MyID MFA and PSM

Version 5.1

Managed Service Provider Quick Start Guide

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

Document reference: IMP2079-5.1.0

May 2025

Copyright

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

1 Introduction

As a Managed Service Provider (MSP), you interact differently with MyID MFA and PSM than other organizations, as you work with multiple customers and have different levels of access to the machines on which MyID MFA and PSM are implemented.

This guide goes into detail on how to set up MyID MFA and PSM for MSPs.

1.1 Considerations

1.1.1 High availability

As a Managed Service Provider, to ensure that your deployment is highly available, you are recommended to deploy a standalone environment with an Active Directory domain consisting of at least:

- Two Domain Controllers.
- Two MyID Authentication Servers.
- A hardware load balancer.

In this scenario, the Active Directory is used only as an LDAP database, not as a traditional domain.

1.1.2 The Web Management Portal

The Web Management Portal is not designed to support MSP environments, as you cannot segregate administrators to specific sets of users. You can, however, use the Web Management Portal for the MSP platform host.

For more information on the Web Management Portal, see the *The Web Management Portal* section in the ***MyID Authentication Server Installation and Configuration Guide***.

1.1.3 Customizing the portal interfaces

You can customize and rebrand the IdP logon page and the Self Service Portal. However, you can set only one customization at a time; you cannot customize the IdP logon page or the Self Service Portal for each end customer.

For more information on customizing portal interfaces, see the *Customizing the portal interfaces* section in the ***MyID Authentication Server Installation and Configuration Guide***.

2 Managed Service Provider configuration for MyID Authentication Servers

As a Managed Service Providers, you are recommended to configure your MyID Authentication Servers with the following differences to the standard configuration:

- Disable the MyID Server Password Vault.

  See section *2.1*, *The MyID Server Password Vault*.
- Additional configuration to the Application properties.

  See section *2.2*, *Application properties*.
- Additional configuration to the Self Service Portal properties.

  See section *2.3*, *Self Service Portal properties*.

2.1 The MyID Server Password Vault

You may want to disable the MyID Server Password Vault so that you do not store the passwords of other organizations. You can enable the local password vault on the desktop using the **Enable Password Vault (Local Only)** Windows Desktop Agent group policy setting, or the following registry setting:

```
HKLM\SOFTWARE\Policies\Authlogics\Windows Desktop
Agent\EnableLocalOnlyPasswordVault
```

For more information on the **Enable Password Vault (Local Only)** group policy setting, see the *General settings* section in the ***Windows Desktop Agent Integration Guide***.

2.2 Application properties

As an MSP, you must set the Application properties in a particular way. For more information on the Application properties dialog, see the *Applications Properties* section in the ***MyID Authentication Server Installation and Configuration Guide***.

The **Authority URI** is the main DNS entry point for MSP customers and therefore must use a publicly trusted SSL certificate and port 443. The **Authority URI** is a combination of the **IdP Host**, **IdP Domain**, and **TCP Port**.

You must enable **Multiple DNS Domains** and add the DNS domain name of every MSP end customer to the list. This is to ensure that each end-customer DNS works with a multi-tenant setup. While you can change this in the Application properties dialog in the MMC, you can also change it more conveniently using the Rest API.

You are recommended to configure two signing certificates with different expiry date, with the Primary IdP Signing Certificate set to expire first. This means that when the Primary IdP Signing Certificate expires, you can swap the certificates and remove the expired certificate, replacing it with a new secondary certificate. This process avoids downