrimarySid
DenyOnlySid
DenyOnlyWindowsDeviceGroup
Dns
Dsa
Email
Expiration
Expired
Gender
GivenName
GroupSid
Hash
HomePhone
IsPersistent
Locality
MobilePhone
Name
NameIdentifier
OtherPhone
PostalCode

Apply

2. Select either a **User** property or an **LDAP** field to which you want to map the attribute.

My OpenID Connect App Properties

Access Control Internal Authentication

External Authentication OpenID Connect Claims Mapping

Subject

NameID property: MailAddress

Attribute Statement

Attribute: Surname

☒ User ☐ LDAP

Attribute

- AccountGuid
- AccountName
- Description
- DomainDns
- ExternalUser
- FirstName
- Groups
- LastName
- MailAddress
- MailAddress2
- MobileNumber
- Realm
- UPN
- ValidFrom
- ValidTo

OK Cancel Apply

3. Click **Add**.

The mapping configuration is now complete and is visible in the list.

My OpenID Connect App Properties

Access Control Internal Authentication

External Authentication OpenID Connect Claims Mapping

Subject

NameID property: MailAddress

Attribute Statement

Attribute:

☒ User ☐ LDAP Add

Attribute	User Property
<input checked="" type="checkbox"/> Surname	LastName

OK Cancel Apply

You can add multiple claim mappings to a single application.

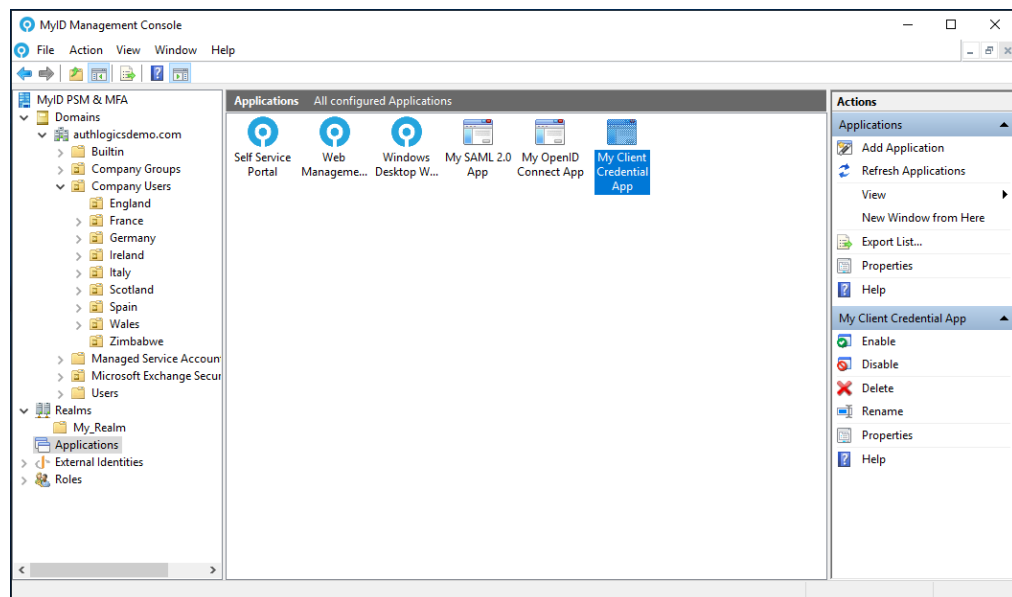
To disable a mapping, deselect it in the list.

5.5.6 Client Credential applications properties

The applications properties dialog of a client credential application allows administrators to control the client credential application. For more information on adding a client credential application, see section [5.6.2, *Creating a client credential application*](#).

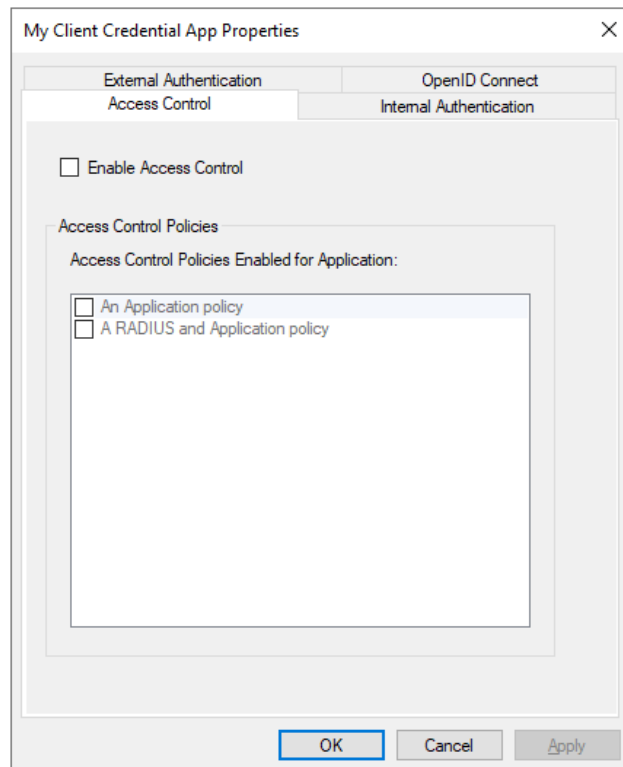
To access the application properties of an client credential application:

1. In the MyID Management Console, enter the **Applications** node.
2. Highlight your client credential application.



3. Click **Properties**, in the **Actions** pane.

5.5.6.1 Access Control tab



The **Access Control** tab allows you to apply access control policies to the current application. For each policy that you have enabled for the application, you can configure unique settings for the internal and external authentication.

Important: If you enable access control, the only policies that apply are those that are configured; if you do not configure any policies, no users can access the application.

To apply access control policies to the application:

1. On the **Access Control** tab, select the **Enable Access Control** option.
2. In the **Access Control Policies Enabled for Application** list, select the access control policies you want to use for the current application.

For information on creating access control policies, see section [5.11.1, Access control policies](#).

3. Click **Apply**.

Note: You must click **Apply** before changing to a different tab to ensure that you have saved the changes to the list of enabled policies.

4. On the **Internal Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.

You can configure the settings for each access control policy, so that different configurations apply to different sets of users.

5. Configure the internal authentication settings for the policy.
6. Click **Apply**.

Note: You must click **Apply** before changing to a different policy to ensure that you have saved the changes for the current policy.

7. On the **External Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.
8. Configure the external authentication settings for the policy.
9. Click **Apply**.
10. Click **OK**.

5.5.6.2 Internal Authentication tab

The screenshot shows the 'My Client Credential App Properties' dialog box with the 'Internal Authentication' tab selected. The 'Access Control' sub-tab is also active. A 'Policy' dropdown menu is visible. Below it, the 'Primary' section contains three checkboxes: 'Password', 'Windows Authentication', and 'Certificate'. The 'Primary Options' section contains two checkboxes: 'Allow password reset via Email' and 'Allow password reset via SMS/Text'. The 'Secondary' section contains six checkboxes: 'Passkey', 'YubiKey OTP', 'Grid Pattern', 'Push', 'One Time Code', and 'Phrase'. The 'Secondary Options' section contains two checkboxes: 'Allow deviceless' and 'Allow any selected user configured technology'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

If you have enabled access control for this application, you can select the **Policy** from the drop-down list and configure the internal authentication settings for each policy. See section [5.5.6.1, Access Control tab](#) for details.

Note: Authentication configuration is irrelevant for client credential applications.

You can specify the logon technology users must use to authenticate to the portal.

You can choose one logon technology from the options in the **Primary** section.

If only a PSM license is installed, the options are limited to **Password** and **Windows Authentication**.

New applications of this type, by default, have no primary technology selected. If you are upgrading from a version earlier than 5.1.0 and **Enable Passwordless MFA** was not selected, **Password** is automatically selected as the primary logon technology.

If you select **Password**, users are required to enter a valid Active Directory password as well as their MFA credentials. If you do not select **Password**, passwordless logins are enabled.

If you select **Windows Authentication** or **Certificate**, the **Primary Options**, **Secondary**, and **Secondary Options** sections are disabled, as these technologies do not require further configuration.

Note: If you select **Windows Authentication**, you must configure IIS to use Windows Authentication – this disables multi-factor authentication for this application. If you enable Windows Authentication in the MyID Management Console without configuring Windows Authentication in IIS, the user is shown the standard Windows prompt to enter their Username and Password.

Similarly, if you select **Certificate** authentication, you must configure IIS to handle the certificate, at which point all other MFA options are no longer valid for this application, and you cannot select them in the MyID Management Console.

You can choose as many or as few **Secondary** logon technologies as you want.

If you select only one secondary option, the user must have that logon technology.

If you select multiple secondary options, the type of technology used is determined after the user has entered their account name and, if required, password. The type of logon technology used is determined based on the selected options and which technologies the user has configured. The priority order for the secondary logon technologies is:

- **Passkey**
- **Grid Pattern** (if **Allow deviceless** is not selected)
- **Push**
- **YubiKey OTP**
- **One Time Code**
- **Phrase** (if **Allow deviceless** is not selected)
- **Grid Pattern** (if **Allow deviceless** is selected)
- **Phrase** (if **Allow deviceless** is selected)

If **Password** is selected as the primary logon technology, and no secondary logon technology is selected, the user requires only a password to log in.

If a user does not have access to any of the secondary logon technologies selected, they cannot log in to the application, unless all of the following are true:

- No primary logon technology is selected.
- All secondary logon technologies selected require devices.
- The user has no device registered.

In that case, fallback password authentication occurs, and the user can log in with just their username and password.

If no logon technologies are selected, no-one can log in.

If the user has a device registered, the technologies that require a device (**Passkey**, and, if **Allow deviceless** is not selected, **Grid Pattern** and **Phrase**) can be selected, whether or not the device is enabled.

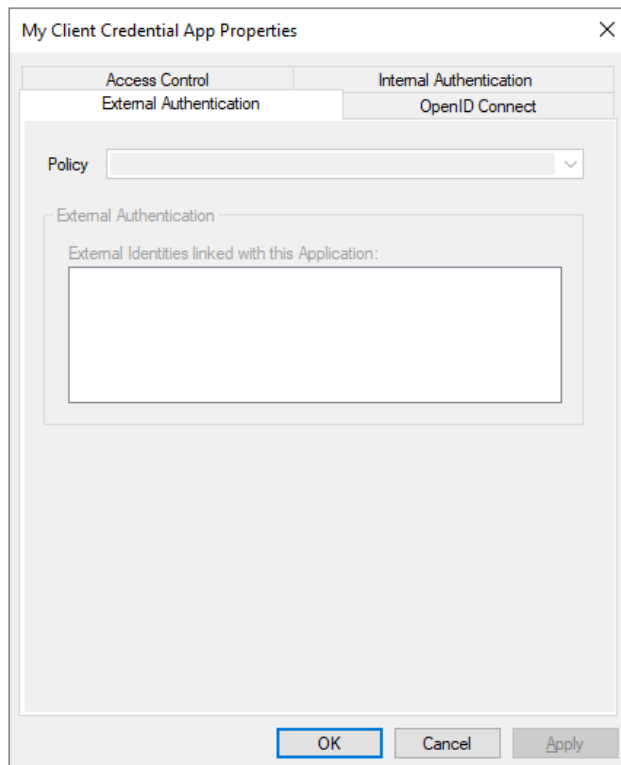
For example, if a user has a FIDO token registered but the device has been disabled, the user is still prompted to authenticate with their FIDO token. This is so that temporarily displaced devices do not allow users to fall back on lesser authentication methods.

If a user temporarily loses their FIDO device, you can give them a temporary access code – by default, this only lasts 24 hours or three logons, whichever comes first. For information on changing temporary access code limitations, see section [5.3.1, General tab](#). If the user finds their FIDO token, you can re-enable it, and if they cannot find it, you can remove the device from their account and issue a new one. For information on assigning temporary access codes, see section [5.9.8, Assigning temporary access codes to a user](#) or the *Assigning a temporary access code to a user* section of the [Web Management Portal User Guide](#).

If you select the **Allow any selected user configured technology** option, users are allowed to authenticate using any MFA technology for which they are provisioned. If this option is not selected, the user can enter only the valid authentication credentials that are shown by the application.

Grid Pattern and Phrase authentication technologies both support deviceless authentication; select the **Allow Deviceless** option to enable this support. If this is selected, you cannot use these technologies with a device, which is less secure. If this is not selected, then multi-factor authentication is always required.

5.5.6.3 External Authentication tab



The screenshot shows a dialog box titled "My Client Credential App Properties" with a close button (X) in the top right corner. The dialog has two tabs: "Access Control" and "Internal Authentication". The "Access Control" tab is selected, and within it, the "External Authentication" sub-tab is active. Below the tabs, there is a "Policy" dropdown menu. Underneath the dropdown, there is a section titled "External Authentication" which contains a label "External Identities linked with this Application:" followed by an empty rectangular box. At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Apply".

If you have enabled access control for this application, you can select the **Policy** from the drop-down list and configure the external authentication settings for each policy. See section [5.5.6.1, Access Control tab](#) for details.

Note: Authentication configuration is irrelevant for client credential applications.

5.5.6.4 OpenID Connect tab

The OpenID Connect tab details the IdP Server and Relying Party trust settings.

The screenshot shows a dialog box titled "My Client Credential App Properties" with a close button (X) in the top right corner. The dialog has two tabs: "External Authentication" and "OpenID Connect", with the latter being selected. The "OpenID Connect" tab contains two main sections: "Identity Provider (IdP)" and "Relying Party (RP)".

Identity Provider (IdP) section:

- Client ID:** A text field containing "MyClientCredentialApp".
- Client Secret:** A text field filled with 20 dots, indicating a masked secret.

Relying Party (RP) section:

- Grant Type:** A dropdown menu set to "Client Credential".
- Scopes:** A list box with two items: "rest_api" (checked with a checkbox) and "rest_api_external" (unchecked).
- Roles:** A dropdown menu set to "Administrator".

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

Through this, you can change the client credential application's **Client Secret**.

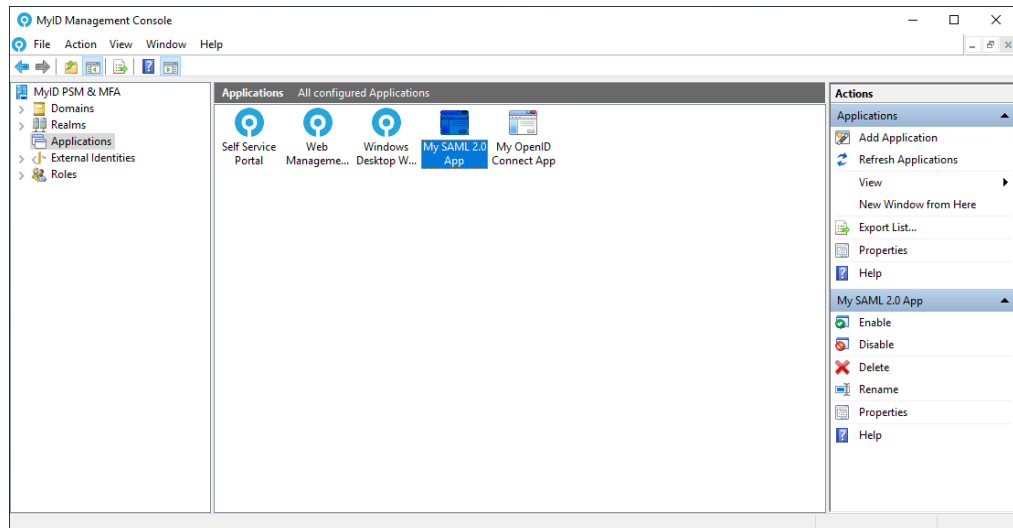
You can also specify the client credential application's **Grant Type**, the **Scopes** for the relying party trust, and the **Roles**.

5.5.7 SAML 2.0 application properties

The applications properties dialog of a SAML 2.0 application allows administrators to control the SAML 2.0 application. For more information on adding a SAML 2.0 application, see section [5.6.3, *Creating a SAML 2.0 application*](#).

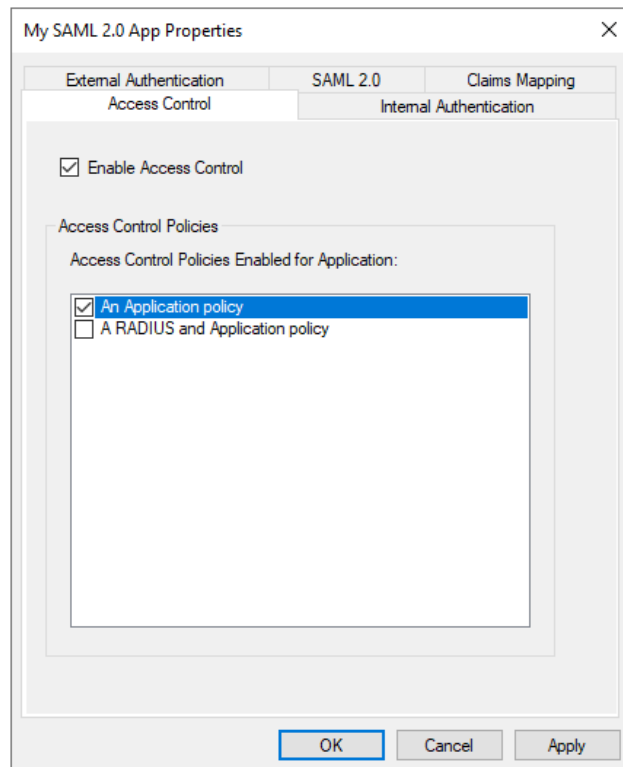
To access the application properties of a SAML 2.0 application:

1. In the MyID Management Console, enter the **Applications** node.
2. Highlight your SAML 2.0 application.



3. Click **Properties**, in the **Actions** pane.

5.5.7.1 Access Control tab



The **Access Control** tab allows you to apply access control policies to the current application. For each policy that you have enabled for the application, you can configure unique settings for the internal and external authentication.

Important: If you enable access control, the only policies that apply are those that are configured; if you do not configure any policies, no users can access the application.

To apply access control policies to the application:

1. On the **Access Control** tab, select the **Enable Access Control** option.
2. In the **Access Control Policies Enabled for Application** list, select the access control policies you want to use for the current application.

For information on creating access control policies, see section [5.11.1, Access control policies](#).

3. Click **Apply**.

Note: You must click **Apply** before changing to a different tab to ensure that you have saved the changes to the list of enabled policies.

4. On the **Internal Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.

You can configure the settings for each access control policy, so that different configurations apply to different sets of users.

5. Configure the internal authentication settings for the policy.
6. Click **Apply**.

Note: You must click **Apply** before changing to a different policy to ensure that you have saved the changes for the current policy.

7. On the **External Authentication** tab, from the **Policy** drop-down list, select the access control policy you want to configure.
8. Configure the external authentication settings for the policy.
9. Click **Apply**.
10. Click **OK**.

5.5.7.2 Internal Authentication tab

The screenshot shows the 'My SAML 2.0 App Properties' dialog box with the 'Internal Authentication' tab selected. The 'Policy' dropdown is set to 'An Application policy'. Under 'Primary', 'Password' is selected. Under 'Primary Options', 'Allow password reset via Email' and 'Allow password reset via SMS/Text' are both selected. Under 'Secondary', 'Passkey', 'YubiKey OTP', 'Grid Pattern', 'Push', 'One Time Code', and 'Phrase' are all unselected. Under 'Secondary Options', 'Allow deviceless' and 'Allow any selected user configured technology' are both unselected. The 'OK' button is highlighted.

External Authentication	SAML 2.0	Claims Mapping
Access Control	Internal Authentication	

Policy: An Application policy

Primary

☒ Password ☐ Windows Authentication ☐ Certificate

Primary Options

☒ Allow password reset via Email ☒ Allow password reset via SMS/Text

Secondary

☐ Passkey ☐ YubiKey OTP ☐ Grid Pattern
☐ Push ☐ One Time Code ☐ Phrase

Secondary Options

☐ Allow deviceless ☐ Allow any selected user configured technology

OK Cancel Apply

If you have enabled access control for this application, you can select the **Policy** from the drop-down list and configure the internal authentication settings for each policy. See [section 5.5.7.1, *Access Control tab*](#) for details.

You can specify the logon technology users must use to authenticate to the portal.

You can choose one logon technology from the options in the **Primary** section.

If only a PSM license is installed, the options are limited to **Password** and **Windows Authentication**.

New applications of this type, by default, have no primary technology selected. If you are upgrading from a version earlier than 5.1.0 and **Enable Passwordless MFA** was not selected, **Password** is automatically selected as the primary logon technology.

If you select **Password**, users are required to enter a valid Active Directory password as well as their MFA credentials. If you do not select **Password**, passwordless logins are enabled.

If you select **Windows Authentication** or **Certificate**, the **Primary Options**, **Secondary**, and **Secondary Options** sections are disabled, as these technologies do not require further configuration.

Note: If you select **Windows Authentication**, you must configure IIS to use Windows Authentication – this disables multi-factor authentication for this application. If you enable Windows Authentication in the MyID Management Console without configuring Windows Authentication in IIS, the user is shown the standard Windows prompt to enter their Username and Password.

Similarly, if you select **Certificate** authentication, you must configure IIS to handle the certificate, at which point all other MFA options are no longer valid for this application, and you cannot select them in the MyID Management Console.

You can choose as many or as few **Secondary** logon technologies as you want.

If you select only one secondary option, the user must have that logon technology.

If you select multiple secondary options, the type of technology used is determined after the user has entered their account name and, if required, password. The type of logon technology used is determined based on the selected options and which technologies the user has configured. The priority order for the secondary logon technologies is:

- **Passkey**
- **Grid Pattern** (if **Allow deviceless** is not selected)
- **Push**
- **YubiKey OTP**
- **One Time Code**
- **Phrase** (if **Allow deviceless** is not selected)
- **Grid Pattern** (if **Allow deviceless** is selected)
- **Phrase** (if **Allow deviceless** is selected)

If **Password** is selected as the primary logon technology, and no secondary logon technology is selected, the user requires only a password to log in.

If a user does not have access to any of the secondary logon technologies selected, they cannot log in to the application, unless all of the following are true:

- No primary logon technology is selected.
- All secondary logon technologies selected require devices.
- The user has no device registered.

In that case, fallback password authentication occurs, and the user can log in with just their username and password.

If no logon technologies are selected, no-one can log in.

If the user has a device registered, the technologies that require a device (**Passkey**, and, if **Allow deviceless** is not selected, **Grid Pattern** and **Phrase**) can be selected, whether or not the device is enabled.

For example, if a user has a FIDO token registered but the device has been disabled, the user is still prompted to authenticate with their FIDO token. This is so that temporarily displaced devices do not allow users to fall back on lesser authentication methods.

If a user temporarily loses their FIDO device, you can give them a temporary access code – by default, this only lasts 24 hours or three logons, whichever comes first. For information on changing temporary access code limitations, see section [5.3.1, General tab](#). If the user finds their FIDO token, you can re-enable it, and if they cannot find it, you can remove the device from their account and issue a new one. For information on assigning temporary access codes, see section [5.9.8, Assigning temporary access codes to a user](#) or the *Assigning a temporary access code to a user* section of the [Web Management Portal User Guide](#).

If you select the **Allow any selected user configured technology** option, users are allowed to authenticate using any MFA technology for which they are provisioned. If this option is not selected, the user can enter only the valid authentication credentials that are shown by the application.

Grid Pattern and Phrase authentication technologies both support deviceless authentication; select the **Allow Deviceless** option to enable this support. If this is selected, you cannot use these technologies with a device, which is less secure. If this is not selected, then multi-factor authentication is always required.

5.5.7.3 External Authentication

My SAML 2.0 App Properties

Access Control Internal Authentication

External Authentication SAML 2.0 Claims Mapping

Policy An Application policy

External Authentication

External Identities linked with this Application:

OK Cancel Apply

If you have enabled access control for this application, you can select the **Policy** from the drop-down list and configure the external authentication settings for each policy. See section [5.5.7.1, Access Control tab](#) for details.

The **External Identities linked with this application** option allows users to authenticate to the website or service using a preconfigured external identity provider; for information on adding an external identity, see section [5.7, Adding External Identities](#).

5.5.7.4 SAML 2.0 tab

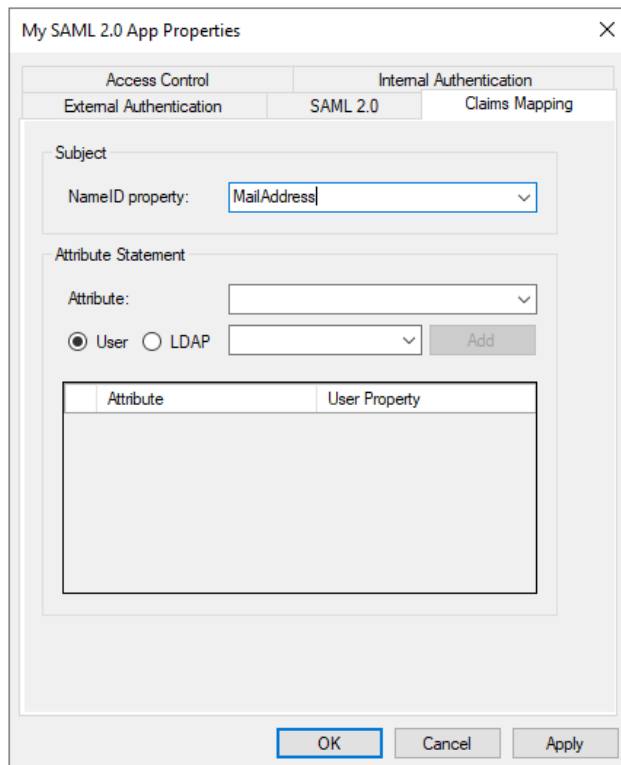
The screenshot shows a dialog box titled "My SAML 2.0 App Properties" with a close button (X) in the top right corner. The dialog has three tabs: "Access Control", "Internal Authentication", and "Claims Mapping". The "SAML 2.0" tab is selected. Inside the dialog, there is a section for "Service Provider (SP)" with the following fields and options:

- Description: [Empty text box]
- Entity ID URI: [/oadbalancer-9.siroe.com]
- Assertion URL: [https://loadbalancer-9.siroe.com:3443/federation]
- Logout URL: [https://loadbalancer-9.siroe.com:3443/federation]
- Artifact URL: [Empty text box]
- NameID Format: [um:oasis:names:tc:SAML:1.1:nameid-format:u] (dropdown)
- Authn Context: [um:oasis:names:tc:SAML:2.0:ac:classes:unsr] (dropdown)
- SP Certificates: [Empty dropdown menu]
- Buttons: Add, Remove, Cert Info
- Checkboxes:
 - ☐ Want Signed Auth Request
 - ☐ Want Signed Logout Request
 - ☐ Sign Assertion to SP
 - ☐ Sign Logout Response to SP

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

The SAML 2.0 tab allows you to change the SAML settings of the application after you have created the application. The options are the same as when you create the application, except that you cannot import a metadata file; see section [5.6.3, Creating a SAML 2.0 application](#) for details. of these options.

5.5.7.5 Claims Mapping tab



The dialog box is titled "My SAML 2.0 App Properties" and has a close button (X) in the top right corner. It contains three tabs: "Access Control", "Internal Authentication", and "Claims Mapping". The "Claims Mapping" tab is selected. Under the "Subject" section, there is a "NameID property:" label and a dropdown menu showing "MailAddress". Under the "Attribute Statement" section, there is an "Attribute:" label and a dropdown menu. Below this, there are two radio buttons: "User" (selected) and "LDAP". To the right of the "LDAP" radio button is another dropdown menu and an "Add" button. At the bottom of the dialog are three buttons: "OK", "Cancel", and "Apply".

The **NameID** is mapped during the application creation.

You can add any other claims required by the application on this tab.

To add a claims sample mapping:

1. Select an **Attribute** from the list or type in a value for a custom attribute.

My SAML 2.0 App Properties

Access Control Internal Authentication

External Authentication SAML 2.0 Claims Mapping

Subject

NameID property: MailAddress

Attribute Statement

Attribute:

☒ User ☐ LDAP

Attribute
Actor
Anonymous
Authentication
AuthenticationInstant
AuthenticationMethod
AuthorizationDecision
CookiePath
Country
DateOfBirth
DenyOnlyPrimaryGroupSid
DenyOnlyPrimarySid
DenyOnlySid
DenyOnlyWindowsDeviceGroup
Dns
Dsa
Email
Expiration
Expired
Gender
GivenName
GroupSid
Hash
HomePhone
IsPersistent
Locality
MobilePhone
Name
NameIdentifier
OtherPhone
PostalCode

Apply

2. Select either a user property or an LDAP field to which you want to map the attribute.

My SAML 2.0 App Properties

Access Control Internal Authentication

External Authentication SAML 2.0 Claims Mapping

Subject

NameID property: MailAddress

Attribute Statement

Attribute: Surname

☒ User ☐ LDAP

Attribute

- AccountGuid
- AccountName
- Description
- DomainDns
- ExternalUser
- FirstName
- Groups
- LastName
- MailAddress
- MailAddress2
- MobileNumber
- Realm
- UPN
- ValidFrom
- ValidTo

OK Cancel Apply

My SAML 2.0 App Properties

Access Control Internal Authentication

External Authentication SAML 2.0 Claims Mapping

Subject

NameID property: MailAddress

Attribute Statement

Attribute: Surname

☒ User ☐ LDAP

Attribute

Add

Attribute	User Property
-----------	---------------

OK Cancel Apply

3. Click **Add**.

The mapping configuration is now complete and is visible in the list.

My SAML 2.0 App Properties

Access Control Internal Authentication

External Authentication SAML 2.0 Claims Mapping

Subject

NameID property: MailAddress

Attribute Statement

Attribute:

☒ User ☐ LDAP Add

Attribute	User Property
<input checked="" type="checkbox"/> Surname	LastName

OK Cancel Apply

You can add multiple claim mappings to a single application.

To disable a mapping, deselect it in the list.

To test the IdP SAML configuration, you can use the following demo site:

sptest.iamshowcase.com

The site displays the information received through SAML attributes. The site does not support testing of SAML signing.

5.5.8 Accessing applications through the IdP page

You can access your applications through the IdP landing page in your browser:

1. In your browser, navigate to the IdP page.

For example:

`https://myserver.example.com:14443/idp`

2. To filter the list of applications, type the name of the application you want to find in the search box.
3. Click **Login** to log in using the most appropriate technology based on your configuration and the applications to which you have access.

The screen displays the applications to which you have access.

See section [5.11.1, Access control policies](#) for details of setting up access control policies to use for your applications.

4. Once you have authenticated, you can click the link to each application, which opens in a new browser tab.

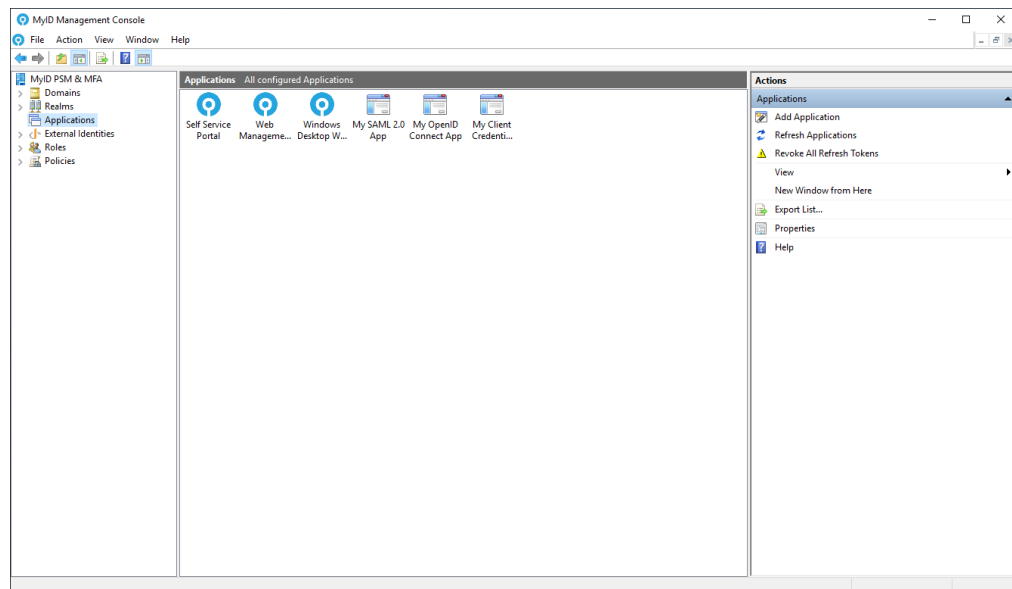
In most cases, you are authenticated with Single Sign On so no additional authentication is required.

Note: If you have an application that requires Push, but you have not yet registered your mobile device, it selects another authentication method. The application that requires Push must authenticate again once you have registered your mobile device.

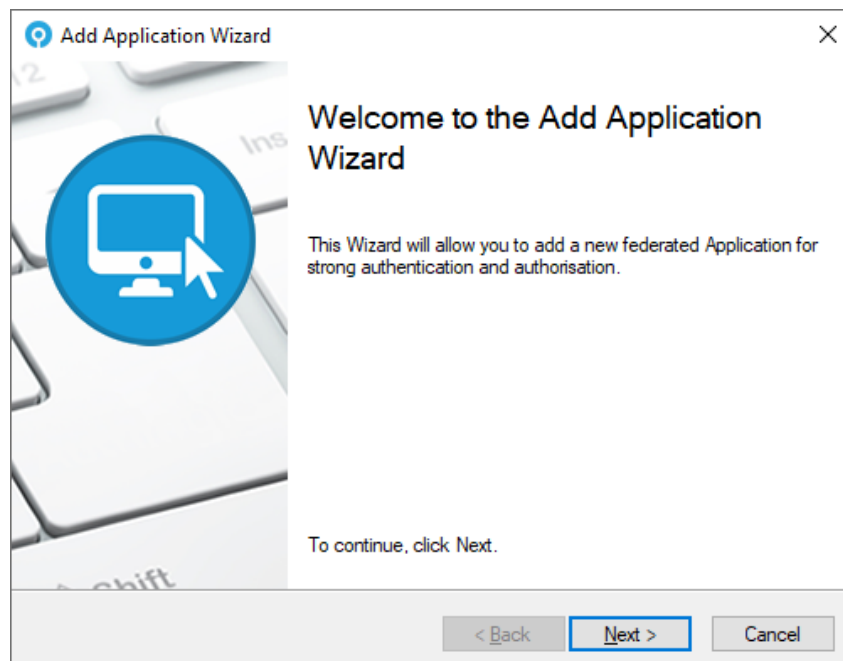
5.6 Adding new applications

Additional websites and services can be added to the IdP Applications. To add a new application:

1. In the MyID Management Console, highlight the **Applications** node.



2. Click **Add Application**, in the **Actions** pane.



3. Click **Next**.
4. Select the **App Type**, provide a descriptive **Name** for the application, and set the application to be **Enabled**.

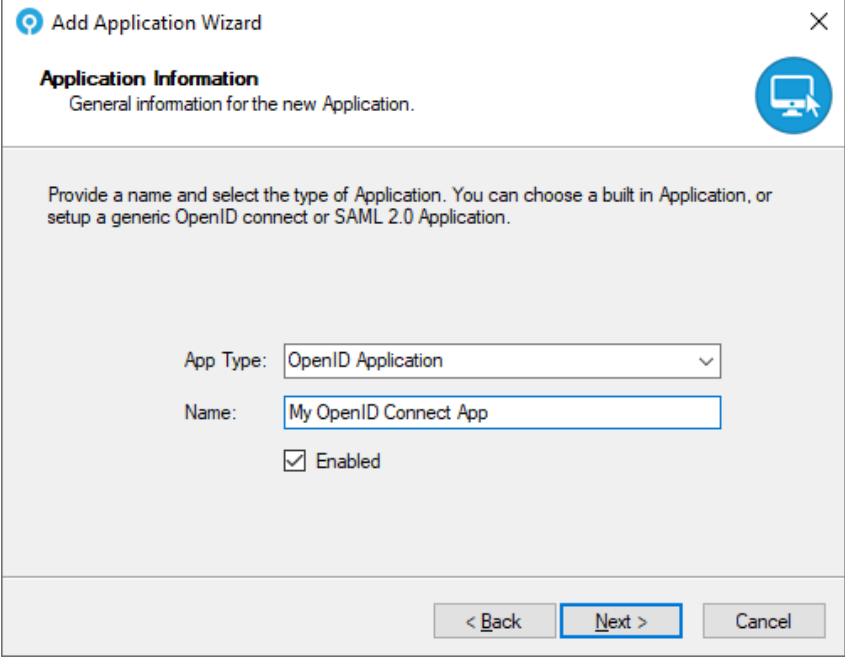
MyID Applications support applications of type:

- OpenID Applications .
See section [5.6.1, Creating an OpenID Connect application.](#)
- Client credential applications.
See section [5.6.2, Creating a client credential application.](#)
- SAML 2.0 Applications.
See section [5.6.3, Creating a SAML 2.0 application.](#)
- MyID CMS.
- Microsoft 365.

For more information on adding a Microsoft 365 application, see the *Adding the Microsoft 365 application* section of the [Federation with Microsoft 365](#) guide.

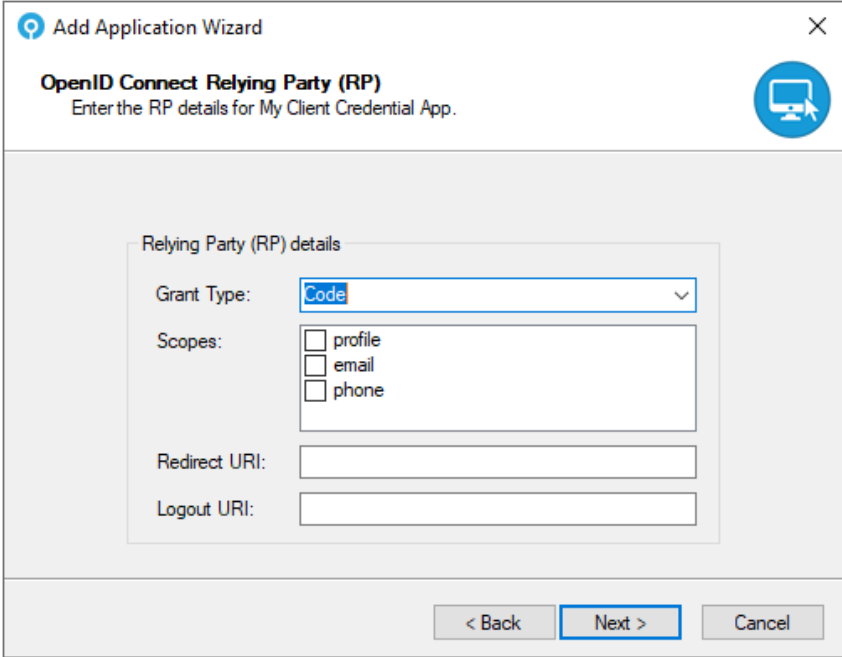
Follow the relevant instructions for the type of application that you want to add.

5.6.1 Creating an OpenID Connect application



The screenshot shows the 'Add Application Wizard' window, specifically the 'Application Information' step. The title bar says 'Add Application Wizard' with a close button. Below the title bar, there's a sub-header 'Application Information' and a description 'General information for the new Application.' To the right of the description is a blue circular icon with a computer monitor and a cursor. The main area contains instructions: 'Provide a name and select the type of Application. You can choose a built in Application, or setup a generic OpenID connect or SAML 2.0 Application.' Below this, there are three input fields: 'App Type' is a dropdown menu set to 'OpenID Application'; 'Name' is a text box containing 'My OpenID Connect App'; and 'Enabled' is a checked checkbox. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

1. Click **Next**.
2. Set the **Grant Type** to **Code**.



The screenshot shows the 'Add Application Wizard' window, specifically the 'OpenID Connect Relying Party (RP)' step. The title bar says 'Add Application Wizard' with a close button. Below the title bar, there's a sub-header 'OpenID Connect Relying Party (RP)' and a description 'Enter the RP details for My Client Credential App.' To the right of the description is a blue circular icon with a computer monitor and a cursor. The main area contains a section titled 'Relying Party (RP) details' which includes four input fields: 'Grant Type' is a dropdown menu set to 'Code'; 'Scopes' is a list of checkboxes for 'profile', 'email', and 'phone', all of which are unchecked; 'Redirect URI' is a text box; and 'Logout URI' is a text box. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

3. Enter the Relying Party trust details.

Add Application Wizard

OpenID Connect Relying Party (RP)
Enter the RP details for My SAML 2.0 App.

Relying Party (RP) details

Grant Type:

Scopes: ☒ profile ☐ email ☐ phone

Redirect URI:

Logout URI:

< Back **Next >** Cancel

4. Click **Next**.

Add Application Wizard

Authentication Options
Select the required authentication options.

Primary

☐ Password ☐ Windows Authentication ☐ Certificate

Primary Options

☐ Allow password reset via Email ☐ Allow password reset via SMS/Text

Secondary

☐ Passkey ☐ YubiKey OTP ☐ Grid Pattern

☐ Push ☐ One Time Code ☐ Phrase

Secondary Options

☐ Allow deviceless ☐ Allow any selected user configured technology

< Back **Next >** Cancel

5. You can specify the logon technology users must use to authenticate to the portal.

You can choose one logon technology from the options in the **Primary** section.

If only a PSM license is installed, the options are limited to **Password** and **Windows Authentication**.

New applications of this type, by default, have no primary technology selected.

If you select **Password**, users are required to enter a valid Active Directory password as well as their MFA credentials. If you do not select **Password**, passwordless logins are enabled.

If you select **Windows Authentication** or **Certificate**, the **Primary Options**, **Secondary**, and **Secondary Options** sections are disabled, as these technologies do not require further configuration.

Note: If you select **Windows Authentication**, you must configure IIS to use Windows Authentication – this disables multi-factor authentication for this application. If you enable Windows Authentication in the MyID Management Console without configuring Windows Authentication in IIS, the user is shown the standard Windows prompt to enter their Username and Password.

Similarly, if you select **Certificate** authentication, you must configure IIS to handle the certificate, at which point all other MFA options are no longer valid for this application, and you cannot select them in the MyID Management Console.

You can choose as many or as few **Secondary** logon technologies as you want.

If you select only one secondary option, the user must have that logon technology.

If you select multiple secondary options, the type of technology used is determined after the user has entered their account name and, if required, password. The type of logon technology used is determined based on the selected options and which technologies the user has configured. The priority order for the secondary logon technologies is:

- **Passkey**
- **Grid Pattern** (if **Allow deviceless** is not selected)
- **Push**
- **YubiKey OTP**
- **One Time Code**
- **Phrase** (if **Allow deviceless** is not selected)
- **Grid Pattern** (if **Allow deviceless** is selected)
- **Phrase** (if **Allow deviceless** is selected)

If **Password** is selected as the primary logon technology, and no secondary logon technology is selected, the user requires only a password to log in.

If a user does not have access to any of the secondary logon technologies selected, they cannot log in to the application, unless all of the following are true:

- No primary logon technology is selected.
- All secondary logon technologies selected require devices.
- The user has no device registered.

In that case, fallback password authentication occurs, and the user can log in with just their username and password.

If no logon technologies are selected, no-one can log in.

If the user has a device registered, the technologies that require a device (**Passkey**, and, if **Allow deviceless** is not selected, **Grid Pattern** and **Phrase**) can be selected, whether or not the device is enabled.

For example, if a user has a FIDO token registered but the device has been disabled, the user is still prompted to authenticate with their FIDO token. This is so that temporarily displaced devices do not allow users to fall back on lesser authentication methods.

If a user temporarily loses their FIDO device, you can give them a temporary access code – by default, this only lasts 24 hours or three logons, whichever comes first. For information on changing temporary access code limitations, see section [5.3.1, General tab](#). If the user finds their FIDO token, you can re-enable it, and if they cannot find it, you can remove the device from their account and issue a new one. For information on assigning temporary access codes, see section [5.9.8, Assigning temporary access codes to a user](#) or the *Assigning a temporary access code to a user* section of the [Web Management Portal User Guide](#).

If you select the **Allow any selected user configured technology** option, users are allowed to authenticate using any MFA technology for which they are provisioned. If this option is not selected, the user can enter only the valid authentication credentials that are shown by the application.

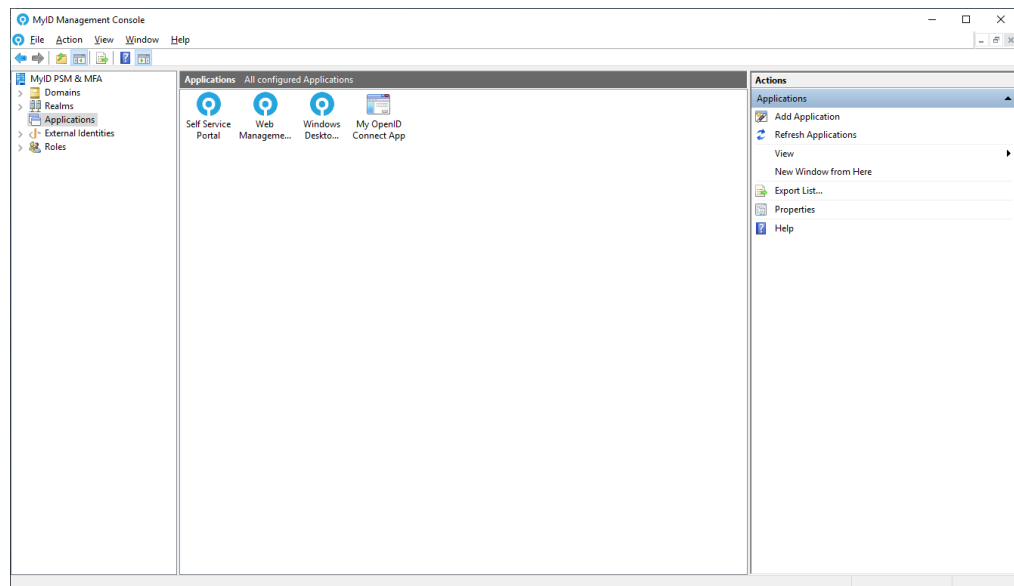
Grid Pattern and Phrase authentication technologies both support deviceless authentication; select the **Allow Deviceless** option to enable this support. If this is selected, you cannot use these technologies with a device, which is less secure. If this is not selected, then multi-factor authentication is always required.

6. Click **Next**.

The screenshot shows the 'Add Application Wizard' dialog box. The title bar says 'Add Application Wizard'. The main heading is 'Apply the configuration?' with the subtext 'Are you ready to apply the settings?'. Below this, it states: 'The Add Application Wizard has gathered all the information required to add the new My OpenID Connect App Application. Click Next to apply the configuration changes.' There is a section titled 'OpenID Connect Summary' containing two text boxes: 'Client ID:' with the value 'MyOpenIDConnectApp' and 'Client Secret:' with the value 'os9SDdp98MOykxBeBzCvsW9Tkt3b57vat'. A red warning message below the secret box says: 'Important: Make a copy of the Client Secret now as it will not be made available again after the wizard is complete.' At the bottom, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

7. Optionally, you can type a new **Client ID**.
8. Make a copy of the **Client Secret** for integration with the calling application.
This is necessary for later authentication and is not available outside of this page. If you lose this, you can edit the application to change the **Client Secret**. See section [5.5.5.4, OpenID Connect tab](#).
9. Click **Next**.

The screenshot shows the 'Add Application Wizard' dialog box. The title bar says 'Add Application Wizard'. The main heading is 'Add Application Configuration' with the subtext 'Authentication Server is updating the Application data.' Below this, there is a section titled 'Update Progress...' containing a text box with the text 'Adding new Application... Done'. At the bottom, there are three buttons: '< Back', 'Finish' (which is highlighted with a blue border), and 'Cancel'.

10. Click **Finish**.

Your application has now been configured.

5.6.2 Creating a client credential application

A screenshot of the 'Add Application Wizard' dialog box. The title bar says 'Add Application Wizard' with a close button. The main heading is 'Application Information' with a subtitle 'General information for the new Application.' and a blue icon of a computer with a user. The text says: 'Provide a name and select the type of Application. You can choose a built in Application, or setup a generic OpenID connect or SAML 2.0 Application.' Below this are two fields: 'App Type:' with a dropdown menu showing 'OpenID Application', and 'Display Name:' with a text box containing 'My Client Credential App'. There is a checked checkbox labeled 'Enabled'. At the bottom are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

1. Click **Next**.
2. Set the Grant Type to **Client Credential**.

Add Application Wizard

OpenID Connect Relying Party (RP)
Enter the RP details for My Client Credential App.

Relying Party (RP) details

Grant Type: Client Credential

Scopes: ☐ rest_api ☐ rest_api_external

Roles: Operator

< Back Next > Cancel

3. Enter the Relying Party trust details.

Add Application Wizard

OpenID Connect Relying Party (RP)
Enter the RP details for My Client Credential App.

Relying Party (RP) details

Grant Type: Client Credential

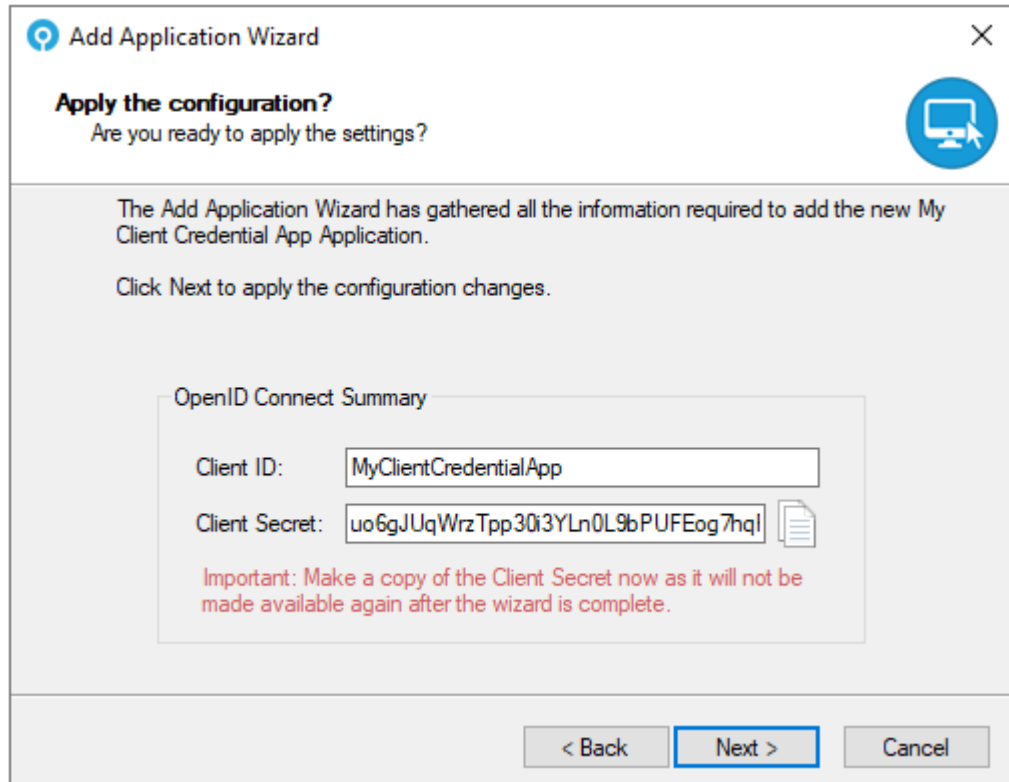
Scopes: ☒ rest_api ☐ rest_api_external

Roles: Administrator

< Back Next > Cancel

For most server-to-server operations, set **Scopes** to `rest_api` and **Roles** to Administrator.

4. Click **Next**.




Add Application Wizard

Apply the configuration?
Are you ready to apply the settings?

The Add Application Wizard has gathered all the information required to add the new My Client Credential App Application.
Click Next to apply the configuration changes.

OpenID Connect Summary

Client ID:

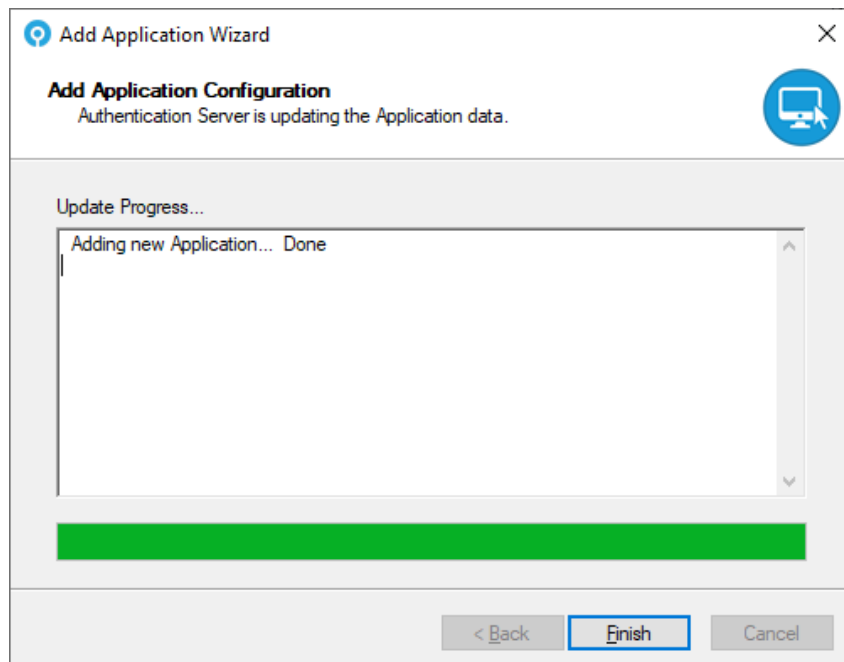
Client Secret: 

Important: Make a copy of the Client Secret now as it will not be made available again after the wizard is complete.

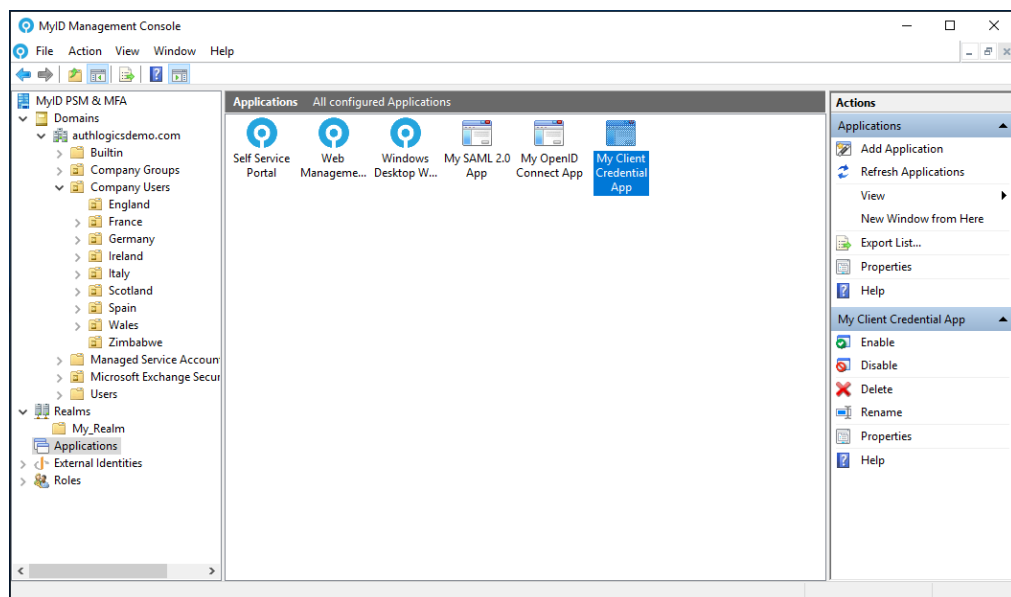
< Back **Next >** Cancel

5. Optionally, you can type a new **Client ID**.
6. Make a copy of the **Client Secret** for integration with the calling application.
This is necessary for later authentication and is not available outside of this page. If you lose this, you can edit the application to change the **Client Secret**. See section [5.5.6.4, OpenID Connect tab](#).

7. Click **Next**.

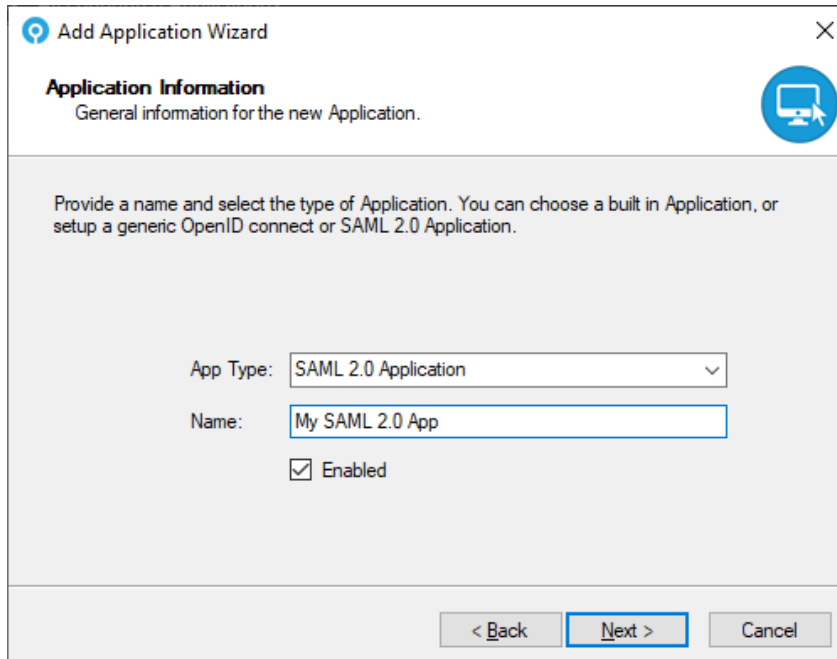


8. Click **Finish**.



Your application has now been configured.

5.6.3 Creating a SAML 2.0 application



Add Application Wizard

Application Information
General information for the new Application.

Provide a name and select the type of Application. You can choose a built in Application, or setup a generic OpenID connect or SAML 2.0 Application.

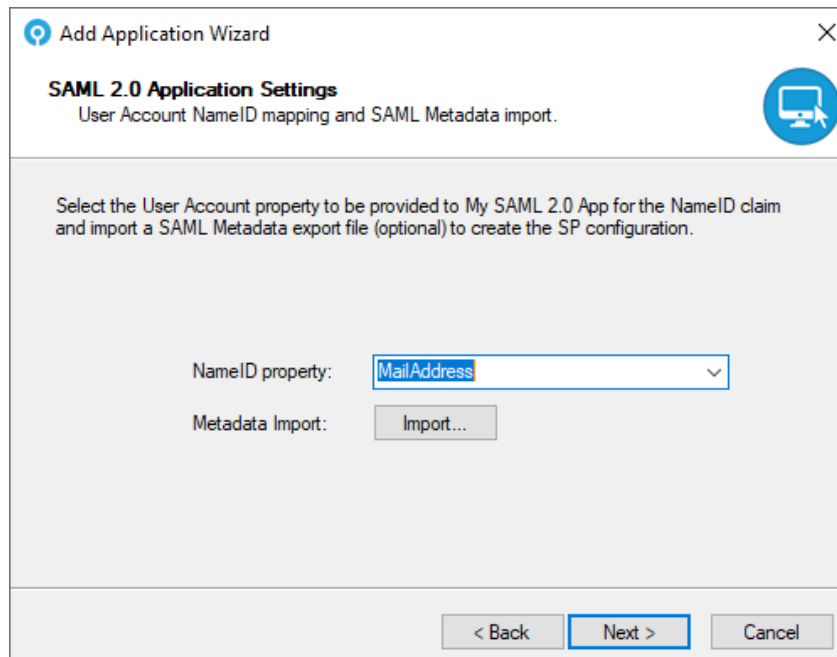
App Type: SAML 2.0 Application

Name: My SAML 2.0 App

☒ Enabled

< Back Next > Cancel

1. Click **Next**.



Add Application Wizard

SAML 2.0 Application Settings
User Account NameID mapping and SAML Metadata import.

Select the User Account property to be provided to My SAML 2.0 App for the NameID claim and import a SAML Metadata export file (optional) to create the SP configuration.

NameID property: MailAddress

Metadata Import: Import...

< Back Next > Cancel

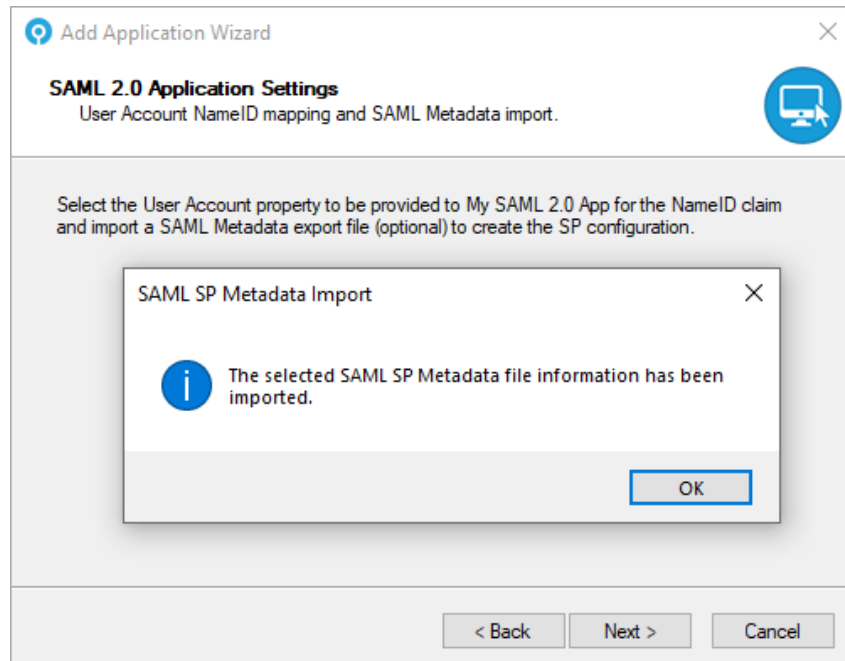
2. Select the user property that contains the information required by the SAML 2.0 application for the **NameID** property.

The **NameID** is normally the main claim that the SAML 2.0 application uses for identifying the user; this is normally an email address or account name.

3. If you have a metadata export file from the application:

- a. Click **Import** to import the metadata.

This can save configuration time, as metadata files contain valuable configuration data about an Application, including signing certificate information.



- b. Click **OK**.

The application metadata is imported. This populates some fields throughout the rest of the wizard.

4. Click **Next**.

The screenshot shows the 'Add Application Wizard' dialog box with the title 'SAML 2.0 Service Provider Configuration'. Below the title is the instruction 'Enter the Service Provider details provided by My SAML 2.0 App.' The main area is titled 'SAML 2.0 Service Provider (SP)' and contains several input fields: 'Description' (empty), 'Entity ID URI' (loadbalancer-9.siroe.com), 'Assertion URL' (https://LoadBalancer-9.siroe.com:3443/federation/Consumer/met...), 'Logout URL' (https://LoadBalancer-9.siroe.com:3443/federation/SPSloRedirect...), 'Artifact URL' (empty), 'NameID Format' (um:oasis:names:tc:SAML:2.0:nameid-format:persistent), and 'Authn Context' (um:oasis:names:tc:SAML:2.0:ac:classes:unspecified). At the bottom are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

5. Enter the settings for the application using the instructions from the vendor of your application.

You may not be required to provide information for every field.

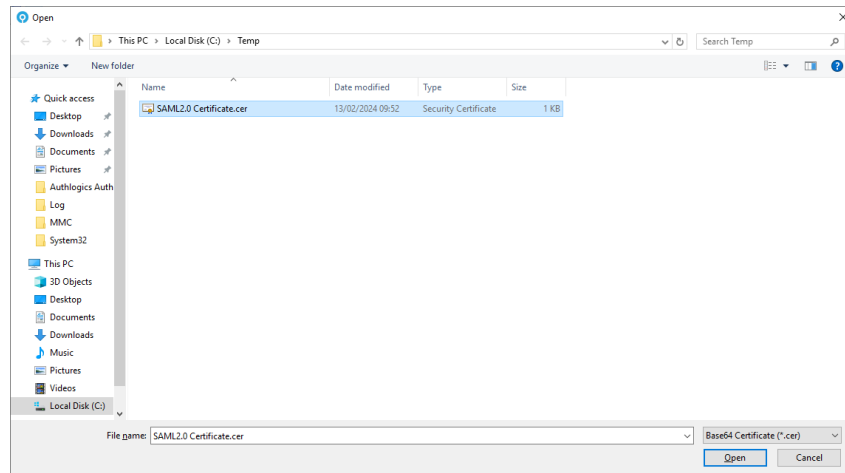
6. Click **Next**.

The screenshot shows the 'Add Application Wizard' dialog box with the title 'SAML 2.0 Service Provider Signing'. Below the title is the instruction 'Select the required Service Provider signing options.' The main area contains a note: 'If a trust relationship is required with the Service Provider (SP) then import at least one SP certificate so the IdP can verify signatures.' Below this is a section titled 'SAML 2.0 Certificates' which includes a dropdown for 'SP Certificates' (CN=loadbalancer-9.siroe.com, O=siroe.com), 'Add' and 'Remove' buttons, and a 'Cert Info' link. There are also four checkboxes: 'Want Signed Auth Request', 'Want Signed Logout Request', 'Sign Assertion to SP', and 'Sign Logout Response to SP'. At the bottom are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

7. If required, choose the SAML 2.0 signing certificate.

Your Application Service Provider should provide one or more signing certificates, which may be included in the metadata export. You can import and remove certificates as required:

- a. To add a certificate, click **Add**.



- b. Browse to the signing certificate and click **Open**.

Note: Not all SAML applications require signing or certificates.

8. Configure the signing requirements for the application.
9. Click **Next**.

A screenshot of the 'Add Application Wizard' dialog box, titled 'Add Application Wizard'. The current step is 'Authentication Options', with the instruction 'Select the required authentication options.' and a computer icon. The dialog is divided into sections for 'Primary', 'Primary Options', 'Secondary', and 'Secondary Options'. Under 'Primary', there are three checkboxes: 'Password', 'Windows Authentication', and 'Certificate'. Under 'Primary Options', there are two checkboxes: 'Allow password reset via Email' and 'Allow password reset via SMS/Text'. Under 'Secondary', there are six checkboxes arranged in two rows: 'Passkey', 'YubiKey OTP', 'Grid Pattern', 'Push', 'One Time Code', and 'Phrase'. Under 'Secondary Options', there are two checkboxes: 'Allow deviceless' and 'Allow any selected user configured technology'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

10. You can specify the logon technology users must use to authenticate to the portal.

You can choose one logon technology from the options in the **Primary** section.

If only a PSM license is installed, the options are limited to **Password** and **Windows Authentication**.

New applications of this type, by default, have no primary technology selected.

If you select **Password**, users are required to enter a valid Active Directory password as well as their MFA credentials. If you do not select **Password**, passwordless logins are enabled.

If you select **Windows Authentication** or **Certificate**, the **Primary Options**, **Secondary**, and **Secondary Options** sections are disabled, as these technologies do not require further configuration.

Note: If you select **Windows Authentication**, you must configure IIS to use Windows Authentication – this disables multi-factor authentication for this application. If you enable Windows Authentication in the MyID Management Console without configuring Windows Authentication in IIS, the user is shown the standard Windows prompt to enter their Username and Password.

Similarly, if you select **Certificate** authentication, you must configure IIS to handle the certificate, at which point all other MFA options are no longer valid for this application, and you cannot select them in the MyID Management Console.

You can choose as many or as few **Secondary** logon technologies as you want.

If you select only one secondary option, the user must have that logon technology.

If you select multiple secondary options, the type of technology used is determined after the user has entered their account name and, if required, password. The type of logon technology used is determined based on the selected options and which technologies the user has configured. The priority order for the secondary logon technologies is:

- **Passkey**
- **Grid Pattern** (if **Allow deviceless** is not selected)
- **Push**
- **YubiKey OTP**
- **One Time Code**
- **Phrase** (if **Allow deviceless** is not selected)
- **Grid Pattern** (if **Allow deviceless** is selected)
- **Phrase** (if **Allow deviceless** is selected)

If **Password** is selected as the primary logon technology, and no secondary logon technology is selected, the user requires only a password to log in.

If a user does not have access to any of the secondary logon technologies selected, they cannot log in to the application, unless all of the following are true:

- No primary logon technology is selected.
- All secondary logon technologies selected require devices.
- The user has no device registered.

In that case, fallback password authentication occurs, and the user can log in with just their username and password.

If no logon technologies are selected, no-one can log in.

If the user has a device registered, the technologies that require a device (**Passkey**, and, if **Allow deviceless** is not selected, **Grid Pattern** and **Phrase**) can be selected, whether or not the device is enabled.

For example, if a user has a FIDO token registered but the device has been disabled, the user is still prompted to authenticate with their FIDO token. This is so that temporarily displaced devices do not allow users to fall back on lesser authentication methods.

If a user temporarily loses their FIDO device, you can give them a temporary access code – by default, this only lasts 24 hours or three logons, whichever comes first. For information on changing temporary access code limitations, see section [5.3.1, General tab](#). If the user finds their FIDO token, you can re-enable it, and if they cannot find it, you can remove the device from their account and issue a new one. For information on assigning temporary access codes, see section [5.9.8, Assigning temporary access codes to a user](#) or the *Assigning a temporary access code to a user* section of the [Web Management Portal User Guide](#).

If you select the **Allow any selected user configured technology** option, users are allowed to authenticate using any MFA technology for which they are provisioned. If this option is not selected, the user can enter only the valid authentication credentials that are shown by the application.

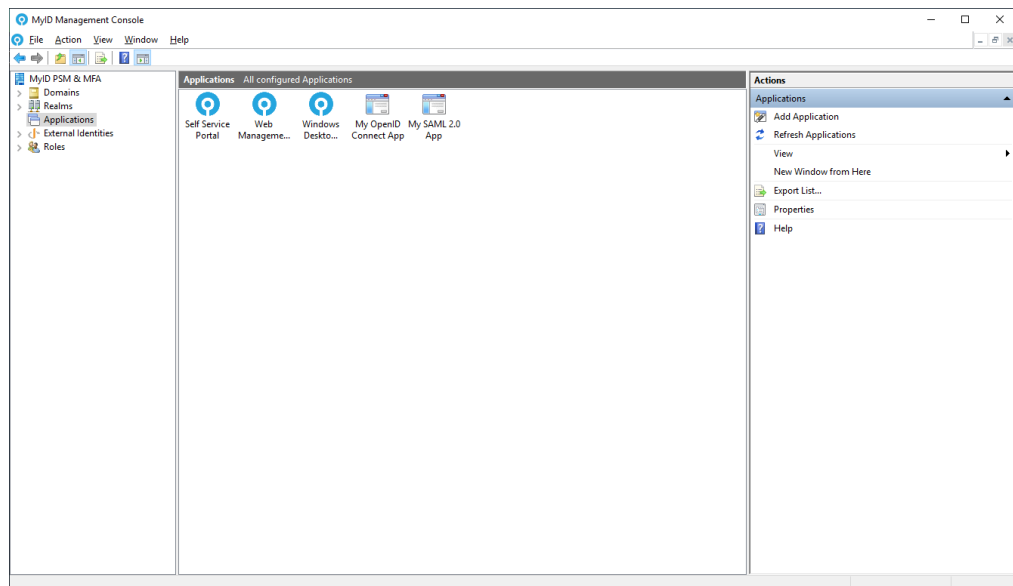
Grid Pattern and Phrase authentication technologies both support deviceless authentication; select the **Allow Deviceless** option to enable this support. If this is selected, you cannot use these technologies with a device, which is less secure. If this is not selected, then multi-factor authentication is always required.

11. Click **Next**.

The screenshot shows a window titled "Add Application Wizard" with a close button (X) in the top right corner. Below the title bar, there is a sub-header "Apply the configuration?" followed by the text "Are you ready to apply the settings?". To the right of this text is a blue circular icon containing a computer monitor with a cursor pointing at it. The main content area contains the text: "The Add Application Wizard has gathered all the information required to add the new My SAML 2.0 App Application. Click Next to apply the configuration changes." Below this is a section titled "SAML 2.0 Summary" which contains a "Host:" label followed by a text box containing the URL "https://idp.federationdemo.com/idp". Below the text box are two blue hyperlinks: "IdP Signing Certificate" and "Copy Base64". At the bottom of the window are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

12. Confirm the **Host** configuration information.
From this screen, you can export or copy the IdP signing certificate that the SAML application requires.
13. Click **Next**.

The screenshot shows a window titled "Add Application Wizard" with a close button (X) in the top right corner. Below the title bar, there is a sub-header "Add Application Configuration" followed by the text "Authentication Server is updating the Application data." To the right of this text is a blue circular icon containing a computer monitor with a cursor pointing at it. The main content area contains the text "Update Progress..." above a progress bar. The progress bar is a horizontal rectangle with a green fill and a white border. Below the progress bar is a text box containing the text "Adding new Application... Done". At the bottom of the window are three buttons: "< Back", "Finish" (which is highlighted with a blue border), and "Cancel".

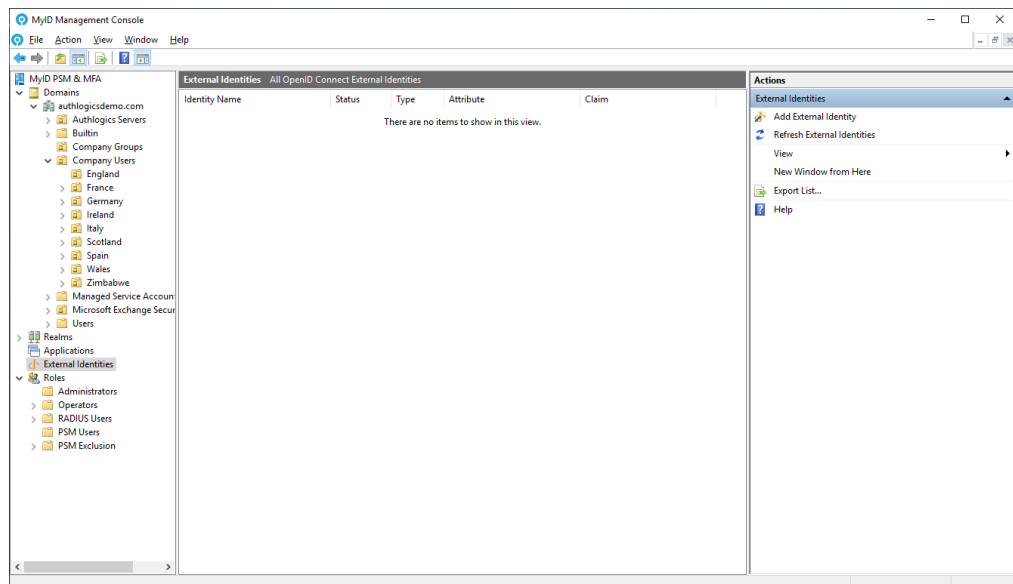
14. Click **Finish**.

Your application has now been configured.

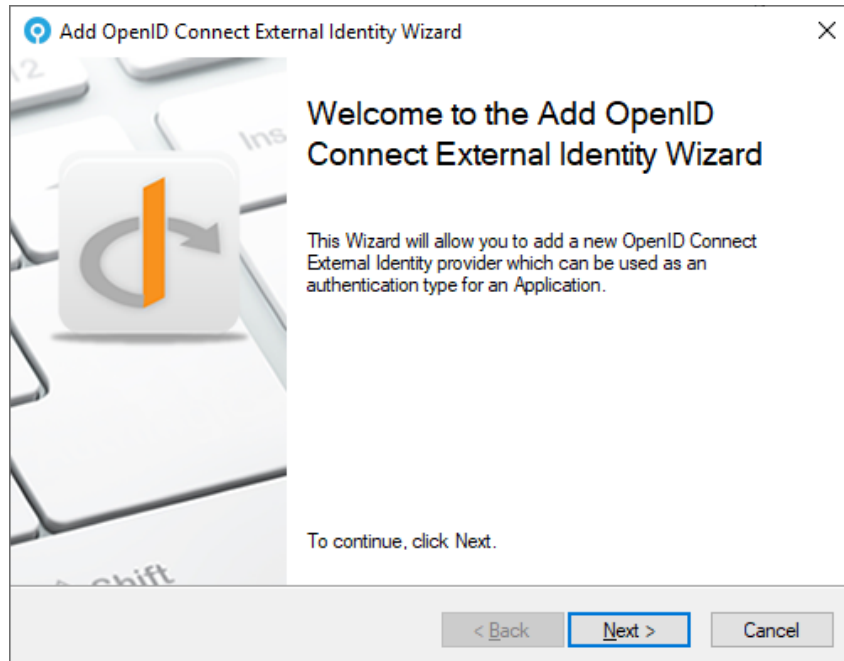
5.7 Adding External Identities

MyID supports OpenID Connect External Identity Providers to be used as an authentication type for applications. To add an External Identity Provider:

1. In the MyID Management Console, highlight the **External Identities** node.



2. Click **Add External Identity**, in the **Actions** pane.



3. Click **Next**.
4. Provide a descriptive **Name** for the external identity and choose a **Provider**.
MyID External Identities supports providers of type:
 - Google
See section [5.7.1, Creating an OpenID Connect External Identity \(Google\)](#).
 - Microsoft
See section [5.7.2, Creating an OpenID Connect External Identity \(Microsoft\)](#).
5. Set the External Identity to be **Enabled**.

5.7.1 Creating an OpenID Connect External Identity (Google)

The screenshot shows the 'Add OpenID Connect External Identity Wizard' window. The title bar says 'Add OpenID Connect External Identity Wizard'. The main heading is 'External Identity Information' with a subtitle 'General information for the new External Identity provider.' Below this, a text box says: 'Provide a name and select the External Identity provider type. The name is for internal reference purposes and can be changed at any time.' There are three input fields: 'Name:' with the value 'Google Identity', 'Provider:' with a dropdown menu showing 'Google', and a checked checkbox labeled 'Enabled'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

1. Click **Next**.
2. Match the **OpenID Connect Claim** with the **Active Directory User Attribute** to link the accounts.

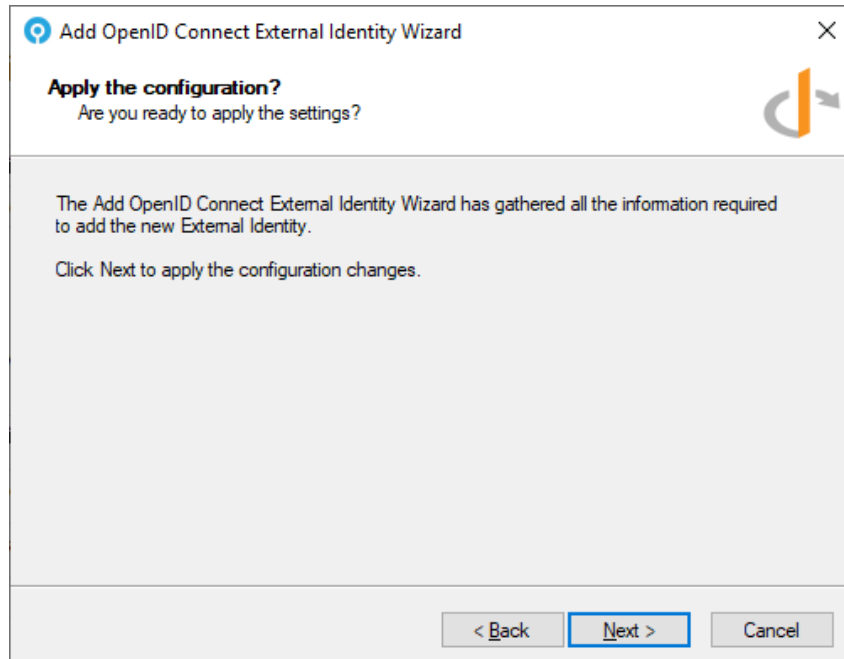
For example, you may want to match the user on the email address where the user's Google email address is stored in the user's Info field in the Active Directory.

The screenshot shows the 'Add OpenID Connect External Identity Wizard' window at the 'Account Mapping' step. The title bar says 'Add OpenID Connect External Identity Wizard'. The main heading is 'Account Mapping' with a subtitle 'Map OpenID Connect to Active Directory'. Below this, a text box says: 'An OpenID Connect Claim from the External Identity must be matched to an Active Directory User attribute to link the accounts.' There are two dropdown menus: 'OpenID Connect Claim:' with the value 'emailaddress' and 'AD User Attribute:' with the value 'info'. A double-headed vertical arrow is positioned between the two dropdowns. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

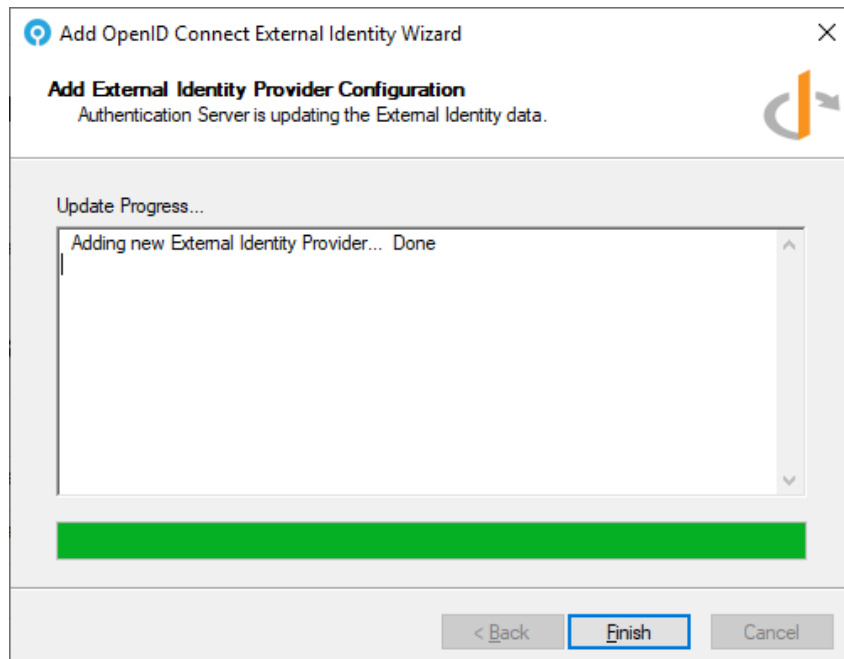
- Click **Next**.
- Enter the **Client ID** and **Client Secret** retrieved from the Google Cloud API Credentials page.

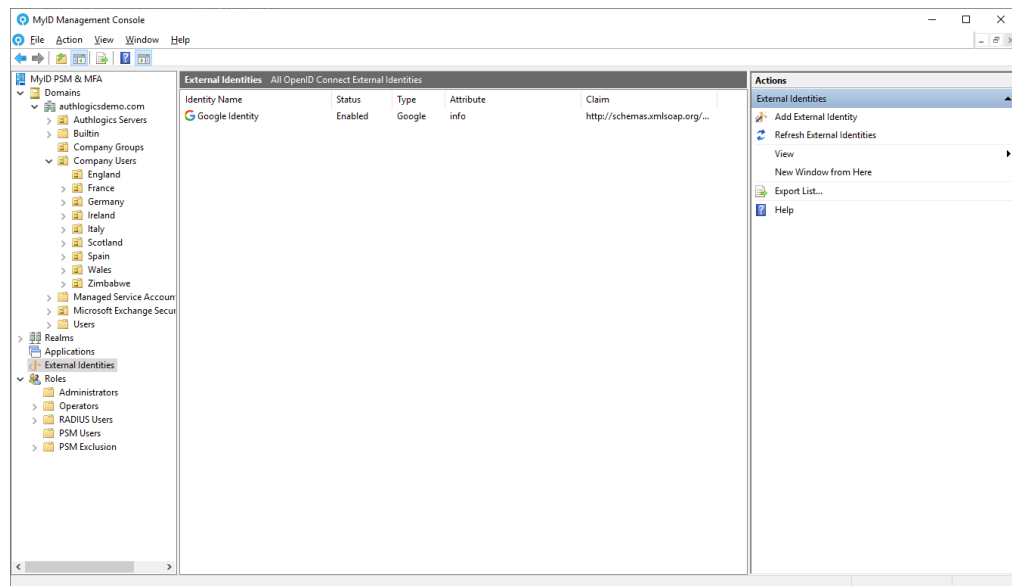
MyID Authentication Server Installation and Configuration Guide

5. Click **Next**.

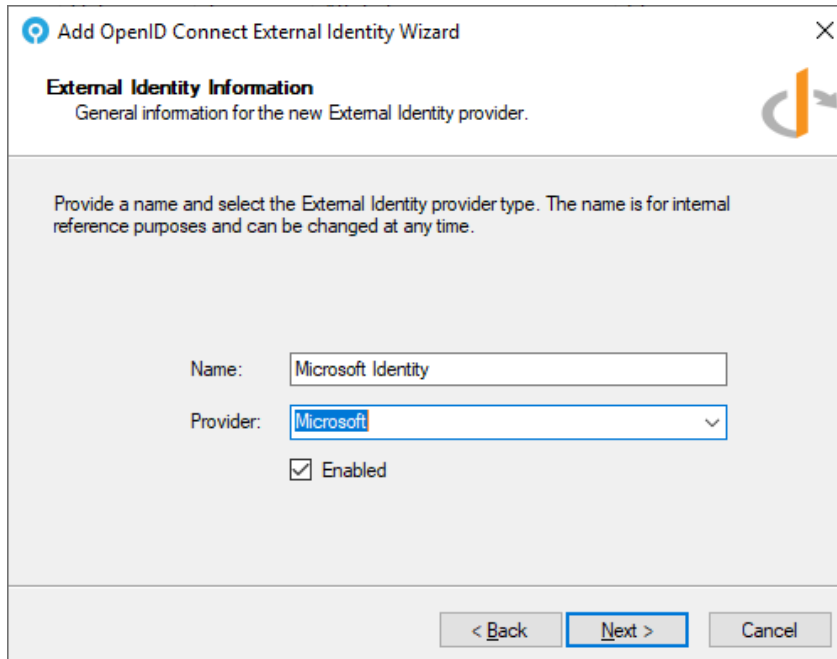


6. Make a copy of the OpenID Connect client secret for integration with the calling application.
7. Click **Next**.



8. Click **Finish**.

5.7.2 Creating an OpenID Connect External Identity (Microsoft)



Add OpenID Connect External Identity Wizard

External Identity Information
General information for the new External Identity provider.

Provide a name and select the External Identity provider type. The name is for internal reference purposes and can be changed at any time.

Name:

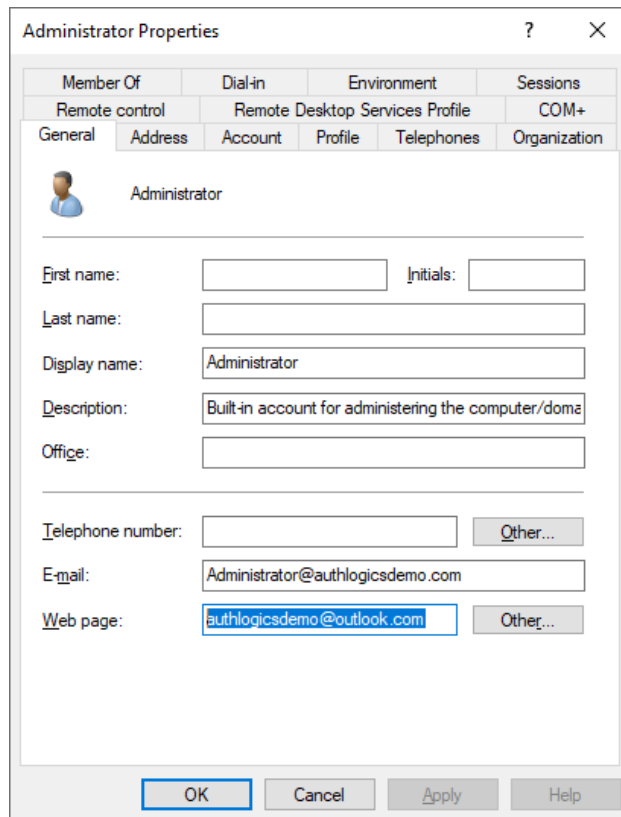
Provider:

☒ Enabled

< Back Next > Cancel

1. Click **Next**.
2. Match the **OpenID Connect Claim** with the **Active Directory User Attribute** to link the accounts.

For example, you may want to match the user by their email address where the user's Microsoft Live email address is stored in the user's Web Page (`wwwHomePage`) field in AD.



The image shows the 'Administrator Properties' dialog box in Windows. The 'General' tab is selected. The user is 'Administrator'. The 'First name' field is empty, 'Initials' is empty, 'Last name' is empty, 'Display name' is 'Administrator', 'Description' is 'Built-in account for administering the computer/domain', 'Office' is empty, 'Telephone number' is empty, 'E-mail' is 'Administrator@authlogicsdemo.com', and 'Web page' is 'authlogicsdemo@outlook.com'. The 'OK' button is highlighted.

Member Of	Dial-in	Environment	Sessions
Remote control	Remote Desktop Services Profile	COM+	

General Address Account Profile Telephones Organization

Administrator

First name: Initials:

Last name:

Display name:

Description:

Office:

Telephone number: Other...

E-mail:

Web page: Other...

OK Cancel Apply Help

3. Click **Next**.

Add OpenID Connect External Identity Wizard

X

Microsoft OAuth 2.0

Enter your details for Microsoft OAuth 2.0.

The ID token introduced by OpenID Connect is issued by the authorization server, the Microsoft identity platform, when the client application requests one during user authentication. The ID token enables a client application to verify the identity of the user and to get other information (claims) about them. ID tokens aren't issued by default for an application registered with the Microsoft identity platform.

Application ID:

Client Secret:

[Microsoft Entra App registrations](#)

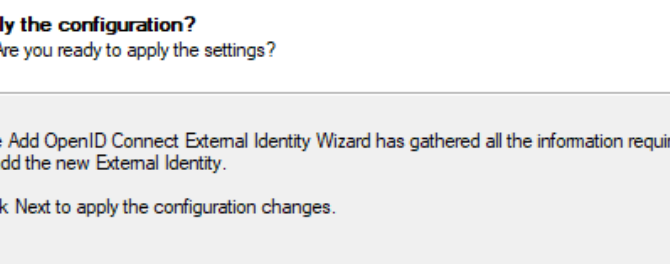
[More Information](#)

< Back

Next >

Cancel

4. Enter the **Application ID** and **Client Secret** retrieved from the Microsoft Identity Platform.
5. Click **Next**.



Add OpenID Connect External Identity Wizard

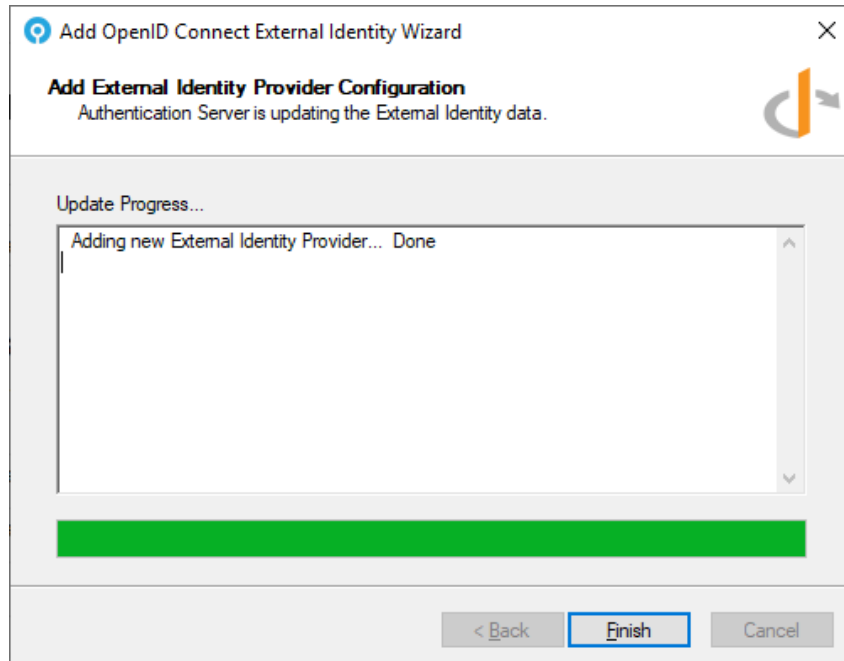
Apply the configuration?
Are you ready to apply the settings?

The Add OpenID Connect External Identity Wizard has gathered all the information required to add the new External Identity.
Click Next to apply the configuration changes.

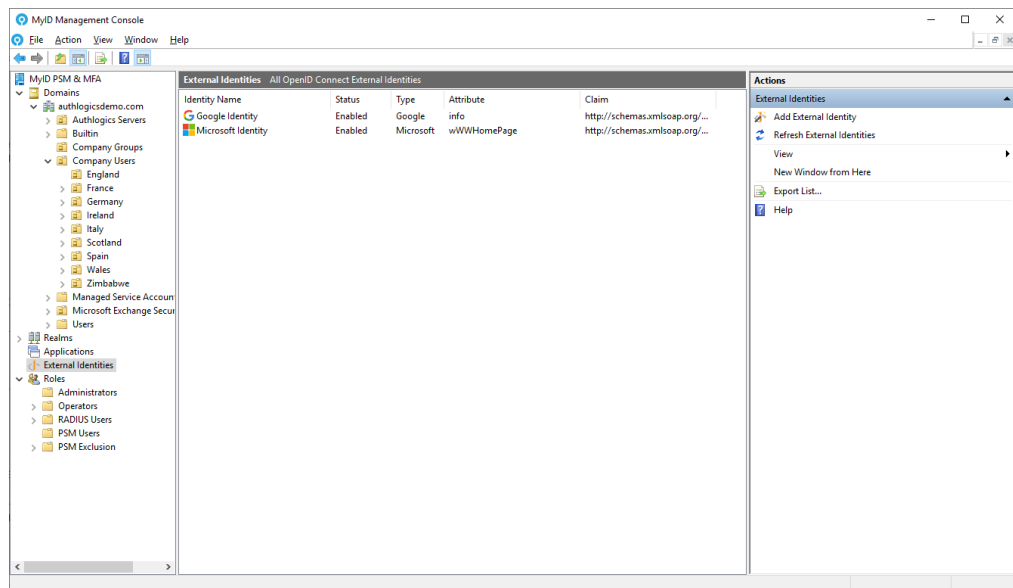
< Back **Next >** Cancel

6. Make a copy of the OpenID Connect client secret for integration with the calling application.

7. Click Next.



8. Click **Finish**.



Your Microsoft External Identity has now been configured and is ready for use.

5.8 Adding users and user functionality

As MyID uses Active Directory as the user account database, the base user accounts may already exist in most cases. You can add Active Directory users one at a time or in bulk to the MyID MMC where they can be set up for various MFA technologies. They can be added from one or multiple OUs at a time as needed.

You can add External User accounts without the need for a full Active Directory Domain user account. These external accounts are stored within the forest root domain as LDAP `person` objects and cannot be used for Windows-based logons. A Realm must be created to contain an External User account.

You can use External User accounts together with the Windows Desktop Agent to add MFA to local Windows user accounts on both domain-joined and workgroup based systems.

Adding a user account to the MyID MMC allows the user to make use of the Self Service Portal and, if an MFA license is installed, they can be provisioned for Multi-Factor Authentication technologies.

You can carry out the following:

- Add a new realm.
See section [5.8.1, Adding a new realm](#).
- View MFA and PSM account types.
See section [5.8.2, User account types – MFA or PSM](#).
- Add a MyID user account.
See section [5.8.3, Adding a new MyID user account](#).
- Add a PSM user account.
See section [5.8.4, Adding a new MyID PSM user account](#).
- Add an external MFA user account.
See section [5.8.5, Adding a new external MFA user account](#).
- Set up Grid Pattern authentication.
See section [5.8.6, Setting up a user for Grid Pattern Authentication](#).
- Set up Phrase authentication.
See section [5.8.7, Setting up a user for Phrase authentication](#).
- Set up One Time Code authentication.
See section [5.8.8, Setting up a user for One Time Code](#).
- Set up YubiKey OTP.
See section [5.8.9, Setting up a user for YubiKey OTP](#).
- Add a YubiKey device to a user's account.
See section [5.8.10, Adding a YubiKey device](#).

For information on managing existing users through the MyID Management Console, see section [5.9, Managing existing users](#).

You can also manage users through the Web Management Portal. For more information, see the [Managing a user](#) section of the [Web Management Portal User Guide](#).

5.8.1 Adding a new realm

A realm is a container to store External User accounts. Each account within a realm must have a unique name. Realms can be nested – you can create a realm inside another realm for easier account management. You can rename realms and account names.

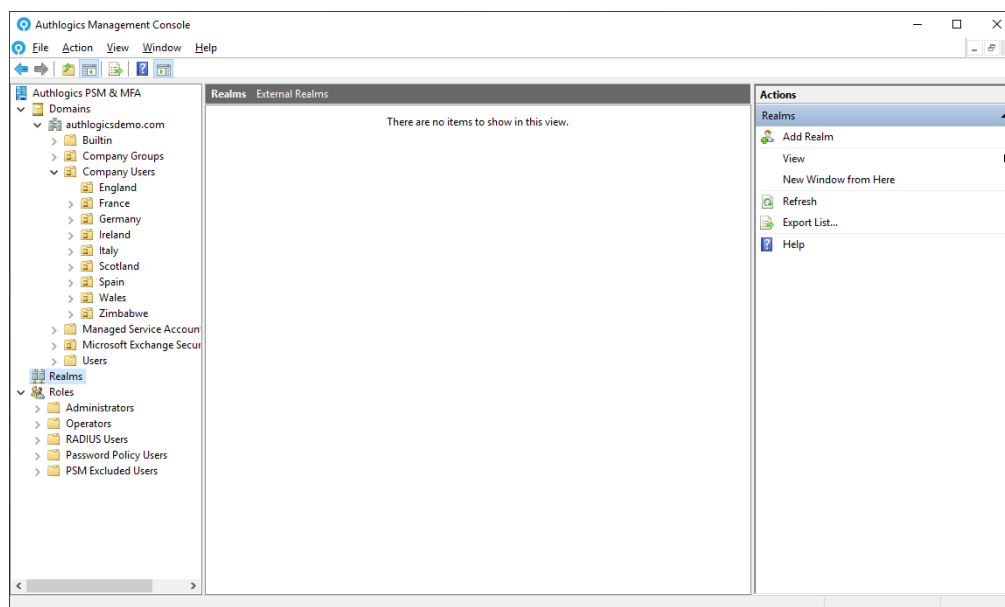
Note: A realm name may contain letters, numbers, dots, and underscores, but cannot be the same as an existing Active Directory domain name.

The realm name forms part of the user logon name. A user would enter their logon names as follows:

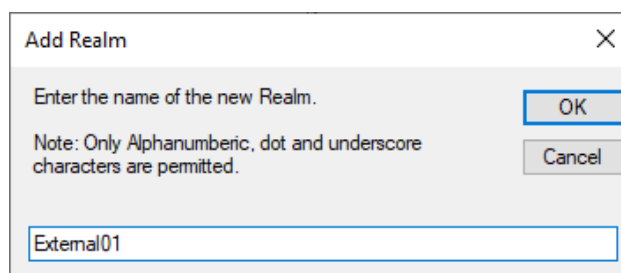
- Domain style: <realm>\<account>
- UPN style: <account>@<realm>

To add a new realm:

1. In the MyID Management Console, highlight the **Realms** node.

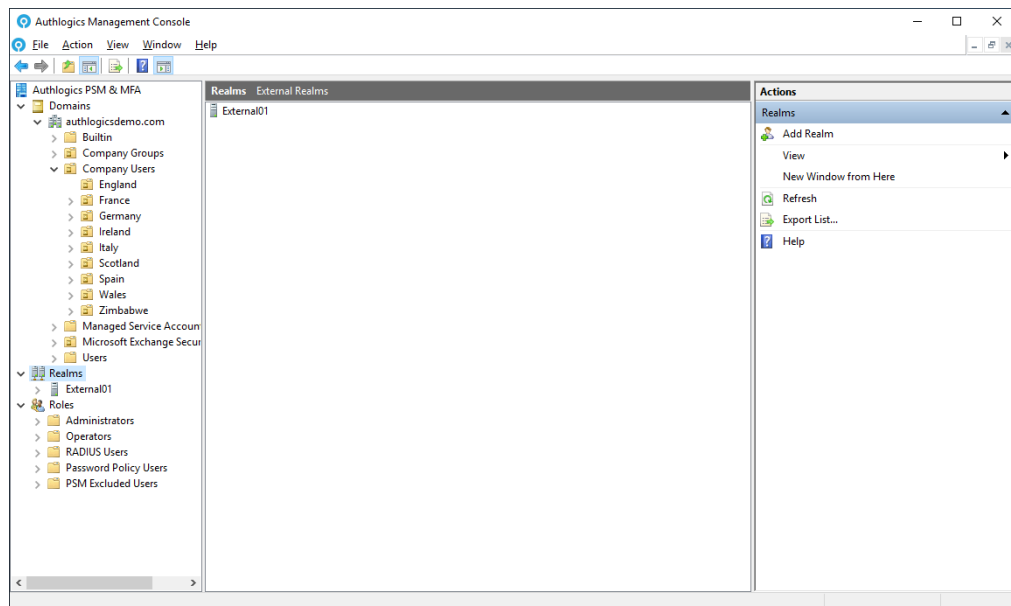


2. Click **Add Realm**, in the **Actions** pane.



3. Enter the name of the new realm.

4. Click **OK**.



You have now added a realm. You can add more realms using the same method if required,

5.8.2 User account types – MFA or PSM

You can add different types of users based on the type of licenses installed. If an MFA license is installed, you can create a user account that can be provisioned for various MFA logon technologies and devices.

If only a PSM license is installed, you can create users with only PSM self-services features. PSM users can access the Self Service Portal to change or reset their password with One Time Codes. PSM users cannot be provisioned for use with Multi-Factor Authentication.

If an MFA license is added to an installation that previously only had a PSM license, existing users can immediately be provisioned for Multi-Factor Authentication.

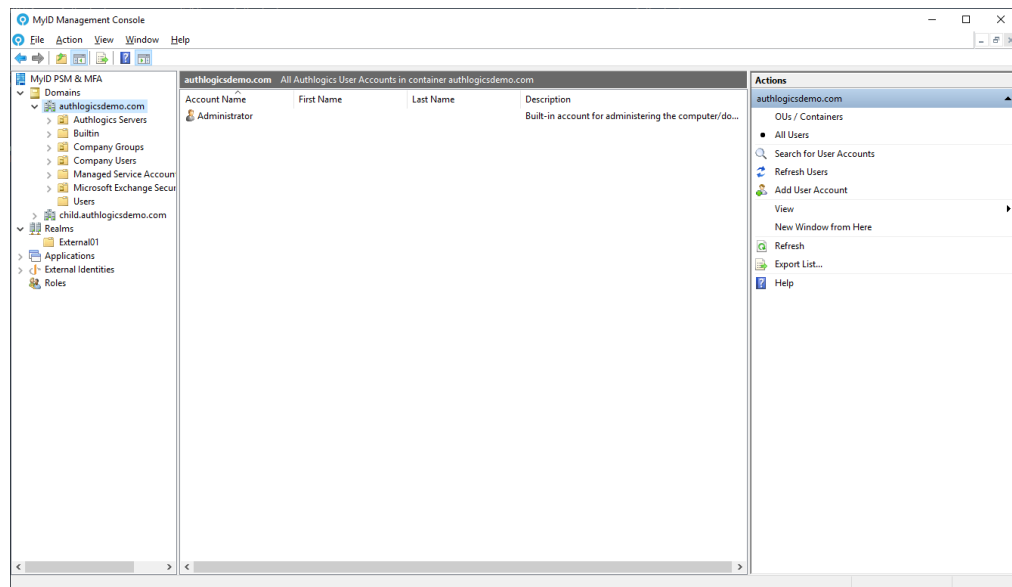
Note: External User Accounts can be used with MFA only, as PSM requires an Active Directory user account.

5.8.3 Adding a new MyID user account

To add a new MyID user account:

1. In the MyID Management Console, expand the **Domains** and select the appropriate domain.

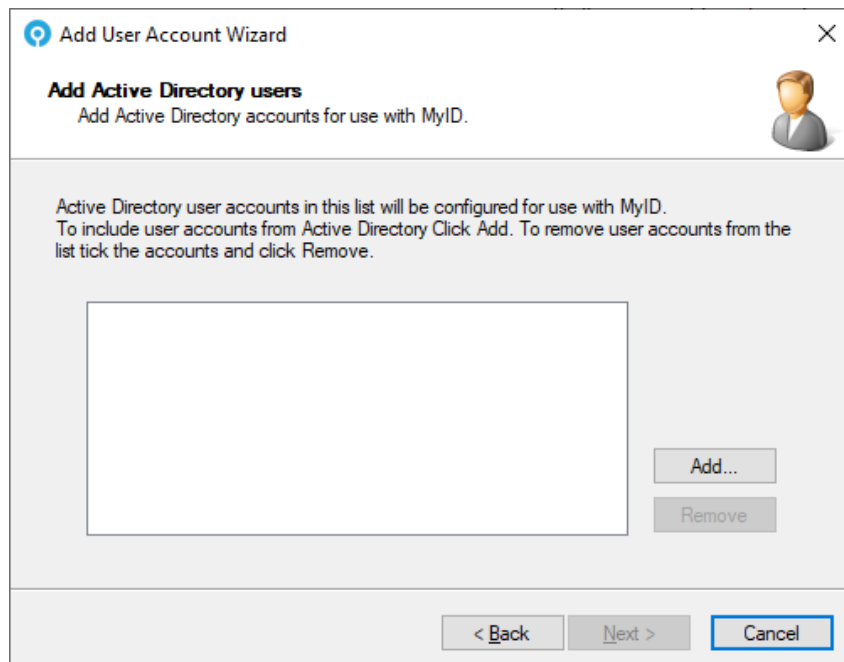
You can expand the list of OUs to see what accounts already exist.



2. Click **Add User Account**, in the **Actions** pane.

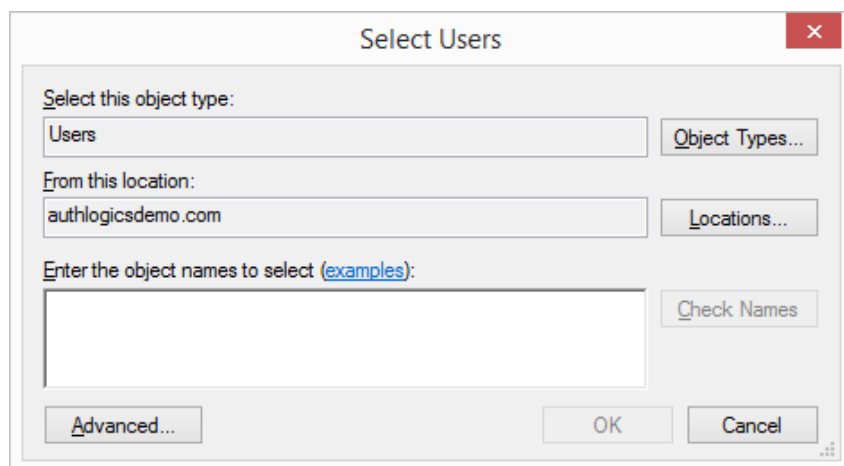


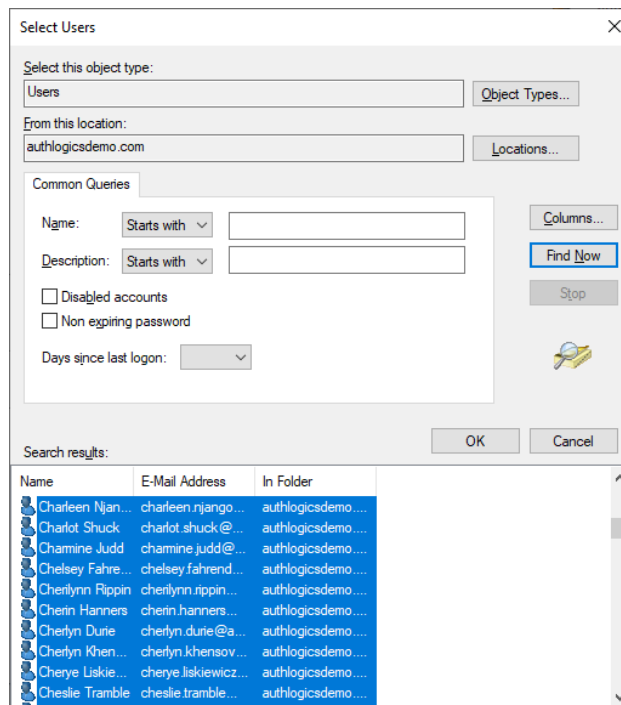
3. Click **Next**.



4. To add existing Active Directory users click **Add**.

Note: This process does not create user accounts in the Active Directory Domain, it simply adds MyID metadata to an *existing* account. Ensure that the domain accounts exist before adding them to the MyID MMC.



5. Click **Advanced**.

Select Users

Select this object type:
Users

From this location:
authlogicsdemo.com

Common Queries

Name: Starts with

Description: Starts with

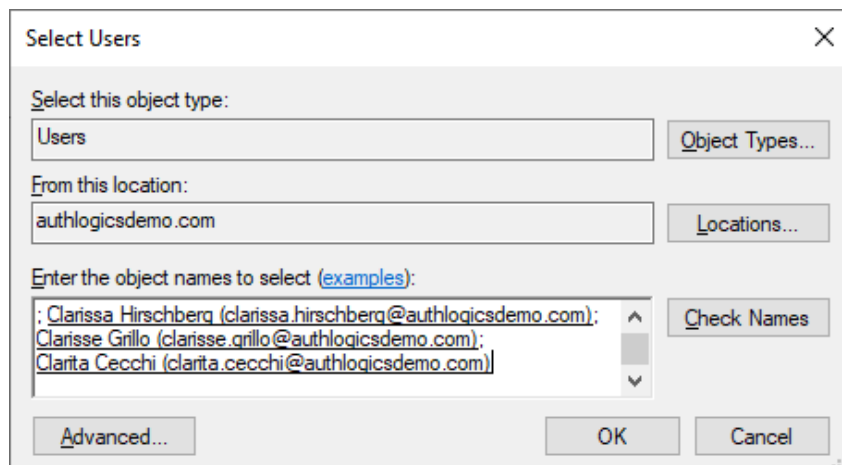
☐ Disabled accounts

☐ Non expiring password

Days since last logon:

Search results:

Name	E-Mail Address	In Folder
Charleen Njan	charleen.njan@authlogicsdemo.com	authlogicsdemo.com
Charlot Shuck	charlot.shuck@authlogicsdemo.com	authlogicsdemo.com
Chamine Judd	chamine.judd@authlogicsdemo.com	authlogicsdemo.com
Chelsey Fahre	chelsey.fahre@authlogicsdemo.com	authlogicsdemo.com
Cherilyn Rippin	cherilyn.rippin@authlogicsdemo.com	authlogicsdemo.com
Cherin Hanners	cherin.hanners@authlogicsdemo.com	authlogicsdemo.com
Cherlyn Durie	cherlyn.durie@authlogicsdemo.com	authlogicsdemo.com
Cherlyn Khen	cherlyn.khensov@authlogicsdemo.com	authlogicsdemo.com
Cheryl Liskie	cheryl.liskiewicz@authlogicsdemo.com	authlogicsdemo.com
Cheslie Tramble	cheslie.tramble@authlogicsdemo.com	authlogicsdemo.com

6. Click **Find Now**.7. Select the required users from Active Directory and click **OK**.

Select Users

Select this object type:
Users

From this location:
authlogicsdemo.com

Enter the object names to select (examples):

: Clarissa Hirschberg (clarissa.hirschberg@authlogicsdemo.com);
Clarisse Grillo (clarisse.grillo@authlogicsdemo.com);
Clarita Cecchi (clarita.cecchi@authlogicsdemo.com)

Advanced...

OK

Cancel

8. Click **OK**.

To remove accounts from the list, check the box next to the name and click **Remove**.

The screenshot shows the 'Add User Account Wizard' window with the title 'Add Active Directory users'. Below the title is the subtitle 'Add Active Directory accounts for use with MyID.' and a user icon. The main text states: 'Active Directory user accounts in this list will be configured for use with MyID. To include user accounts from Active Directory Click Add. To remove user accounts from the list tick the accounts and click Remove.' Below this is a list of Active Directory users with checkboxes next to them. The users listed are: AUTHLOGICSDemo\Becky Shandro (becky.shandro@autl), AUTHLOGICSDemo\Belinda Coomey (belinda.coomey@au), AUTHLOGICSDemo\Bellanca Chiszar (bellanca.chiszar@a), AUTHLOGICSDemo\Bellina Zehring (bellina.zehring@authl), AUTHLOGICSDemo\Bernardina Weems (bernardina.weem), AUTHLOGICSDemo\Bernardine Iler (bernardine.iler@authl), AUTHLOGICSDemo\Bemetta Currington (bemetta.curingt), and AUTHLOGICSDemo\Berry Mesko (berny.mesko@authlogic). To the right of the list are 'Add...' and 'Remove' buttons. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

9. Click **Next**.

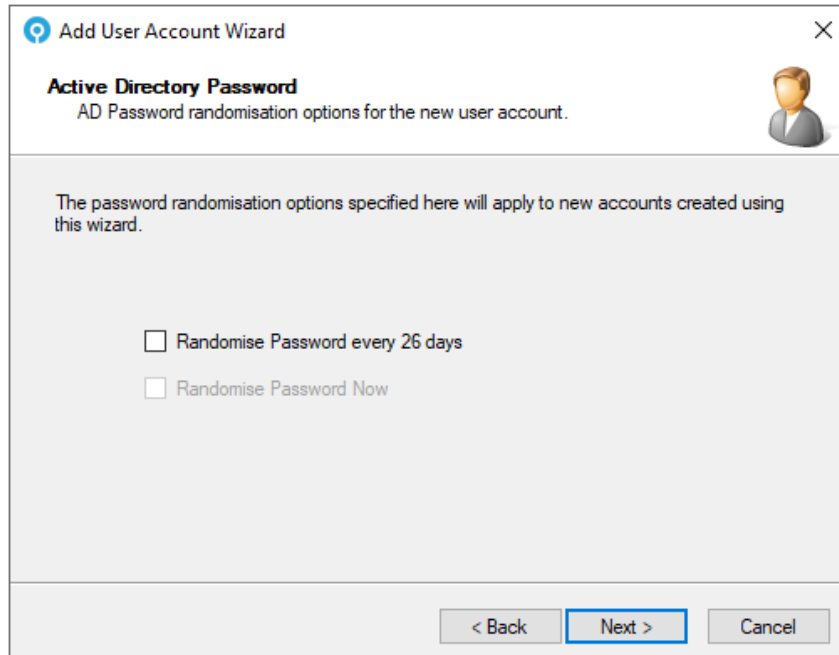
The screenshot shows the 'Add User Account Wizard' window with the title 'Account Options'. Below the title is the subtitle 'General options for the new user account.' and a user icon. The main text states: 'The account options specified here will apply to new user accounts created by this wizard. By default user accounts are enabled from the date of creation and do not expire.' Below this is a section titled 'Account options' with the following settings: 'Account is disabled' (unchecked), 'Mobile phone private' (unchecked), 'Valid from:' (01 November 2024), 'Valid to:' (01 November 2024), 'Always' (unchecked) for 'Valid from', and 'Always' (checked) for 'Valid to'. At the bottom are '< Back', 'Next >', and 'Cancel' buttons.

10. Set the account options.

Account options determine the user's state. You can give accounts start and end validity dates, and can disable the account if required.

You can also specify the mobile phone privacy setting.

11. Click **Next**.

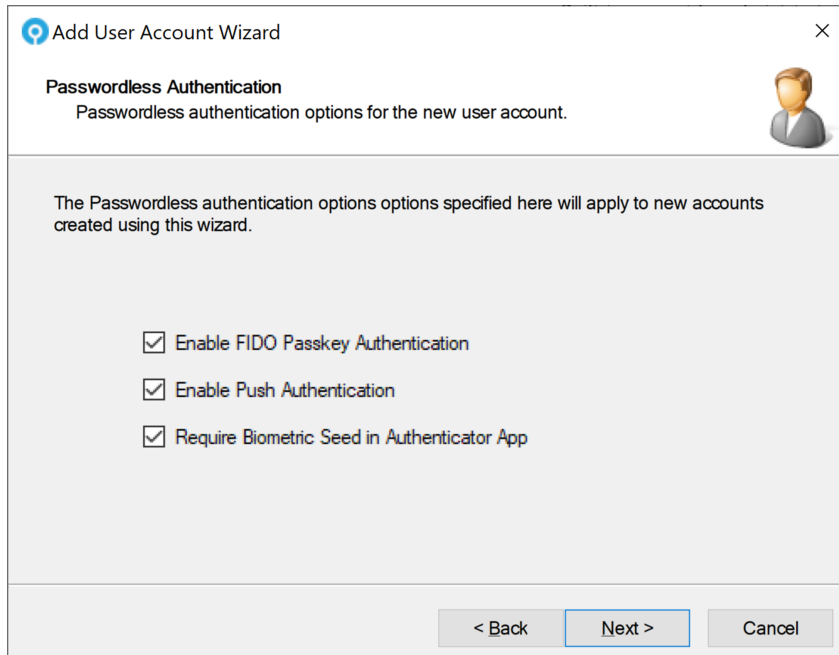


The screenshot shows the 'Add User Account Wizard' dialog box. The title bar says 'Add User Account Wizard'. The main heading is 'Active Directory Password' with a subtitle 'AD Password randomisation options for the new user account.' and a user icon. The text says 'The password randomisation options specified here will apply to new accounts created using this wizard.' There are two checkboxes: 'Randomise Password every 26 days' and 'Randomise Password Now'. At the bottom are buttons for '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

12. If you have set the **Randomise AD Passwords every x days** setting in the domain dialog, choose if the users have their passwords randomized, and whether the passwords are initially randomized.

For more information on setting password randomization, see section [5.4.1, Domain Properties dialog](#).

13. Click **Next**.



The screenshot shows the 'Add User Account Wizard' dialog box. The title bar says 'Add User Account Wizard'. The main heading is 'Passwordless Authentication' with a subtitle 'Passwordless authentication options for the new user account.' and a user icon. The text says 'The Passwordless authentication options specified here will apply to new accounts created using this wizard.' There are three checkboxes: 'Enable FIDO Passkey Authentication', 'Enable Push Authentication', and 'Require Biometric Seed in Authenticator App'. At the bottom are buttons for '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

14. Choose whether the users are enabled for FIDO and/or Mobile Push authentication.

15. Click **Next**.

The screenshot shows the 'Add User Account Wizard' dialog box, titled 'Add User Account Wizard'. The main heading is 'FIDO usage instruction email', with a subtext: 'FIDO usage instructions can be emailed to the user using an HTML template.' There is a small icon of a person in the top right corner. Below the heading, there are two radio buttons: 'Don't output user details' (unselected) and 'Email user details' (selected). To the right of these radio buttons is the 'fido ALLIANCE' logo. Below the radio buttons, there is a text box labeled 'Send to Email Addresses:' with an empty input field. Below this text box is a checkbox labeled 'Use Secondary Email Address if available' (unchecked). Below the checkbox is a text box labeled 'Email HTML Template Path:' with the text 'C:\Program Files\Authlogics Authentication Server\Fidc' and a 'Browse...' button. At the bottom of the dialog box, there are three buttons: '< Back' (highlighted with a blue border), 'Next >', and 'Cancel'.

The screenshot shows the 'Add User Account Wizard' dialog box, titled 'Add User Account Wizard'. The main heading is 'Push usage instruction email', with a subtext: 'Push usage instructions can be emailed to the user using an HTML template.' There is a small icon of a person in the top right corner. Below the heading, there are two radio buttons: 'Don't output user details' (unselected) and 'Email user details' (selected). Below the radio buttons, there is a text box labeled 'Send to Email Addresses:' with an empty input field. Below this text box is a checkbox labeled 'Use Secondary Email Address if available' (unchecked). Below the checkbox is a text box labeled 'Email HTML Template Path:' with the text 'C:\Program Files\Authlogics Authentication Server\Pus' and a 'Browse...' button. At the bottom of the dialog box, there are three buttons: '< Back', 'Next >', and 'Cancel' (highlighted with a blue border).

16. Choose if or how the users receive their welcome email.

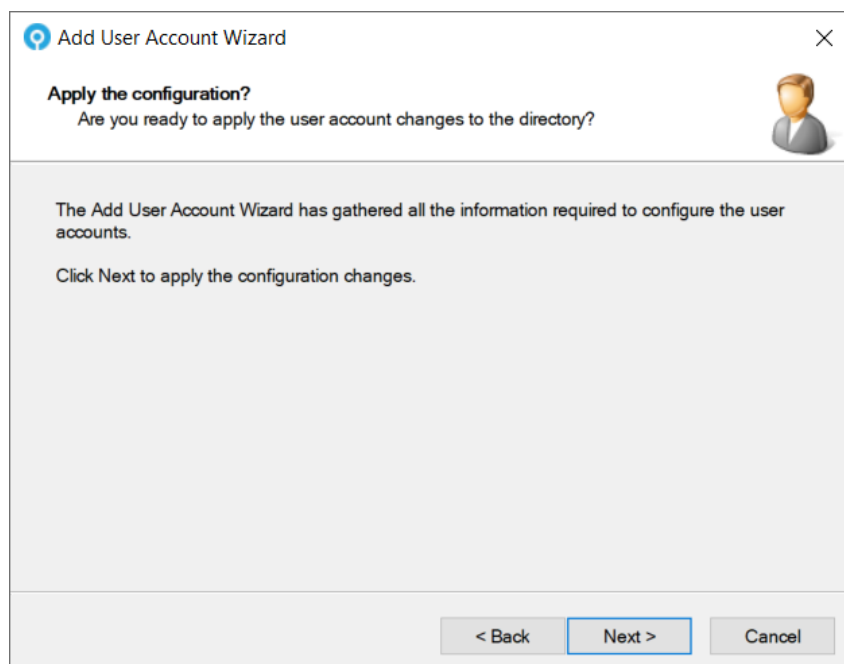
The welcome email contains instructions on how to set up their device for FIDO and Mobile Push based on your selection above.

If a single user is selected, you can specify the email address to which you want to send the email.

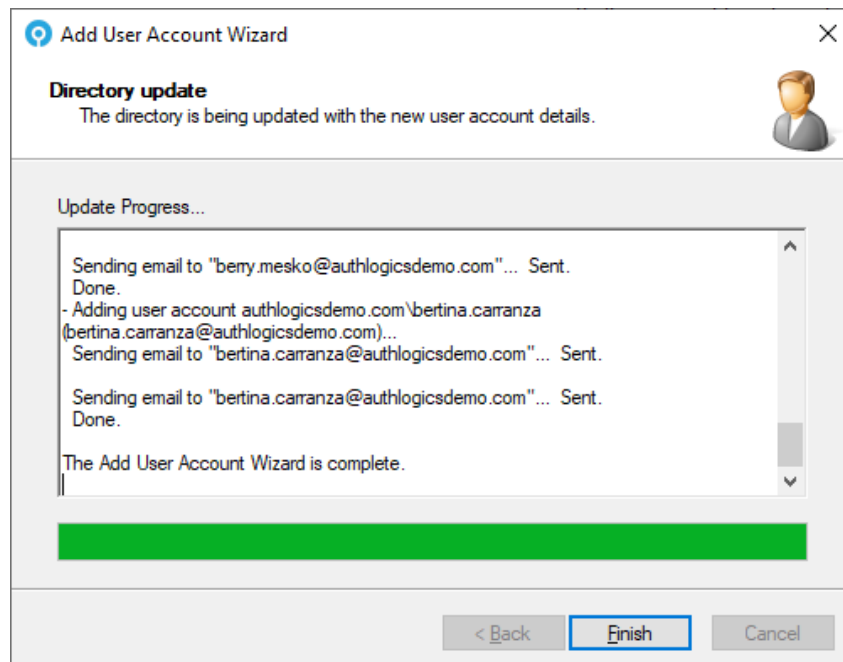
When adding multiple users, the user's email address is retrieved from Active Directory or the alternate email address field and sent to them automatically.

The appropriate FIDO and PUSH HTML template files can be selected to use for the email.

17. Click **Next**.

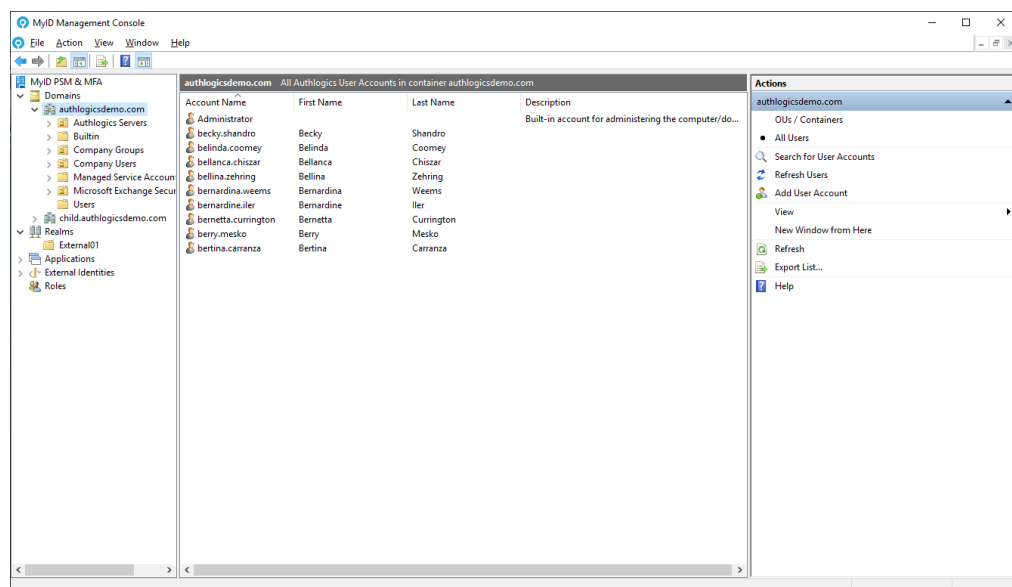


18. Click **Next**.



The new user accounts have been created.

19. Click **Finish**.

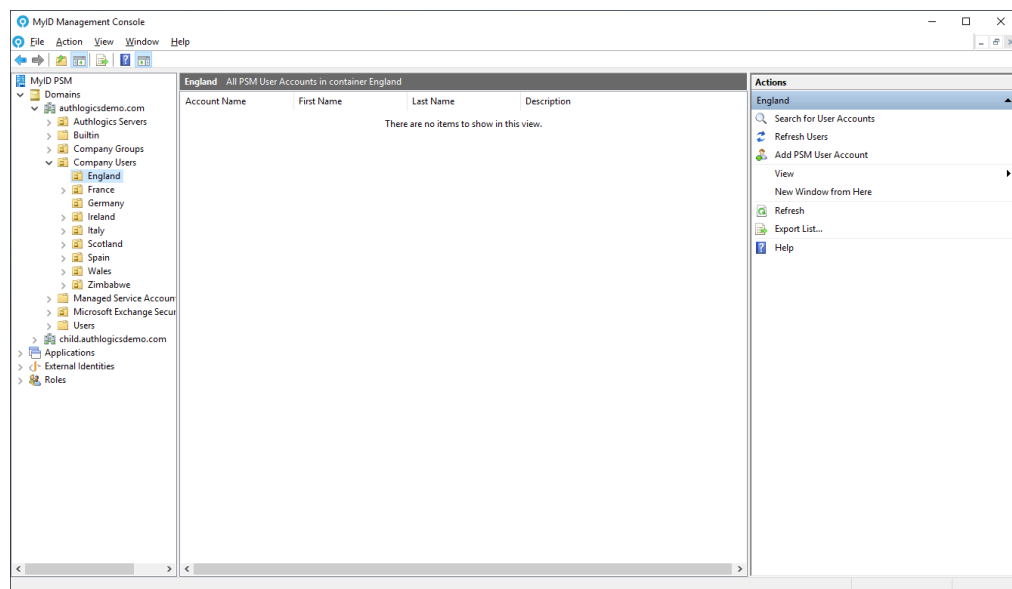


5.8.4 Adding a new MyID PSM user account

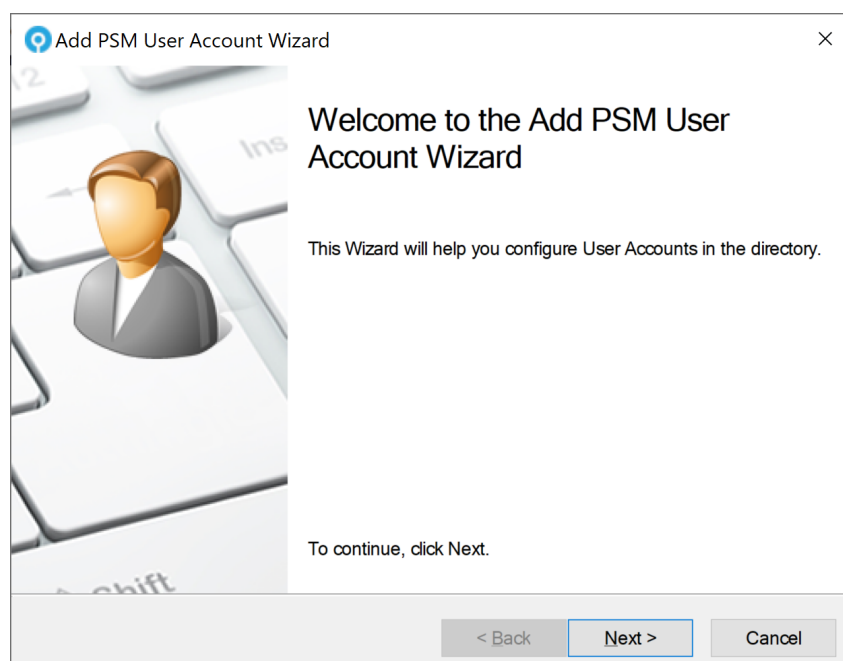
PSM user accounts can be manually added if required, however PSM users automatically appear in the MMC when a user changes their password or logs onto the Self Service Portal.

1. In the MyID Management Console, expand the **Domains** and select the appropriate domain.

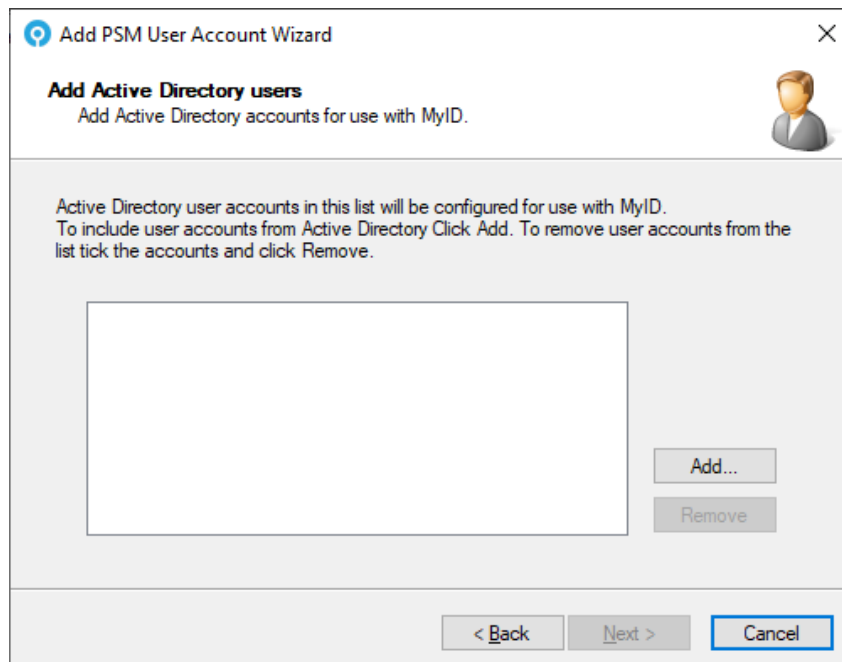
You can expand the list of OUs to see what accounts already exist.



2. Click **Add PSM User Account**, in the **Actions** pane.

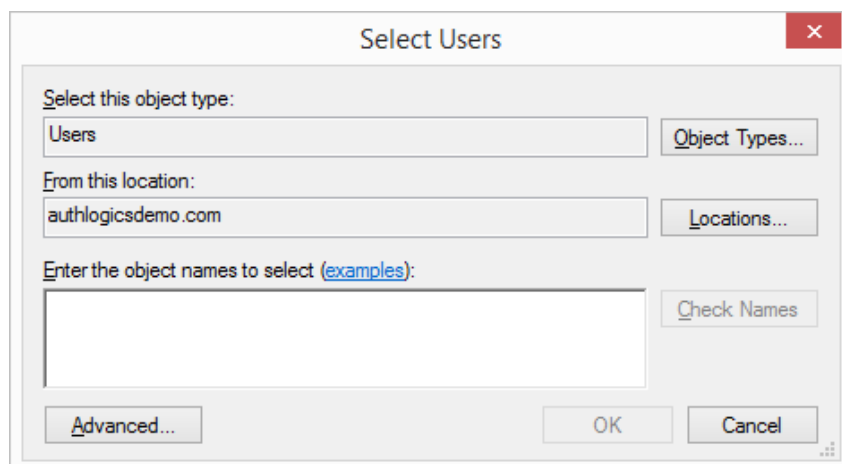


3. Click **Next**.



4. To add existing Active Directory users, click **Add**.

Note: This process does not create user accounts in the Active Directory Domain, it simply adds MyID metadata to an *existing* account. Ensure that the domain accounts exist before adding them to the MyID MMC.



5. Click **Advanced**.

Select Users

Select this object type:
Users

From this location:
England

Common Queries

Name: Starts with

Description: Starts with

☐ Disabled accounts

☐ Non expiring password

Days since last logon:

Find Now

Search results:

Name	E-Mail Address	In Folder
Adrianna Cancini	adrianna.cancini@authlogi...	authlogicsdemo.com/Company User
Ame Threats	ame.threats@authlogicsde...	authlogicsdemo.com/Company User
Anny Larason	anny.larason@authlogicsd...	authlogicsdemo.com/Company User
Arabela Waman	arabela.waman@authlogi...	authlogicsdemo.com/Company User
Ardenia Ruchi	ardenia.ruchi@authlogicsd...	authlogicsdemo.com/Company User
Arluene Feigenbaum	arluene.feigenbaum@authl...	authlogicsdemo.com/Company User
Arly Uzdygan	arly.uzdygan@authlogicsd...	authlogicsdemo.com/Company User
Athene Grieshaber	athene.grieshaber@authlo...	authlogicsdemo.com/Company User
Auberta Crisco	auberta.crisco@authlogics...	authlogicsdemo.com/Company User

6. Click **Find Now**.7. Select the required users from Active Directory and click **OK**.

Select Users

Select this object type:
Users

From this location:
England

Enter the object names to select (examples):

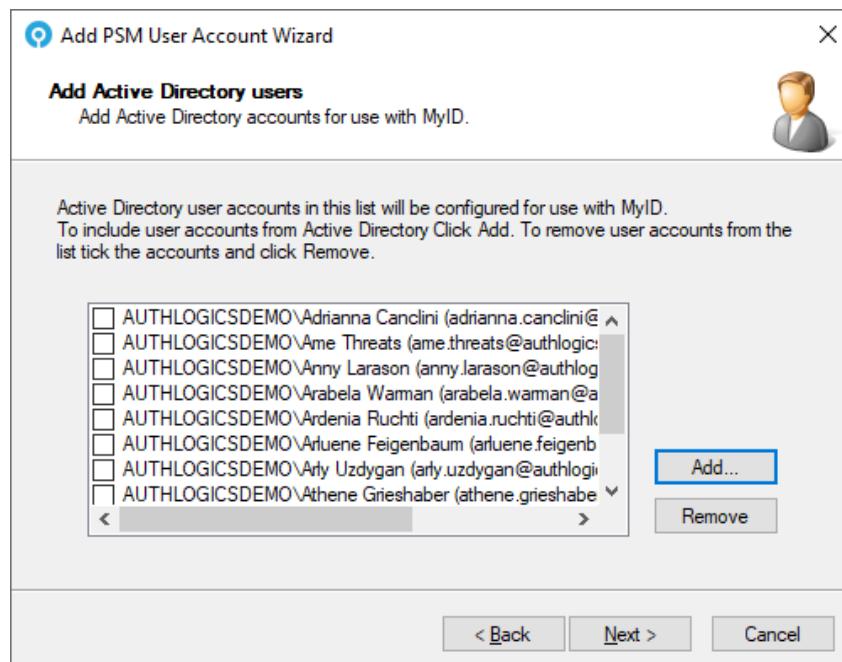
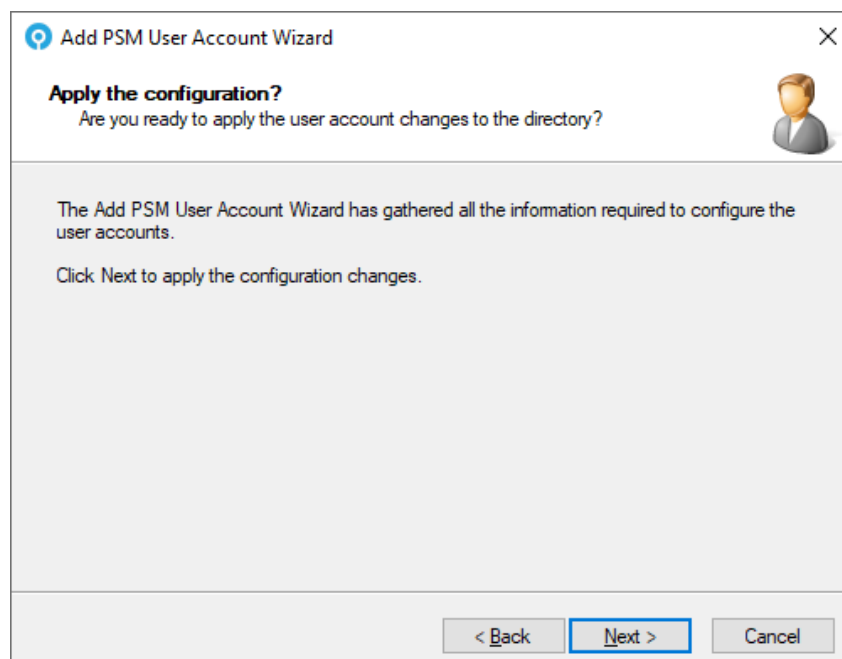
Arly Uzdygan (arly.uzdygan@authlogicsdemo.com);
Athene Grieshaber (athene.grieshaber@authlogicsdemo.com);
Auberta Crisco (auberta.crisco@authlogicsdemo.com)

Check Names

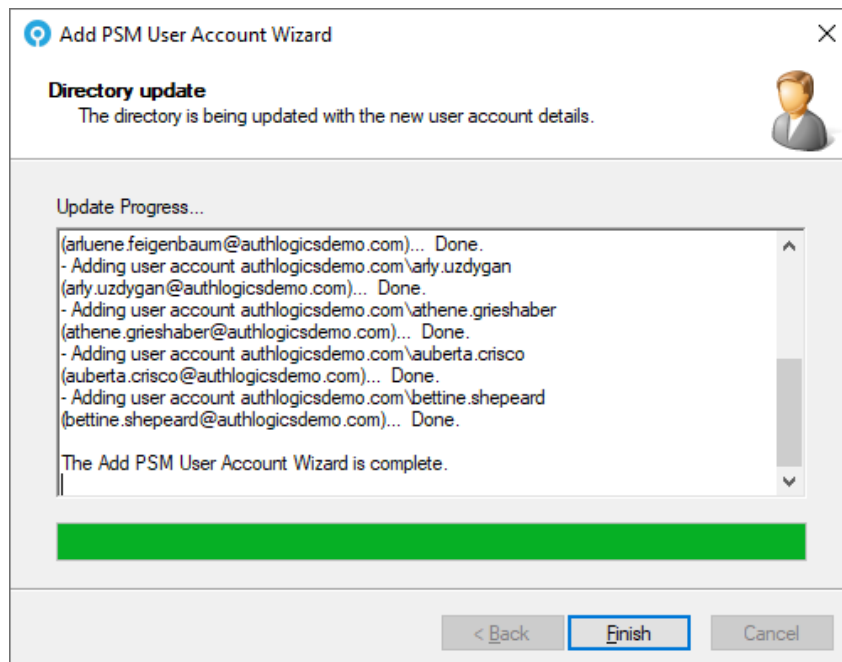
Advanced... OK Cancel

8. Click **OK**.

To remove accounts from the list, check the box next to the name and click **Remove**.

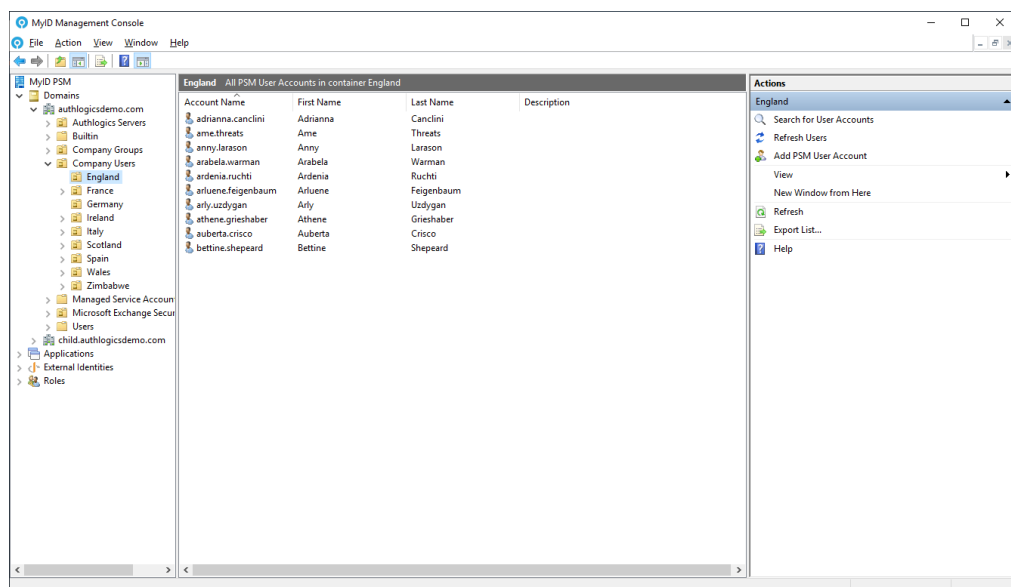
9. Click **Next**.

10. Click **Next**.



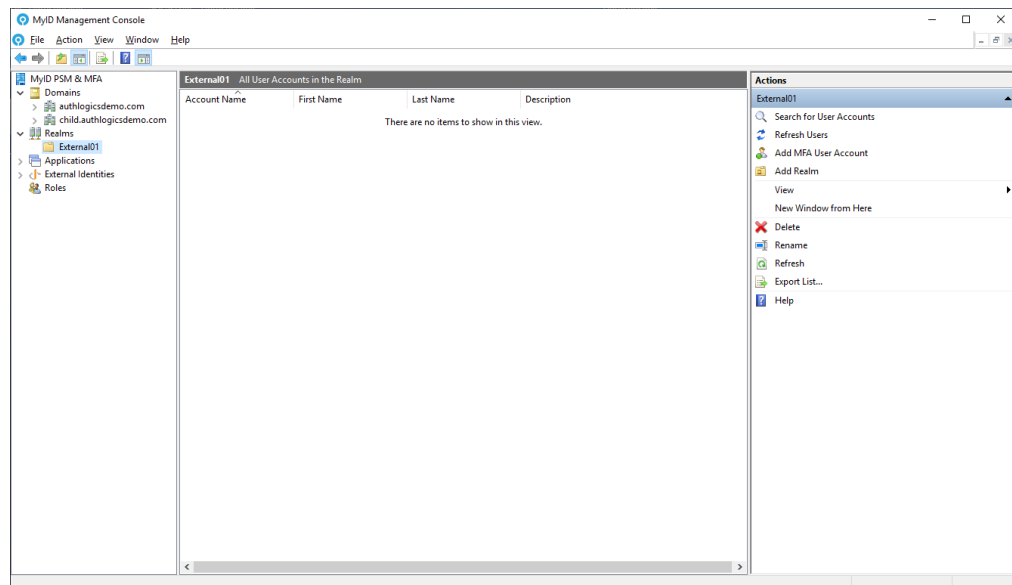
The new user accounts have been created.

11. Click **Finish**.

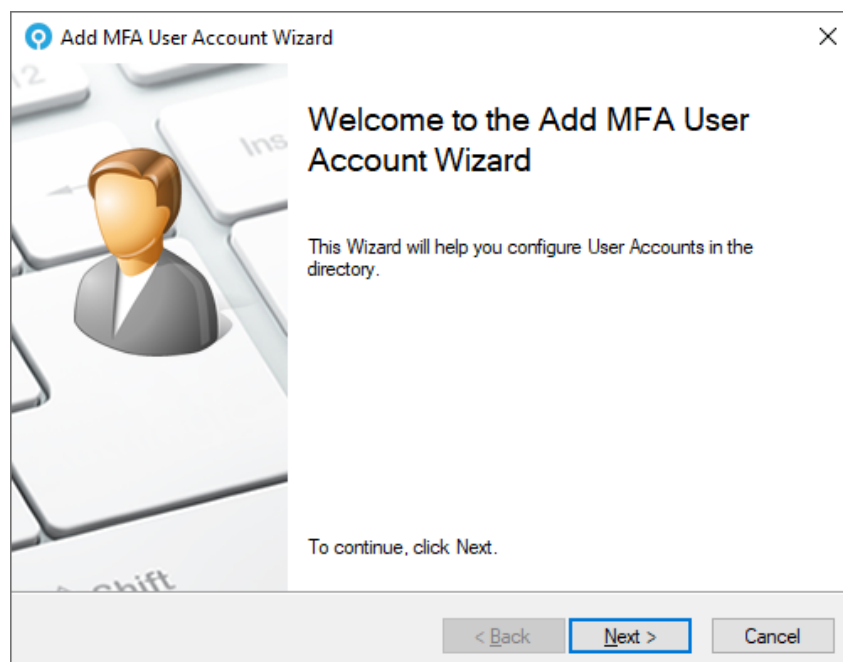


5.8.5 Adding a new external MFA user account

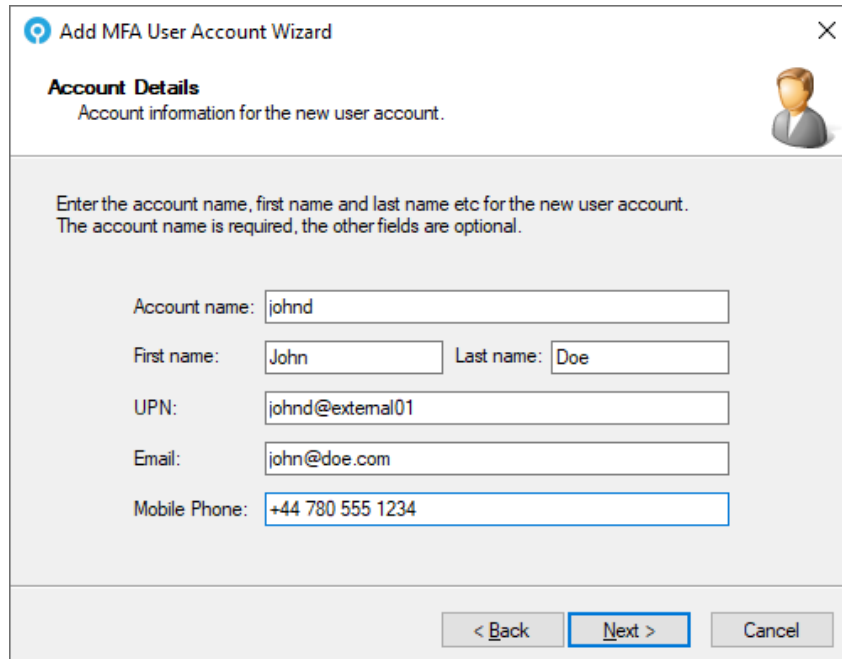
1. In the MyID Management Console, expand the **Realms** and select the appropriate realm.



2. Click **Add MFA User Account**, in the **Actions** pane.



3. Click **Next**.



Add MFA User Account Wizard

Account Details
Account information for the new user account.

Enter the account name, first name and last name etc for the new user account.
The account name is required, the other fields are optional.

Account name: johnd

First name: John Last name: Doe

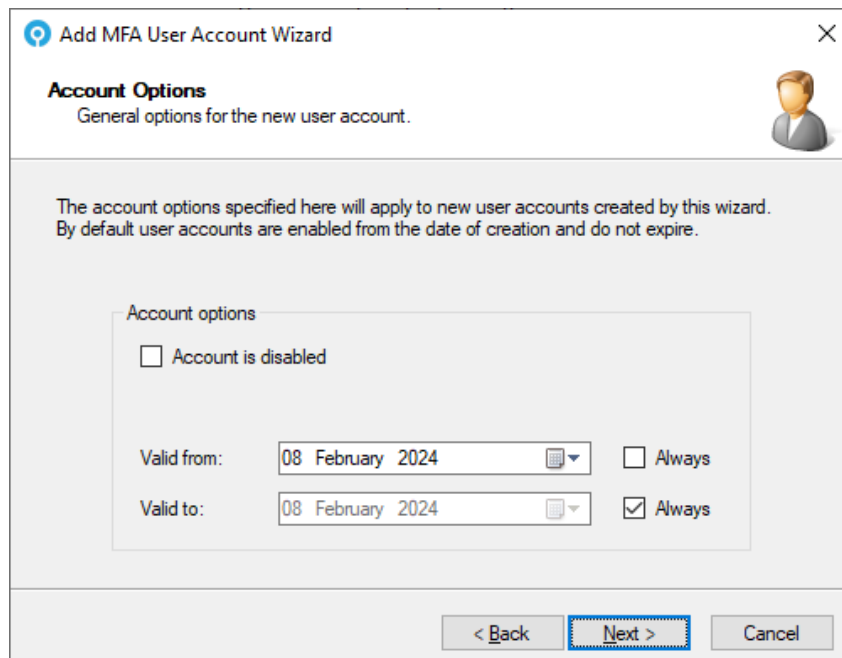
UPN: johnd@external01

Email: john@doe.com

Mobile Phone: +44 780 555 1234

< Back **Next >** Cancel

4. Enter the details for the new user account.
Only the **Account name** is required, all other fields are optional.
The UPN is automatically generated based on the **Realm** and **Account name**; however, it may be manually edited as needed.
5. Click **Next**.



Add MFA User Account Wizard

Account Options
General options for the new user account.

The account options specified here will apply to new user accounts created by this wizard.
By default user accounts are enabled from the date of creation and do not expire.

Account options

☐ Account is disabled

Valid from: 08 February 2024 ☐ Always

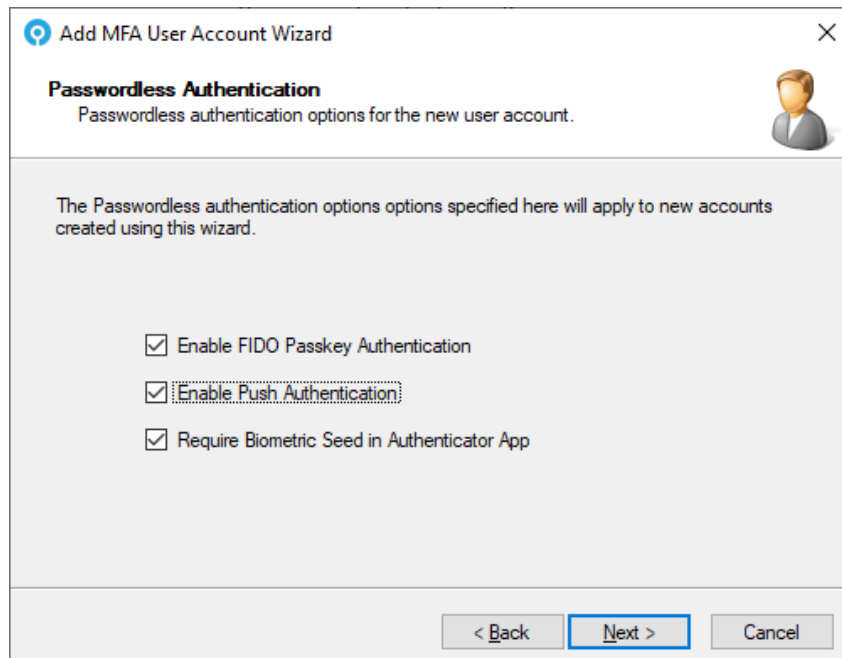
Valid to: 08 February 2024 ☒ Always

< Back **Next >** Cancel

6. Set the account options.

Account options determine the user's initial state. Accounts can be given the start and end validity dates and can be created as disabled accounts for later use.

7. Click **Next**.

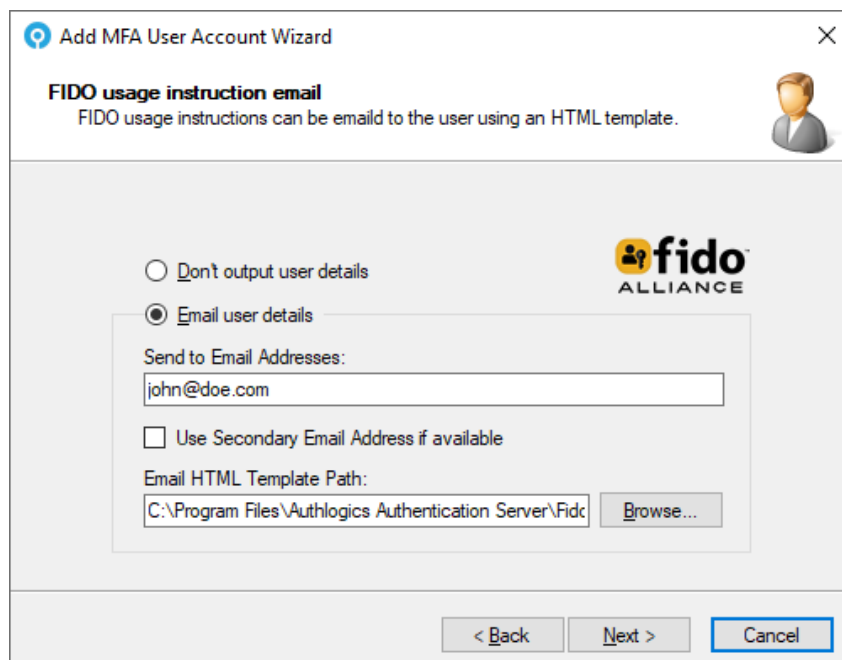


The screenshot shows the 'Add MFA User Account Wizard' dialog box, specifically the 'Passwordless Authentication' step. The title bar says 'Add MFA User Account Wizard'. Below the title, it says 'Passwordless Authentication' and 'Passwordless authentication options for the new user account.' There is a user icon on the right. The main text says: 'The Passwordless authentication options specified here will apply to new accounts created using this wizard.' Below this, there are three checked checkboxes: 'Enable FIDO Passkey Authentication', 'Enable Push Authentication', and 'Require Biometric Seed in Authenticator App'. At the bottom, there are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

8. Choose whether to enable the users for FIDO and/or Mobile Push authentication.

At this stage, you can force Mobile App users to provide Biometric information as part of the authentication process.

9. Click **Next**.



The screenshot shows the 'Add MFA User Account Wizard' dialog box, specifically the 'FIDO usage instruction email' step. The title bar says 'Add MFA User Account Wizard'. Below the title, it says 'FIDO usage instruction email' and 'FIDO usage instructions can be email to the user using an HTML template.' There is a user icon on the right. The main text says: 'FIDO usage instructions can be email to the user using an HTML template.' Below this, there are two radio buttons: 'Don't output user details' and 'Email user details' (selected). To the right of the radio buttons is the 'fido ALLIANCE' logo. Below the radio buttons, there is a text box labeled 'Send to Email Addresses:' containing 'john@doe.com'. Below this, there is a checkbox labeled 'Use Secondary Email Address if available'. Below the checkbox, there is a text box labeled 'Email HTML Template Path:' containing 'C:\Program Files\Authlogics Authentication Server\Fido' and a 'Browse...' button. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel' (highlighted with a blue border).

10. Choose if or how the users receive their welcome email.

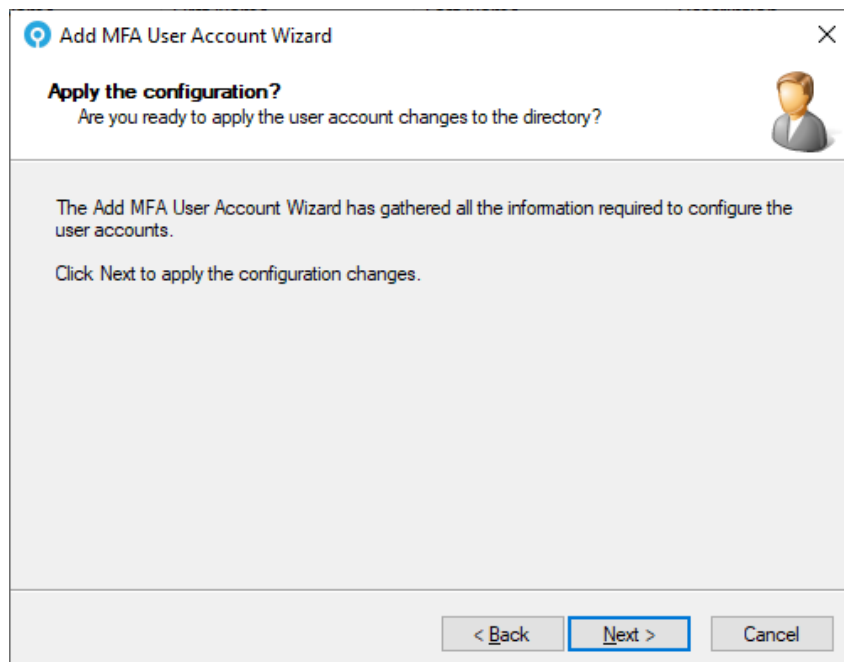
The welcome email contains instructions on how to set up their device for FIDO and Mobile Push based on your selection above.

If a single user is selected, you can specify the email address to which you want to send the email.

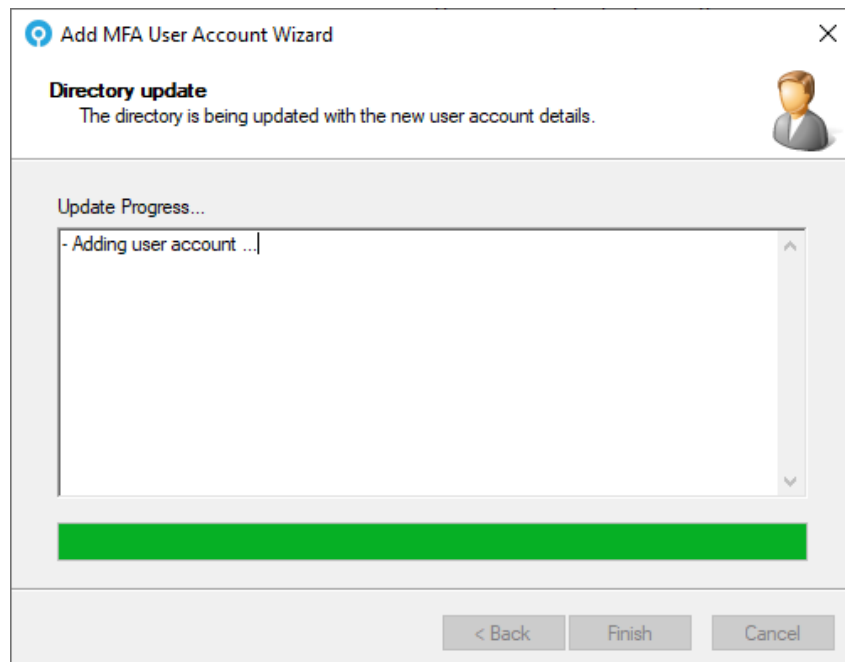
When adding multiple users, the user's email address is retrieved from Active Directory or the alternate email address field and sent to them automatically.

The appropriate FIDO and PUSH HTML template files can be selected to use for the email.

11. Click **Next**.

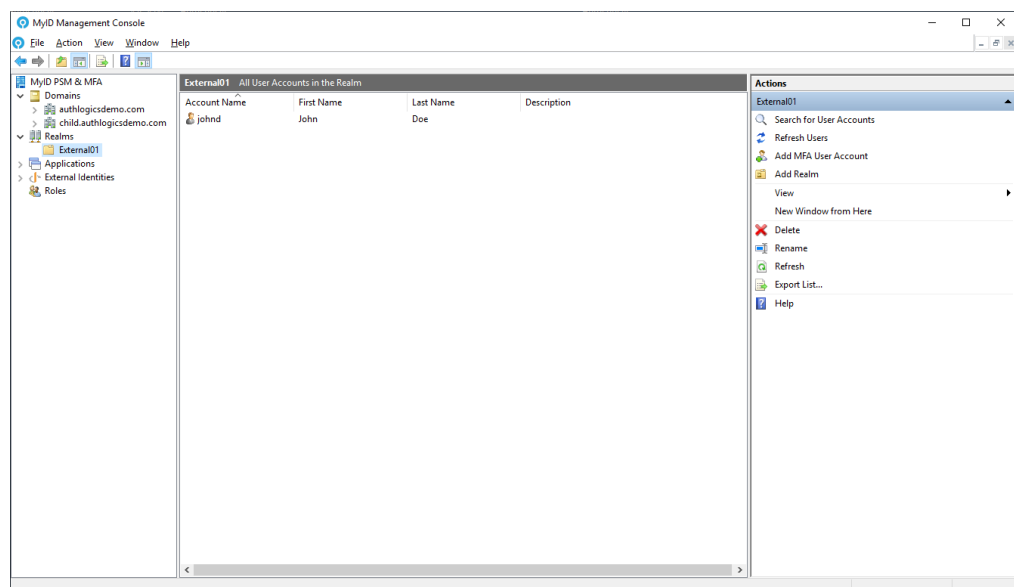


12. Click **Next**.



The new user account is created.

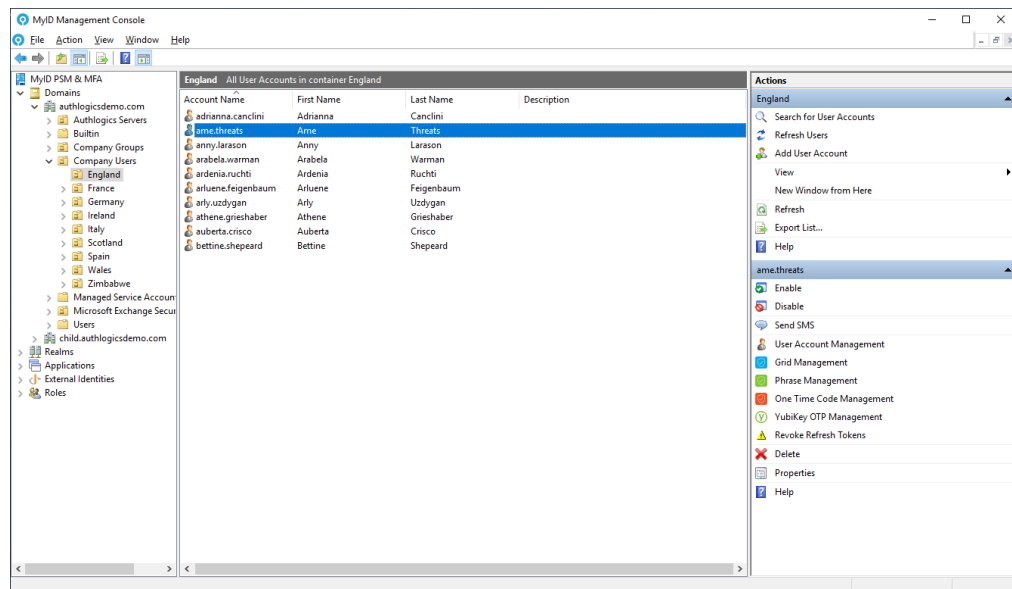
13. Click **Finish**.



5.8.6 Setting up a user for Grid Pattern Authentication

Once you have created a MyID user account, you can configure it for use with Grid Pattern Authentication.

1. In the MyID Management Console, either expand the **Domains** and select the appropriate OU, or expand the **Realms** and select the appropriate realm.
2. Select the user account (or accounts) for which you want to manage the Grid settings.



3. Click **Grid Management**, in the **Actions** pane, or from right-clicking the account (or accounts).



4. Click **Next**.

The screenshot shows a window titled "Grid User Management Wizard" with a close button (X) in the top right corner. The main heading is "Grid Pattern creation method" followed by the question "What size and method do you wish to use to create a new Grid Pattern for the user?". Below this, a text box explains: "A new Pattern can be automatically generated or the administrator can manually specify a Pattern for the user. A generated Pattern will be created that matches policy using either a 6x6 or 8x8 grid." There are two radio button options: "Manually Specified Pattern" and "Automatically Generate Pattern", with the latter being selected. A checkbox labeled "Generate Pattern that matches policy" is checked. Below these is a "Grid Size" section with four radio button options: "4 X 4 Grid", "5 X 5 Grid" (selected), "6 X 6 Grid", and "8 X 8 Grid". At the bottom right are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

5. Choose the Pattern provisioning method for the selected users:
- **Manually Specified Pattern** – the administrator can choose to specify the user's Pattern manually.
 - **Automatically Generate Pattern** – MyID MFA generates a random Pattern for each user. This is the default option.

Also by default, MyID MFA generates a complex pattern for the user that matches the grid policy. You can deselect the **Generate Pattern that matches policy** option to generate a simple pattern instead, although this is not recommended.

If you are applying these settings to multiple accounts simultaneously, only the **Automatically Generate Pattern** option is available.

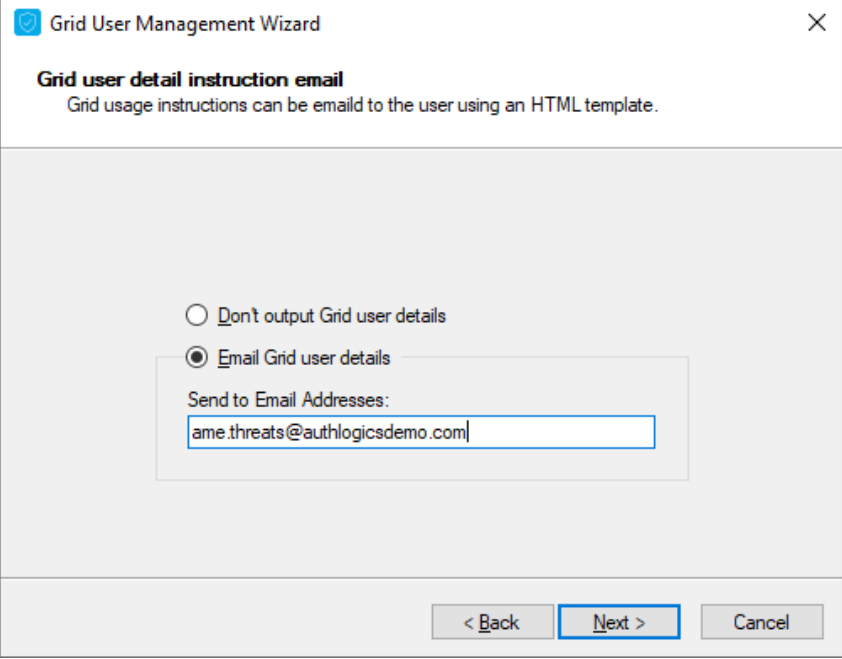
6. Set the **Grid Size** for the selected users. You can choose from the following options:
- **4 X 4 Grid**
 - **5 X 5 Grid**
 - **6 X 6 Grid**
 - **8 X 8 Grid**

The options available depend on the grid sizes allowed; for information on setting the **Allowed grid sizes**, see section [5.3.12, Grid Options tab](#).

If the user has had a Grid Pattern, the **Grid Size** defaults to the same as their previous grid. If the user has not had a Grid Pattern before, then by default the 5 x 5 grid is selected; you are recommended to use the 5 x 5 grid, as it is more secure. 6 x 6 and 8 x 8 grids are larger, but allow only numeric characters, while 4 x 4 and 5 x 5 grids allow alphanumeric characters. If the 5 x 5 grid is not available, the smallest grid size available is selected.

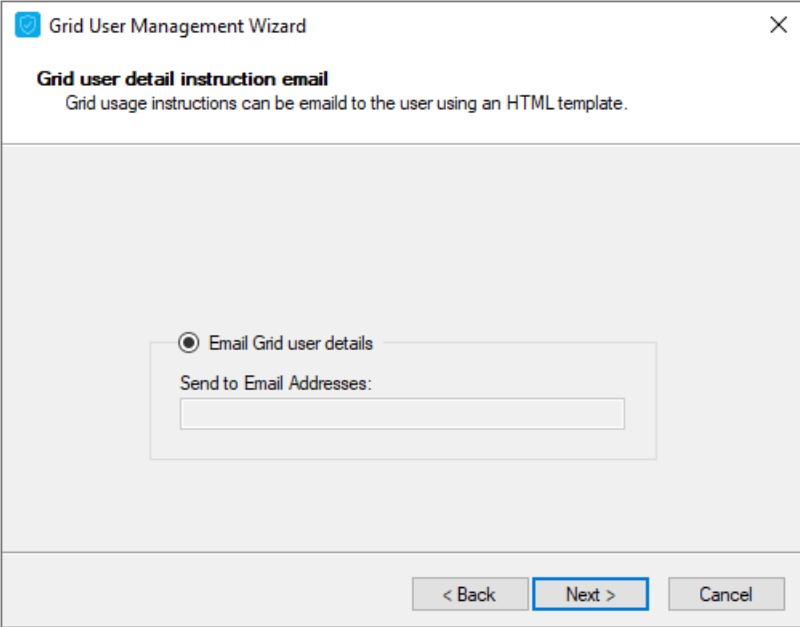
7. Click **Next**.

If you have a single user selected, you can specify the email address to which you want to send the email:



The dialog box is titled "Grid User Management Wizard" and has a close button (X) in the top right corner. Below the title bar, the text "Grid user detail instruction email" is displayed, followed by the subtitle "Grid usage instructions can be emailed to the user using an HTML template." The main content area contains two radio buttons: "Don't output Grid user details" (unselected) and "Email Grid user details" (selected). Below the radio buttons is a text input field labeled "Send to Email Addresses:" containing the email address "ame.threats@authlogicsdemo.com". At the bottom of the dialog are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

If you have multiple users selected, the user's email address is retrieved from Active Directory or the alternate email address field and sent to them automatically:



The dialog box is titled "Grid User Management Wizard" and has a close button (X) in the top right corner. Below the title bar, the text "Grid user detail instruction email" is displayed, followed by the subtitle "Grid usage instructions can be emailed to the user using an HTML template." The main content area contains two radio buttons: "Don't output Grid user details" (unselected) and "Email Grid user details" (selected). Below the radio buttons is a text input field labeled "Send to Email Addresses:" which is currently empty. At the bottom of the dialog are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

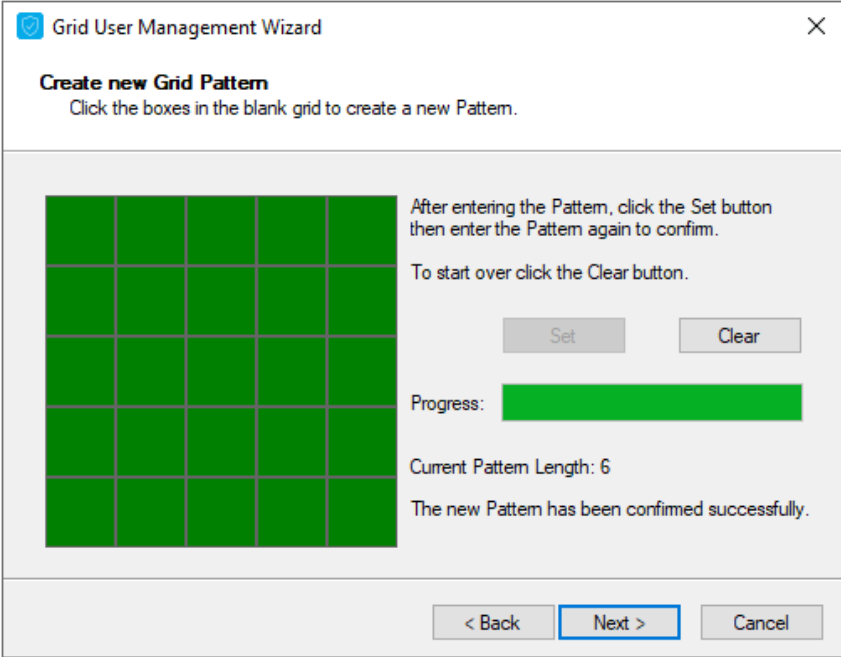
8. Select the method used to distribute the Pattern and grid usage instructions to the user.
Auto-generated information can be emailed to the user. Additionally, if you provide manually specified settings, you can specify not to output any details; this option is not available for auto-generated details.
You can send the email to multiple addresses by entering multiple email addresses separated by a semi-colon (;).
9. Click **Next**.
10. If you are manually specifying a pattern:
 - a. Enter the required pattern.

The screenshot shows a dialog box titled "Grid User Management Wizard" with a close button (X) in the top right corner. Below the title bar, the text "Create new Grid Pattern" is displayed, followed by the instruction "Click the boxes in the blank grid to create a new Pattern." The main area contains a 5x5 grid of colored squares. The colors are: Row 1: Red, Orange, Blue, Blue, Light Blue; Row 2: Orange, Red, Grey, Light Blue, Blue; Row 3: Orange, Grey, Grey, Grey, Green; Row 4: Yellow, Yellow, Grey, Green, Green; Row 5: Yellow, Yellow, Yellow, Green, Green. To the right of the grid, there is instructional text: "After entering the Pattern, click the Set button then enter the Pattern again to confirm." and "To start over click the Clear button." Below this text are two buttons: "Set" and "Clear". A progress bar is shown with the label "Progress:" and a green bar that is approximately 60% full. Below the progress bar, the text "Current Pattern Length: 6" and "Minimum Pattern Length: 6" is displayed. At the bottom of the dialog box, there are three buttons: "< Back", "Next >", and "Cancel".

Note: Which boxes are available depends on the size of grid selected.

- b. Click **Set**.

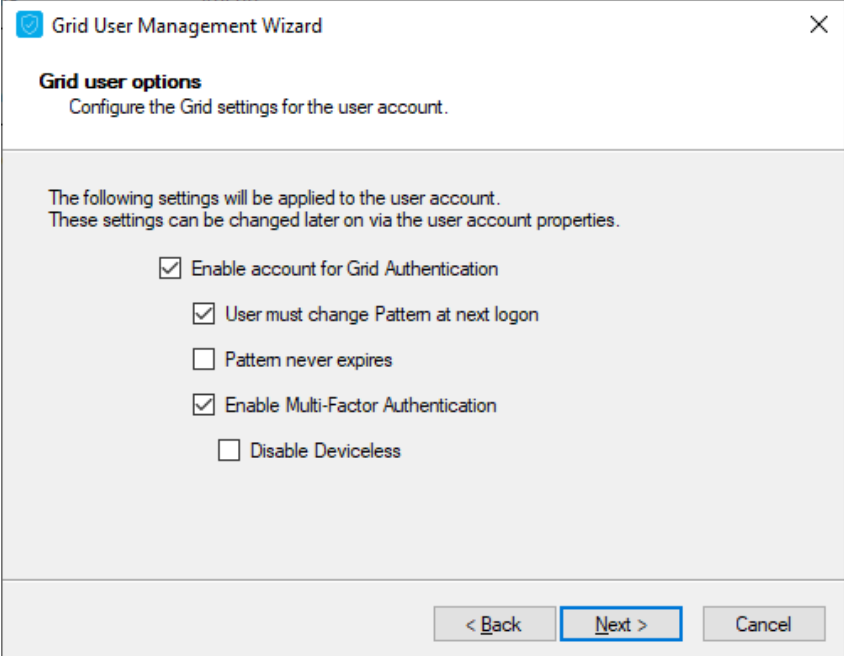
- c. Confirm the Pattern entered previously.



The screenshot shows the 'Grid User Management Wizard' window with the 'Create new Grid Pattern' step. It features a 5x5 grid of green boxes. To the right of the grid, there is instructional text: 'After entering the Pattern, click the Set button then enter the Pattern again to confirm. To start over click the Clear button.' Below this text are 'Set' and 'Clear' buttons. A progress bar is shown with the label 'Progress:'. Below the progress bar, it says 'Current Pattern Length: 6' and 'The new Pattern has been confirmed successfully.' At the bottom of the window are '< Back', 'Next >', and 'Cancel' buttons.

If the patterns match, the displayed grid turns green. If the patterns do not match, the grid turns red.

- d. Click **Clear** to re-enter the pattern or click **Next** to continue.

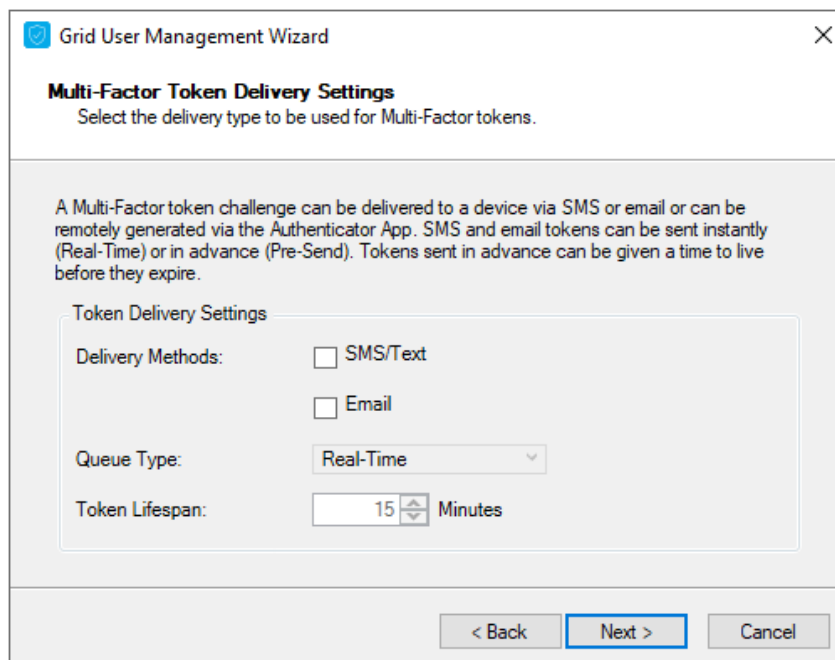


The screenshot shows the 'Grid User Management Wizard' window with the 'Grid user options' step. It features a list of settings to be applied to the user account. The settings are: 'Enable account for Grid Authentication' (checked), 'User must change Pattern at next logon' (checked), 'Pattern never expires' (unchecked), 'Enable Multi-Factor Authentication' (checked), and 'Disable Deviceless' (unchecked). At the bottom of the window are '< Back', 'Next >', and 'Cancel' buttons.

11. Configure the Grid pattern user options:

- You can specify whether the account is enabled for Grid Patterns authentication by selecting or deselecting **Enable account for Grid authentication**.
- You can set a user's Pattern to expire the next time that they log in, forcing them to change the pattern, by selecting **User must change Pattern at next login**.
- You can also set a user's Pattern to never expire by selecting **Pattern never expires**.
- You can enable the user for multi-factor authentication for Grid Patterns by selecting **Enable Multi-Factor authentication**.
- You can enforce the user account to use a Multi-Factor device by selecting **Disable Deviceless**. An MFA device must be registered with the user account, otherwise the challenge delivered through email or SMS/TEXT fails.
- You can view the **Grid Size**.

12. Click **Next**.



The screenshot shows a 'Grid User Management Wizard' window with a close button (X) in the top right corner. The title bar reads 'Grid User Management Wizard'. The main heading is 'Multi-Factor Token Delivery Settings' with a subtitle 'Select the delivery type to be used for Multi-Factor tokens.' Below this is a descriptive paragraph: 'A Multi-Factor token challenge can be delivered to a device via SMS or email or can be remotely generated via the Authenticator App. SMS and email tokens can be sent instantly (Real-Time) or in advance (Pre-Send). Tokens sent in advance can be given a time to live before they expire.' Under the heading 'Token Delivery Settings', there are four configuration items: 'Delivery Methods' with checkboxes for 'SMS/Text' and 'Email'; 'Queue Type' with a dropdown menu set to 'Real-Time'; and 'Token Lifespan' with a spinner box set to '15' and the unit 'Minutes'. At the bottom right, there are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

13. Select the delivery method for Multi-Factor tokens. This is available only if you have enabled multi-factor authentication.

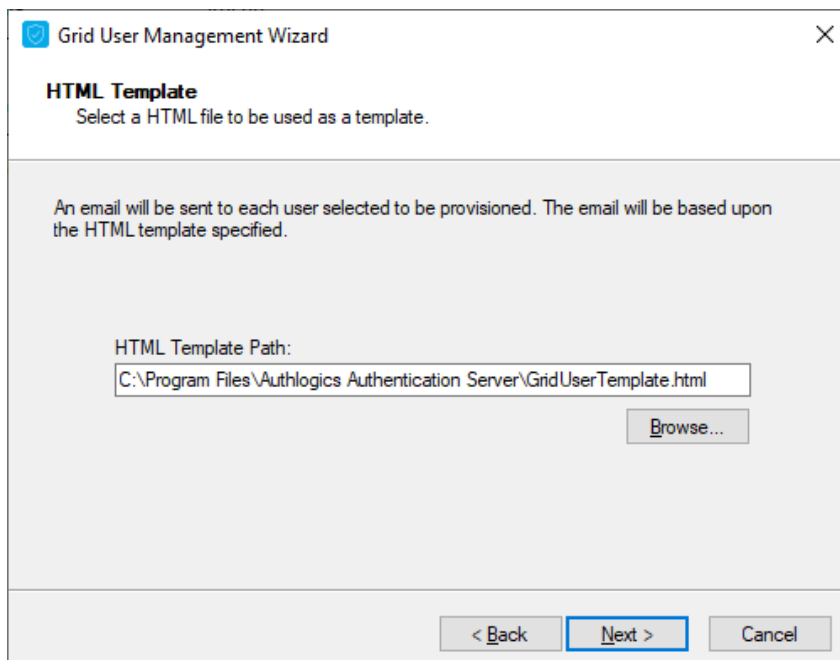
Users can always use their MyID Authentication app to receive any multi-factor authentication tokens for which they are configured, if the user has a device with the app configured.

You can select additional **Delivery Methods** of *SMS / Text* and *Email*. If you select one or more of these options, you must:

- Ensure that the user has a Mobile Number or an Email Address set to which the tokens can be sent.
- Set the **Queue Type**; choose if the Grid Patterns are sent only when requested (*Real-Time*) or if they are sent ahead of time (*Pre-Send*).

If you set the **Queue Type** to *Pre-Send*, you must specify the **Token Lifespan** for these token types; by default, the **Token Lifespan** is 1 day.

14. Click **Next**.



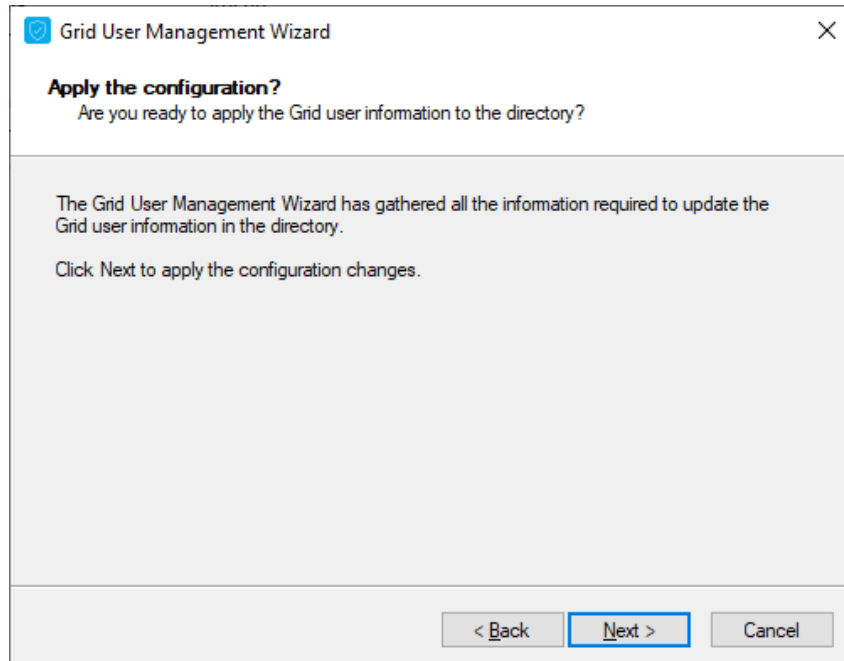
The screenshot shows a window titled "Grid User Management Wizard" with a close button in the top right corner. Below the title bar, the text "HTML Template" is displayed, followed by the instruction "Select a HTML file to be used as a template." A large text area contains the message: "An email will be sent to each user selected to be provisioned. The email will be based upon the HTML template specified." Below this, the label "HTML Template Path:" is followed by a text box containing the path "C:\Program Files\Authlogics Authentication Server\GridUserTemplate.html". To the right of the text box is a "Browse..." button. At the bottom of the window, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

15. Specify the **HTML Template Path** to the automated notification letter or email.

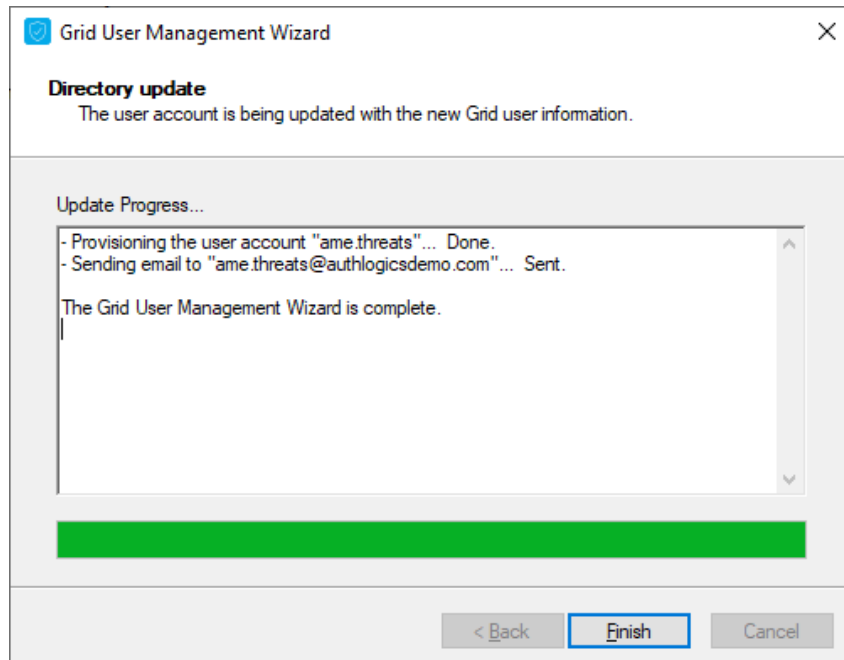
This HTML file can be modified and customized for your organization. Each letter or email is customized for the user to contain their unique information by substituting HTML comment values in the template.

To locate a custom template click **Browse**.

16. Click **Next**.



17. Click **Next**.

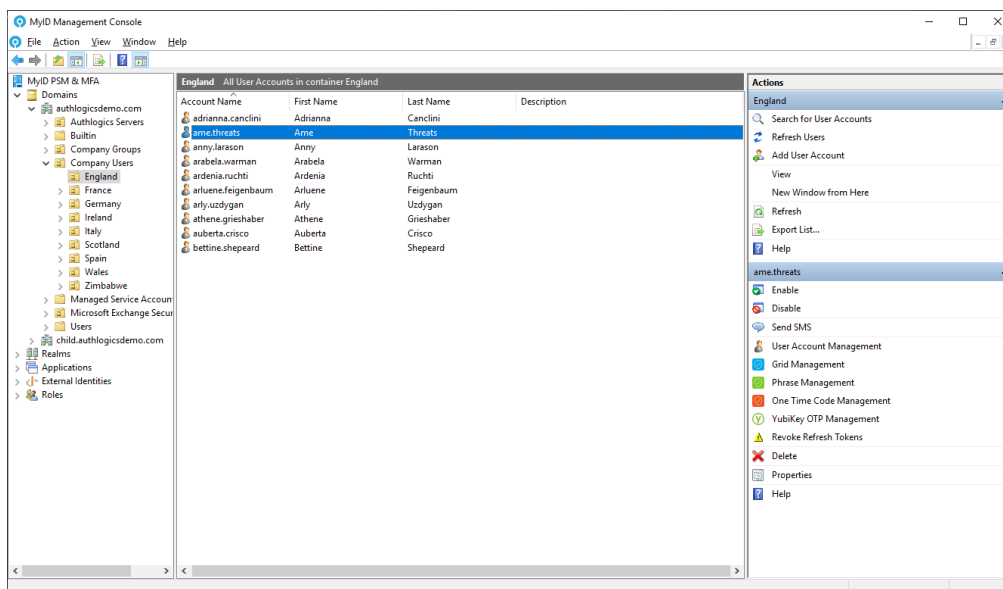


18. Click **Finish**.

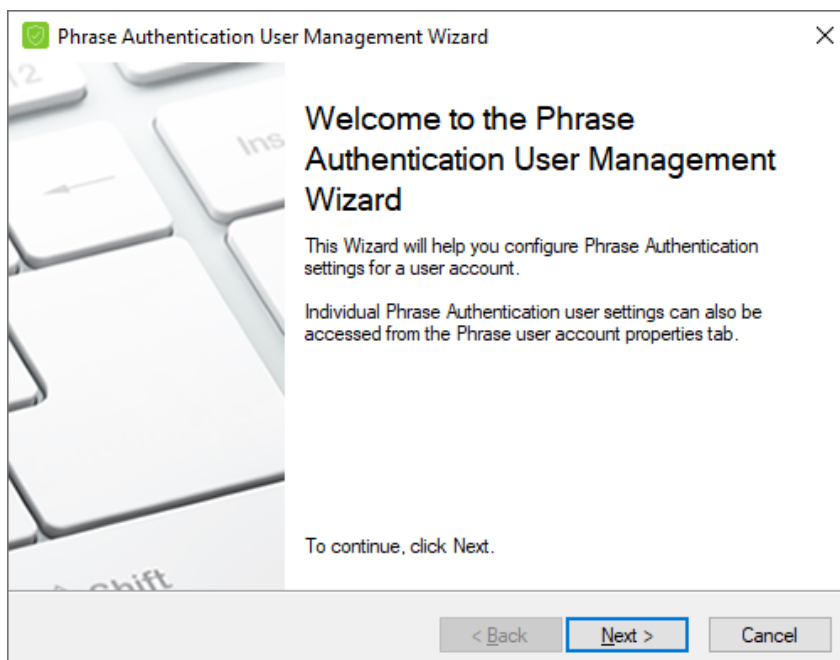
5.8.7 Setting up a user for Phrase authentication

Once you have created a MyID user account, you can configure it for use with Phrase Pattern Authentication.

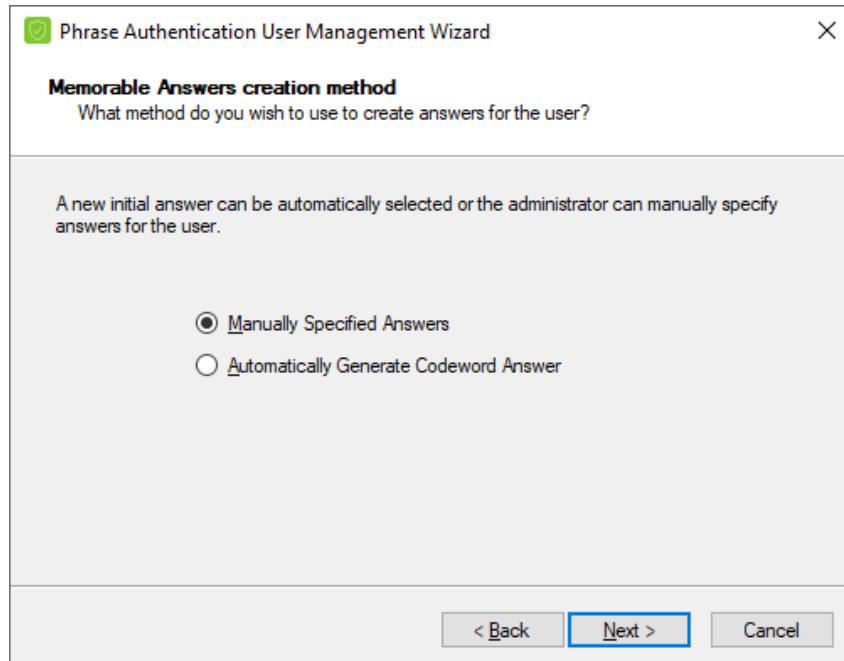
1. In the MyID Management Console, either expand the **Domains** and select the appropriate OU, or expand the **Realms** and select the appropriate realm.
2. Select the user account (or accounts) for which you want to manage the Phrase settings.



3. Click **Phrase Management**, in the **Actions** pane, or from right-clicking the account (or accounts).



4. Click **Next**.



The screenshot shows a dialog box titled "Phrase Authentication User Management Wizard" with a close button (X) in the top right corner. The main heading is "Memorable Answers creation method" followed by the question "What method do you wish to use to create answers for the user?". Below this, a text block states: "A new initial answer can be automatically selected or the administrator can manually specify answers for the user." There are two radio button options: "Manually Specified Answers" (which is selected) and "Automatically Generate Codeword Answer". At the bottom right, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

5. Choose the provisioning method.

You can set a user to get a randomly generated Codeword answer, or the administrator can choose to manually configure the user's information. If multiple accounts were selected before starting the wizard, only the automatic option is available.

6. Click **Next**.

Phrase Authentication User Management Wizard

Phrase Authentication user detail instruction email
Phrase usage instructions can be emailed to the user using an HTML template.

☐ Don't output Phrase user details

☒ Email Phrase user details

Send to Email Addresses:
ame.threats@authlogicsdemo.com

< Back Next > Cancel

Select the delivery method for Phrase settings and usage instructions.

Auto-generated information can be emailed to the user.

If you manually specified the settings, you can specify not to output any details – this option is not available for auto-generated details.

7. Click **Next**.

Phrase Authentication User Management Wizard

Memorable Answers
Complete the answers to the questions which are specific to the user.

Answer a minimum of 1 questions from the list below. Each answer must be at least 6 characters long. Note: All spaces will be removed.

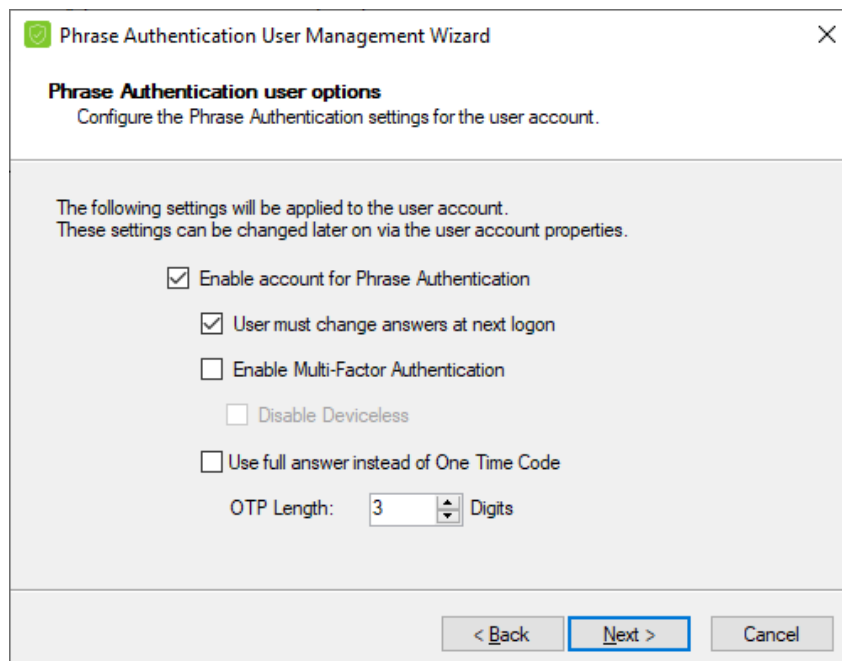
Question	Answer
Question: What is...	Answer:
your Codeword	SecretWord

< Back Next > Cancel

8. To specify the pattern manually, enter answers for the questions ensuring that each answer is at least the minimum number of prescribed characters and that enough questions have been answered.

The **Next** button appears only when these conditions are satisfied.

9. Click **Next**.



The screenshot shows a dialog box titled "Phrase Authentication User Management Wizard" with a close button (X) in the top right corner. Below the title bar, the text "Phrase Authentication user options" is displayed, followed by the instruction "Configure the Phrase Authentication settings for the user account." The main area of the dialog contains the following settings:

- A message: "The following settings will be applied to the user account. These settings can be changed later on via the user account properties."
- Five checkboxes:
 - ☒ Enable account for Phrase Authentication
 - ☒ User must change answers at next logon
 - ☐ Enable Multi-Factor Authentication
 - ☐ Disable Deviceless
 - ☐ Use full answer instead of One Time Code
- An "OTP Length" field with a value of "3" and a "Digits" label.

At the bottom of the dialog, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

10. Configure the Phrase Authentication user options.
 - You can specify whether the account is enabled for Phrase authentication by selecting or deselecting **Enable account for Phrase authentication**.
 - You can set the user's Phrase to expire the next time that they log in, forcing them to change the Phrase, by selecting **User must change answers at next logon**.
 - You can enable the user for multi-factor authentication for Phrases by selecting **Enable Multi-Factor authentication**.
 - You can require the user account to use a Multi-Factor device by selecting **Disable Deviceless**. An MFA device must be registered with the user account. If **Disable Deviceless** is not enabled, the challenge is delivered through email or SMS/TEXT.
 - You can either make the user use the whole Phrase when logging in by selecting **Use full answer instead of One Time Code**, or you can set how many characters of the Phrase the user is prompted for when logging in by setting the **OTP Length**. By default, this is 3 characters.

Note: As Phrases are not meant to be used like passwords in a true password-based system, **Use full answer instead of One Time Code** is disabled by default.

Set the **OTC Length** to the number of characters a user needs to provide from the predetermined answer.

11. Click **Next**.

The screenshot shows a window titled "Phrase Authentication User Management Wizard" with a close button (X) in the top right corner. Below the title bar, the section "Multi-Factor Token Delivery Settings" is displayed, followed by the instruction "Select the delivery type to be used for Multi-Factor tokens." A descriptive paragraph states: "A Multi-Factor token challenge can be delivered to a device via SMS or email. SMS and email tokens can be sent instantly (Real-Time) or in advance (Pre-Send). Tokens sent in advance can be given a time to live before they expire." Below this, the "Token Delivery Settings" section contains four fields: "Delivery Methods" with checkboxes for "SMS/Text" and "Email"; "Queue Type" with a dropdown menu currently set to "Real-Time"; and "Token Lifespan" with a numeric input set to "15" and a unit dropdown set to "Minutes". At the bottom of the window are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

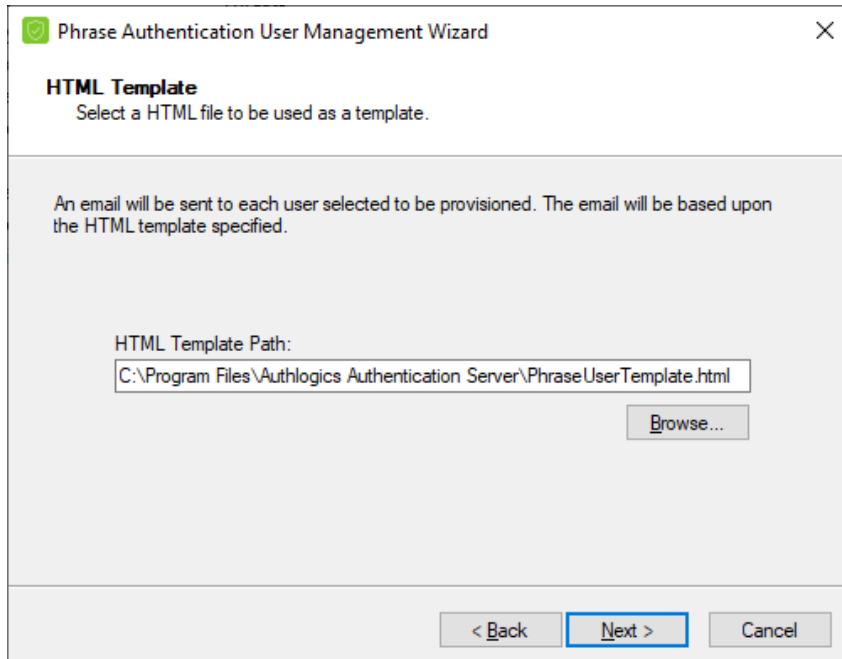
If you enabled the user for multi-factor authentication, you can select how the Phrase One Time Codes are delivered.

You can select additional **Delivery Methods** of `SMS / Text` and `Email`. If you select one or more of these options, you must:

- Ensure that the user has a Mobile Number or an Email Address set to which the tokens can be sent.
- Set the **Queue Type**; choose if the Phrase One Time Codes are sent only when requested (`Real-Time`) or if they are sent ahead of time (`Pre-Send`).

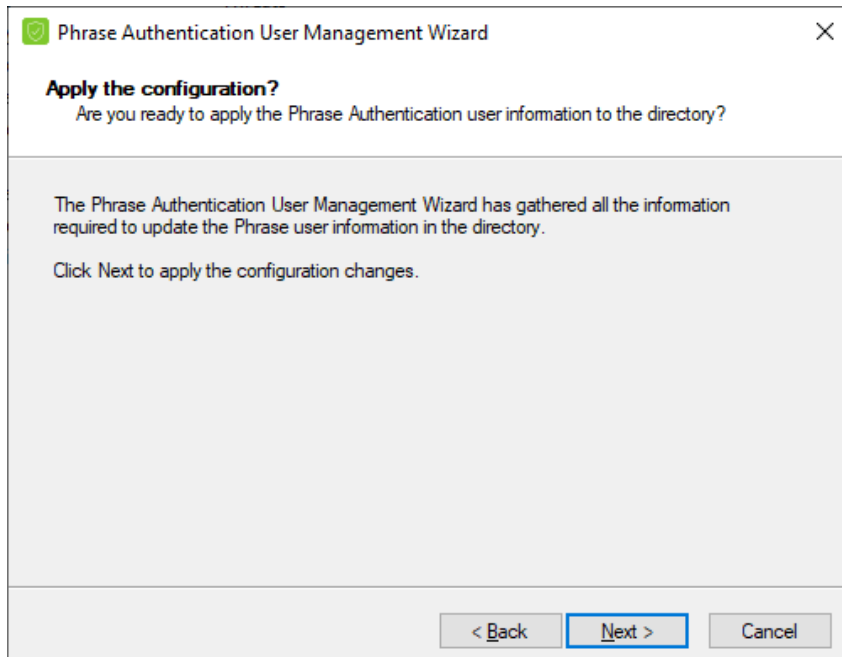
If you set the **Queue Type** to `Pre-Send`, you must specify the **Token Lifespan** for these token types; by default, the **Token Lifespan** is 1 day.

12. Click **Next**.



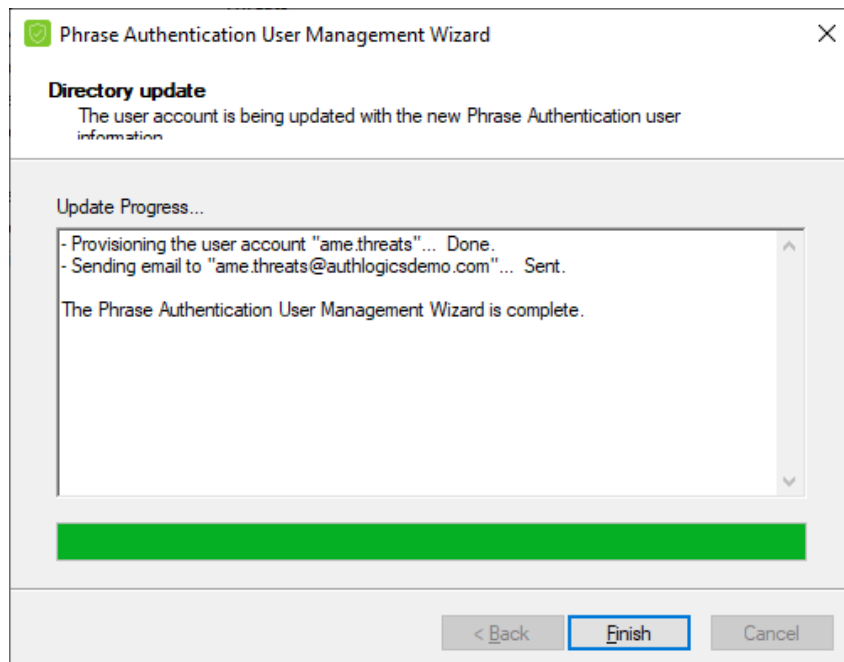
The screenshot shows the 'HTML Template' step of the 'Phrase Authentication User Management Wizard'. The window title is 'Phrase Authentication User Management Wizard'. The main heading is 'HTML Template' with the instruction 'Select a HTML file to be used as a template.' Below this, a message states: 'An email will be sent to each user selected to be provisioned. The email will be based upon the HTML template specified.' There is a text field labeled 'HTML Template Path:' containing the path 'C:\Program Files\Authlogics Authentication Server\PhraseUserTemplate.html'. To the right of the text field is a 'Browse...' button. At the bottom of the window are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

13. Specify the **HTML Template Path** to the automated notification letter or email.
This HTML file can be modified and customized for your organization. Each letter or email is customized for the user to contain their unique information by substituting HTML comment values in the template.
To locate a custom template click **Browse**.
14. Click **Next**.



The screenshot shows the 'Apply the configuration?' step of the 'Phrase Authentication User Management Wizard'. The window title is 'Phrase Authentication User Management Wizard'. The main heading is 'Apply the configuration?' with the question 'Are you ready to apply the Phrase Authentication user information to the directory?'. Below this, a message states: 'The Phrase Authentication User Management Wizard has gathered all the information required to update the Phrase user information in the directory. Click Next to apply the configuration changes.' At the bottom of the window are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

15. Click **Next**.



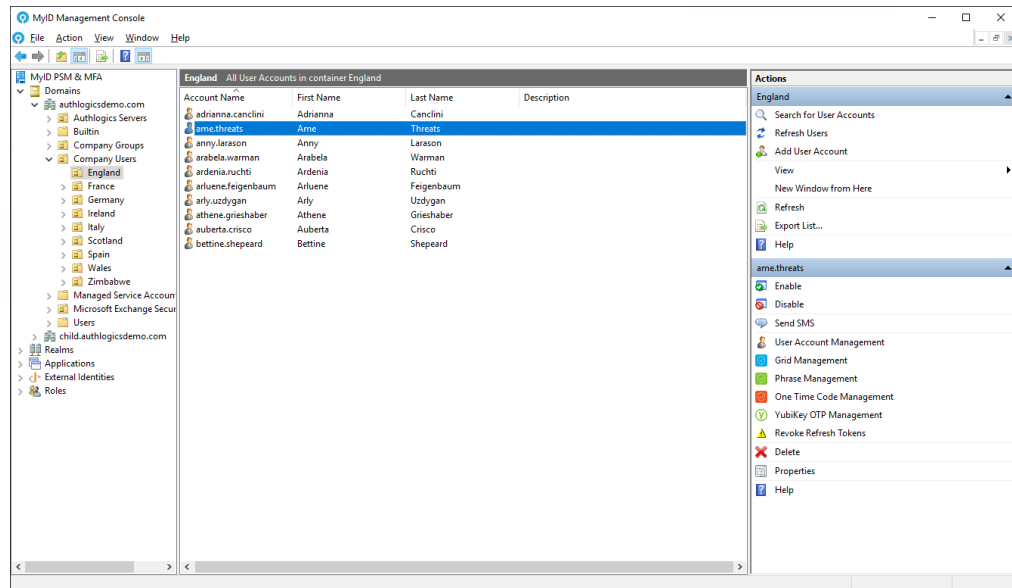
The configuration changes are applied.

16. Click **Finish**.

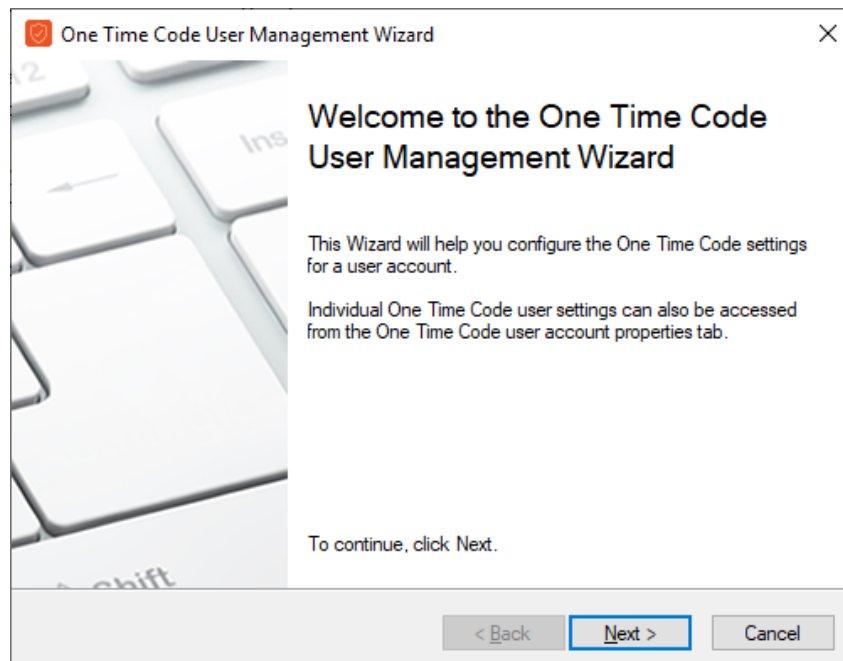
5.8.8 Setting up a user for One Time Code

Once you have created a MyID user account, you can configure it for use with One Time Code.

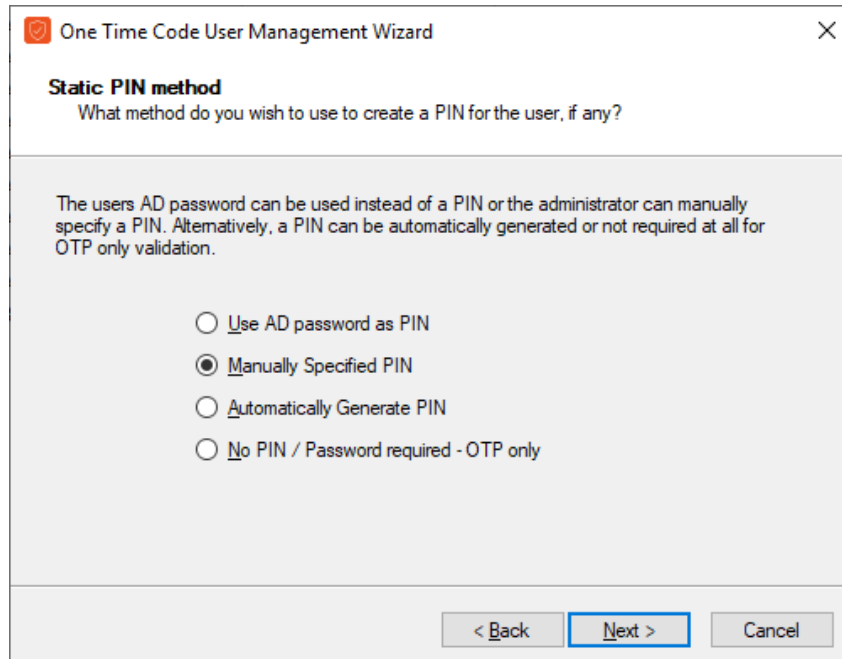
1. In the MyID Management Console, either expand the **Domains** and select the appropriate OU, or expand the **Realms** and select the appropriate realm.
2. Select the user account (or accounts) for which you want to manage the One Time Code settings.



3. Click **One Time Code Management**, in the **Actions** pane, or from right-clicking the account (or accounts).



4. Click **Next**.



The dialog box is titled "One Time Code User Management Wizard" and has a close button (X) in the top right corner. Below the title bar, the section "Static PIN method" is displayed, followed by the question "What method do you wish to use to create a PIN for the user, if any?". A descriptive text block states: "The users AD password can be used instead of a PIN or the administrator can manually specify a PIN. Alternatively, a PIN can be automatically generated or not required at all for OTP only validation." Below this text are four radio button options: "Use AD password as PIN", "Manually Specified PIN" (which is selected), "Automatically Generate PIN", and "No PIN / Password required - OTP only". At the bottom of the dialog are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

5. Choose the Static PIN Method.

The following PIN options exist:

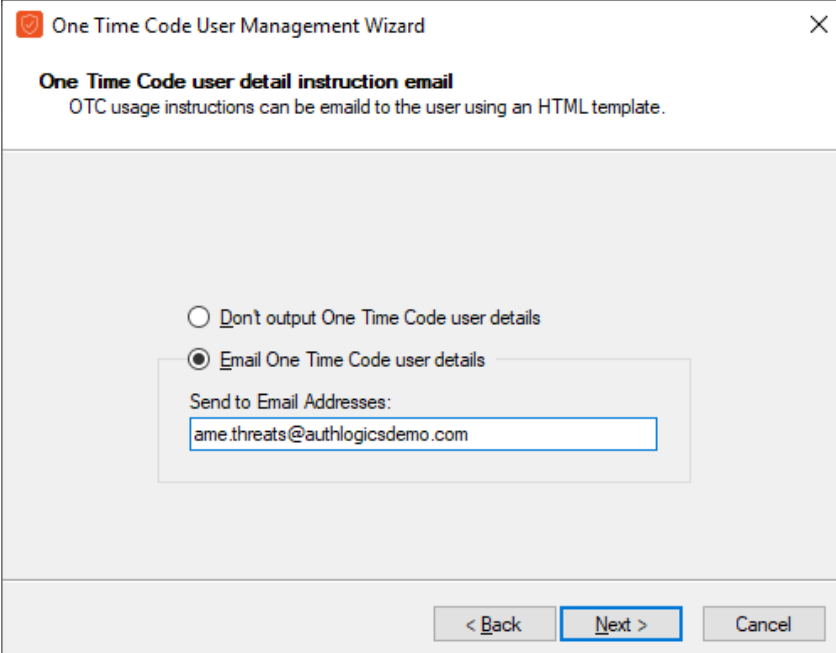
- **Use AD Password as PIN** – The user's Active Directory password is used instead of a PIN.
- **Manually Specified PIN** – The administrator manually specifies a PIN.

If multiple accounts were selected before starting the wizard, this option is not available.

- **Automatically Generate PIN** – The PIN is automatically generated.
- **No PIN / Password required – OTP only** – The PIN is not required at all for OTP only validation.

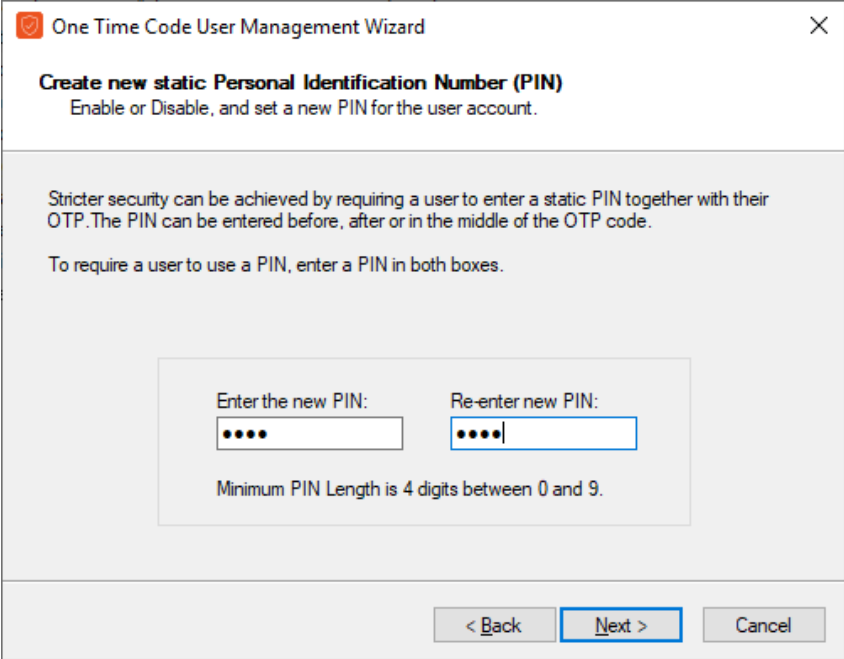
This option is only available if you enabled it through Global settings.

6. Click **Next**.



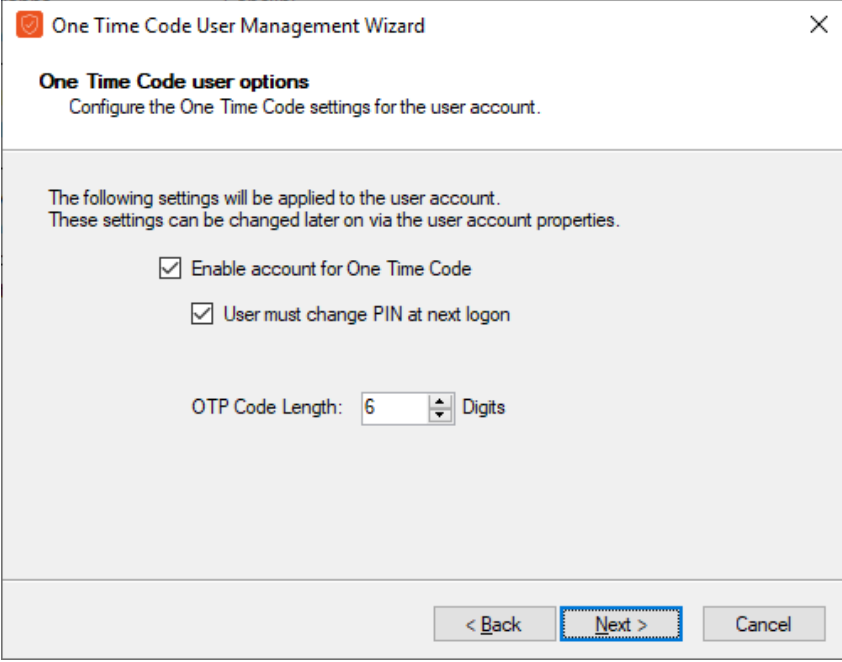
The screenshot shows a window titled "One Time Code User Management Wizard" with a close button (X) in the top right corner. Below the title bar, there is a sub-header "One Time Code user detail instruction email" and a note: "OTC usage instructions can be emailed to the user using an HTML template." The main content area contains two radio buttons: "Don't output One Time Code user details" (unselected) and "Email One Time Code user details" (selected). Below the selected radio button is a text box labeled "Send to Email Addresses:" containing the email address "ame.threats@authlogicsdemo.com". At the bottom of the window are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

7. Select the delivery method for One Time Code settings and usage instructions.
Auto-generated information can be printed or emailed to the user.
If you manually specified the settings, you can specify not to output any details – this option is not available for auto-generated details.
8. Click **Next**.
9. If you are manually specifying the PIN, enter the user's PIN and confirm the PIN.



The screenshot shows a window titled "One Time Code User Management Wizard" with a close button (X) in the top right corner. Below the title bar, there is a sub-header "Create new static Personal Identification Number (PIN)" and a note: "Enable or Disable, and set a new PIN for the user account." The main content area contains a paragraph: "Stricter security can be achieved by requiring a user to enter a static PIN together with their OTP. The PIN can be entered before, after or in the middle of the OTP code." followed by "To require a user to use a PIN, enter a PIN in both boxes." Below this text are two text boxes: "Enter the new PIN:" and "Re-enter new PIN:". Both boxes contain four dots (••••). Below the text boxes is a note: "Minimum PIN Length is 4 digits between 0 and 9." At the bottom of the window are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel".

10. Click **Next**.



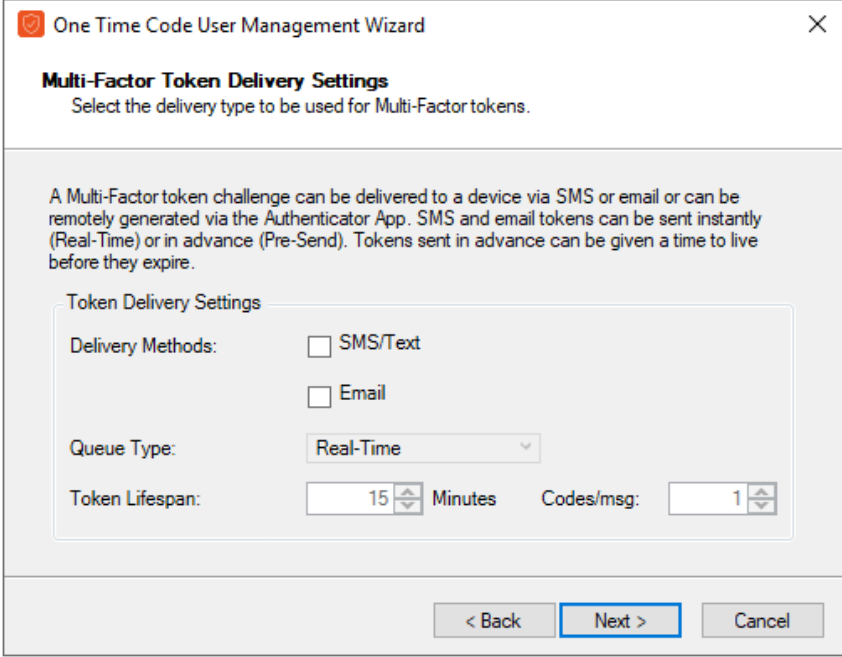
The screenshot shows the 'One Time Code User Management Wizard' window. The title bar says 'One Time Code User Management Wizard' with a close button. The main heading is 'One Time Code user options' with a subtitle 'Configure the One Time Code settings for the user account.' Below this, a message states: 'The following settings will be applied to the user account. These settings can be changed later on via the user account properties.' There are two checked checkboxes: 'Enable account for One Time Code' and 'User must change PIN at next logon'. Below these is a field for 'OTP Code Length' set to '6' with a spinner and the unit 'Digits'. At the bottom are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

11. Configure One Time Code user options.

You can set an account so that the next time the user logs in with this account, the user is forced to change the PIN at the next logon.

Set the **OTP Code Length** to the number of characters long that you want the OTP code to be.

12. Click **Next**.



The screenshot shows the 'One Time Code User Management Wizard' window. The title bar says 'One Time Code User Management Wizard' with a close button. The main heading is 'Multi-Factor Token Delivery Settings' with a subtitle 'Select the delivery type to be used for Multi-Factor tokens.' Below this, a message states: 'A Multi-Factor token challenge can be delivered to a device via SMS or email or can be remotely generated via the Authenticator App. SMS and email tokens can be sent instantly (Real-Time) or in advance (Pre-Send). Tokens sent in advance can be given a time to live before they expire.' There is a section titled 'Token Delivery Settings' containing: 'Delivery Methods' with checkboxes for 'SMS/Text' and 'Email'; 'Queue Type' with a dropdown menu set to 'Real-Time'; and 'Token Lifespan' with a spinner set to '15' and the unit 'Minutes', and 'Codes/msg' with a spinner set to '1'. At the bottom are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

13. Select the delivery method for Multi-Factor tokens.

You can select how the One Time Codes are delivered.

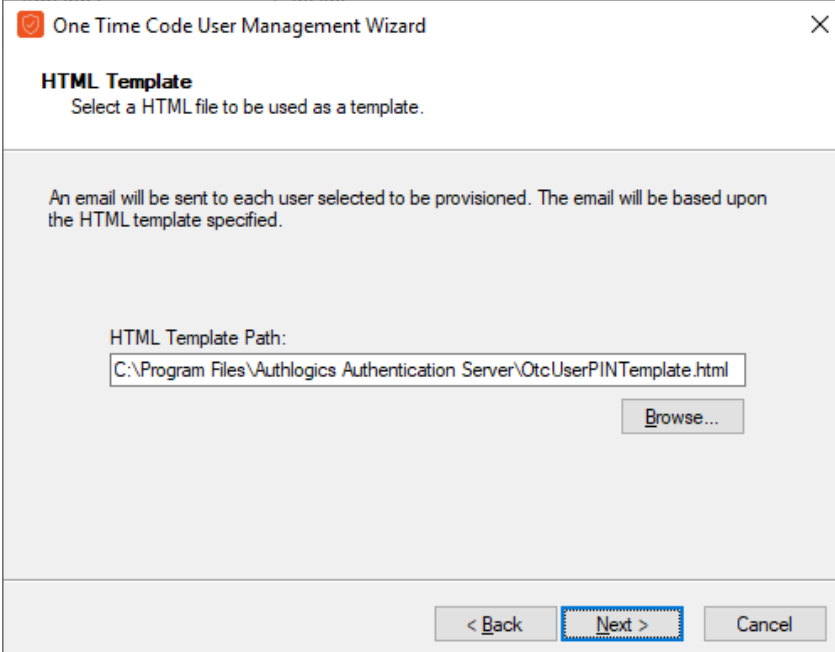
Users can always use their MyID Authentication app to receive any multi-factor authentication tokens for which they are configured, if the user has a device with the app configured.

You can select additional **Delivery Methods** of SMS / Text and Email. If you select one or more of these options, you must:

- Ensure that the user has a Mobile Number or an Email Address set to which the tokens can be sent.
- Set the **Queue Type**; choose if the One Time Codes are sent only when requested (Real-Time) or if they are sent ahead of time (Pre-Send).

If you set the **Queue Type** to Pre-Send, you must specify the **Token Lifespan** for these token types; by default, the **Token Lifespan** is 1 day. You must also set the number of codes sent at a time in a message; by default, the **Codes/msg** is 3.

14. Click **Next**.



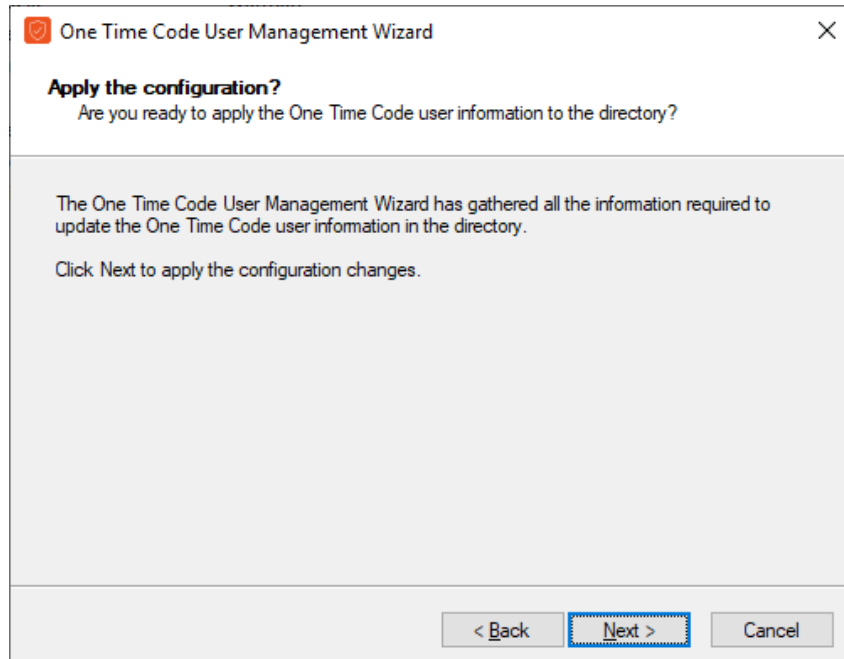
The screenshot shows a window titled "One Time Code User Management Wizard" with a close button (X) in the top right corner. Below the title bar, the section is labeled "HTML Template" with the instruction "Select a HTML file to be used as a template." A paragraph of text states: "An email will be sent to each user selected to be provisioned. The email will be based upon the HTML template specified." Below this text, there is a label "HTML Template Path:" followed by a text box containing the path "C:\Program Files\Authlogics Authentication Server\OtcUserPINTemplate.html". To the right of the text box is a "Browse..." button. At the bottom of the window, there are three buttons: "< Back", "Next >" (which is highlighted with a blue dashed border), and "Cancel".

15. Specify the **HTML Template Path** to the automated notification letter or email.

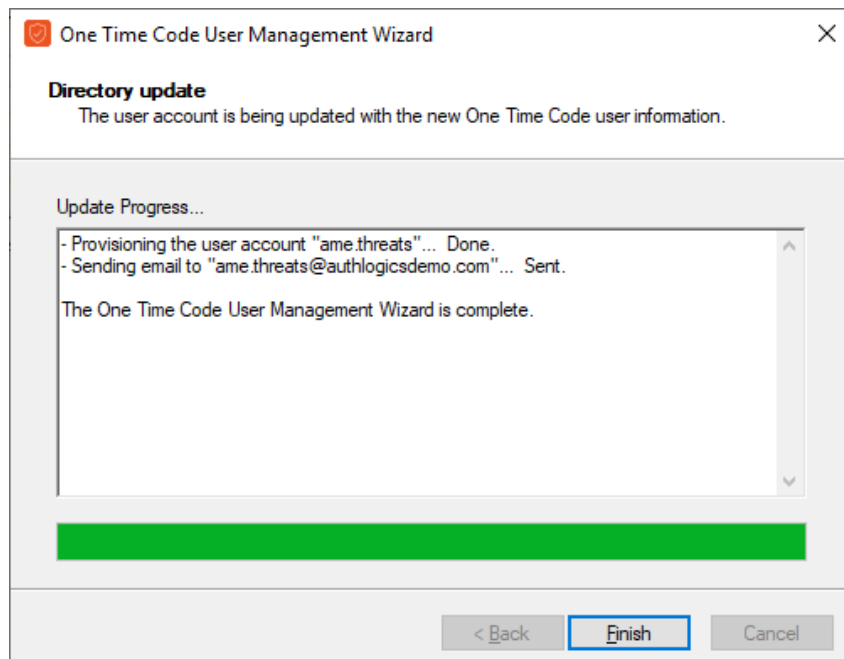
This HTML file can be modified and customized for your organization. Each letter or email is customized for the user to contain their unique information by substituting HTML comment values in the template.

To locate a custom template click **Browse**.

16. Click **Next**.



17. Click **Next**.



The configuration changes are applied.

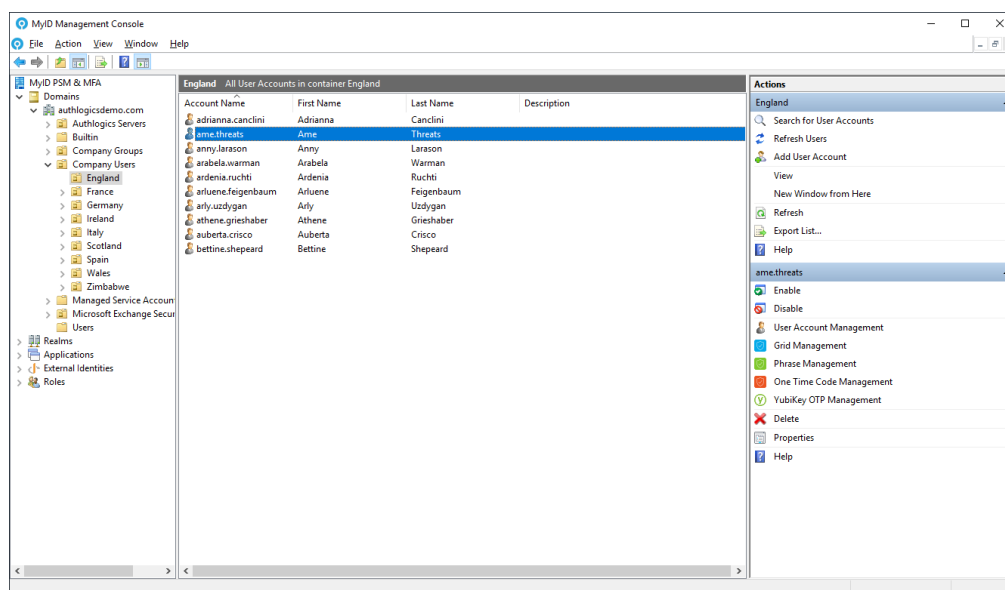
18. Click **Finish**.

5.8.9 Setting up a user for YubiKey OTP

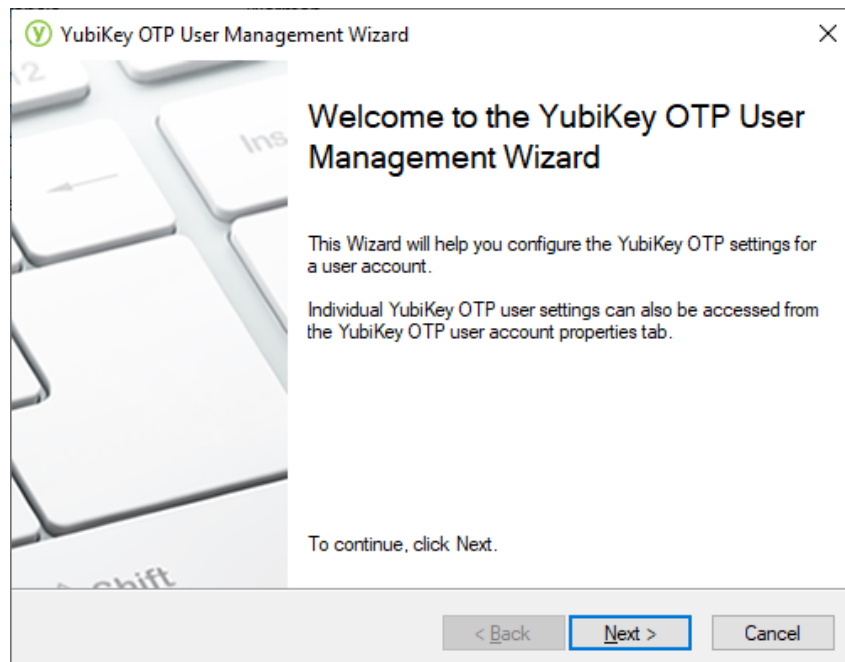
Once you have created a MyID user account, you can configure it for use with YubiKey OTP.

Note: To be able to set up a user for YubiKey OTPs, you must enable YubiKey OTPs on the **YubiKey OTP** tab of the global settings. For more information, see section [5.3.15, YubiKey OTP tab](#).

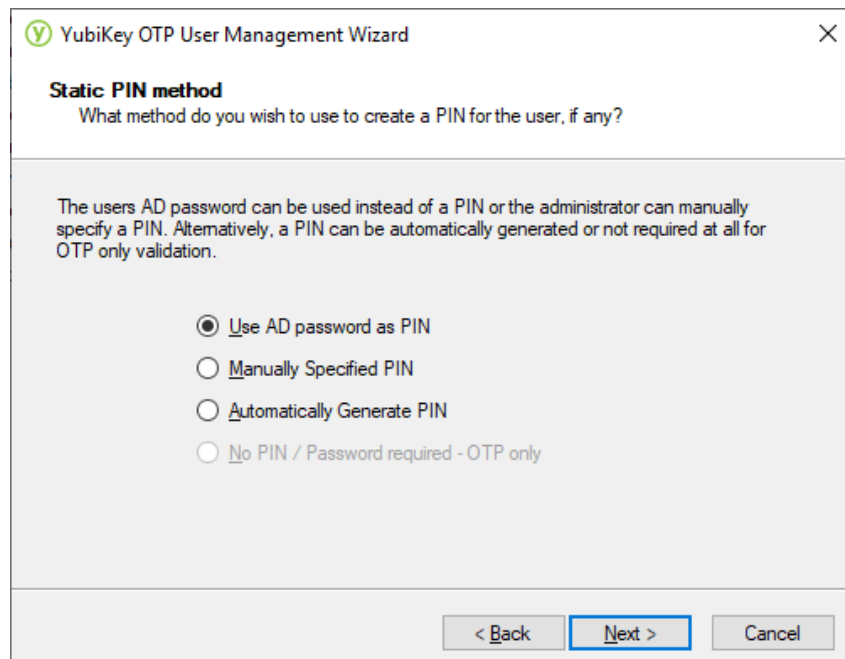
1. In the MyID Management Console, either expand the **Domains** and select the appropriate OU, or expand the **Realms** and select the appropriate realm.
2. Select the user account (or accounts) for which you want to manage the YubiKey One Time Code settings.



3. Click **YubiKey One Time Code Management**, in the **Actions** pane, or from right-clicking the account (or accounts).



4. Click **Next**.



5. Choose the Static PIN Method.

The following PIN options exist:

- **Use AD Password as PIN** – The user's Active Directory password is used instead of a PIN.
- **Manually Specified PIN** – The administrator manually specifies a PIN.
If multiple accounts were selected before starting the wizard, this option is not available.
- **Automatically Generate PIN** – The PIN is automatically generated.
- **No PIN / Password required – OTP only** – The PIN is not required at all for OTP only validation.

This option is available only if you enabled it through Global settings.

6. Click **Next**.

The screenshot shows a window titled "YubiKey OTP User Management Wizard" with a close button (X) in the top right corner. Below the title bar, the text "YubiKey OTP user detail instruction email" is displayed, followed by a subtitle: "YubiKey OTP usage instructions can be emailed to the user using an HTML template." The main area of the window contains two radio button options: "Don't output YubiKey OTP user details" (which is unselected) and "Email YubiKey OTP user details" (which is selected). Below these options is a text input field labeled "Send to Email Addresses:" containing the email address "ame.threats@authlogicsdemo.com". At the bottom of the window, there are three buttons: "< Back", "Next >" (which is highlighted with a blue border), and "Cancel".

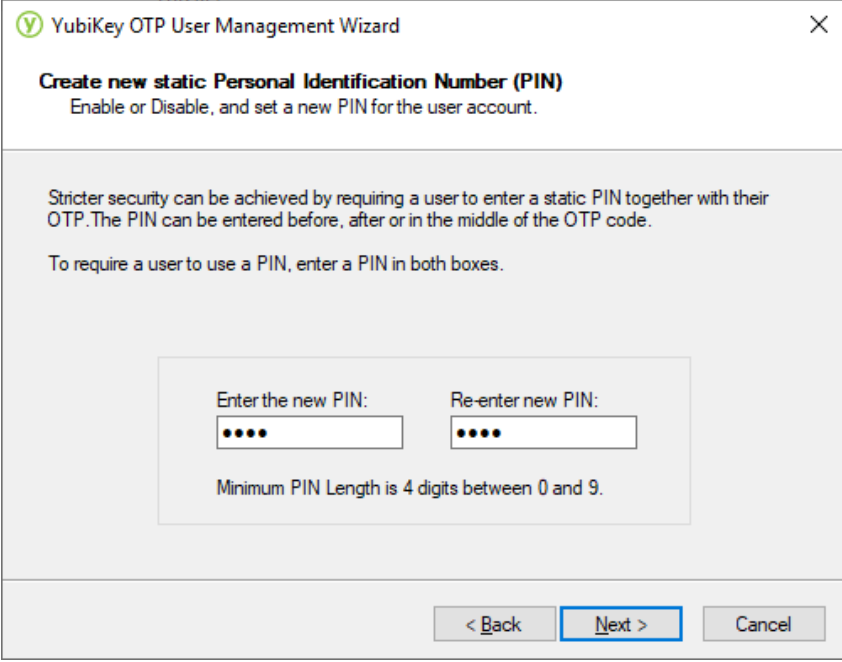
7. Select the delivery method for One Time Code settings and usage instructions.

Auto-generated information can be printed or emailed to the user.

If you manually specified the settings, you can specify not to output any details – this option is not available for auto-generated details.

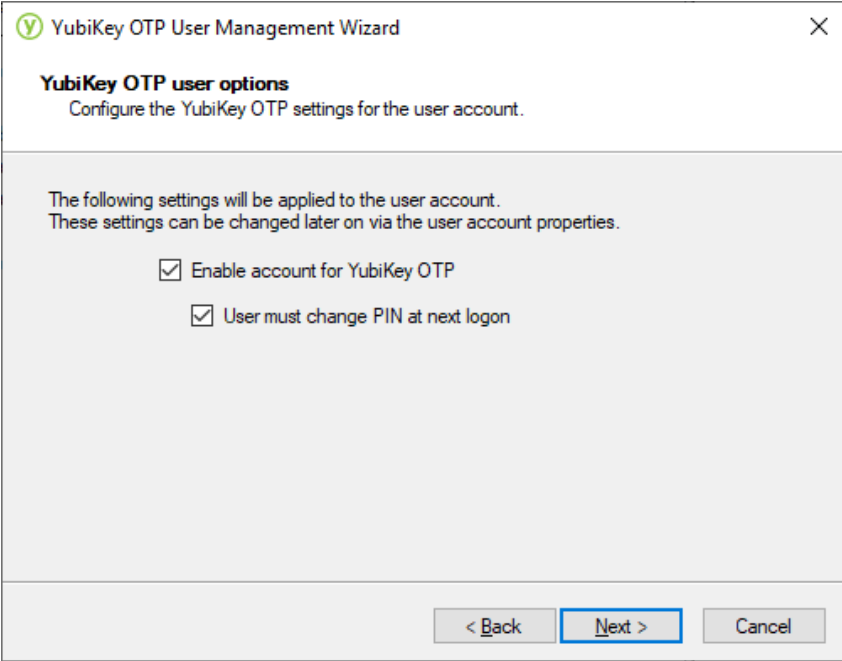
8. Click **Next**.

9. If you are manually specifying the PIN, enter the user's PIN and confirm the PIN.



The screenshot shows the 'YubiKey OTP User Management Wizard' window. The title bar includes a green 'Y' icon and the text 'YubiKey OTP User Management Wizard'. The main heading is 'Create new static Personal Identification Number (PIN)' with a subtitle 'Enable or Disable, and set a new PIN for the user account.' Below this, explanatory text states: 'Stricter security can be achieved by requiring a user to enter a static PIN together with their OTP. The PIN can be entered before, after or in the middle of the OTP code. To require a user to use a PIN, enter a PIN in both boxes.' There are two input fields: 'Enter the new PIN:' and 'Re-enter new PIN:', both containing four dots. Below the fields, it says 'Minimum PIN Length is 4 digits between 0 and 9.' At the bottom right are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

10. Click **Next**.



The screenshot shows the 'YubiKey OTP User Management Wizard' window at the 'YubiKey OTP user options' step. The title bar includes a green 'Y' icon and the text 'YubiKey OTP User Management Wizard'. The main heading is 'YubiKey OTP user options' with a subtitle 'Configure the YubiKey OTP settings for the user account.' Below this, explanatory text states: 'The following settings will be applied to the user account. These settings can be changed later on via the user account properties.' There are two checked checkboxes: 'Enable account for YubiKey OTP' and 'User must change PIN at next logon'. At the bottom right are three buttons: '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

11. Configure YubiKey One Time Code user options.

To set an account so that the next time the user logs in with this account, the user is forced to change the PIN, select **User must change PIN at next logon**.

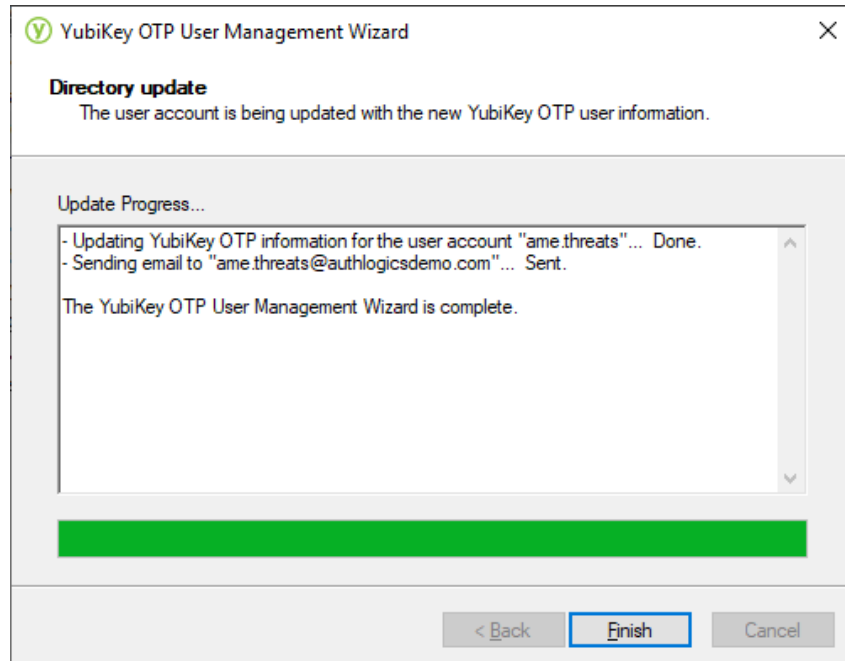
12. Click **Next**.

The screenshot shows the 'HTML Template' step of the 'YubiKey OTP User Management Wizard'. The window title is 'YubiKey OTP User Management Wizard'. The main heading is 'HTML Template' with the instruction 'Select a HTML file to be used as a template.' Below this, a message states: 'An email will be sent to each user selected to be provisioned. The email will be based upon the HTML template specified.' There is a text box labeled 'HTML Template Path:' containing the path 'C:\Program Files\Authlogics Authentication Server\YubiKeyOtpUserPINTempla'. To the right of the text box is a 'Browse...' button. At the bottom of the window are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

13. Specify the **HTML Template Path** to the automated notification letter or email.
This HTML file can be modified and customized for your organization. Each letter or email is customized for the user to contain their unique information by substituting HTML comment values in the template.
To locate a custom template click **Browse**.
14. Click **Next**.

The screenshot shows the 'Apply the configuration?' step of the 'YubiKey OTP User Management Wizard'. The window title is 'YubiKey OTP User Management Wizard'. The main heading is 'Apply the configuration?' with the question 'Are you ready to apply the YubiKey OTP user information to the directory?'. Below this, a message states: 'The YubiKey OTP User Management Wizard has gathered all the information required to update the YubiKey OTP user information in the directory. Click Next to apply the configuration changes.' At the bottom of the window are three buttons: '< Back', 'Next >' (which is highlighted with a blue border), and 'Cancel'.

15. Click **Next**.



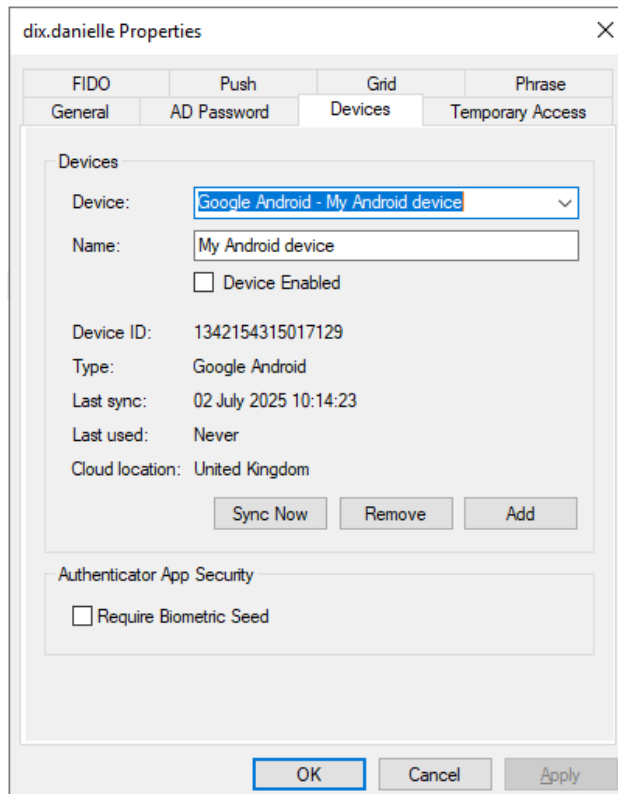
16. Click **Finish**.

5.8.10 Adding a YubiKey device

You can add a YubiKey device to a user's account through the user's Properties.

To add a YubiKey device:

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account to manage.
2. Click **Properties**, in the **Actions** pane.
3. Select the **Devices** tab.



dix.danielle Properties

FIDO Push Grid Phrase
General AD Password **Devices** Temporary Access

Devices

Device: Google Android - My Android device

Name: My Android device

☐ Device Enabled

Device ID: 1342154315017129

Type: Google Android

Last sync: 02 July 2025 10:14:23

Last used: Never

Cloud location: United Kingdom

Sync Now Remove Add

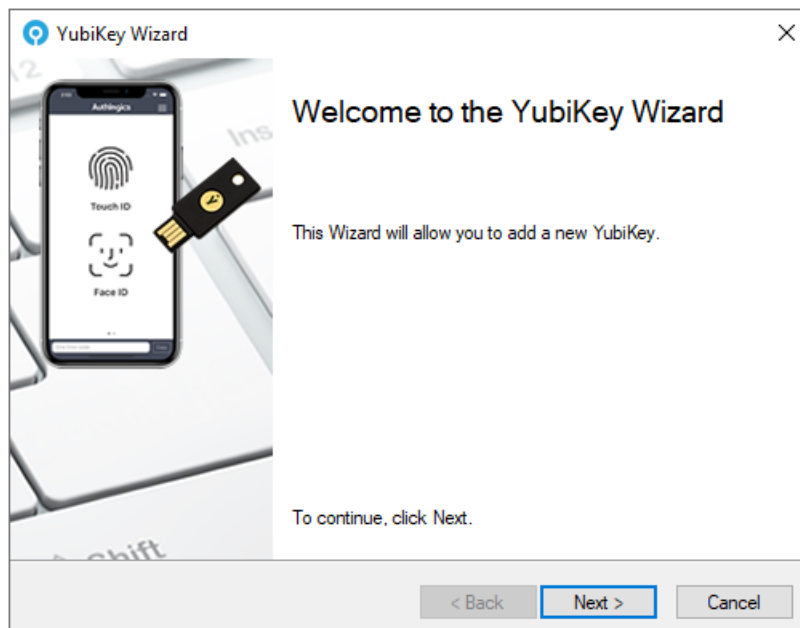
Authenticator App Security

☐ Require Biometric Seed

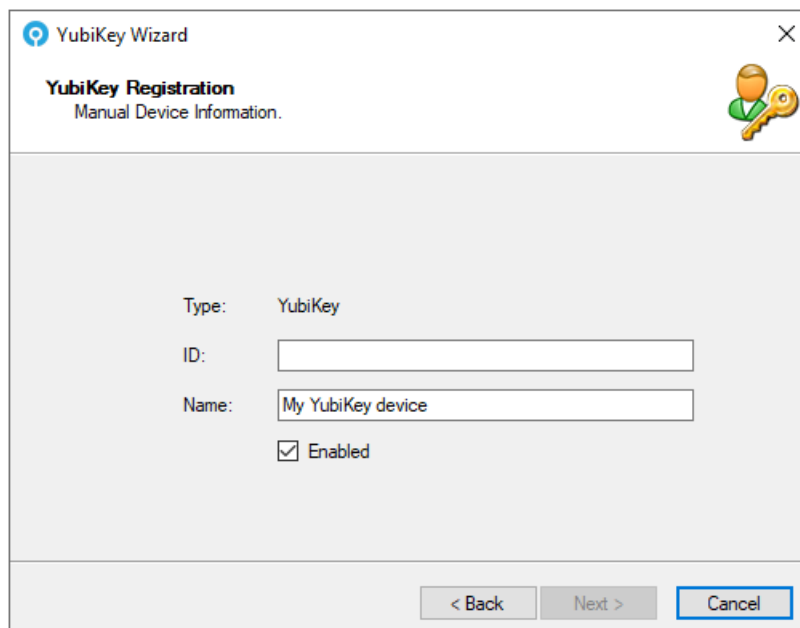
OK Cancel Apply

4. Click **Add**.

This launches the YubiKey Wizard.

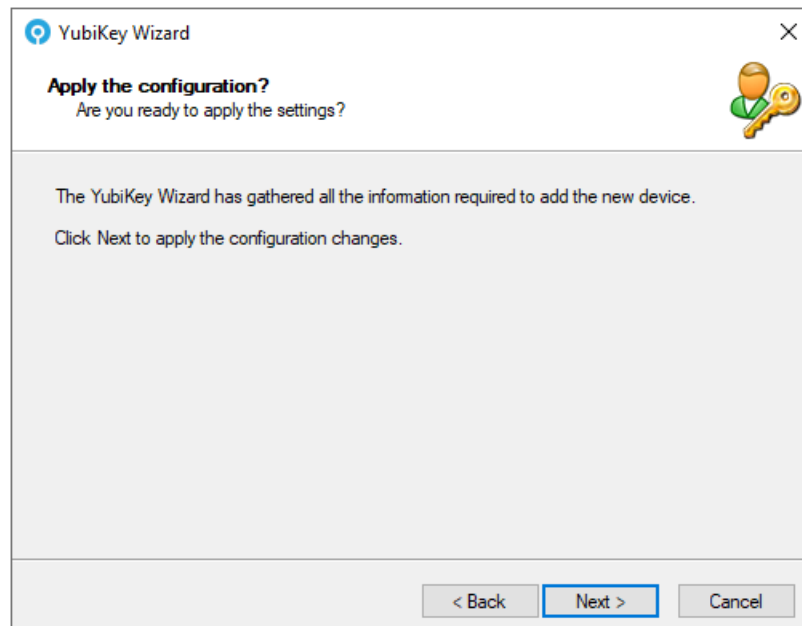


5. Click **Next**.

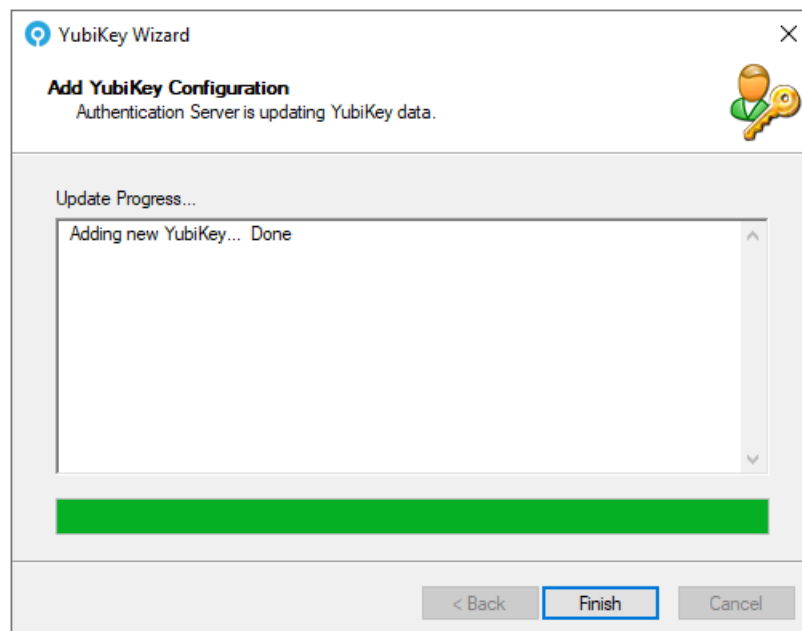


6. Click the **ID** field.
7. Insert your YubiKey and touch it. This generates a code. The first twelve characters of the code are the device ID. These characters are automatically entered.
Alternatively, you can manually type the YubiKey's device ID. Make sure to press Enter to enable the **Next** button.
8. Type an alternative **Name** for the YubiKey device.

9. To disable the device, deselect the **Enabled** option.
10. Click **Next**.



11. Click **Next**.



12. Click **Finish**.

ame.threats Properties

Push Grid Phrase One Time Code YubiKey OTP

General AD Password **Devices** Temporary Access FIDO

Devices

Device: Yubico YubiKey - My YubiKey device

Name: My YubiKey device

☒ Device Enabled

Device ID: ertgbryeagd

Type: Yubico YubiKey

Registration: Manual

Last used: Never

Remove Add

Authenticator App Security

☐ Require Biometric Seed

OK Cancel Apply

The YubiKey device is added to the account.

You can manage your new device from the **Devices** tab. For more information, see section [5.9.2, Multi-Factor devices assigned to a user account](#).

5.9 Managing existing users

After you have created a user and set them up for technologies, you may want to view or modify their options.

To do this, you can either re-run the various wizards on a user, or use the user's Properties dialog.

- You can reconfigure the base settings of user accounts using the User Account Management wizard or the user's Properties dialog.
See section [5.9.1, Managing a user's base settings](#).
- You can view the MFA devices for a user using the user's Properties dialog.
See section [5.9.2, Multi-Factor devices assigned to a user account](#).
- You can manage a user's Grid Pattern without changing it using the user's Properties dialog.
See section [5.9.3, Managing a user's Grid Patterns](#).
- You can manage a user's Phrases using the user's Properties dialog.
See section [5.9.4, Managing a user's Phrases](#).
- You can manage a user's One Time codes using the user's Properties dialog.
See section [5.9.5, Managing a user's One Time Codes](#).
- You can manage a user's YubiKey OTPs through the user properties dialog.
See section [5.9.6, Managing a user's YubiKey OTP](#).
- You can manage user passwords using the user's Properties dialog.
See section [5.9.7, Managing user passwords](#).
- You can assign temporary access codes using the user's Properties dialog.
See section [5.9.8, Assigning temporary access codes to a user](#).
- You can revoke the refresh tokens of specific users.
See section [5.9.9, Revoking specific users' refresh tokens](#).

You can use the wizards to manage the following:

- You can use the Grid User Management wizard to reconfigure Grid Patterns.
See section [5.8.6, Setting up a user for Grid Pattern Authentication](#).
- You can use the Phrase Authentication Management wizard to manage Phrases more comprehensively.
See section [5.8.7, Setting up a user for Phrase authentication](#).
- You can use the One Time Code User Management wizard to manage One Time Codes.
See section [5.8.8, Setting up a user for One Time Code](#).
- You can use the YubiKey OTP User Management wizard to manage YubiKey OTPs.
See section [5.8.9, Setting up a user for YubiKey OTP](#).

You can also manage users through the Web Management Portal. For more information, see the *Managing a user* section of the [Web Management Portal User Guide](#).

5.9.1 Managing a user's base settings

You can manage a user's base settings – the account options and the passwordless authentication options of the user accounts – together through the User Account Management wizard, or separately through the user's Properties dialog.

You may want to use the User Account Management wizard if you want to edit multiple accounts at once.

You may want to use a user's Properties dialog if you want to look at and edit a single user's base settings quickly, or view whether a user is Push throttled, and clear it .

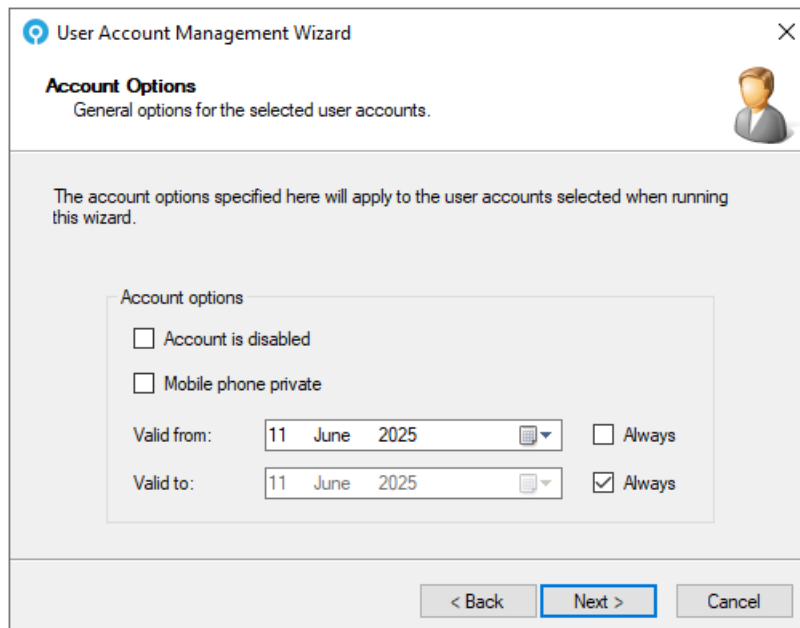
5.9.1.1 Using the User Account Management wizard

The User Account Management wizard allows you reconfigure the base settings of user accounts:

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account or user accounts to manage.



2. Click **Next**.



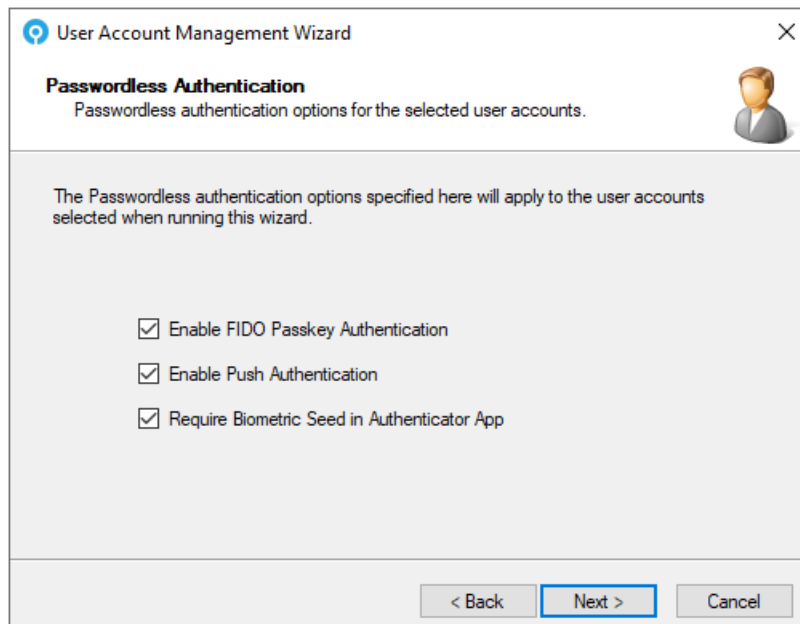
The screenshot shows the 'User Account Management Wizard' window, specifically the 'Account Options' step. The title bar says 'User Account Management Wizard' with a close button. Below the title bar, the section is 'Account Options' with a subtitle 'General options for the selected user accounts.' and a user icon. A note states: 'The account options specified here will apply to the user accounts selected when running this wizard.' The main area contains a box titled 'Account options' with the following settings: 'Account is disabled' (unchecked), 'Mobile phone private' (unchecked), 'Valid from:' (11 June 2025), 'Valid to:' (11 June 2025), 'Always' (unchecked) for both dates, and 'Always' (checked) for the 'Valid to' date. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

3. Set the account options.

Account options determine the user's state. You can give accounts start and end validity dates, and can disable the account if required.

You can also specify the mobile phone privacy setting.

4. Click **Next**.



The screenshot shows the 'User Account Management Wizard' window, specifically the 'Passwordless Authentication' step. The title bar says 'User Account Management Wizard' with a close button. Below the title bar, the section is 'Passwordless Authentication' with a subtitle 'Passwordless authentication options for the selected user accounts.' and a user icon. A note states: 'The Passwordless authentication options specified here will apply to the user accounts selected when running this wizard.' The main area contains three checked checkboxes: 'Enable FIDO Passkey Authentication', 'Enable Push Authentication', and 'Require Biometric Seed in Authenticator App'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

5. Choose whether the users are enabled for FIDO and/or Mobile Push authentication.
6. Click **Next**.

User Account Management Wizard

FIDO usage instruction email
FIDO usage instructions can be emailed to the user using an HTML template.

☒ Don't output user details
☐ Email user details

Send to Email Addresses:
gretel.tarenis@authlogicsdemo.com

☐ Use Secondary Email Address if available

Email HTML Template Path:
C:\Program Files\Authlogics Authentication Server\Fido Browse...

< Back Next > Cancel

User Account Management Wizard

Push usage instruction email
Push usage instructions can be emailed to the user using an HTML template.

☒ Don't output user details
☐ Email user details

Send to Email Addresses:

☐ Use Secondary Email Address if available

Email HTML Template Path:
C:\Program Files\Authlogics Authentication Server\Pus Browse...

< Back Next > Cancel

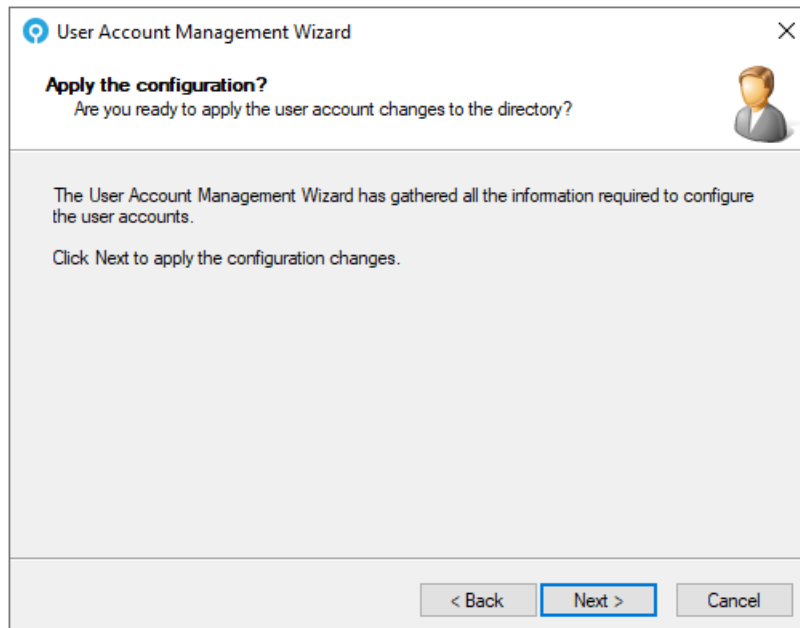
7. Choose how the instruction email is delivered – this email contains instructions on how to set up their device for FIDO and Mobile Push based on your selection above.

If a single user is selected, you can specify the email address to which to deliver the email.

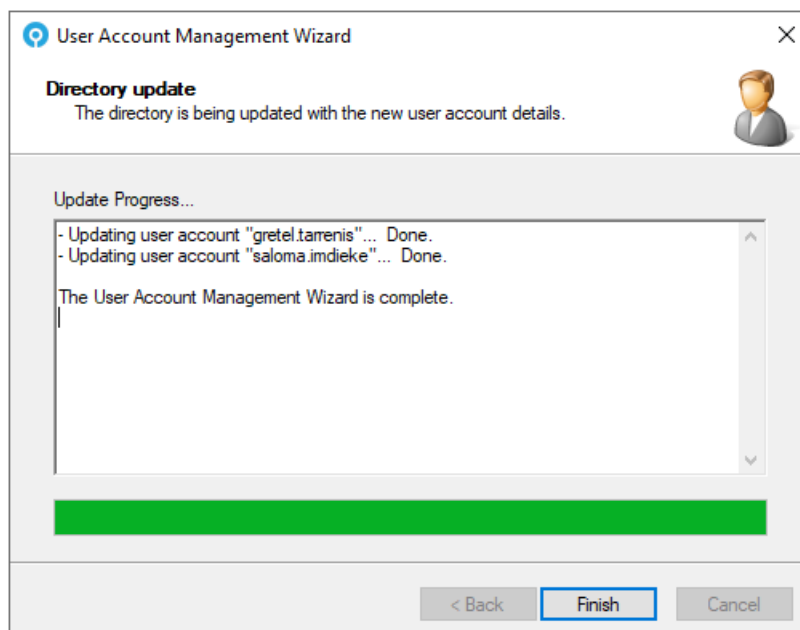
When adding multiple users, the user's email address is retrieved from Active Directory or the alternate email address field and sent to them automatically.

The appropriate FIDO and PUSH HTML template files can be selected to use for the email.

8. Click **Next**.



9. Click **Next**.



The new user accounts have been created.

10. Click **Finish**.

5.9.1.2 Updating account options only

If you want to update only a user's account options, you can use the user's Properties dialog.

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account to manage.

2. Click **Properties**, in the **Actions** pane.

The screenshot shows the 'ame.threats Properties' dialog box with the 'General' tab selected. The 'Account Info' section contains the following fields: First name (Ame), Last name (Threats), Description (empty), UPN (ame.threats@authlogicsdemo.com), E-mail (ame.threats@authlogicsdemo.com), Phone (empty), and a 'Private' checkbox. The 'Account' field is 'ame.threats' and the 'Entra ID' is 'l-ZT2YWtFpEEA=='. The 'MFA Account options' section has two checkboxes: 'Account is disabled' (unchecked) and 'Account is locked out' (unchecked). Below these are date selectors for 'Valid from' (09 April 2025) and 'Valid to' (12 June 2025), each with an 'Always' checkbox. The 'Valid to' 'Always' checkbox is checked. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

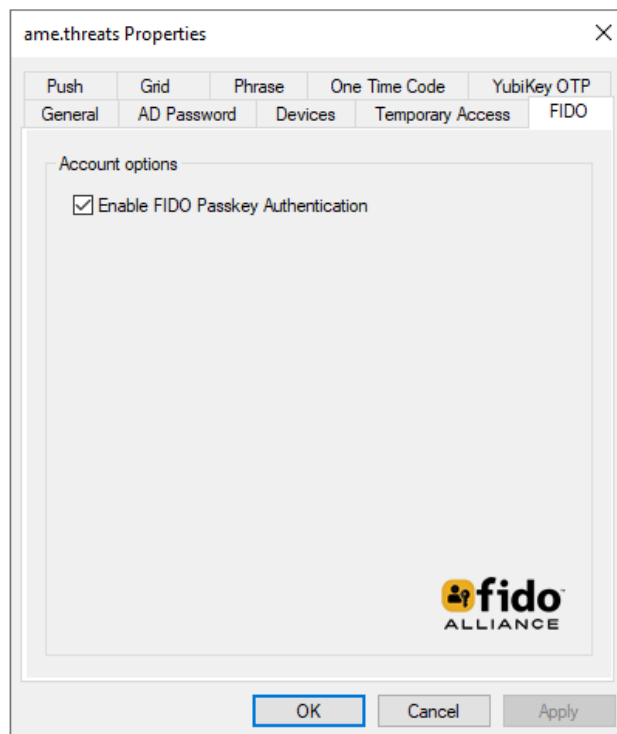
This opens the properties to the **General** tab.

3. In the MFA Account options section, you can specify whether the account is disabled by selecting or deselecting **Account is disabled**.
4. You can specify whether the account is locked by selecting or deselecting **Account is locked out**.
5. You can select the validity period (when the account is **Valid from**, and when it is **Valid to**) with the date selectors.
You can set the account to always be valid.
6. Click **OK**.

5.9.1.3 Updating FIDO passkey authentication only

If you want to enable or disable a user only for FIDO passkey authentication, you can use the user's properties dialog.

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account to manage.
2. Click **Properties**, in the **Actions** pane.
3. Select the **FIDO** tab.

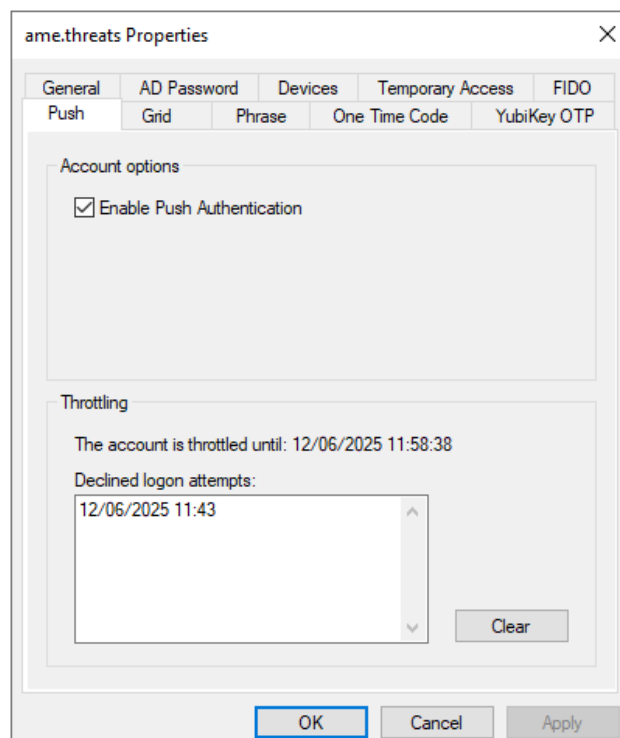


4. You can specify whether the account is enabled for FIDO Passkey authentication by selecting or deselecting **Enable FIDO Passkey Authentication**.
5. Click **OK**.

5.9.1.4 Updating Push Authentication

If you only want to update or view, you can use the the user's properties dialog.

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account to manage.
2. Click **Properties**, in the **Actions** pane.
3. Select the **Push** tab.



4. You can specify whether the account is enabled for Push authentication by selecting or deselecting **Enable Push Authentication**.
5. You can view whether a user has their Push notifications throttled.

Push notification throttling occurs when a user declines a Push notification and states that they did not attempt that logon. The user cannot use Push notifications as a logon technology while they are throttled. Regardless of the device on which the failed malicious attempt occurs, Push notifications are throttled for all of the user's devices.

When a single Push notification is declined as a failed malicious attempt, the account is throttled for 15 minutes.

The amount of time for which Push notifications are blocked is increased by 15 minutes for each attempted malicious Push notification within the last four hours.

For example, if there have been three malicious attempts in the last four hours, Push notifications are blocked for 45 minutes.

Each declined logon attempt is displayed in the Throttling section by date and time, with the time being local to the server.

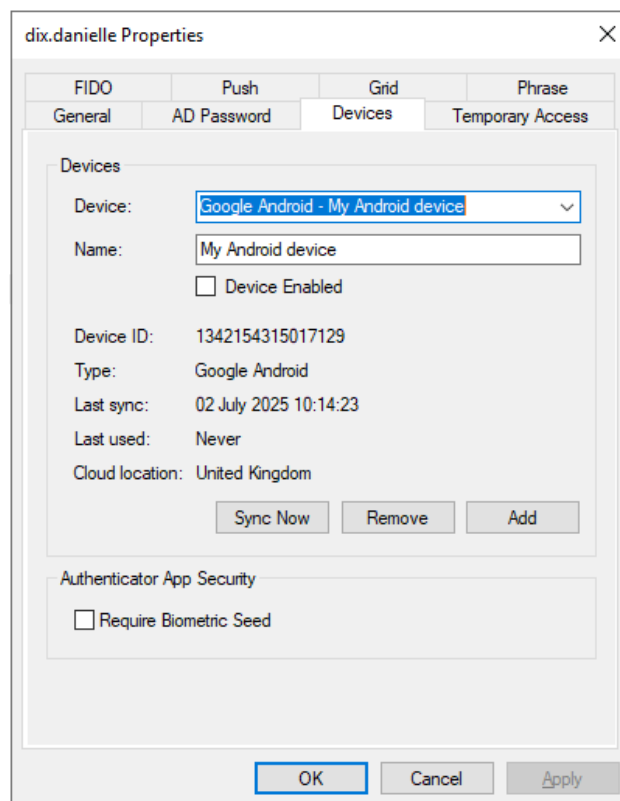
Push notification throttling occurs to help protect a user from MFA fatigue.

6. You can clear the account of throttling by clicking **Clear**.
7. Click **OK**.

5.9.2 Multi-Factor devices assigned to a user account

Users can enroll their MFA device or devices through the self-service portal or through the MyID Windows Desktop Agent. You can view the devices assigned to the user by using the MyID MMC.

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account to manage.
2. Click **Properties**, in the **Actions** pane.
3. Select the **Devices** tab.



The screenshot shows the 'dix.danielle Properties' dialog box with the 'Devices' tab selected. The dialog has four tabs: FIDO, Push, Grid, and Phrase. Below these are sub-tabs: General, AD Password, Devices, and Temporary Access. The 'Devices' sub-tab is active, showing a list of devices. The first device is 'Google Android - My Android device'. Below the device name is a text field for 'Name' containing 'My Android device'. There is a checkbox for 'Device Enabled' which is currently unchecked. Below this are fields for 'Device ID' (1342154315017129), 'Type' (Google Android), 'Last sync' (02 July 2025 10:14:23), 'Last used' (Never), and 'Cloud location' (United Kingdom). At the bottom of the device list are buttons for 'Sync Now', 'Remove', and 'Add'. Below the device list is a section for 'Authenticator App Security' with a checkbox for 'Require Biometric Seed' which is currently unchecked. At the bottom of the dialog are buttons for 'OK', 'Cancel', and 'Apply'.

Each user can have up to ten Multi-Factor Authentication devices. You can view any device assigned to a user by selecting it as a **Device**.

You can enable or disable each device as needed. You may want to do this if the device is temporarily misplaced.

You can view the cloud location under which the device was registered – this is the cloud location set when the device was registered. For more information, see section [5.3.9, Authenticator App tab](#).

If you want to change the cloud location to match the updated global cloud location, you must remove and re-register the device.

You can also require the user to provide biometrics when using access tokens that support biometric validation.

You can add a YubiKey device from this tab. For more information, see section [5.8.10, Adding a YubiKey device](#).

5.9.3 Managing a user's Grid Patterns

You can manage a single user's Grid Pattern settings through the user's Properties. If you want to reset the user's Grid Pattern yourself, you must re-run the Grid User Management Wizard; for more information, see section [5.9.3, Managing a user's Grid Patterns](#).

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account to manage.
2. Click **Properties**, in the **Actions** pane.
3. Select the **Grid** tab.

The screenshot shows the 'ame.threats Properties' dialog box with the 'Grid' tab selected. The dialog has a tabbed interface with 'General', 'AD Password', 'Devices', 'Temporary Access', and 'FIDO'. Under 'Grid', there are sub-tabs: 'Push', 'Grid', 'Phrase', 'One Time Code', and 'YubiKey OTP'. The 'Grid' sub-tab is active, showing 'Account options' and 'Token Delivery Settings'. In 'Account options', 'Enable account for Grid authentication' is checked, 'User must change Pattern at next logon' is unchecked, 'Pattern never expires' is checked, 'Enable Multi-Factor Authentication' is checked, and 'Disable Deviceless' is unchecked. The 'Grid Size' is set to '6 x 6'. In 'Token Delivery Settings', 'Delivery Methods' shows 'SMS/Text' unchecked and 'Email' checked. 'Queue Type' is set to 'Real-Time' and 'Token Lifespan' is set to '1 Minutes'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

4. You can specify whether the account is enabled for Grid Patterns authentication by selecting or deselecting **Enable account for Grid authentication**.
5. You can set a user's Pattern to expire the next time that they log in, forcing them to change the pattern, by selecting **User must change Pattern at next logon**.
6. You can also set a user's Pattern to never expire by selecting **Pattern never expires**.
7. You can enable the user for multi-factor authentication for Grid Patterns by selecting **Enable Multi-Factor authentication**.
8. You can require the user account to use a Multi-Factor device by selecting **Disable Deviceless**. An MFA device must be registered with the user account, otherwise the challenge delivered through email or SMS/TEXT fails.
9. You can view the **Grid Size**.
10. You can select how the challenge is delivered. This is available only if you have enabled multi-factor authentication.

Users can always use their MyID Authentication app to receive any multi-factor authentication tokens for which they are configured, if the user has a device with the app configured.

You can select additional **Delivery Methods** of SMS / Text and Email. If you select one or more of these options, you must:

- Ensure that the user has a Mobile Number or an Email Address set to which the tokens can be sent.
- Set the **Queue Type**; choose if the Grid Patterns are sent only when requested (Real-Time) or if they are sent ahead of time (Pre-Send).

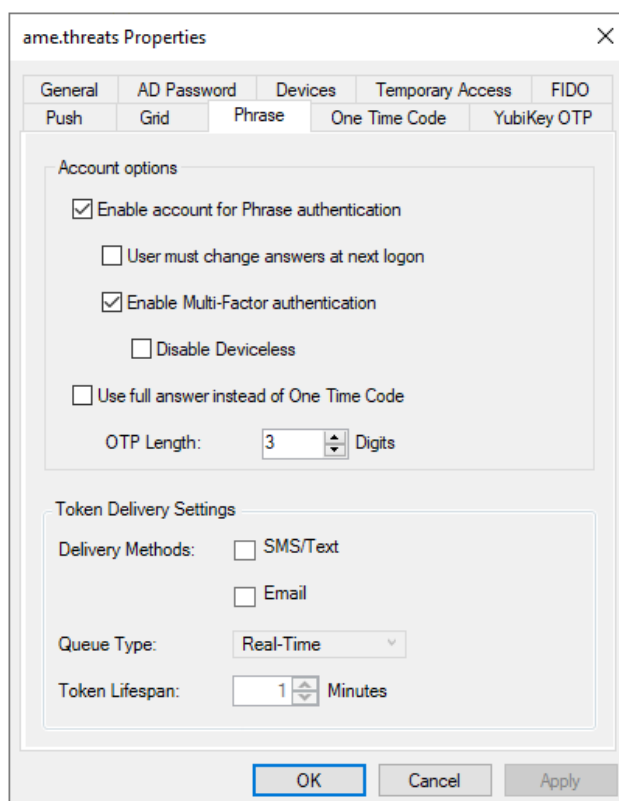
If you set the **Queue Type** to Pre-Send, you must specify the **Token Lifespan** for these token types; by default, the **Token Lifespan** is 1 day.

11. Click **OK**.

5.9.4 Managing a user's Phrases

You can manage a single user's Phrase settings through the user's Properties. If you want to reset the user's Phrase yourself, you must re-run the Phrase Authentication User Management Wizard; for more information, see section [5.8.7, Setting up a user for Phrase authentication](#).

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account to manage.
2. Click **Properties**, in the **Actions** pane.
3. Select the **Phrases** tab.



The image shows a screenshot of the 'ame.threats Properties' dialog box, specifically the 'Phrases' tab. The dialog has a title bar with a close button (X). Below the title bar are several tabs: 'General', 'AD Password', 'Devices', 'Temporary Access', 'FIDO', 'Push', 'Grid', 'Phrase' (selected), 'One Time Code', and 'YubiKey OTP'. The 'Phrase' tab contains two main sections: 'Account options' and 'Token Delivery Settings'. In the 'Account options' section, there are four checkboxes: 'Enable account for Phrase authentication' (checked), 'User must change answers at next logon' (unchecked), 'Enable Multi-Factor authentication' (checked), and 'Disable Deviceless' (unchecked). Below these is a checkbox for 'Use full answer instead of One Time Code' (unchecked) and an 'OTP Length' field set to '3' with a 'Digits' label. The 'Token Delivery Settings' section has a 'Delivery Methods' group with 'SMS/Text' and 'Email' checkboxes (both unchecked). Below this is a 'Queue Type' dropdown menu set to 'Real-Time' and a 'Token Lifespan' field set to '1' with a 'Minutes' label. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

4. You can specify whether the account is enabled for Phrase authentication by selecting or deselecting **Enable account for Phrase authentication**.
5. You can set a user's Phrase to expire the next time that they log in, forcing them to change the Phrase, by selecting **User must change answers at next logon**.
6. You can enable the user for multi-factor authentication for Phrases by selecting **Enable Multi-Factor authentication**.
7. You can require the user account to use a Multi-Factor device by selecting **Disable Deviceless**. An MFA device must be registered with the user account. If **Disable Deviceless** is not enabled, the challenge is delivered through email or SMS/TEXT.
8. You can either make the user use the whole Phrase when logging in by selecting **Use full answer instead of One Time Code**, or you can set how many characters of the Phrase the user is prompted for when logging in by setting the **OTP Length**. By default, this is 3 characters.

Note: As Phrases are not meant to be used like passwords in a true password-based system, **Use full answer instead of One Time Code** is disabled by default.

9. You can select how the Phrase One Time Codes are delivered. This is available only if you have enabled multi-factor authentication.

You can select additional **Delivery Methods** of `SMS / Text` and `Email`. If you select one or more of these options, you must:

- Ensure that the user has a Mobile Number or an Email Address set to which the tokens can be sent.
- Set the **Queue Type**; choose if the Phrase One Time Codes are sent only when requested (`Real-Time`) or if they are sent ahead of time (`Pre-Send`).

If you set the **Queue Type** to `Pre-Send`, you must specify the **Token Lifespan** for these token types; by default, the **Token Lifespan** is 1 day.

5.9.5 Managing a user's One Time Codes

You can manage the account options and delivery settings for a user's One Time codes through the user's Properties.

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account to manage.
2. Click **Properties**, in the **Actions** pane.

3. Select the **One Time Codes** tab.

The screenshot shows the 'ame.threats Properties' dialog box with the 'One Time Code' tab selected. The 'Account options' section includes checkboxes for 'Enable account for One Time Code authentication' and 'User must change PIN at next logon', both of which are checked. Below these are three radio buttons: 'PIN On' (selected), 'PIN Off', and 'Use AD password as PIN'. A 'Reset PIN' button is also present. The 'OTP Length' is set to 6 Digits. The 'Token Delivery Settings' section includes checkboxes for 'SMS/Text' and 'Email', both of which are unchecked. The 'Queue Type' is set to 'Real-Time'. The 'Token Lifespan' is set to 1 Minutes, and the 'Codes/msg' is set to 1. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

4. You can specify whether the account is enabled for One Time Codes authentication by selecting or deselecting **Enable account for One Time Code authentication**.
5. You can set a user's One Time Code PIN to expire the next time that they log in, forcing them to change the YubiKey OTP by selecting **User must change PIN at next logon**.
6. You can select what type of PIN is used for the One Time Codes:
 - **PIN On** – a set PIN for One Time Codes is used.
 - **PIN Off** – no PIN is used.
 - **User AD password as PIN** – the user's AD password is used.
7. To reset the user's One Time Codes PIN, click **Reset PIN**.
8. You can set the length of the generated One Time Code by setting the **OTP length**.
9. You can select how the One Time Codes are delivered.

Users can always use their MyID Authentication app to receive any multi-factor authentication tokens for which they are configured, if the user has a device with the app configured.

You can select additional **Delivery Methods** of SMS / Text and Email. If you select one or more of these options, you must:

- Ensure that the user has a Mobile Number or an Email Address set to which the tokens can be sent.
- Set the **Queue Type**; choose if the One Time Codes are sent only when requested (Real-Time) or if they are sent ahead of time (Pre-Send).

If you set the **Queue Type** to `Pre-Send`, you must specify the **Token Lifespan** for these token types; by default, the **Token Lifespan** is 1 day. You must also set the number of codes sent at a time in a message; by default, the **Codes/msg** is 3.

10. Click **OK**.

5.9.6 Managing a user's YubiKey OTP

You can manage a user's account options for a YubiKey OTP, including changing their PIN, through the user's Properties.

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU and user account to manage.
2. Click **Properties**, in the **Actions** pane.
3. Select the **YubiKey OTP** tab.

The screenshot shows a dialog box titled 'ame.threats Properties' with a close button (X) in the top right corner. The dialog has several tabs: 'General', 'AD Password', 'Devices', 'Temporary Access', 'FIDO', 'Push', 'Grid', 'Phrase', 'One Time Code', and 'YubiKey OTP'. The 'YubiKey OTP' tab is selected. Inside the dialog, there is a section titled 'Account options' containing the following controls:

- ☒ Enable account for YubiKey OTP
- ☐ User must change PIN at next logon
- ☒ PIN On ☐ PIN Off ☐ Use AD password as PIN
- Reset PIN button

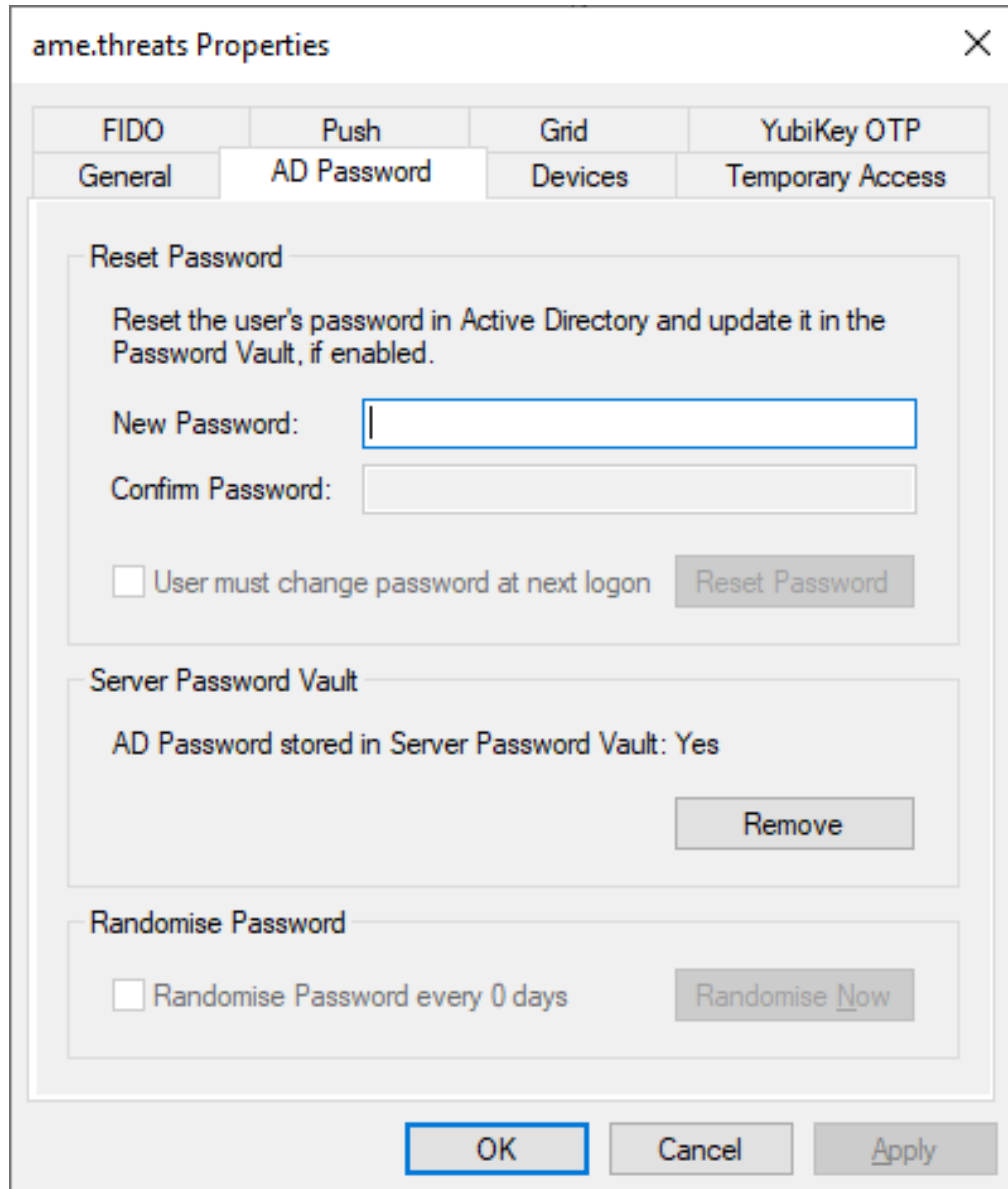
At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

4. You can specify whether the account is enabled for YubiKey OTP authentication by selecting or deselecting **Enable account for YubiKey OTP**.
5. You can set a user's YubiKey OTP PIN to expire the next time that they log in, forcing them to change the YubiKey OTP by selecting **User must change PIN at next logon**.
6. You can select what type of PIN is used for the YubiKey OTP:
 - **PIN On** – a set PIN for YubiKey OTPs is used with the YubiKey OTP.
 - **PIN Off** – no PIN is used, just the YubiKey OTP.
 - **User AD password as PIN** – the user's AD password is used with the YubiKey OTP.
7. To reset the user's YubiKey OTP PIN, click **Reset PIN**.

5.9.7 Managing user passwords

You can manage user passwords using the MMC. The extent to which you can manage a user's password depends on whether the user is imported from the Active Directory, or if they are an external MFA user.

5.9.7.1 Managing an Active Directory user's password



The screenshot shows the 'ame.threats Properties' dialog box with the 'AD Password' tab selected. The dialog has a title bar with a close button. Below the title bar are four tabs: 'FIDO', 'Push', 'Grid', and 'YubiKey OTP'. The 'AD Password' tab is active, showing three sections: 'Reset Password', 'Server Password Vault', and 'Randomise Password'. The 'Reset Password' section includes a description, two password input fields, a checkbox for 'User must change password at next logon', and a 'Reset Password' button. The 'Server Password Vault' section shows 'AD Password stored in Server Password Vault: Yes' and a 'Remove' button. The 'Randomise Password' section has a checkbox for 'Randomise Password every 0 days' and a 'Randomise Now' button. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

ame.threats Properties

FIDO Push Grid YubiKey OTP

General AD Password Devices Temporary Access

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

To manage an Active Directory user's password:

1. In the MyID Management Console, expand the **Domains** and select the appropriate OU.
2. Select the user account (or accounts) that you want to manage.
3. Click **Properties** in the **Actions** pane.

4. Select the **AD Password** tab.

From here, you can:

- Reset the user's password.
See section [5.9.7.2, Resetting an Active Directory user's password](#).
- Check if the password is in the MyID Server Password Vault.
See section [5.9.7.3, Managing an Active Directory user's password in the MyID Password Vault](#).
- Configure password randomization.
See section [5.9.7.4, Managing an Active Directory user's password randomization](#).

5.9.7.2 Resetting an Active Directory user's password

To reset an Active Directory user's password:

1. In the **AD Password** tab, type a **New Password** and confirm it by typing it again.
2. If you want the user to change the password when they next log in, select **User must change password at next logon**.
3. Click **Reset Password**.

Note: Users can reset their own passwords in the Self Service Portal; for more information, see the *Resetting your password* section in the [Self Service Portal User Guide](#).

5.9.7.3 Managing an Active Directory user's password in the MyID Password Vault

Note: To enable the MyID Password Vault, you must set the **Enable MyID Password Vault** setting in the Domain Properties. For more information, see section [5.4.1, Domain Properties dialog](#).

If the Active Directory user's password is in the MyID Server Password Vault, **AD Password stored in Server Password Vault** is set to **Yes** in the **AD Password** tab. If otherwise, it is set to **No**.

If the Active Directory user's password is in the MyID Server Password Vault, you can remove it by clicking **Remove**.

5.9.7.4 Managing an Active Directory user's password randomization

Note: To enable randomized passwords, and to configure how often the passwords are randomized, you must set the **Randomise AD Passwords every x days** setting in the Domain Properties. For more information, see section [5.4.1, Domain Properties dialog](#).

To enable the user for randomized passwords, on the **AD Password** tab, enable **Randomise Passwords every x days**.

To randomize the user's password immediately, click **Randomise now**.

5.9.7.5 Managing an external MFA user's password

The screenshot shows a dialog box titled "External.User.Example Properties" with a close button (X) in the top right corner. The dialog has several tabs: "General", "Password", "Devices", "Temporary Access", "FIDO", and "Push". The "Password" tab is currently selected. Inside the "Password" tab, there is a section titled "Server Password Vault". Below this title, it says "Password stored in Server Password Vault: No". To the right of this text is a "Remove" button. At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Apply". The "OK" button is highlighted with a blue border.

To manage an external MFA user's password:

1. In the MyID Management Console, expand the **Realms** and select the appropriate realm.
2. Select the user account (or accounts) that you want to manage.
3. Click **Properties**, in the **Actions** pane.
4. Select the **Password** tab.

If the external MFA user's password is in the MyID Server Password Vault, **Password stored in Server Password Vault** is set to **Yes**. Otherwise, it is set to **No**.
5. If the external MFA user's password is in the MyID Server Password Vault, to remove it, click **Remove**.

5.9.8 Assigning temporary access codes to a user

To assign a temporary access code to a user:

1. Ensure that **Allow Temporary Access Codes** is enabled on the global settings General tab.

For more information, see section [5.3.1, General tab](#).

2. In the MyID Management Console, either expand the **Domains** and select the appropriate OU, or expand the **Realms** and select the appropriate realm.
3. Select the user account (or accounts) that you want to manage.
4. Click **Properties**, in the **Actions** pane.
5. Select the **Temporary Access** tab.

The screenshot shows the 'ame.threats Properties' dialog box with the 'Temporary Access' tab selected. The dialog has a title bar with a close button (X). Below the title bar are tabs: 'General', 'AD Password', 'Devices', 'Temporary Access' (selected), 'FIDO', and 'Push'. The 'Temporary Access' tab contains two sections: 'Usage and Expiry' and 'Code Type'. In the 'Usage and Expiry' section, there is a checkbox 'Enable Temporary Access Code' which is currently unchecked. Below it are three radio button options: 'Expire after 3 logins or 22/03/2024 14:04:48' (selected), 'Expire after 3 logins', and 'Expire after 22/03/2024 14:04:48'. In the 'Code Type' section, there are two radio button options: 'Use Active Directory password' (selected) and 'Use static PIN / Password'. Below these is a text input field. At the bottom of the 'Code Type' section are three buttons: 'Random Code', 'Random Word', and 'Clear'. At the bottom of the dialog are three buttons: 'OK' (highlighted with a blue border), 'Cancel', and 'Apply'.

6. Select the **Enable Temporary Access Code** option.

The screenshot shows the 'ame.threats Properties' dialog box with the 'Temporary Access' tab selected. The 'Usage and Expiry' section has 'Enable Temporary Access Code' checked. Under 'Code Type', 'Use static PIN / Password' is selected, and the text 'phosphonic' is entered in the field below. The 'Random Word' button is highlighted.

Select when temporary access codes are automatically disabled. Options include at a specific date and time, after a specific number of uses or both; the default is both.

You can configure the user to use their existing Active Directory password as a temporary access code as it is something they should already know.

Alternatively, specify a PIN or a password for the user of at least six digits. To assist in choosing a PIN or password you can click the **Random Code** or **Random Word** buttons to create one for you.

7. Click **Apply** or **OK** to save the configured settings for the user account.

5.9.8.1 Known issues

- **IKB-441 – Unable to carry out an offline logon after using a temporary access code**

When the **Manage the Windows password** option is enabled on the **FIDO2** tab of the global settings, if you use a temporary access code before going offline, all cached credentials are cleared, preventing you from carrying out an offline logon with either biometric or non-biometric FIDO devices, even if you have successfully logged in with FIDO devices before.

5.9.9 Revoking specific users' refresh tokens

You can revoke the refresh tokens of a specific user or selected group of users.

When you revoke a user's refresh tokens:

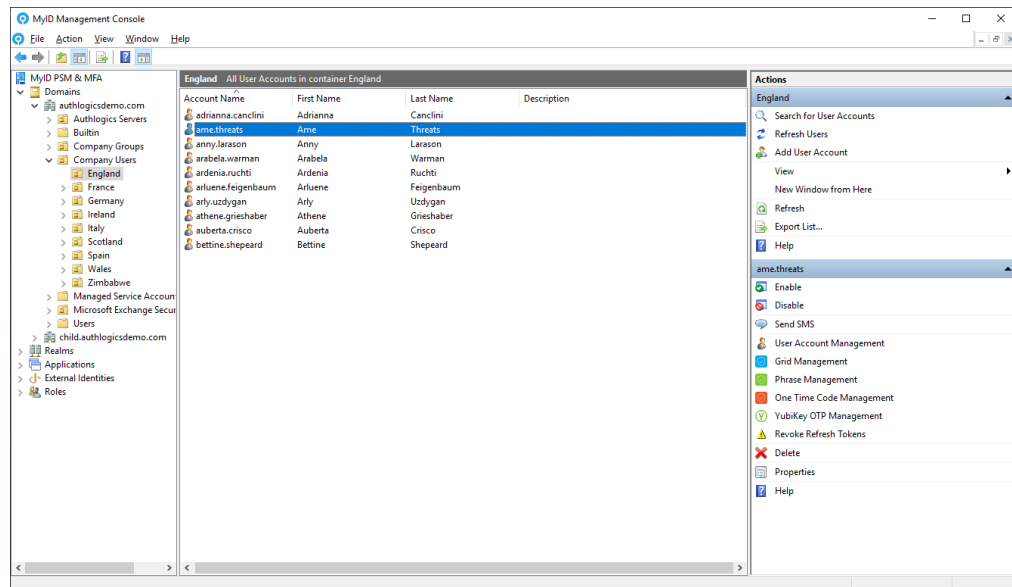
- Their access tokens expire based on the set **Access Token Lifetime**; when the access tokens expire, the users with those tokens must reauthenticate.
- They cannot change their mobile phone number or password in the Self Service Portal until they reauthenticate.

Users with revoked refresh tokens regain full functionality when they reauthenticate.

For more information on access and refresh tokens, see section [5.5.1.4, *Token Settings tab*](#).

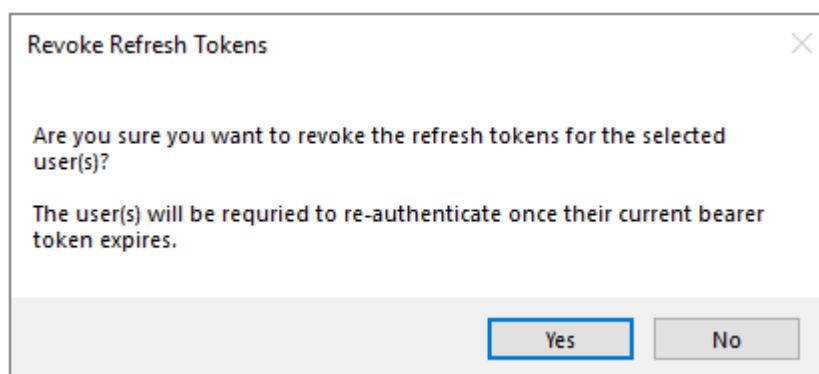
To revoke specific users' refresh tokens:

1. In the MyID Management Console, either expand the **Domains** and select the appropriate OU, or expand the **Realms** and select the appropriate realm.
2. Select the user account or accounts that for which you want to revoke the refresh tokens.



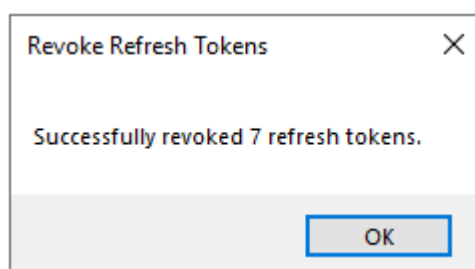
3. Click **Revoke Refresh Tokens**.

A pop-up appears to confirm that you want to revoke the refresh tokens of the user or users .



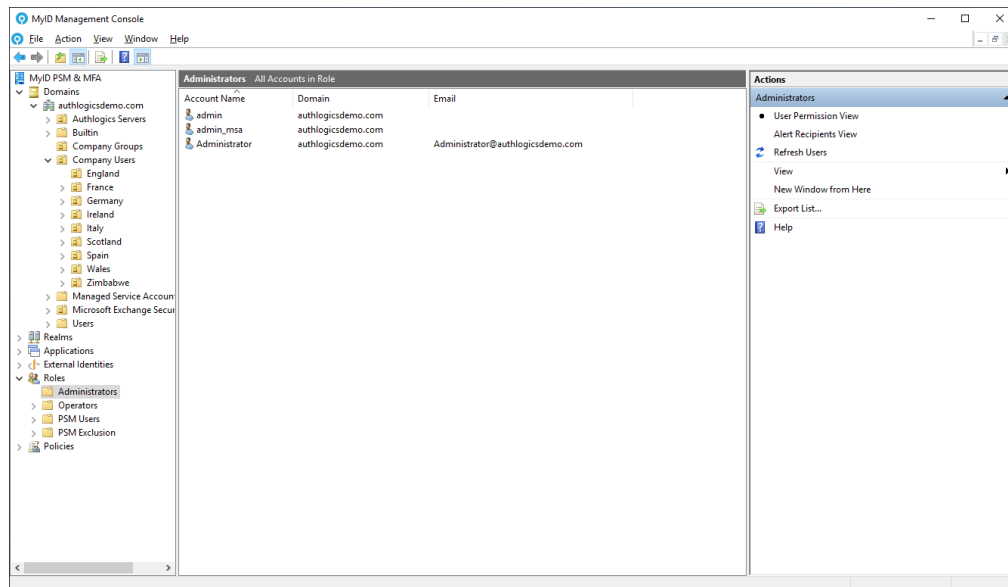
4. Click **Yes**.

A pop-up appears to confirm how many refresh tokens have been revoked.



5.10 Roles

The MyID Authentication Server provides administrators with the ability to assign rights to users for MyID administrative functions and product features. Users can be designated as Administrators and Operators.



Administrators can fully administer MyID using the MyID Management Console and can perform day-to-day operational functions using the Web Management Portal.

Operators can access the Web Management Portal, which provides day-to-day operational functions, but they do not have access to the MyID Management Console.

Auditors can view the Web Management Portal, but cannot change user settings.

If you have MyID PSM and you do not want to protect every account with PSM, user accounts that should be protected by PSM can be specified using the PSM Users role.

Note: Active Directory groups are created automatically for Administrators and Operators and are assigned to the roles by default. For all other roles, an Active Directory group must be created manually first.

You can:

- Use groups with roles.
See section [5.10.1, Active Directory Group types for roles](#).
- Work with administrator roles.
See section [5.10.2, Administrator role views](#).
- Manage administrative roles (the **Administrators** and **Operators** roles).
See section [5.10.3, Managing administrative roles](#).
- Manage the auditors role.
See section [5.10.4, Managing the Auditors role](#).
- Manage the role for PSM users.
See section [5.10.5, Managing the Password Security Management Users role](#).
- Manage the role for users excluded from remediation and alerts.
See section [5.10.6, Managing the Remediation and Alerts Exclusion role](#).

5.10.1 Active Directory Group types for roles

Both Global and Universal Security groups can be used with all MyID Roles. Group nesting is supported – groups may contain other groups.

In addition, both Global and Universal Distribution groups can be used with the MyID Administrators Role to allow people to receive administrative alerts, but not have administrative permissions. For more information, see section [5.10.2, Administrator role views](#).

For multi-domain forests, the groups can be created in any domain in the forest. It is recommended that Universal groups are used in multi-domain forests so that Global Catalog servers can be contacted to check role membership, otherwise, Domain Controllers from other domains may need to be contacted, which can affect performance depending on the infrastructure.

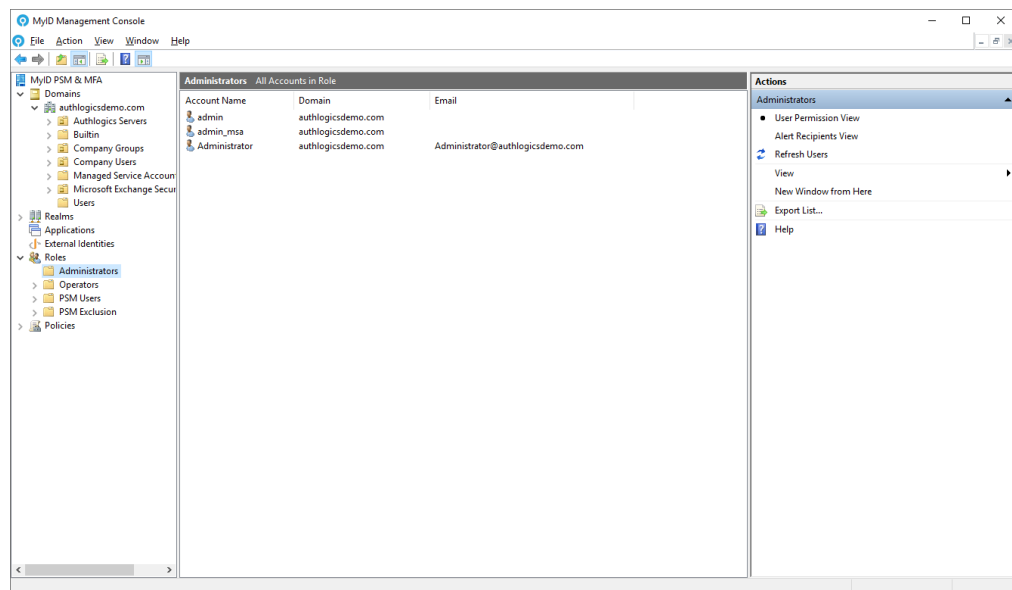
5.10.2 Administrator role views

The Administrator Role is dual purpose and therefore has the following views:

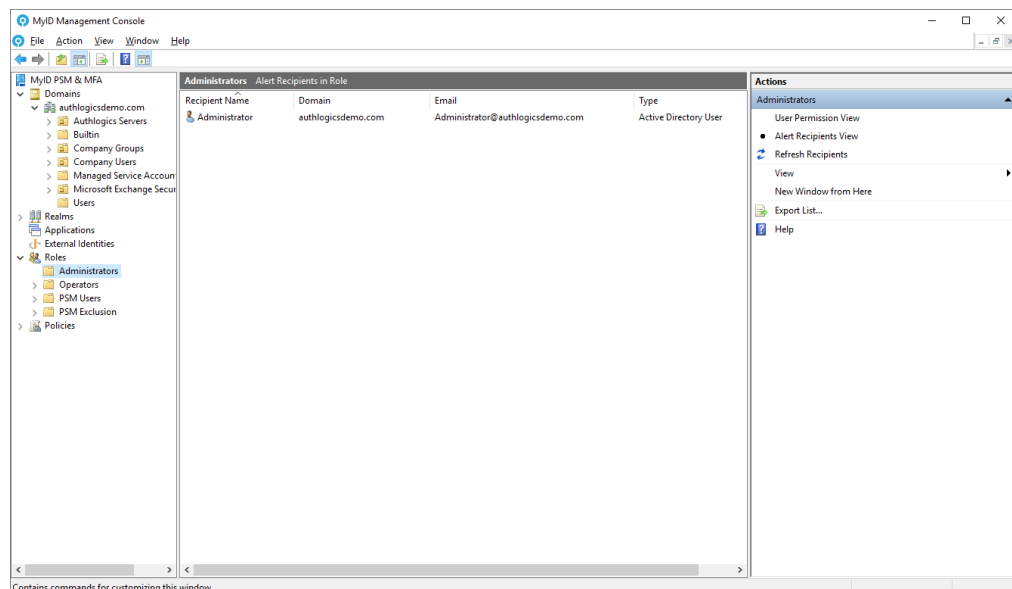
- **User Permissions View** – User accounts that have MyID Administrative permissions.
- **Alert Recipients View** – Email addresses that should receive Admin Alerts.

To toggle these views:

1. In the MyID Management Console, under **Roles**, expand **Administrators**.



2. In the **Actions** pane, select the view that you want.



This allows you to determine the resultant set of users of that case.

This feature may be useful if your admin personnel have split role user accounts and need to use their admin user account to perform administrative tasks but need to receive Admin Alerts on a non-admin user account.

Administrative Permissions can only be assigned to Active Directory User Accounts through either direct membership of the MyID Administrators group, or by being a member of a nested **Security group** (Global or Universal). Permissions are not assigned to Active Directory Contacts or through membership of a Distribution Group. The existence of an email address on a user account or group has no effect.

Admin Alerts can be sent to Active Directory User Accounts, Contacts or Groups (Global or Universal, Security or Distribution) that have an email address configured. They can be direct members of the Authlogics Administrators group, or a member of a nested Security or Distribution group (Global or Universal). If a nested group does not have an email address configured on it, the members of the group are processed individually, including other nested groups. However, if a group does have an email address configured on it, the email address of the group is used, and the members of the group are ignored, leaving the email system (for example, Microsoft Exchange) to deliver the email to the group members.

To use split role user accounts for Admin Alerts, create a Distribution group in the Active Directory, add the non-admin user accounts to it, then add the group to the Authlogics Administrators group.

When using Microsoft Exchange, create a Mail Enabled Distribution group, add the non-admin user accounts to it, then add the group to the Authlogics Administrators group. MyID then sends Admin Alerts to the group and not directly to the member.

5.10.3 Managing administrative roles

Role membership is managed through the corresponding Active Directory groups. These groups are created during the directory configuration and can be renamed and moved to different OUs as needed. You *must not* delete these groups.

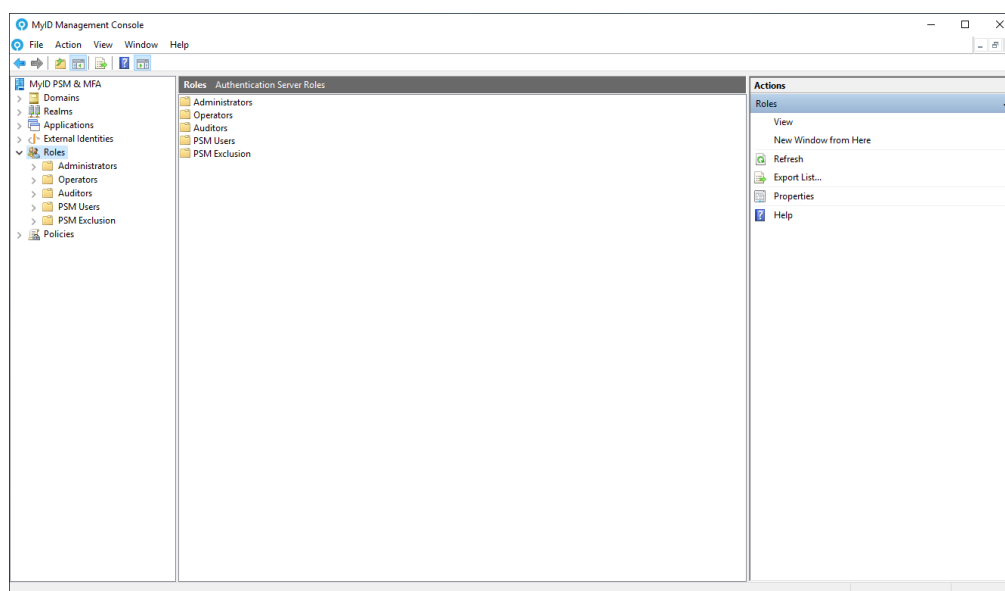
Non-administrative roles are optional and the group filtering for the role can be enabled or disabled as needed.

Role members cannot be added and removed using the MyID Management Console – this must be done by editing the appropriate Windows group using either the Active Directory Users and Computers MMC, or the Local Users and Groups MMC.

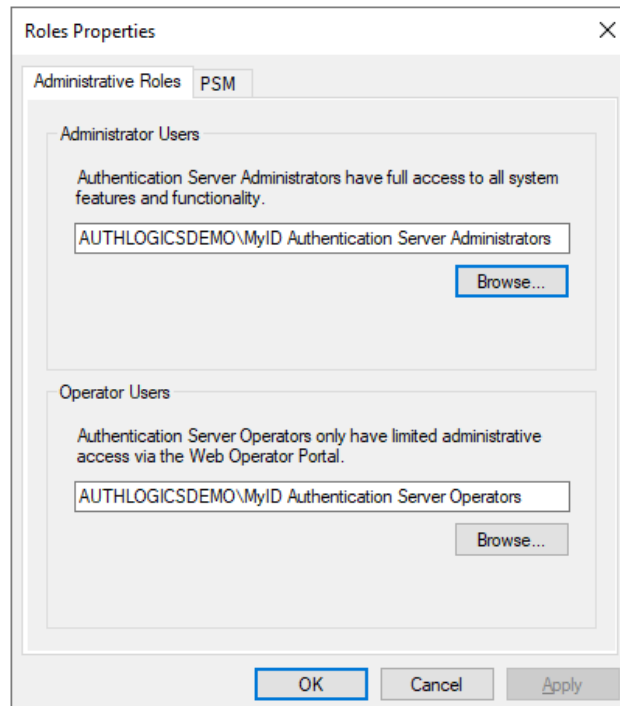
Note: When assigning Active Directory groups to MyID administrative roles, the Active Directory groups must already exist in the domain.

To assign Active Directory groups to MyID administrative roles:

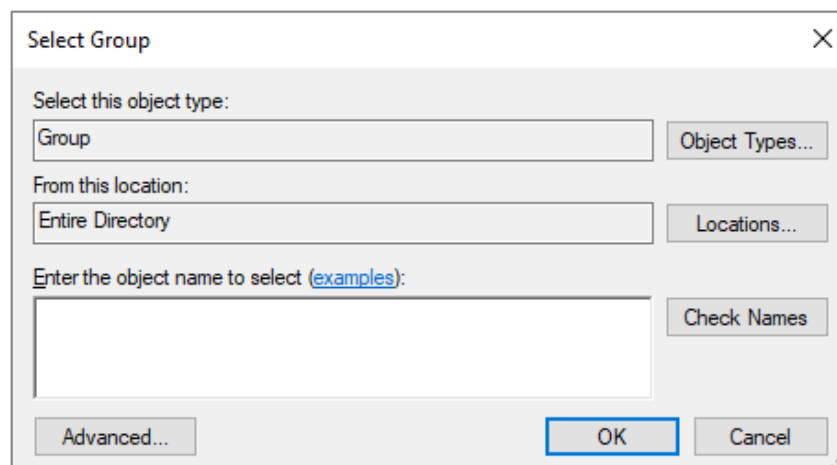
1. In the MyID Management Console, highlight the **Roles** node.



2. Click **Properties**, in the **Actions** pane.

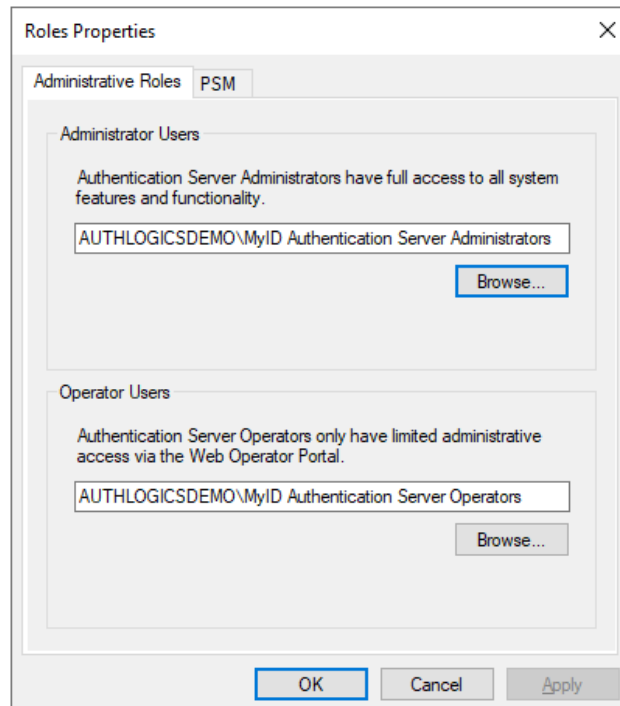


3. To select administrators, click **Browse** in the Administrator Users section.

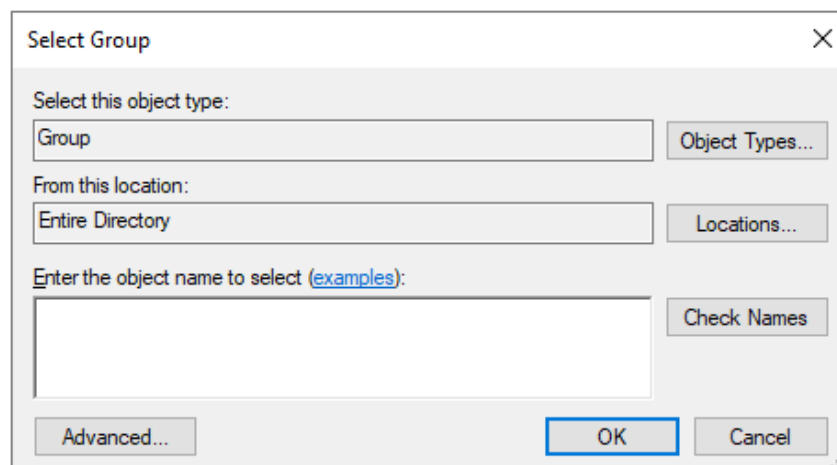


4. Locate the Active Directory group.

5. Click **OK**.



6. To select operators, click **Browse** in the Operator Users section.



7. Locate the Active Directory group.
8. Click **OK** to close the Select Group dialog.
9. Click **OK** to close the Roles Properties dialog.

You can view the users that have the Administrator Users and Operator Users roles in the **Administrators** and **Operators** sections, respectively, under **Roles**. You may need to refresh the users by clicking **Refresh** in the Action pane.

5.10.4 Managing the Auditors role

You can grant users read-only access to the Web Management Portal. This allows them to view dashboards, reports, and individual users' settings, but does not allow them to change user settings.

To enable a user for read-only access to the Web Management Portal, you must put the user in the Active Directory group assigned to the Auditors role.

The Active Directory group assigned to the Auditors role is the **MyID Authentication Server Auditors** group.

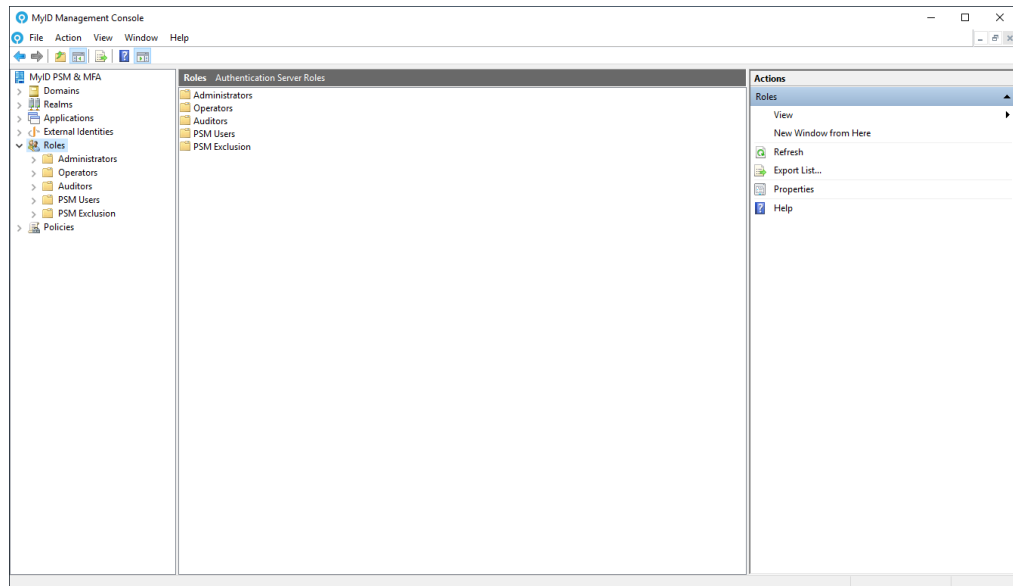
You can view the members of the Auditors role in the **Auditors** section, under **Roles**. You may need to refresh the users by clicking **Refresh** in the Action pane.

Note: If the user is enabled for both read-only access and full access of the Web Management Portal, they can fully access the Web Management Portal. Users with the **Administrators** or **Operators** role have full access to the Web Management Portal.

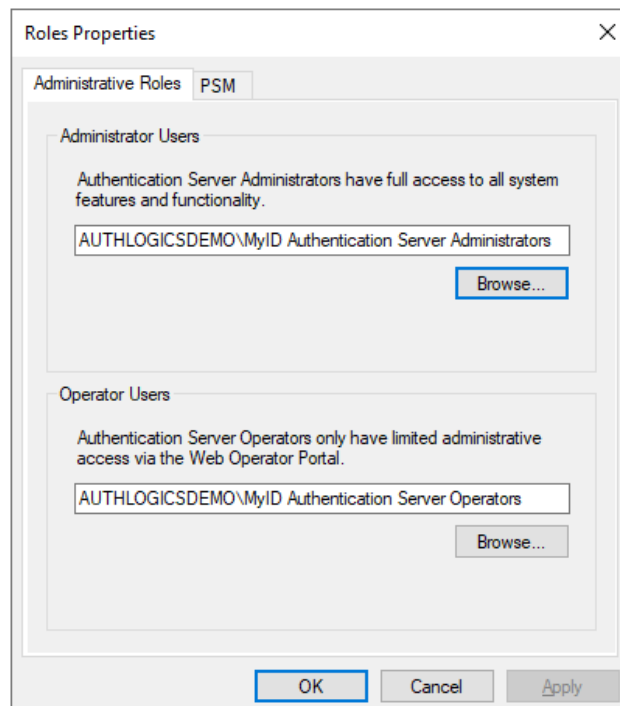
5.10.5 Managing the Password Security Management Users role

To assign an Active Directory group to the MyID Password Security Management Users role:

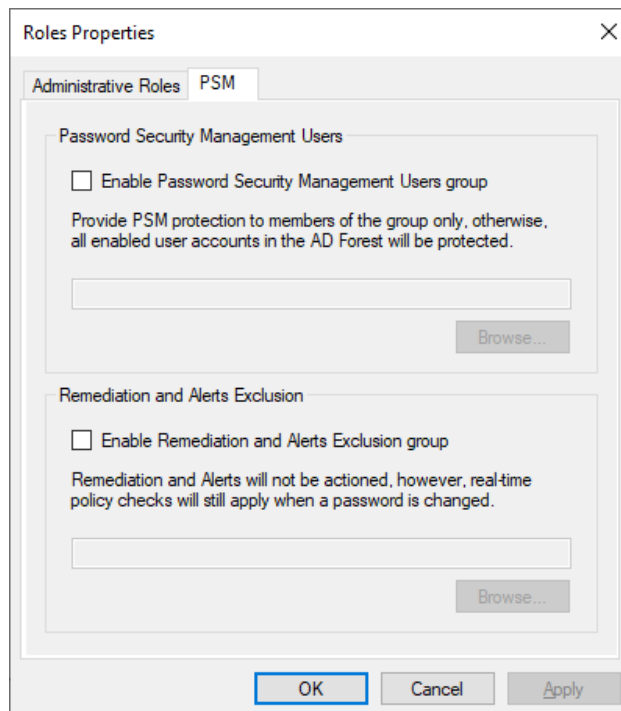
1. In the MyID Management Console, highlight the **Roles** node.



2. Click **Properties**, in the **Actions** pane.

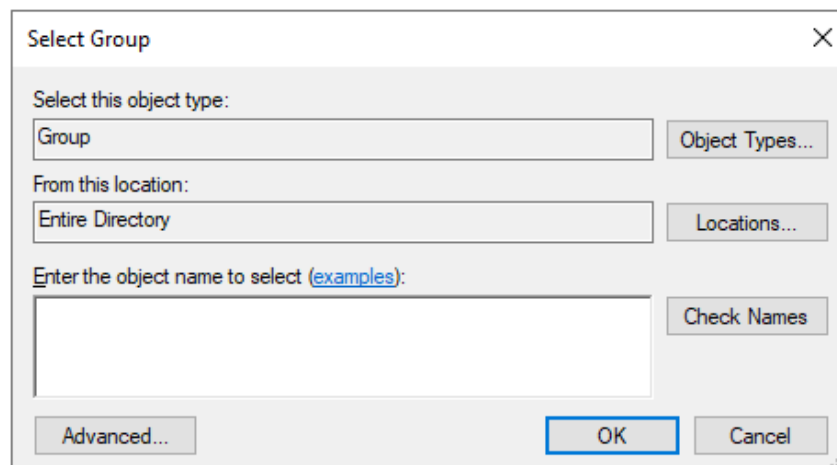


3. Select the **PSM** tab.



The image shows the 'Roles Properties' dialog box with the 'PSM' tab selected. The 'Administrative Roles' tab is also visible. The 'Password Security Management Users' section has an unchecked checkbox 'Enable Password Security Management Users group'. Below it is a text box and a 'Browse...' button. The 'Remediation and Alerts Exclusion' section also has an unchecked checkbox 'Enable Remediation and Alerts Exclusion group', a text box, and a 'Browse...' button. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

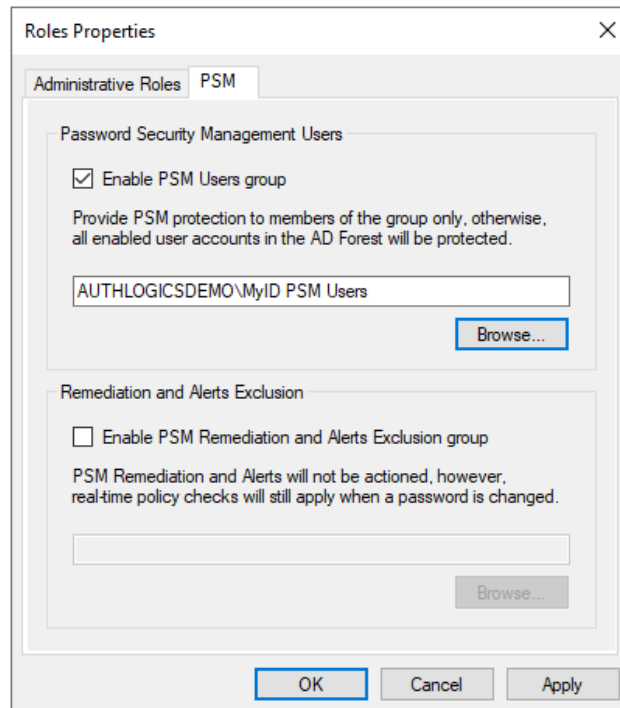
4. Select the **Enable Password Security Management Users group** option.
5. Click **Browse**.



The image shows the 'Select Group' dialog box. It has three main sections: 'Select this object type:' with a dropdown set to 'Group' and an 'Object Types...' button; 'From this location:' with a dropdown set to 'Entire Directory' and a 'Locations...' button; and 'Enter the object name to select (examples):' with a text box and a 'Check Names' button. At the bottom are 'Advanced...', 'OK', and 'Cancel' buttons.

6. Locate the Active Directory Password Policy group that you created.

7. Click **OK**.



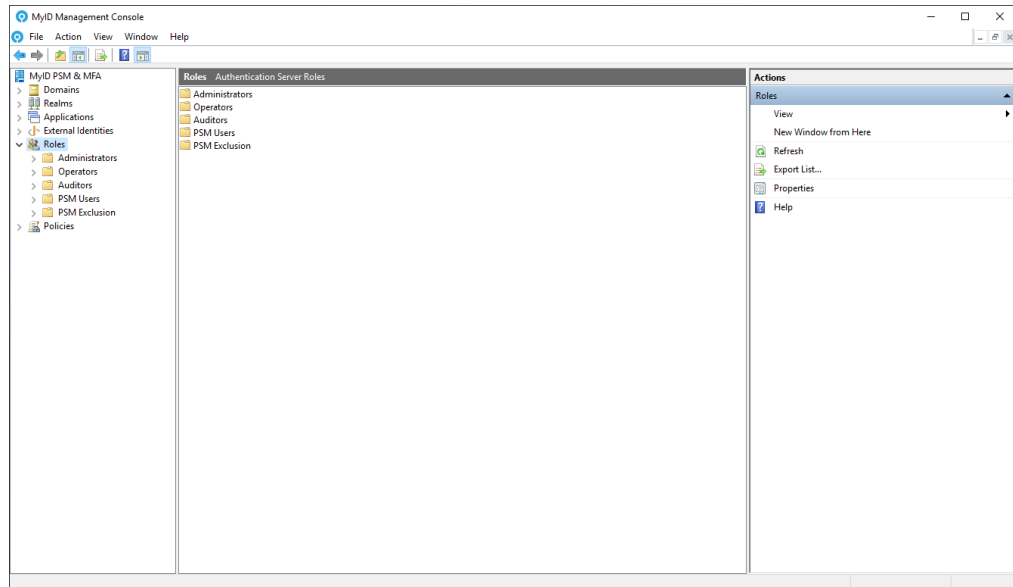
8. Click **OK**.

You can view the members of the Password Security Management Users role in the **PSM Users** section, under **Roles**. You may need to refresh the users by clicking **Refresh** in the Action pane.

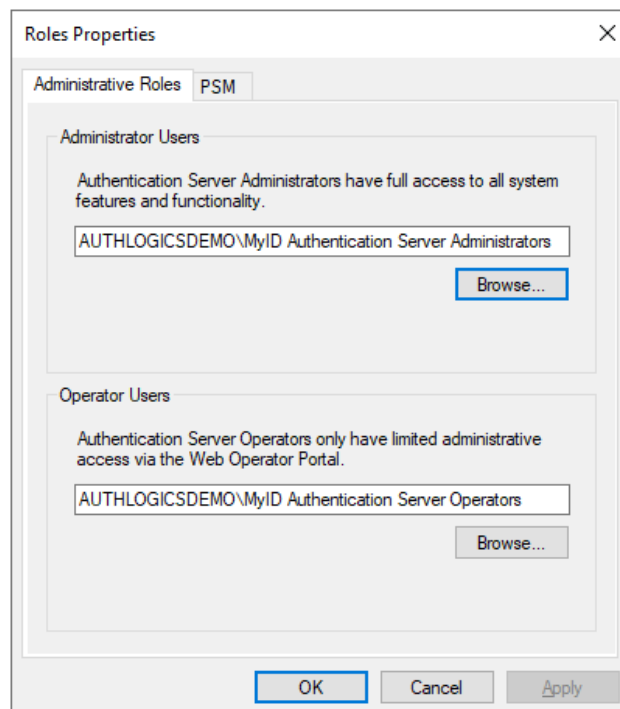
5.10.6 Managing the Remediation and Alerts Exclusion role

You can create a group that is not affected by alert or remediation policies; administrators do not receive alerts regarding the members of this group, and the members of this group do not have to carry out remediation actions. To enable the Remediation and Alerts Exclusion role and assign an Active Directory group to the role:

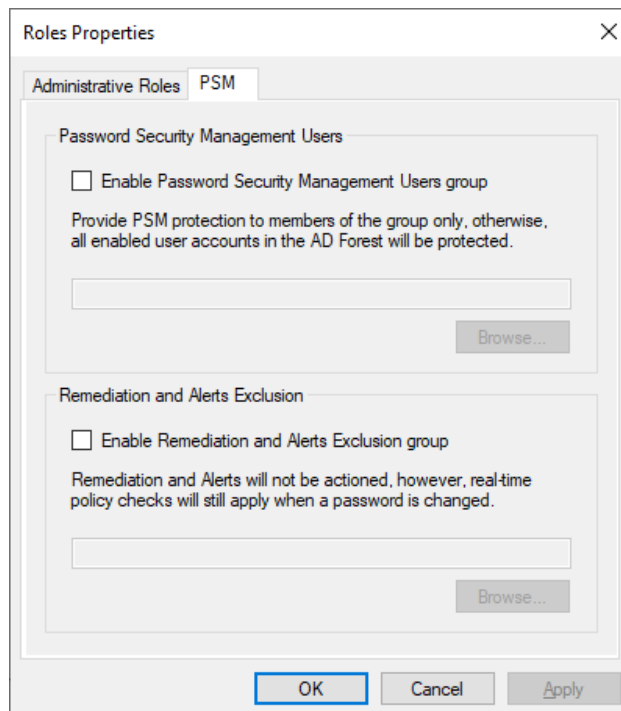
1. In the MyID Management Console, highlight the **Roles** node.



2. Click **Properties**, in the **Actions** pane.



3. Select the **PSM** tab.



The image shows the 'Roles Properties' dialog box with the 'PSM' tab selected. It contains two sections: 'Password Security Management Users' and 'Remediation and Alerts Exclusion'. Each section has an unchecked checkbox, a descriptive text, an empty text box, and a 'Browse...' button. At the bottom are 'OK', 'Cancel', and 'Apply' buttons.

Roles Properties

Administrative Roles PSM

Password Security Management Users

☐ Enable Password Security Management Users group

Provide PSM protection to members of the group only, otherwise, all enabled user accounts in the AD Forest will be protected.

Browse...

Remediation and Alerts Exclusion

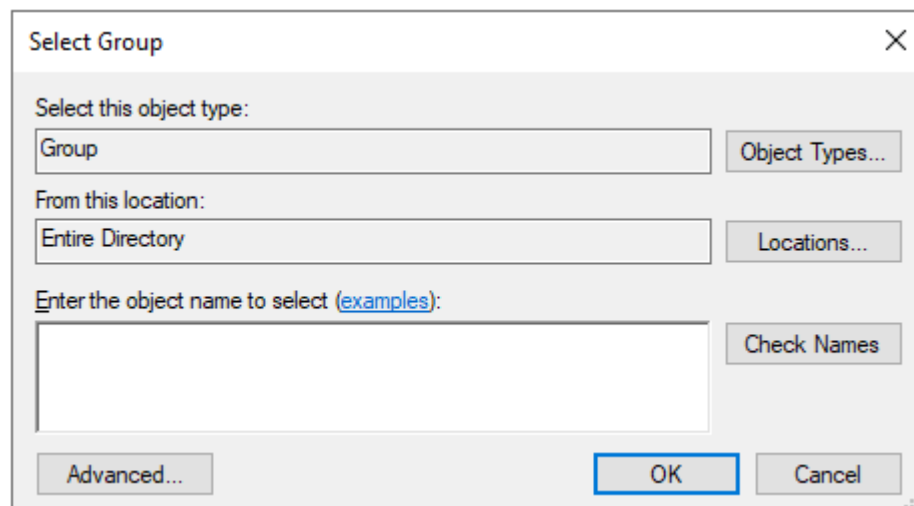
☐ Enable Remediation and Alerts Exclusion group

Remediation and Alerts will not be actioned, however, real-time policy checks will still apply when a password is changed.

Browse...

OK Cancel Apply

4. Select the **Enable Remediation and Alerts Exclusion group** option.
5. Click **Browse**.



The image shows the 'Select Group' dialog box. It has fields for 'Select this object type:' (set to 'Group'), 'From this location:' (set to 'Entire Directory'), and 'Enter the object name to select (examples):'. There are buttons for 'Object Types...', 'Locations...', 'Check Names', 'Advanced...', 'OK', and 'Cancel'.

Select Group

Select this object type:

Group Object Types...

From this location:

Entire Directory Locations...

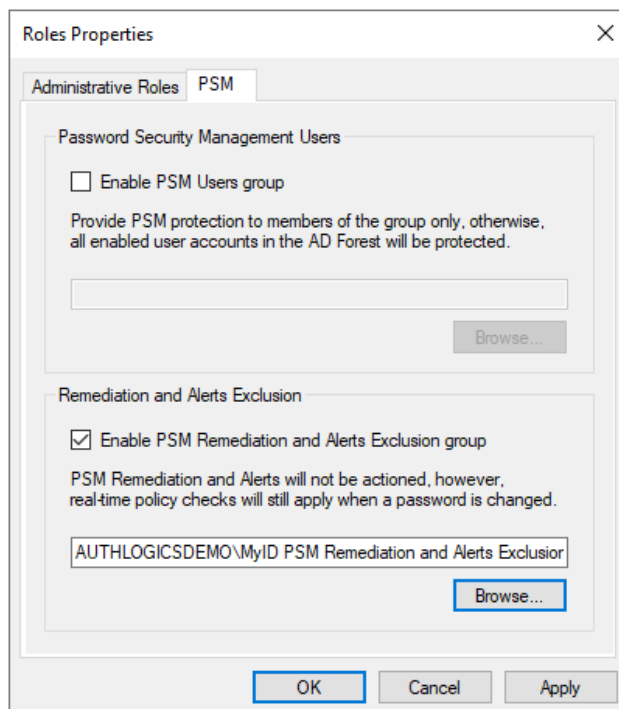
Enter the object name to select (examples):

Check Names

Advanced... OK Cancel

6. Locate the Active Directory Password Policy group that you created.

7. Click **OK**.



8. Click **OK**.

You can view the members of the Remediation and Alerts Exclusion role in the **PSM Exclusion** section, under **Roles**. You may need to refresh the users by clicking **Refresh** in the Action pane.

You can also enable the Remediation and Alerts Exclusion role and assign an Active Directory group to the role from the Remediation tab of the global settings; for more information, see section [5.3.4, Remediation tab](#).

5.11 Policies

The MyID Authentication Server provides administrators with the ability to manage policies.

You can manage the following type of policy:

- Access control policies

See section [5.11.1, Access control policies](#).

5.11.1 Access control policies

Access control policies allow you to specify who can access RADIUS authentication or applications.

5.11.1.1 Adding an access control policy

To add an access control policy:

1. In the MyID Management Console, under the **Policies** node, highlight the **Access Control Policy** node.
2. Click **Add Policy** in the **Actions** pane.

The Add a new Policy dialog opens.

3. Select the features to which the policy can apply.

You can select the following options:

- **RADIUS** – select this option, and you can view and edit the RADIUS options of this policy on the **RADIUS** tab of the global settings. For more information, see the section [5.3.2, RADIUS tab](#).
- **Applications** – select this option, and you can use the **Access Control** tab on the application properties dialog to enable policies for the application, then use those policies on the **Internal Authentication** or **External Authentication** tabs. For more information, see section [5.11.1.4, Access control policies for applications](#).

You can enable one or both of these options.

4. Type a **Policy Name**.

This field is mandatory. The name of your policy must be unique.

5. Type a **Policy Priority**.

This must be a value between 1 and 255.

Policies are evaluated in order of priority – if a user matches multiple policies, the policy with the highest priority takes effect; lower numbers represent a higher priority.

This field is mandatory.

6. If you want this policy to apply only to specific IP address, enable the **Apply policy to the following IP addresses (RADIUS only)** option and type one or more IP addresses.

If you enter more than one IP address, each new IP address must be on a new line.

This option is available only if you enable the policy for RADIUS, as applications do not support filtering by IP address. If you specify that the access control policy is for both RADIUS and applications, and specify one or more IP addresses to filter, the IP address list is used for RADIUS, but ignored for applications.

Note: Only IP addresses are supported; DNS names in this field cause RADIUS authentication to fail.

7. If you want this policy to apply only to specific groups:

Note: These groups must be configured in the Active Directory *before* you add the new policy.

- a. Enable the **Apply policy to the following groups of users** option.
- b. Click **Add** and select the groups to which you want the policy to apply.

Select Groups

Select this object type:
Groups Object Types...

From this location:
Entire Directory Locations...

Enter the object names to select (examples):
Check Names

Advanced... OK Cancel

- c. Click **OK**.

Add a new Policy

Access Control Policy

Enable the policy for : ☒ RADIUS ☒ Applications

Policy Name: Policy Priority:

My Policy 1

☒ Apply policy to the following IP address (RADIUS only):

192.168.200.3
192.168.200.4

☒ Apply policy to the following groups of users:

AUTHLOGICSDEMO\MyID Authentication Server Administrators
AUTHLOGICSDEMO\MyID Authentication Server Operators

Add

OK Cancel

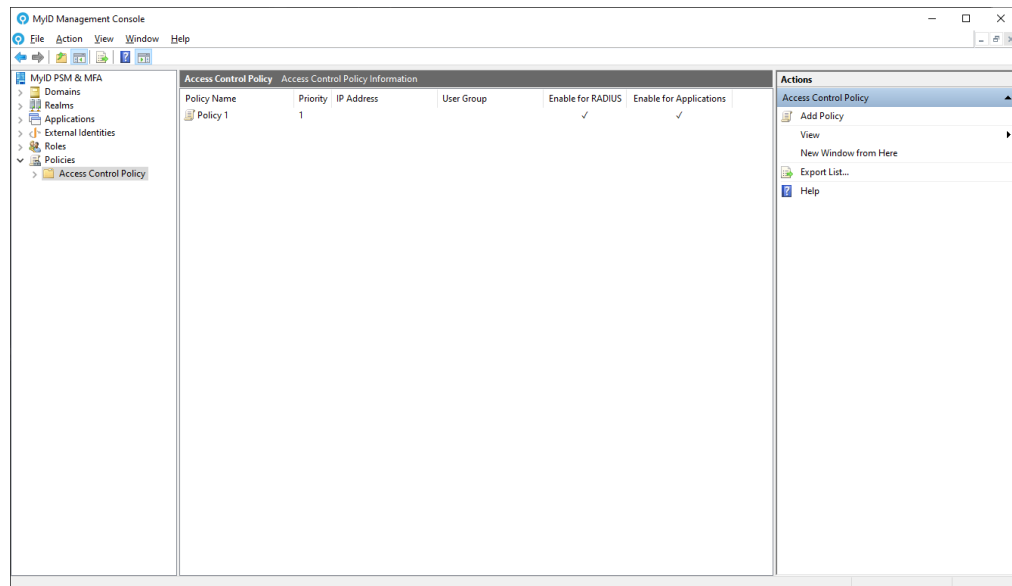
8. Click **OK**.

Note: If a section is invalid, it has a red background. If any section is invalid, the **OK** button is disabled.

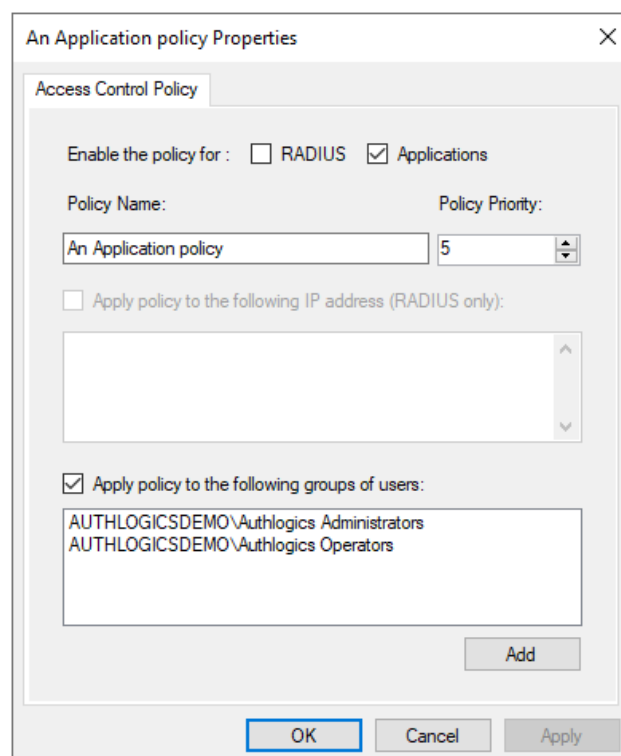
5.11.1.2 Editing an access control policy

To edit an access control policy:

1. In the MyID Management Console, under the **Policies** node, open the **Access Control Policy** node.



2. Double-click the access control policy you want to edit.



To remove a group from the list, select it and press the Delete key, or right-click the group and from the pop-up menu select **Delete**.

Note: To add a new line to the IP addresses list, you must press the Down Arrow key from your current final line or click below your current final line. You must not press Enter; Enter automatically maps to the **OK** button and closes the dialog.

Important: If you have not made changes, or if your changes are invalid, the **Apply** button is disabled. If a section is invalid, it has a red background. If you click **OK** with any invalid information in the application properties dialog, your changes are not applied.

5.11.1.3 Deleting an access control policy

To delete an access control policy:

1. In the MyID Management Console, under the **Policies** node, open the **Access Control Policy** node.
2. Highlight the access control policy that you want to delete and click **Delete** in the **Actions** pane, or right click the policy and click **Delete**.

5.11.1.4 Access control policies for applications

When you create access control policies for applications, you can configure your applications with different authentication options for different policies.

Use the **Access Control** tab on the Properties dialog for your application to specify which policies apply to the application, then use the **Internal Authentication** and **External Authentication** tabs to configure your authentication options for each policy.

See:

- Self Service Portal – section [5.5.2.1, Access Control tab](#).
- Web Management Portal – section [5.5.3.1, Access Control tab](#).
- Windows Desktop Agent – section [5.5.4.1, Access Control tab](#).
- OpenID Connect applications – section [5.5.5.1, Access Control tab](#).
- Client Credential applications – section [5.5.6.1, Access Control tab](#).
- SAML 2.0 applications – section [5.5.7.1, Access Control tab](#).

If you attempt to access the application using an authentication method that is not permitted by the policy that applies to you, you are prevented from accessing the application.

You are not authorised to access this application

If you attempt to access the application, but no authentication methods are configured for the application, an error stating that authentication is not enabled is displayed.

Authentication is not enabled

For information on accessing your applications through the IdP page, see section [5.5.8, Accessing applications through the IdP page](#).

5.12 Customizing the portal interfaces

You can customize the portal interfaces in the following ways:

- Customize authentication for the Web Management Portal or the Self Service Portal.
See section [5.12.1, Portal authentication type settings](#).
- Customize the password setting tooltips in the Self Service Portal.
See section [5.12.2, Self Service Portal password tooltips](#).
- Customize the IdP logon page.
See section [5.12.3, IdP Logon Page customization](#).
- Customize the Self Service Portal.
See section [5.12.4, SSP customization](#).
- Carry out advanced customization of the Self Service Portal.
See section [5.12.5, Advanced Self Service Portal UI customization](#).

5.12.1 Portal authentication type settings

The Self Service Portal and Web Management Portal support both Windows Authentication and other forms of authentication – for example, One Time Codes and Grids.

A logon page can be displayed to require strong authentication using MyID supported MFA technologies or password. See section [5.5.3, Web Management Portal Properties](#) and section [5.5.2, Self Service Portal Properties](#) for details.

5.12.1.1 Using Deviceless OTP with non-Windows authentication

MyID Grid Pattern and Phrase questions can be displayed on the login page to cater for Deviceless OTP authentication. If Deviceless OTP authentication is not required, the logon challenge can be disabled on the logon page.

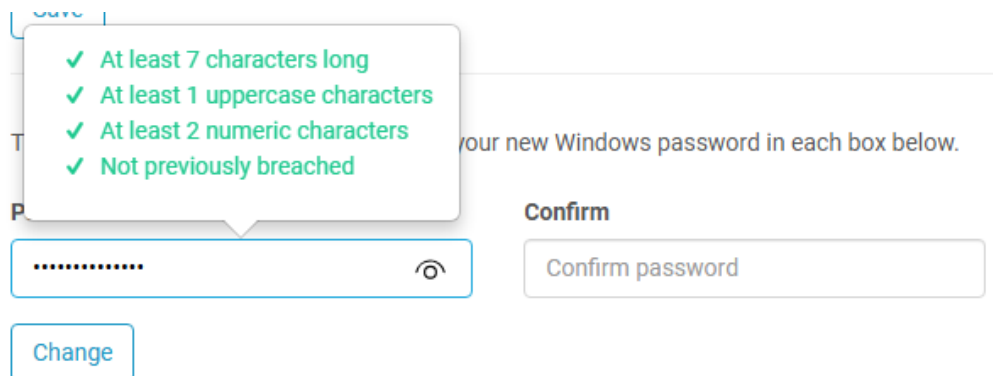
To allow this, enable the **Allow deviceless** option on the relevant portal.

5.12.2 Self Service Portal password tooltips

When a user resets their password using the Self Service Portal, they are shown tooltips along with ticks and crosses to indicate which policies their password aligns with and which it does not. Each tooltip relates to a Password Security Management GPO.

Tooltips can be displayed in one of the following situations:

- As the user types in their password.



The screenshot shows a password reset form. A tooltip is displayed over the password input field, listing four requirements with green checkmarks: 'At least 7 characters long', 'At least 1 uppercase characters', 'At least 2 numeric characters', and 'Not previously breached'. The form includes a password input field with a toggle for visibility, a 'Confirm' section with a 'Confirm password' input field, and a 'Change' button.

- When the user clicks **Change**.

Password invalid. Choose a password with:
No more than 3 keyboard characters in a sequence (e.g. querty)
At least 14 characters long

For information on resetting your password as a user, see the *Resetting your password* section of the [Self Service Portal User Guide](#).

To customize the tooltips:

- On your MyID Authentication Server, navigate to the Self Service Portal `config.js` file.
By default, this is in the following location:
`C:\Program Files\Authlogics Authentication Server\Web\SSP\wwwroot\js`
- Back up the `config.js` file before making any changes.
- To customize the order of the tooltips, change the order of the policies in the `PolicyDisplayOrder` list.

For information on which policies are related to which tooltips, see section [5.12.2.1, Tooltip Group Policy Objects and defaults](#).

Any policies you do not include in the `PolicyDisplayOrder` list are still displayed, but appear below the policies you include in the list.

For more information on PSM password policies, see section [7, Configuring the PSM password policy](#).

4. To customize the text of a tooltip, in the relevant node, set the `text` to your personalized text.

By default, the `config.js` file contains references to a localization function that returns the default text in the appropriate language.

For example:

```
text: jsLocalizer["PSMMinSpecialChars"]
```

You can override this to provide your own text for each tooltip.

For example:

```
text: "You have not used a sufficient number of special characters."
```

You can use `{value}` as a placeholder for the number set in the relevant policy. You can also use `{value-1}` and `{value+1}`.

Do not attempt to use the `{value}` placeholder if the relevant policy does not contain a number to set.

For example:

```
text: "You must have {value} special characters or more."
```

or

```
text: "You must have more than {value-1} special characters."
```

Note: Because the customized text overrides the localization function, customized tooltip text cannot currently be translated.

You can revert the text of a tooltip back to the default, translatable state. For information on the default values for the tooltips, see section [5.12.2.1, Tooltip Group Policy Objects and defaults](#).

5. To prevent a tooltip from displaying when the user is typing, and instead show only when the user attempts to set a password that does not work for that policy, in the relevant node, set `errorOnly` to `true`.
6. Back up your customized `config.js` file.
Your customized file may be overwritten when upgrading.
7. Copy your `config.js` file to Self Service Portal folder on your other MyID Authentication Servers.
8. To ensure your changes are immediately enforced, you must refresh the application pool. To recycle the Self Service Portal application pool:
 - a. On the MyID Authentication Server, in Internet Information Services (IIS) Manager, select **Application Pools**.
 - b. Right-click the **Authlogics Authentication Server SSP** application pool, then from the pop-up menu click **Recycle**.
9. Refresh any open Self Service Portal tabs.

5.12.2.1 Tooltip Group Policy Objects and defaults

Tooltip	Group Policy Object	Default
AllowUsername	Allow Full User Account name in password	jsLocalizer["PSMAAllowUsername"]
DisableSharedPasswordProtection	Disable Shared Password Protection	jsLocalizer["PSMDisableSharedPasswordProtection"]
DisableBreachDatabaseChecking ¹	Disable Online Password Breach Database checking Disable Offline Password Breach Database checking	jsLocalizer["PSMDisableOnlineBreachDatabase"]
DisableCustomBlacklist	Disable Custom Password Blacklist checking	jsLocalizer["PSMDisableCustomBlacklist"]
DisallowMonthAndDay	Disallow Month and Day names	jsLocalizer["PSMDisallowMonthAndDay"]
DisallowSpaces	Disallow spaces	jsLocalizer["PSMDisallowSpaces"]
DisallowNumericOnlyChanges	Disallow Incremental / Numeric-Only changes	jsLocalizer["PSMDisallowNumericOnlyChanges"]
DisallowFirstOrLastNumeric	Disallow First or Last Character being a number	jsLocalizer["PSMDisallowFirstOrLastNumeric"]

¹The `DisableBreachDatabaseChecking` tooltip requires at least one of the two related policies to be disabled to appear.

Tooltip	Group Policy Object	Default
MaxAllowedUsernameCharacters	Maximum Allowed characters from User Account name	jsLocalizer["PSMMaxAllowedUsernameCharacters"]
MaxLength	Maximum Password Length	jsLocalizer["PSMMaxLength"]
MaxRepeatingChars	Maximum Repeating Characters	jsLocalizer["PSMMaxRepeatingChars"]
MaxConsecutiveRepeatingChars	Maximum Consecutive Repeating Characters	jsLocalizer["PSMMaxConsecutiveRepeatingChars"]
MaxSequentialChars	Maximum Sequential Characters	jsLocalizer["PSMMaxSequentialChars"]
MaxSequentialKeyBoardChars	Maximum Sequential Keyboard Characters	jsLocalizer["PSMMaxSequentialKeyBoardChars"]
MinLength	Minimum Password Length	jsLocalizer["PSMMinLength"]
MinLowerCaseChars	Minimum Lowercase Characters	jsLocalizer["PSMMinLowerCaseChars"]
MinNumericChars	Minimum Numeric Characters	jsLocalizer["PSMMinNumericChars"]
MinSpecialChars	Minimum Special Characters	jsLocalizer["PSMMinSpecialChars"]
MinUnicodeChars	Minimum Unicode Characters	jsLocalizer["PSMMinUnicodeChars"]
MinUpperCaseChars	Minimum Uppercase Characters	jsLocalizer["PSMMinUpperCaseChars"]

5.12.3 IdP Logon Page customization

You can customize the branding look of the IdP logon page. To do this:

1. If you do not have an `appsettings.Production.json` file for the IdP logon page, create it in the IdP settings folder. By default this is the following location:

`C:\Program Files\Authlogics Authentication Server\Web\IdP`

Note: Do not use the `appsettings.json` file – that file can be overwritten when you update or upgrade MyID MFA and PSM.

2. In a text editor, open the `appsettings.Production.json` file for the IdP logon page.
3. Create a `Customisation` section. Within this section you can set the following values:

Option	Default value	Details
LogoPath	/img/logo-colour-transparent.png	A full or relative path to a graphic file such as a company logo.
UserGuideUrl	The URL of the current version of the SSP guide.	A full or relative path to a downloadable user guide document.
PasswordLabelText	Password	Any custom text to help the user know which password is required; for example, Coprnet Password.

For example:

```
{
  "Customisation": {
    "LogoPath": "/img/my-personal-logo.png",
    "UserGuideUrl": "https://www.intercede.com/download/myid-self-service-portal-user-guide-5-1",
    "PasswordLabelText": "Password",
  }
}
```

Note: Due to the limitations of PDFs, some whitespace characters may not come across cleanly. You are recommended to validate and sanitize your JSON; for example, you can use a JSON reformatter.

If you do not specify a value for an option, the default value is used.

4. Save the `appsettings.Production.json` file.
5. To ensure that this change is immediately enforced, you must refresh the application pool. To recycle the IdP application pool:
 - a. On the MyID Authentication Server, in Internet Information Services (IIS) Manager, select **Application Pools**.
 - b. Right-click the **Authlogics Authentication Server IdP** application pool, then from the pop-up menu click **Recycle**.
6. Check that the MyID MFA and PSM server is still operational by logging in to the Web Management Portal or the Self Service Portal.

5.12.4 SSP customization

You can customize the branding look and other user interface features of the Self Service Portal page. To do this:

1. If you do not have an `appsettings.Production.json` file for the Self Service Portal, create it in the Self Service Portal settings folder. By default this is the following location:

`C:\Program Files\Authlogics Authentication Server\Web\SSP`

Note: Do not use the `appsettings.json` file – that file can be overwritten when you update or upgrade MyID MFA and PSM.

2. In a text editor, open the `appsettings.Production.json` file for the Self Service Portal logon page.
3. Create a **Customisation** section. Within this section you can set the following values:

Option	Default value	Details
Title	Self Service Portal	Any custom text. The title of the SSP web page.
DisplayText	Self Service Portal	Any custom text. This is displayed at the top of the SSP web page.
LogoPath	/ssp/img/myid-none-grey.png	A full or relative path to a graphic file such as a company logo.
UserGuideUrl	The URL of the current version of the SSP guide.	A full or relative path to a downloadable user guide document.
PasswordLabelText	Password	Any custom text to help the user know which password is required; for example, Coprnet Password.

Option	Default value	Details
IncreasedAccessibilityRequirements	False	If set to <code>True</code> , this enables the high-contrast UI customization. For more information, see section 5.12.5, Advanced Self Service Portal UI customization .
ShowResetPinGridIndicators	True	If set to <code>False</code> , the user cannot choose to display the numbered indicators that appear when they click on the grid on the Grid Settings screen.

For example:

```
{
  "Customisation": {
    "Title": "Self Service Portal",
    "DisplayText": "My favourite Self Service Portal!",
    "LogoPath": "/ssp/img/my-logo-for-the-ssp.png",
    "UserGuideUrl": "https://www.intercede.com/download/myid-self-service-portal-user-guide-5-1",
    "PasswordLabelText": "Password",
    "ShowPasswordExpiryMeter": "True",
    "IncreasedAccessibilityRequirements": "False",
    "ShowResetPinGridIndicators": "True",
  }
}
```

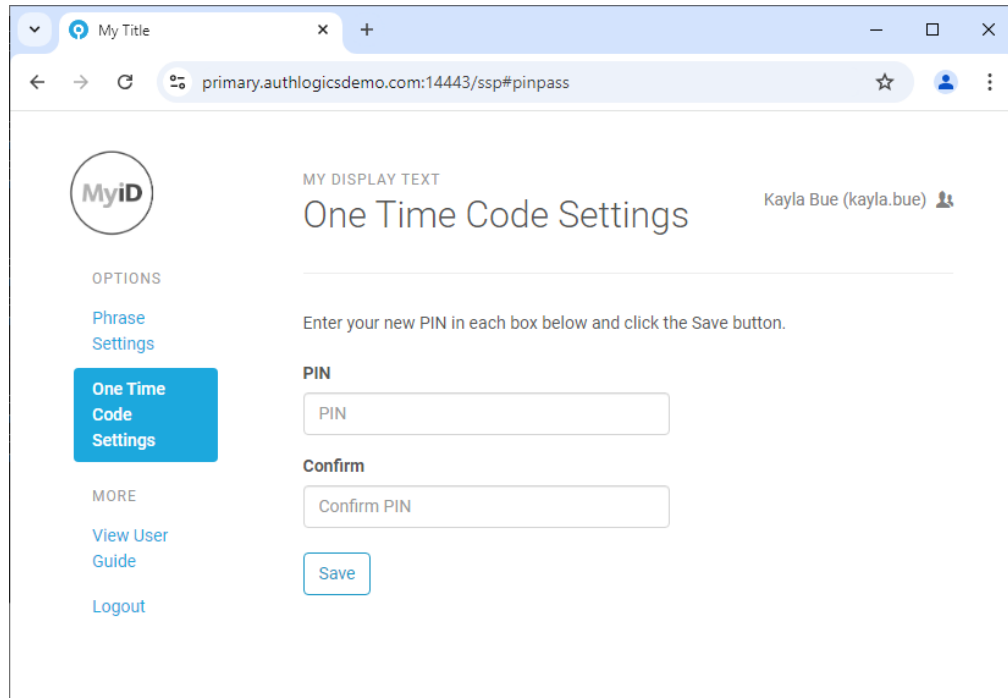
Note: Due to the limitations of PDFs, some whitespace characters may not come across cleanly. You are recommended to validate and sanitize your JSON; for example, you can use a JSON reformatter.

If you do not specify a value for an option, the default value is used.

4. Save the `appsettings.Production.json` file.
5. To ensure that this change is immediately enforced, you must refresh the application pool. To recycle the Self Service Portal application pool:
 - a. On the MyID Authentication Server, in Internet Information Services (IIS) Manager, select **Application Pools**.
 - b. Right-click the **Authlogics Authentication Server SSP** application pool, then from the pop-up menu click **Recycle**.

6. Check that the changes are successful by logging in to the Self Service Portal.

This is an example of the SSP with the `Title` set to `My Title` and the `DisplayText` set to `My Display Text`.



Note: While the content of the SSP appears in the primary language of the browser, assuming the language is supported, the `Title` and the `DisplayText` are not translated, and you must change them in the `appsettings.json` file. For information on which languages are supported, see the *Language requirements* section of the [Self Service Portal User Guide](#).

5.12.5 Advanced Self Service Portal UI customization

You can carry out advanced customization of the Self Service Portal using CSS and JavaScript. The portal has built-in customization files where all customizations can be placed. These are in the following locations:

```
C:\Program Files\Authlogics Authentication  
Server\Web\SSP\wwwroot\css\custom.css
```

```
C:\Program Files\Authlogics Authentication  
Server\Web\SSP\wwwroot\js\custom.js
```

There is a high-contrast UI customization file for SSP in the following location:

```
C:\Program Files\Authlogics Authentication Server\Web\SSP\wwwroot\css\high-  
contrast.css
```

To allow a more accessible, high contrast customization:

1. Update your custom CSS file:
 - If you already have UI customizations that you want to preserve, copy the contents of the SSP `high-contrast.css` file and add it into your `custom.css`.
 - If you do not have an existing UI customization, rename the SSP `high-contrast.css` file to `custom.css`.
2. Enable the SSP `IncreasedAccessibilityRequirements` flag.

For more information, see section [5.12.4, SSP customization](#).

5.12.5.1 Advanced Web Management Portal UI customization

You can customize the Web Management Portal using CSS. The portal has a built-in customization file where you can place customizations:

```
C:\Program Files\Authlogics Authentication  
Server\Web\Admin\wwwroot\css\custom.css
```

5.12.5.2 Advanced IdP UI customization

You can customize the IdP login page using CSS. The portal has a built-in customization file where you can place customizations:

```
C:\Program Files\Authlogics Authentication  
Server\Web\IdP\wwwroot\css\custom.css
```

There is a high-contrast UI customization file for IdP in the following location:

```
C:\Program Files\Authlogics Authentication Server\Web\IdP\wwwroot\css\high-  
contrast.css
```

To allow a more accessible, high contrast customization, update your custom CSS file:

- If you already have UI customizations that you want to preserve, copy the contents of the IdP `high-contrast.css` file and add it into your `custom.css`.
- If you do not have an existing UI customization, rename the IdP `high-contrast.css` file to `custom.css`.

5.12.5.3 Advanced UI customization considerations

The web pages within the portal load the custom CSS and JS files automatically. The files are loaded last in the load order to allow custom code to override code in built-in functions if required.

Editing of any other files in the portal folder structure is *not* supported. The custom files may be replaced by future updates or upgrades and existing customizations may not be compatible with future product versions. Intercede is unable to provide product support for any third-party code placed in the `custom.css` or `custom.js` files and any additions to the files are done so at your own risk.

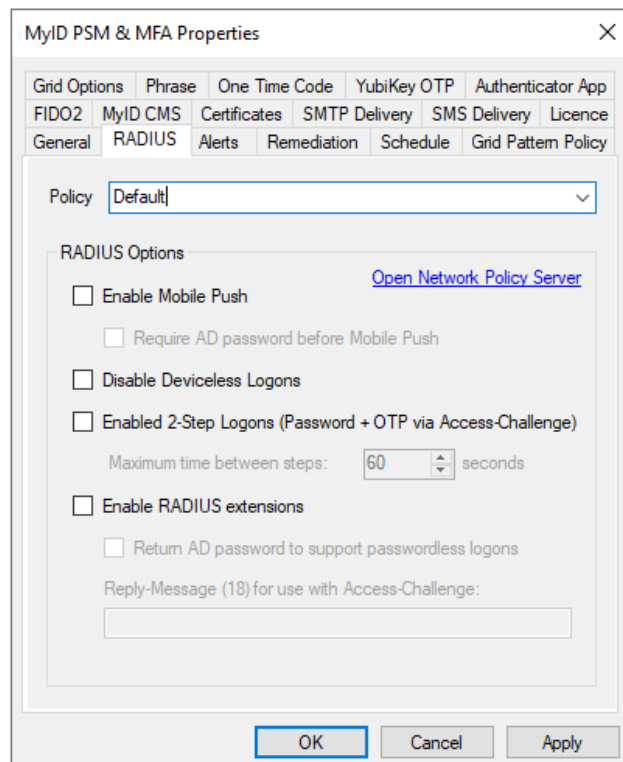
Note: The installer attempts to retain your `custom.css` and `custom.js` files, but you should always keep a backup of your custom files to ensure they are not lost after an upgrade.

5.13 RADIUS communication

The MyID Authentication Server leverages the Windows Network Policy Server role to provide RADIUS connectivity. This is a high performance and robust RADIUS server that allows you to configure a flexible RADIUS policy, including RADIUS proxy capabilities that can simplify migrations from other token solutions.

The MyID RADIUS server supports only PAP authentication from RADIUS client devices.

You can carry out RADIUS configuration in the MyID MMC as well as the Microsoft Network Policy Server MMC.



This section contains information on:

- Mobile Push MFA.
- 2-step logons (Access-Challenge).
- RADIUS extensions.
- RADIUS server ports and protocols.
- Adding a RADIUS client.
- RADIUS policies.

5.13.1 Mobile Push MFA

You can enable and disable Mobile Push MFA through RADIUS to other mechanisms.

When a RADIUS request is received containing only a username, the MyID Authentication Server triggers a Mobile Push to the user's device only if the user is configured for Mobile Push. You may configure it so that a username and password is required before a Mobile Push notification is triggered; to do this, enable the **Require AD password before Mobile Push** option.

5.13.2 2-step logons (Access-Challenge)

RADIUS Access-Challenge is supported by some RADIUS clients. It allows for a two-step logon process where the client sends their username and password to the server for verification and the server responds with either an Access-Challenge or Access-Reject. If the client supports Access-Challenge, the user is prompted for a second set of credentials, for example an OTP, which are then sent to the server. The server then processes the username and OTP and responds with an Access-Accept (only if an Access-Challenge preceded the request) or Access-Reject.

5.13.3 RADIUS extensions

You can enable RADIUS extensions to send metadata from the server back to the RADIUS client. This can return the following:

- The user's Active Directory password to support single sign-on to certain applications such as Citrix Access Gateway.
- Custom reply text for the RADIUS client to display when using Access-Challenge (where supported by the RADIUS client).

5.13.4 RADIUS server ports and protocols

The MyID RADIUS server uses the IANA assigned ports for authentication and accounting, as well as the unofficial ports for backward compatibility with legacy RADIUS clients.

- Authentication:
 - UDP:1812
 - UDP:1645
- Accounting:
 - UDP:1812
 - UDP:1645

Both IPv4 and IPv6 are supported for communication with RADIUS clients.

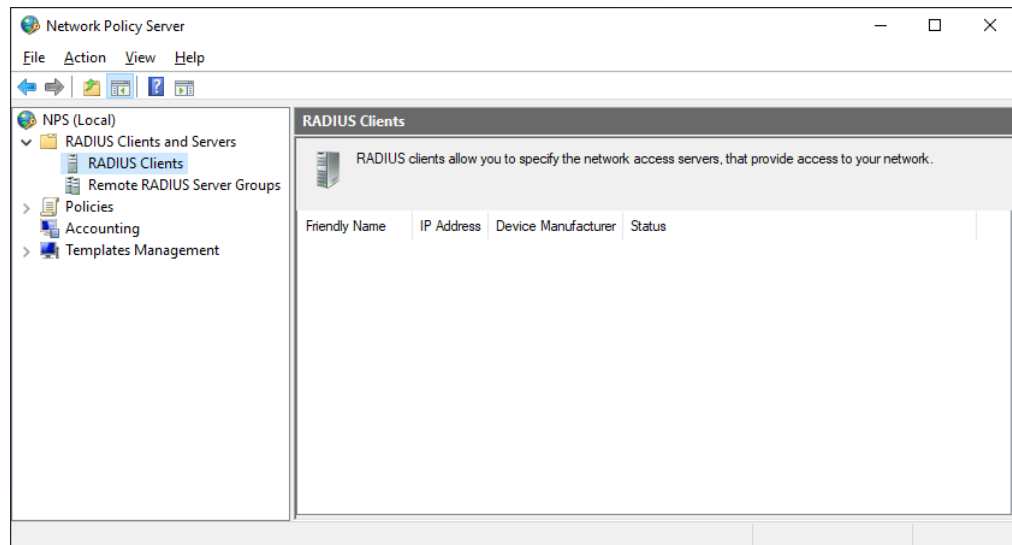
5.13.5 Adding a RADIUS client

A RADIUS client device is typically a VPN concentrator or remote access server; however, it can also be a wireless access point or a door access system. RADIUS is a common system used by a multitude of applications and platforms.

Note: This section of the installation process requires Local Administrator rights on the server. Domain rights are not required at this stage.

To add a RADIUS client:

1. Open the Network Policy Server from the Administrative Tools start menu group.



2. Expand the **RADIUS Clients and Servers** node, and select **RADIUS Clients**.

3. Right-click **RADIUS Clients** and click **New**.

The screenshot shows the 'New RADIUS Client' dialog box with the 'Advanced' tab selected. The 'Enable this RADIUS client' checkbox is checked. Below it is a dropdown menu for 'Select an existing template:' which is currently empty. The 'Name and Address' section contains a 'Friendly name:' field with the text 'VPN Server' and an 'Address (IP or DNS):' field with the text 'vpn.authlogicsdemo.com'. A 'Verify...' button is next to the address field. The 'Shared Secret' section has a dropdown for 'Select an existing Shared Secrets template:' set to 'None'. Below this is a text box explaining that users can manually type a shared secret or generate one. There are two radio buttons: 'Manual' (selected) and 'Generate'. Under 'Manual', there are two password fields: 'Shared secret:' and 'Confirm shared secret:', both filled with dots. At the bottom are 'OK' and 'Cancel' buttons.

New RADIUS Client

Settings Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:
VPN Server

Address (IP or DNS):
vpn.authlogicsdemo.com [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:
.....

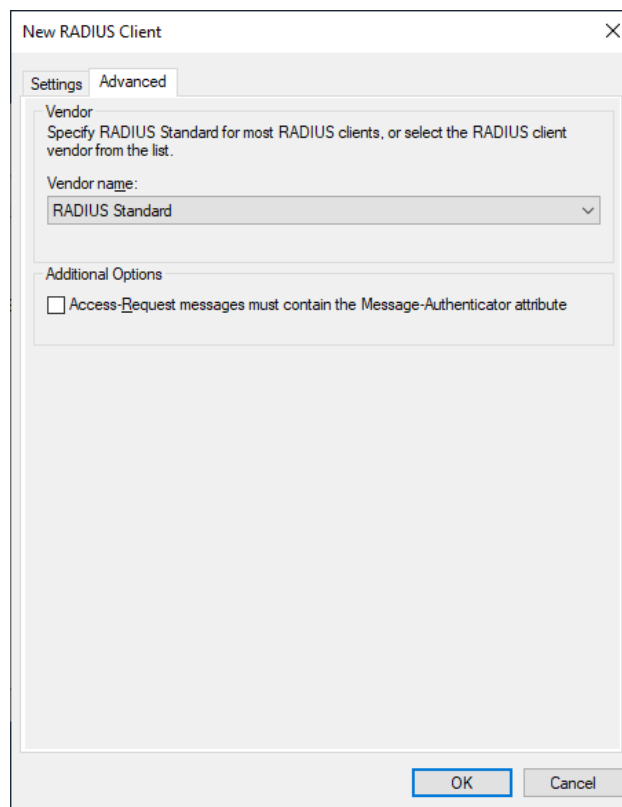
OK Cancel

4. On the **Settings** tab, set the following:

- **Enable this RADIUS client** – ensure that this option is enabled.
- **Friendly name** – a friendly name for the remote RADIUS client.
- **Address (IP address or DNS)** – the address of the RADIUS client.

To ensure that entered IP Address or DNS name is valid, click **Verify**.

- **Shared secret** – enter and confirm your shared secret, ensuring that the shared secret matches the secret entered on the RADIUS client device. You can also use the **Generate** option to generate a highly secure random secret.



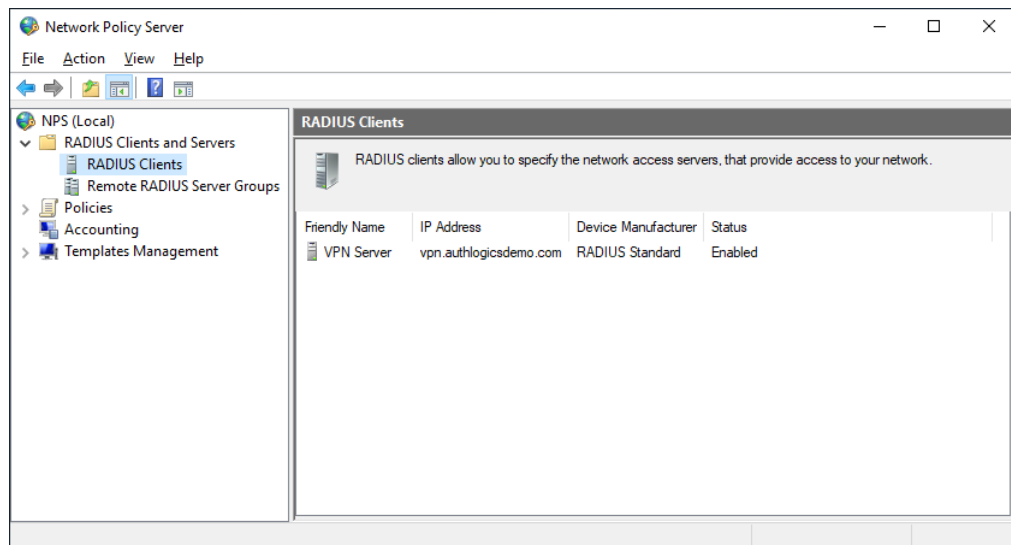
The screenshot shows a dialog box titled "New RADIUS Client" with a close button (X) in the top right corner. It has two tabs: "Settings" (selected) and "Advanced". Under the "Settings" tab, there is a section labeled "Vendor" with the instruction "Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list." Below this is a dropdown menu labeled "Vendor name:" with "RADIUS Standard" selected. Further down is a section labeled "Additional Options" containing a checkbox labeled "Access-Request messages must contain the Message-Authenticator attribute", which is currently unchecked. At the bottom of the dialog are "OK" and "Cancel" buttons.

5. On the **Advanced** tab, ensure that the following are set:

- **Vendor name** – must be set to `RADIUS Standard`.
- **Access-Request messages must contain the Message-Authenticator attribute** – optional, but must be set the same as on the RADIUS client device.

Note: Ensure that the Message-Authenticator attribute status is set to the same value on the RADIUS client devices as on the RADIUS server. They can either both be enabled or both disabled.

6. Click **OK**.



You may add as many RADIUS clients as required.

5.13.6 RADIUS policies

The MyID Authentication Server installation automatically configures a Connection Request Policy within NPS, which allows MyID to support configured RADIUS clients automatically. A Network Policy is not required as the MyID NPS plug-in functions without one.

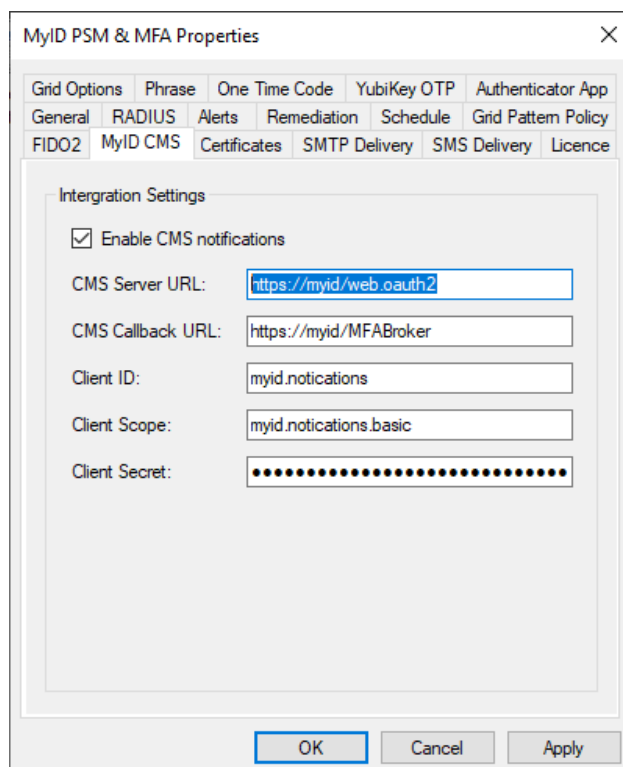
If you need to modify the default Connection Request Policy it is recommended that you duplicate (right-click, **Duplicate Policy**) the default policy as a backup and then disable it. Once complete you can modify the duplicated policy as needed.

6 Configuring MyID CMS settings

The MFA Broker Service module allows you to integrate the MyID credential management system (CMS) with MyID MFA. It allows you to use features from both products in an integrated fashion; for example, you can manage both smart cards and PIN grids for your users. The MFA Broker Service allows you to manage credentials in the MyID MFA system using the MyID CMS.

For instructions on configuring the connection between MyID CMS and MyID MFA, see the *MFA Broker Service* guide provided with the MFA Broker Service module.

You can configure the MyID CMS settings in the MyID Authentication Server through the **MyID CMS** tab in Global Settings.



The image shows a screenshot of the 'MyID PSM & MFA Properties' dialog box, specifically the 'MyID CMS' tab. The dialog has a title bar with a close button (X). Below the title bar is a tabbed interface with the following tabs: Grid Options, Phrase, One Time Code, YubiKey OTP, Authenticator App, General, RADIUS, Alerts, Remediation, Schedule, Grid Pattern Policy, FIDO2, MyID CMS (selected), Certificates, SMTP Delivery, SMS Delivery, and Licence. The 'MyID CMS' tab contains a section titled 'Integration Settings' with a checkbox labeled 'Enable CMS notifications' which is checked. Below this are five text input fields: 'CMS Server URL' with the value 'https://myid/web.oauth2', 'CMS Callback URL' with the value 'https://myid/MFABroker', 'Client ID' with the value 'myid.notifications', 'Client Scope' with the value 'myid.notifications.basic', and 'Client Secret' which is masked with dots. At the bottom of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'.

You require the following information to complete the configuration:

- **CMS Server URL** – the MyID CMS OAuth2 Authentication Service URL.

For example:

```
https://myid/web.oauth2
```

- **CMS Callback URL** – the MyID CMS MFA Broker Service URL.

For example:

```
https://myid/MFABroker
```

- **Client ID** – the MyID CMS Client ID used to authenticate.

For example:

```
myid.notifications
```

- **Client Scope** – the MyID CMS Client Scope used to authenticate.

For example:

```
myid.notifications.basic
```

- **Client Secret** – the MyID CMS Client Secret used to authenticate.

For example:

```
4116e8f9-92e2-48b1-8616-5fb3d130b91d
```

7 Configuring the PSM password policy

To deploy the MyID PSM Password Policy:

1. In Active Directory Group Policy, create a MyID PSM Password Policy.
2. Deploy the Domain Controller Agent.
3. Make the following Group Policy changes:
 - Assign the MyID Password Policy to the Domain Controllers OU.
 - Assign the MyID Password Policy to the Authlogics Authentication Servers group.
 - Modify the built-in Default Domain Policy.

7.1 Configuring the MyID Password Policy settings

The MyID Authentication Server includes Active Directory Group Policy Template files `AuthlogicsPasswordPolicy.admx` and `AuthlogicsPasswordPolicy.adml`, which are used to create policies. The **User Configuration** section of the GPO can be disabled as the settings only apply to the **Computer Configuration**.

7.1.1 The PSM Users role

The PSM Users role is disabled by default. To enable it you must assign an Active Directory group to the role. For more information, see section [5.10.5, Managing the Password Security Management Users role](#).

If the PSM Users role is not enabled, all Active Directory users have the MyID Password Policy applied to them. If enabled, only members of this group have the MyID Password Policy applied to them and non-members have the Exception Password Policy applied to them, which mirrors the equivalent default Windows password policy settings.

7.2 Main settings

Setting	Enable Authlogics Password Policy
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting enables the MyID Password Policy functionality on all Agents and Servers where this Group Policy is applied.</p> <p>If you enable this policy complexity and validity checks will be performed on the passwords.</p> <p>If you disable or do not configure this policy then no password processing will function as per the configured policy thus deeming all passwords as acceptable.</p>

7.2.1 Primary password policy

These settings control the MyID specific password policy. The default settings work in most scenarios and are NIST 800-63B compliant by default.

Setting	Disable Online Password Breach Database checking
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting prevents querying the MyID Password Breach Database in the Cloud consisting of billions of known previously breached passwords.</p> <p>If you enable this policy then no checks against the MyID Password Breach Database in the Cloud will be performed.</p> <p>If you disable or do not configure this policy a partial HASH of the password will be sent over SSL to Intercede for analysis. The password will be rejected if it is a known/previously breached password to comply with to comply with NIST SP 800-63B.</p>

Setting	Disable Offline Password Breach Database checking
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting prevents querying the offline MyID Password Breach Database installed on the MyID Authentication Server.</p> <p>If you enable this policy then no checks against the offline MyID Password Breach Database will be performed.</p> <p>If you disable or do not configure this policy passwords will be checked against the offline database and will be rejected if it is found in order to comp with NIST SP 800-63B.</p>

Setting	Disable Custom Password Blacklist checking
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting prevents querying the custom Password Blacklist consisting of passwords entered by an administrator.</p> <p>If you enable this policy then no checks against the custom Blacklist file will be performed.</p> <p>If you disable or do not configure this policy then entered passwords will be compared with the contents of the custom blacklist file and is also be available for use by the heuristics engine. The password will be rejected if it is found on the custom blacklist to comply with NIST SP 800-63B.</p>

Setting	Disable Shared Password Protection
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting prevents checking if the password is already in use by another user account in the Domain.</p> <p>If you enable this policy then no checks against the Domain for shared passwords will be performed.</p> <p>If you disable or do not configure this policy the Domain will be checked and the password will be rejected if it is currently in use.</p>

Setting	Enable Passphrases
Values	(6 - 30)
Default	12
Description	<p>This policy setting enables the use of passphrases if a password is longer than the specified value. Passphrases do not have to pass the following complexity checks if they are long enough:</p> <ul style="list-style-type: none">• Minimum Lowercase Characters• Minimum Uppercase Characters• Minimum Numeric Characters• Minimum Special Characters• Minimum Unicode Characters• Maximum Repeating Characters• Maximum Allowed Characters From Username <p>If you enable this policy then the specified complexity checks will be skipped only if the password length is equal to or longer than the specified value.</p> <p>If you disable or do not configure this policy then users may find it difficult to set a passphrase as all configured complexity checks must pass.</p>

Setting	Override Password Policy for new User Accounts
Values	(1 - 30)
Default	5
Description	<p>This policy setting overrides password the password policy checks for accounts that have been created within a specified time period and will be accepted.</p> <p>If you enable this policy, specify the number of seconds from when an account has been created for it to be deemed as being a new account.</p> <p>If you disable or do not configure this policy then the password policy will apply to passwords specified during the Active Directory account creation process.</p>

Setting	Disable Heuristic Scanning
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting controls the heuristic scanning engine behaviour on password checks. Heuristic scanning will undergo a series of checks where known character replacements are detected and reverted to their original base value and then revalidated for compliance. For example, '@' reverts to 'a', '!' to 'i' etc.</p> <p>If you enable this policy the heuristic scanning engine will not be active for any checks.</p> <p>If you disable or do not configure this policy then heuristic scanning will be performed to comply with NIST SP 800-63B against the Offline Password Breach Database, Custom Password Blacklist, all or part of the username, and Month and Day names.</p>

For more information on heuristic scanning, see section [7.6.1, Heuristic scanning](#).

Setting	Breached Passwords Check Type
Values	Default / Stemmed / Disabled
Default	Disabled
Description	<p>This policy setting enables alternate methods of password checking against both the online and offline Authlogics Password Breach Databases.</p> <p>If this policy is configured to Stemmed checking then any password checks performed will check for use of similar vulnerable passwords rather than strict password matches.</p> <p>If you disable or do not configure this policy then password checks will perform the default method of strict checking passwords against whichever breach database is configured.</p>

For more information on password stemming, see section [7.6.2, Password stemming](#).

7.2.1.1 Complexity rules

These settings provide fine grain control of password complexity settings.

If you set too many of these settings, users may find it too difficult to choose a memorable password, which may encourage them to write passwords down.

Setting	Disallow Incremental / Numeric-Only changes
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting prevents changing only a single digit, or appending a single digit compared to the existing password.</p> <p>If you enable this policy then users must change more than just a single digit compared to their old password.</p> <p>If you disable or do not configure this policy then entered passwords with a simple numeric change from the previous password will be allowed.</p> <p>Note: This check requires that the PSM Wizard has been run and enabled on the domain.</p>

Setting	Disallow First or Last Character being a number
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting disallows passwords that start or end with a numeric character.</p> <p>If you enable this policy then users cannot use a password that begins or ends with a number.</p> <p>If you disable or do not configure this policy then passwords which start or end with a numeric character will be allowed.</p>

Setting	Disallow Month and Day names
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting disallows the use of month and day names in the password.</p> <p>If you enable this policy a password will be rejected if a month or day name is found in an entered password.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

Setting	Disallow spaces
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting disallows the use of a space character in a password.</p> <p>If you enable this policy a password will be rejected if a space is found in an entered password.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

Setting	Minimum Password Length
Values	(4 - 127)
Default	8
Description	<p>This policy setting sets the minimum number of characters allowed for a compliant password. Setting this value too high may make the password too difficult for users to remember password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the length of the password is less than the value specified.</p> <p>Note: Consecutive space characters will be counted as a single space character as per NIST SP 800-63B guidance.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the default value of 8 will be used to comply with NIST SP 800-63B.</p>

Setting	Maximum Password Length
Values	(4 - 127)
Default	127
Description	<p>This policy setting sets the maximum number of characters allowed for a compliant password. Setting this value too low may stop users from selecting passphrases which are typically more secure than passwords. The password will be rejected if the length of the password is more than the value specified.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the default value of 127 will be used to comply with NIST SP 800-63B.</p>

Setting	Minimum Lowercase Characters
Values	(1 - 127)
Default	2
Description	<p>This policy setting sets the minimum number of allowed lowercase characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of lowercase letters in the password is less than the value specified.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

Setting	Minimum Uppercase Characters
Values	(1 - 127)
Default	2
Description	<p>This policy setting sets the minimum number of allowed uppercase characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of uppercase letters in the password is less than the value specified.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

Setting	Minimum Numeric Characters
Values	(1 - 127)
Default	2
Description	<p>This policy setting sets the minimum number of allowed numeric digits a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of numeric digits in the password is less than the value specified.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

Setting	Minimum Special Characters
Values	(1 - 127)
Default	2
Description	<p>This policy setting sets the minimum number of allowed special characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of special characters in the password is less than the value specified.</p> <p>The following are recognised as special characters ! " # % & ' () * , - . / : ; ? @ [\] _ { } '</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

Setting	Minimum Unicode Characters
Values	(1 - 127)
Default	2
Description	<p>This policy setting sets the minimum number of allowed Unicode characters a compliant password must have. Setting this value too high may make it too difficult for users to enter a valid password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of Unicode characters in the password is less than the value specified.</p> <p>Unicode characters are non-printable characters that are not punctuation or alphanumeric characters.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

Setting	Maximum Repeating Characters
Values	(0 - 126)
Default	8
Description	<p>This policy setting sets the maximum number of times a character can be repeated anywhere within a compliant password. Setting this value too low may make it too difficult for users to enter a valid password, whereas setting this value too high could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if a character is repeated in the password more times than the value specified.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed to comply with NIST SP 800-63B.</p>

Setting	Maximum Consecutive Repeating Characters
Values	(0 - 126)
Default	3
Description	<p>This policy setting sets the maximum number of times a character can be repeated anywhere within a compliant password. Setting this value too low may make it too difficult for users to enter a valid password, whereas setting this value too high could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if a character is repeated in the password more times than the value specified.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed to comply with NIST SP 800-63B.</p>

Setting	Maximum Sequential Characters
Values	(0 - 127)
Default	3
Description	<p>This policy setting sets the maximum number of times a sequence of characters can be used within a compliant password. Setting this value too low may make it too difficult for users to enter a valid password, whereas setting this value too high could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the number of characters in a sequence is more than the value specified.</p> <p>Sequential characters are both forward and backwards i.e. ABC and CBA are deemed to be sequential.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed to comply with NIST SP 800-63B.</p>

Setting	Maximum Sequential Keyboard Characters
Values	(0 - 5)
Default	2
Description	<p>This policy setting sets the maximum sequential keyboard characters allowed within a compliant password. The password will be rejected if the number of keyboard layout characters in sequence is more than the value specified.</p> <p>Sequential characters are both forward and backwards i.e. "qwerty" and "ytrewq" with both be deemed to be sequential.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

Setting	Maximum Allowed characters from User Account name
Values	(1 - 127)
Default	3
Description	<p>This policy setting sets the maximum number of characters from a user account name that are allowed in a password. Passwords will be rejected if the number of characters from the user account name in a password is more than this value specified. e.g. If the user account name is Robert and the value is 3 then passwords containing "robe", "ober" and "bert" will be rejected.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

Setting	Allow Full User Account name in password
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting allows the use of the full user account name within the password.</p> <p>If you enable this policy a password will not be blocked if the full user account name is found within the entered password.</p> <p>If you disable or do not configure this policy then the password may not contain the full user account name to comply with NIST SP 800-63B.</p>

7.2.1.2 Dynamic password expiry

These settings dynamically control the maximum age of a password depending on its length. This allows for passwords to be used for longer the longer they are, which encourages users to create longer, and thus more secure, passwords.

A password is matched to the highest zone possible depending on the length of the password. When MyID detects that a password has dynamically expired, the user account is be configured to change password at next login.

There are five password expiry zones, each consisting of a minimum password length and maximum password age in days. A sixth zone can be used to configure accounts to never expire if they are over the specified length.

Setting	Password Expiry Default Zone
Values	Maximum Age in days: (1 - 999)
Default	42
Description	<p>This policy setting configures the default password expiry period.</p> <p>If a password length is unknown or less than what is required by any other Zone then the Default Zone will apply.</p> <p>Note: If a password was created prior to installing MyID its length will be unknown and the Default Zone will apply. Once the password has been changed the length will be known and other Zones may then apply.</p> <p>If you enable this policy you must specify the Maximum Age in days until the user account's password will be set to expire.</p> <p>If you disable or do not configure this policy then the setting will not take effect.</p>

Setting	Password Expiry Zone 1	
Values	Minimum Password Length: (6 - 100)	Maximum Age in days: (1 - 999)
Default	8	60
Description	<p>This policy setting configures the dynamic password expiry period for this zone.</p> <p>If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account's password will be set to expire.</p> <p>If you disable or do not configure this policy then the zone setting will not take effect.</p>	

Setting	Password Expiry Zone 2	
Values	Maximum Age in days: (1 - 999)	Maximum Age in days: (1 - 999)
Default	90	90
Description	<p>This policy setting configures the dynamic password expiry period for this zone.</p> <p>If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account's password will be set to expire.</p> <p>If you disable or do not configure this policy then the zone setting will not take effect.</p>	

Setting	Password Expiry Zone 3	
Values	Minimum Password Length: (6 - 100)	Maximum Age in days: (1 - 999)
Default	10	180
Description	<p>This policy setting configures the dynamic password expiry period for this zone.</p> <p>If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account's password will be set to expire.</p> <p>If you disable or do not configure this policy then the zone setting will not take effect.</p>	

Setting	Password Expiry Zone 4	
Values	Minimum Password Length: (6 - 100)	Maximum Age in days: (1 - 999)
Default	11	270
Description	<p>This policy setting configures the dynamic password expiry period for this zone.</p> <p>If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account's password will be set to expire.</p> <p>If you disable or do not configure this policy then the zone setting will not take effect.</p>	

Setting	Password Expiry Zone 5	
Values	Minimum Password Length: (6 - 100)	Maximum Age in days: (1 - 999)
Default	12	365
Description	<p>This policy setting configures the dynamic password expiry period for this zone.</p> <p>If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect and the Maximum Age in days until the user account's password will be set to expire.</p> <p>If you disable or do not configure this policy then the zone setting will not take effect.</p>	

Setting	Password Never Expires Zone	
Values	Minimum Password Length: (6 - 100)	
Default	20	
Description	<p>This policy setting configures the dynamic password expiry period for this zone.</p> <p>If you enable this policy you must specify both the Minimum Password Length for which this policy shall take effect.</p> <p>If you disable or do not configure this policy then the zone setting will not take effect.</p>	

7.2.1.3 Security phrases

These settings control the way that security phrases are generated.

Security phrases are a replacement for passwords that provide a long, random, and memorable phrase that provides greater security.

Note: Security phrases are not the same as multi-factor authentication Phrases.

For more information on security phrases, see section [7.4, Security phrases](#).

Setting	Disable Segment Number
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting prevents insertion of a random number during phrase generation.</p> <p>If you enable this policy generated phrases will not contain any randomly inserted numbers.</p> <p>If you disable or do not configure this policy then the setting will not take effect.</p>

Setting	Disable Segment Casing
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting prevents upper casing of the first character of a random segment during phrase generation.</p> <p>If you enable this policy the phrases generated will not contain any upper cased characters.</p> <p>If you disable or do not configure this policy then the setting will not take effect.</p>

Setting	Enable Security Phrase Generation
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting enables security phrase generation.</p> <p>If you enable this policy you must ensure that your password complexity policy is configured to ensure generated phrases comply.</p> <p>If you disable or do not configure this policy then the setting will not take effect.</p>

If you have security phrases enabled, normal password complexity rules do not apply, except password breach checking and blacklist checking.

Setting	Maximum Phrase Segment Word Length
Values	3 - 8
Default	8
Description	<p>This policy setting configures the maximum character length of segment words in generated phrases.</p> <p>If you enable this policy then generated phrases will contain segment words of the specified maximum length between 3 and 8.</p> <p>Ensure that is not set below the minimum allowed number of characters in a phrase word.</p> <p>If you disable or do not configure this policy then the maximum character length of generated segment words will default to 8.</p>

Setting	Minimum Phrase Segment Word Length
Values	3 - 8
Default	4
Description	<p>This policy setting configures the minimum character length of segment words in generated phrases.</p> <p>If you enable this policy then generated phrases will contain segment words of the specified minimum length between 3 and 8.</p> <p>Ensure that is not set above the maximum allowed number of characters in a phrase word.</p> <p>If you disable or do not configure this policy then the minimum character length of generated segment words will default to 4.</p>

Setting	Segment Number Length
Values	1 - 9
Default	1
Description	<p>This policy setting configures the character length of segment numbers in generated phrases.</p> <p>If you enable this policy then generated phrase numbers will be the specified number of characters long between 1 and 9.</p> <p>If you disable or do not configure this policy then the character length of generated numbers will default to 1.</p>

Setting	Number of Phrase Segments
Values	3 - 6
Default	3
Description	<p>This policy setting configures the number of word segments in generated phrases.</p> <p>If you enable this policy then generated phrases will contain the specified number of generated word segments between 3 and 6.</p> <p>If you disable or do not configure this policy then the number of generated word segments will default to 3.</p>

7.2.2 Exception password policy

These settings control the exception settings to the Primary Password Policy. The default settings mirror the equivalent default Windows password policy settings.

These settings apply only to the users who are *not* members of the PSM Users role, if you have configured a group for that role. For more information, see section [7.1.1, The PSM Users role](#).

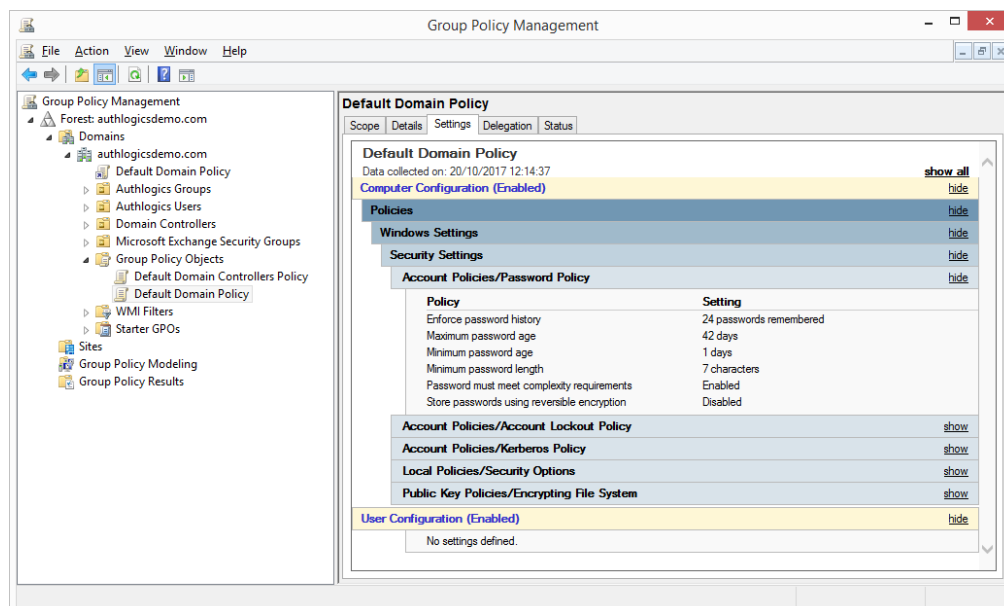
Setting	Maximum Password Age
Values	Maximum Age in days: (1 - 999)
Default	42
Description	<p>This policy setting configures the maximum password age for accounts that are NOT a member of the PSM Users Role.</p> <p>If you enable this policy you must specify the Maximum Age in days until the user account's password will be set to expire.</p> <p>If you disable or do not configure this policy then the setting will not take effect.</p>

Setting	Minimum Password Length
Values	(1 - 127)
Default	7
Description	<p>This policy setting sets the minimum number of characters allowed for a compliant password for accounts that are NOT a member of the PSM Users Role. Setting this value too high may make the password too difficult for users to remember password, whereas setting this value too low could result in the password becoming too weak and easily guessed or brute forced. The password will be rejected if the length of the password is less than the value specified.</p> <p>If you enable this policy then you must specify a value.</p> <p>If you disable or do not configure this policy then the default value of 7 will be used as per Windows password policy.</p>

Setting	Mirror Windows 'Password Complexity' requirements
Values	Enabled / Disabled
Default	Disabled
Description	<p>This policy setting mirrors the Windows built in 'Password must meet complexity requirements' restriction for accounts that are NOT a member of the PSM Users Role. This check ensures that a password does not contain the username, that it contains a minimum of 3 of the following character types: uppercase, lowercase, numeric, non-alphabetic/special characters.</p> <p>If you disable or do not configure this policy then the check will not be performed.</p>

7.3 Modifying the default domain policy

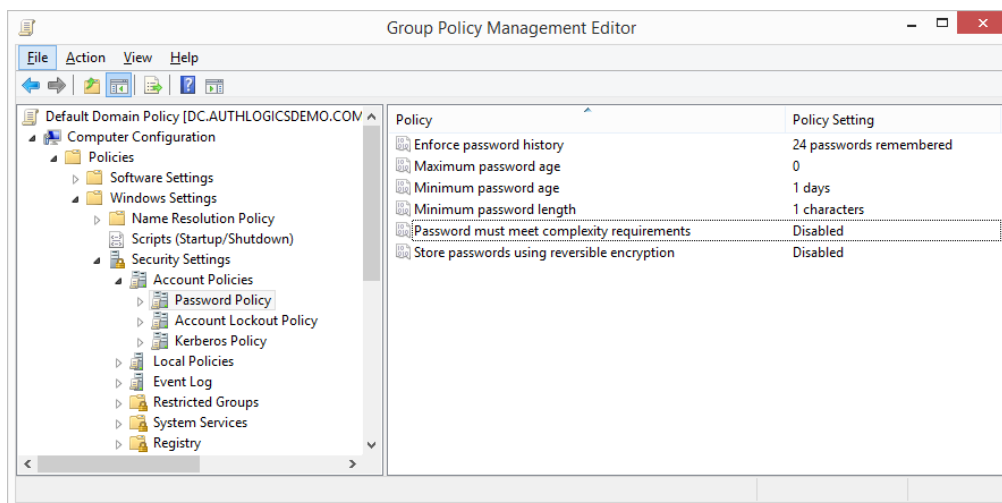
The following password settings apply to the Default Domain Policy by default:



The following password settings for the Default Domain Policy must be changed so that the built-in Windows policy does not conflict with the MyID Password Policy and NIST guidance:

- Maximum password age:** 0
 This should be set to 0 when MyID PSM **Dynamic Password Complexity** is used, or to comply with NIST SP 800-63, which states that passwords should not periodically expire.
- Minimum password length:** 1
 This should be set to 1 so that it does not conflict with MyID PSM **Minimum Password Length** complexity rule setting.
- Passwords must meet complexity requirements:** Disabled
 This should be set to Disabled to allow the MyID PSM policy to function, or to comply with NIST SP 800-63B which states that passwords should not be forced to contain complexity rules.

Note: You *must not* set these settings to Not Configured, as this causes Windows to revert to default settings.



7.4 Security phrases

Security phrases are a replacement for passwords that provide a long, random, and memorable phrase that provides greater security; the length and randomness help protect the security phrase from being guessed or cracked by increasing the entropy of the password, and the memorability discourages the user from writing the password down in insecure locations.

If security phrases are enabled, users use them in place of passwords.

Security phrases are generated on the server, and if required users can generate new security phrases themselves using the Self Service Portal or the Windows Desktop Agent:

- For information on changing a security phrase through the Self Service Portal, see the *Resetting your security phrase* section in the [Self Service Portal User Guide](#).
- For information on changing a security phrase through the Windows Desktop Agent, see the *Changing an Active Directory password* section in the [Windows Desktop Agent Integration Guide](#).

Note: Security phrases are not the same as multi-factor authentication Phrases.

Security phrases are not limited by password complexity rules, as the length and randomness of the generated phrases provide sufficient security; however, security phrases *are* checked against the configured breach databases, and if the phrase has been found in a breach, it is regenerated. Security phrases are also checked against your blacklist; security phrases that contain blacklisted patterns are regenerated.

Security phrases are generated from controlled dictionaries to avoid unwanted words from being used in the security phrases. The language of dictionary used is localized. If you are using an unsupported language, the security phrases are generated using the English dictionary by default. The following languages are supported:

- English
- German

Security phrases are built out of segments which, depending on your settings, may or may not be capitalized, or contain numbers; for example, a three segment security phrase with one number and capitalization may be generated as follows:

```
purse-Layer3-bless
```

You can customize the lengths of the words used, the number of segments, the length of numbers, and whether any capitalization occurs.

To enable security phrases, and to set up the way that security phrases are generated, you must configure the Security Phrases GPO settings; see section [7.2.1.3, Security phrases](#) for details.

7.5 Configuring custom password blacklist checking

MyID PSM provides administrators with the ability to add their own unwanted passwords to a blacklist text file. The blacklist allows for the rejection password based on full passwords as well as those matching wildcard characters, * and #. For more information on wildcard characters, see section [7.5.1, Wildcard usage within local blacklist](#).

The heuristics engine also adds further protection to the file by substituting common letter substitutions withing passwords, for example @ to a, and 5 to s.

To enable the local password blacklist, modify the contents of the following text file:

```
C:\Program Files\Authlogics Authentication Server\blacklist.txt
```

Once a blacklist file has been updated it must be copied to all MyID Authentication Servers. The file is not required to be placed on Domain Controllers.

The custom blacklist can be disabled by emptying the contents of the file or by enabling the **Disable Custom Password Blacklist checking** Group Policy.

7.5.1 Wildcard usage within local blacklist

To enforce password rejection, full words and the wildcards characters * and # can be added to the local blacklist file. If a password matches what is defined in the local blacklist file, the password is rejected. How a password is processed depends on the positioning of the wildcard in the entry.

The wildcard * refers to any character for any length, if a * is entered on its own, all passwords are rejected.

The wildcard # refers to a single numeric character and translates to 9 – ## = 99. Numeric characters within passwords are converted to a number and then, if they are less than the restricted value, the password is rejected.

This table shows examples of how MyID Authentication Server processes a password based on the blacklist entry:

Blacklist Entry	Description	Password	Result
Authlogics	Reject any direct matches to the restricted word Authlogics.	Authlogics	Rejected
		Authlogics01	Accepted
Auth*	Reject any password starting with Auth.	Authlogics	Rejected
		HelloAuthlogics	Accepted
Auth	Reject any password with Auth in the middle.	Authlogics01	Accepted
		helloAuth123	Rejected
*Auth	Reject any password ending with Auth.	helloAuth123	Accepted
		Authlogics	Accepted
		helloAuth	Rejected
Authlogics##	Reject any password starting with word Authlogics ending in two digits.	Authlogics12	Rejected
		Authlogics12	Rejected
		Authlogics112	Accepted
		Helloworld12	Accepted
##Authlogics	Reject any password starting with two digits and ending with the word Authlogics.	12Authlogics	Rejected
		123Authlogics	Accepted
##*	Reject any password starting with two digits.	12Authlogics	Rejected
		Authlogics12	Accepted
		1Authlogics	Accepted
		123Authlogics	Rejected
*##	Reject any password ending with two digits.	12Authlogics	Accepted
		Authlogics12	Rejected
		Authlogics123	Accepted
##	Reject any password with two consecutive digits in the middle of the password.	12Authlogics	Accepted
		Authlogics12	Accepted
		Auth12logics	Rejected
		Authlogics123	Accepted

7.6 Advanced password checking

You can configure the following methods of advanced password checking through GPOs:

- Heuristic scanning.
- Password stemming.
- A combination of heuristic scanning and password stemming.

7.6.1 Heuristic scanning

Heuristic scanning replaces symbols and numbers with letters. By default, the following symbols are replaced:

Symbol	Possible replacements
!	!il
\$	s
@	a
1	1il
5	5s
3	3e
0	0o

Each symbol is replaced with one character from the possible replacements, and the resulting password is checked. If there are multiple possible replacements, each combination is checked.

Note: \$ and @ are never replaced by themselves.

For example, a password of `MF@0For3ver++`, with heuristic scanning (but not password stemming) enabled, creates the following password variations:

`MF@0For3ver++` (the original password with no substitutions)

`MFa0For3ver++`

`MFaoFor3ver++`

`MFa0Forever++`

`MFaoForever++`

In the above example:

- The @ symbol is replaced with the letter a.
- The 0 digit is replaced with the letter o, or the digit 0.
- The 3 digit is replaced with the letter e, or the digit 3.

Each combination of these substitutions is generated as a variation. Note that the @ symbol is replaced with the letter a only, and so does not generate any further combinations.

Each of these password variations is checked against the Offline Password Breach Database, Custom Password Blacklist, all or part of the username, and Month and Day names. This complies with NIST SP 800-63B .

Note: All instances of the same symbol in a password are replaced by the same replacement. For example, a password of `MFA!sCoo!`, with heuristic scanning (but not password stemming) enabled, creates the following password variations to be checked:

`MFA!sCoo!`

`MFA!sCooi`

`MFA!sCool`

You can disable heuristic scanning using the **Disable Heuristic Scanning** GPO. For more information, see section [7.2.1, Primary password policy](#).

7.6.2 Password stemming

Password stemming strips out symbols and numbers, and changes all letters to lowercase.

This new, stemmed password is checked against the MyID Password Breach Database and the blacklists (unless the stemmed password is less than six characters, or has been reduced to less than 60% of the password's original size).

For example if you have password stemming (but not heuristic scanning) configured:

Original password	Stemmed password	Checked	Description
<code>MF@0For3ver++</code>	<code>mfaforver</code>	Yes	
<code>we<3MFA</code>	<code>wemfa</code>	No	Stemmed password not checked because it is less than six characters long.
<code>+We+all+<3+MF@+</code>	<code>weallmf</code>	No	Stemmed password not checked because it is less than 60% of the password's original size.

You can enable heuristic scanning by enabling the **Breached Passwords Check Type** GPO and setting it to `Stemmed`. For more information on enabling heuristic scanning, see section [7.2.1, Primary password policy](#).

When the **Breached Passwords Check Type** GPO is enabled, and the value is set to `Stemmed`, if the user is performing offline breach checks and you want them to do to do password stemming checks, the user *must* have the offline `Full` *and* `Stem` databases installed; if the user has only the `Full` or `Min` offline password breach database, no password stemming checks occur.

7.6.3 Using both heuristic scanning and password stemming

If you have enabled both heuristic scanning and password stemming, MyID PSM uses them in combination.

For example, with both heuristic scanning and password stemming enabled, a password of `MF@0For3ver` creates the following password variations:

`mfaoforever`

`mfaforever`

`mfaoforver`

`mfaforver`

`mfforver`

Each of these password variations is then checked against the MyID Password Breach Database and the blacklists.

8 Advanced configuration

Advanced configuration options for MyID are controlled using the Windows registry. The following entries are created during the installation of MyID server components and most of them should typically only be changed if instructed by Intercede support.

Note: After changing a registry key on the MyID Server, the IIS components must be restarted by running `IISRESET` from an elevated admin command prompt.

You can carry out the following:

- Specify Active Directory Domain Controllers.
See section [8.1, Specifying Active Directory Domain Controllers](#).
- Add an SSL certificate.
See section [8.2, Adding a trusted SSL certificate for secure connections](#).
- Configure the connection timeout for Active Directory.
See section [8.3, Active Directory timing](#).
- Log diagnostic messages.
See section [8.4, Diagnostics logging](#).

Important: Changing other registry values is *not* supported unless instructed by Intercede Support.

8.1 Specifying Active Directory Domain Controllers

The MyID Authentication Server automatically locates Domain Controllers as needed. In environments where network segmentation exists, the MyID Authentication Server may not be able to contact all Domain Controllers. This can cause connectivity problems and logon delays.

In these environments, you can specify which Domain Controllers and Global Catalog Servers should be used using registry keys. Each key can contain one or many server names (FQDN recommended) separated by commas.

8.1.1 Specifying Global Catalog Servers

To specify the global catalog server to access from the MyID Authentication Server, set the following registry value:

```
HKLM\SOFTWARE\Authlogics\Authentication Server\DomainGCs
```

By default, this is blank.

Accepted values:

- One or more server names (FQDN recommended), separated by commas.

Used by components: MyID Authentication Server; Management Console

The MyID Authentication Server attempts to connect to each specified global catalog server and then remains connected to the server that responds to LDAP queries the quickest.

Note: This setting disables the auto-detect global catalog servers functionality within MyID.

8.1.2 Specifying Domain Controllers

To specify the Domain Controllers to access from the MyID Authentication Server, set the following registry value:

```
HKLM\SOFTWARE\Authlogics\Authentication Server\DomainDCs
```

By default, this is blank.

Accepted values:

- One or more Domain Controller names (FQDN recommended), separated by commas.

Used by components: MyID Authentication Server; Management Console

The MyID Authentication Server attempts to connect to each specified Domain Controller and then remains connected to the server that responds to LDAP queries the quickest. The MyID Authentication Server initially finds the names of all the Domains in the Forest, and the Domain Controllers in each Domain by querying the Global Catalog. It then maps the results against the Domain Controllers list in the registry to calculate which server to use for each Domain. If a Domain does not have a Domain Controllers specified, one is selected automatically.

Note: This setting disables the auto-detect Domain Controller functionality within MyID.

8.2 Adding a trusted SSL certificate for secure connections

When replacing the self-signed SSL certificate on the MyID server with an alternative from a trusted root authority, the certificate must obey the following:

- The Common Name (CN or SAN) in the certificate must match the DNS value use by MyID agents or make use of a wide card certificate.
- The certificate must be trusted by all systems that connect directly to the MyID server.

To do the replacing, using Internet Information Services (IIS) Manager, edit the HTTPS IIS bindings for the MyID web site and select the new SSL certificate.

8.3 Active Directory timing

You can set the following values in the registry:

- Domain access timeout.
- Domain controller refresh.

8.3.1 Domain access timeout

`HKLM\SOFTWARE\Authlogics\Authentication Server\DomainAccessTimeout`

Default value: 60

Accepted values:

- 0 – disabled, indefinite timeout.
- 1 to 120 – timeout in seconds.

The time taken in seconds before a connection established by a MyID component to a Domain Controller times out.

8.3.2 Domain Controller refresh

`HKLM\SOFTWARE\Authlogics\Authentication Server\DomainControllerRefreshTime`

Default value: 15

Accepted values:

- 1 to 9999 – timeout in minutes.

The time taken in minutes before a new search is done to locate the quickest Global Catalog Server and Domain Controller.

8.4 Diagnostics logging

You can control the diagnostics logging using the Windows registry.

8.4.1 Enabling logging

To enable or disable diagnostics logging, set the following registry value:

`HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingEnabled`

The default value is 1.

Accepted values:

- 0 – disabled.
- 1 – enabled.

When you enable this value, various log files are created in the logging folder. Intercede support may request these logs from you.

8.4.2 Setting the logging location

To control the location of the log files, set the following registry value:

`HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingFolder`

The default value is:

`C:\Program Files\Authlogics Authentication Server\Log\`

Accepted values:

- Any valid local folder with the same NTFS permissions as the default folder.

8.4.3 Setting the retention time for rolling logs

Old logs are deleted after a specified interval has passed; for example, after three days (which is the default), or two months. You specify this retention time using the interval type (`LoggingRollingIntervalType`) – for example, days or months, and the number of intervals (`LoggingFileCountLimit`) – for example, three (days) or two (months).

To set the interval type, set the following registry value:

`HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingRollingIntervalType`

The default value is 3 (days).

Accepted values:

- 0 – Infinite time between rolling logs – this means that old logs are never deleted.
- 1 – Years.
- 2 – Months.
- 3 – Days.
- 4 – Hours.
- 5 – Minutes.

This setting also determines when new logs are created; for example, new logs are created every day, or every year. Multiple logs may be created within each interval depending on the size limit you have set for the logs; see section [8.4.4, Size limit of rolling log files](#).

To set the number of intervals of logs stored, for example, three (days) or two (months), set the following registry value:

```
HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingFileCountLimit
```

The default value is 3 – after three intervals, the logs from the first interval are deleted.

Accepted values:

- A number of intervals.

8.4.4 Size limit of rolling log files

New log files are created every interval (for example, every day, or every month). To prevent these files from becoming too large, you can set the maximum size of each log file. When this size is reached, a new log file is created within the same interval; for example, if you are using day interval logs:

```
AuthlogicsIdentityServer-20250325-0001.log
```

```
AuthlogicsIdentityServer-20250325-0002.log
```

or for year interval logs:

```
AuthlogicsIdentityServer-2025-0001.log
```

```
AuthlogicsIdentityServer-2025-0002.log
```

To set the maximum size of each log file, set the following registry value:

```
HKLM\SOFTWARE\Authlogics\Authentication Server\LoggingRollingSizeLimit
```

The default value is 20 megabytes.

Accepted values:

- A number in megabytes.

Note: This setting does not reduce the total size of the logs; by limiting the size of the individual files, it increases the number of files.

8.4.5 Example of rolling logs

With the default values of:

- `LoggingRollingIntervalType` – 3 (day intervals)
- `LoggingFileCountLimit` – 3 (three days)
- `LoggingRollingSizeLimit` – 20 (MB)

Old log files are deleted after three days.

An example of rolling log files produced starting on the March 25th 2025 is:

```
AuthlogicsIdentityServer-20250325-0001.log
AuthlogicsIdentityServer-20250325-0002.log
AuthlogicsIdentityServer-20250326-0001.log
AuthlogicsIdentityServer-20250326-0002.log
AuthlogicsIdentityServer-20250326-0003.log
AuthlogicsIdentityServer-20250327-0001.log
AuthlogicsIdentityServer-20250327-0002.log
AuthlogicsRestApi-20250325-0001.log
AuthlogicsRestApi-20250325-0002.log
AuthlogicsRestApi-20250326-0001.log
AuthlogicsRestApi-20250326-0002.log
AuthlogicsRestApi-20250326-0003.log
AuthlogicsRestApi-20250327-0001.log
AuthlogicsRestApi-20250327-0002.log
```

Each day has several files, each with a maximum size of 20 megabytes. When the logger starts writing to the first file of March 28th, the cleanup process is triggered, deleting the files from March 25th, as those are then more than three days old.

8.4.6 Enabling verbose logging

You can enable more verbose logging for the following websites:

- Identity provider
- Web Management Portal
- Self Service Portal

To enable verbose logging:

1. If you do not have an `appsettings.Production.json` file for the website, create it in the website folder. By default, the settings files belong in the following locations:

- Identity provider:

`C:\Program Files\Authlogics Authentication Server\Web\IdP\`

- Web Management Portal:

`C:\Program Files\Authlogics Authentication Server\Web\Admin\`

- Self Service Portal:

`C:\Program Files\Authlogics Authentication Server\Web\SSP\`

Note: Do not use the `appsettings.json` file – that file can be overwritten when you update or upgrade MyID MFA and PSM.

2. In a text editor, open the `appsettings.Production.json` file for the website.

Edit the file to include the following:

```
{
  "Logging":{
    "LogLevel":{
      "Default":"Information"
    }
  }
}
```

3. Set the value of `Default` to one of the following, from most verbose to least:

- Trace
- Debug
- Information
- Warning
- Error
- Critical

By default, the logging is set to `Information` level.

4. Save the `appsettings.Production.json` file.
5. To ensure that this change is immediately enforced, you must refresh the application pool. To recycle the application pool:
 - a. On the MyID Authentication Server, in Internet Information Services (IIS) Manager, select **Application Pools**.

- b. Right-click the appropriate application pool:
 - Identity provider:
Authlogics Authentication Server IdP
 - Web Management Portal:
Authlogics Authentication Server WMP
 - Self Service Portal:
Authlogics Authentication Server SSP
 - c. From the pop-up menu click **Recycle**.
6. Check that the changes are successful by accessing the appropriate website; for example, log into the Web Management Portal.

9 Integration with external systems

Intercede provides integration guides for various external systems that may include step-by-step instructions or custom integration components.

You are recommended to use the [MyID Authentication Server Developers Guide](#) when planning to access the MyID Authentication Server programmatically for automation, scripting, or app integration. You can achieve extensive provisioning and workflow integration by using the Web Services APIs to create, delete, enable, disable accounts.

You can integrate MyID Authentication Server with any other external or third-party systems using Web Services or RADIUS, or a combination of the two.

If you are using Multi-Factor Authentication with an SSL VPN, no logon screen customization is required as a logon challenge is not displayed on a login screen. In this scenario a soft token, hardware token, or a SMS/TEXT token must be used, and the SSL VPN can use RADIUS to validate login requests.

If you are using deviceless authentication with an SSL VPN, you need to modify the login page of the SSL VPN to display a challenge. The SSL VPN can request the image from the MyID server using the `GetToken.ashx` web service with some coding effort. The SSL VPN can still use RADIUS to validate login requests but may alternatively use Web Services, if supported by the SSL VPN vendor.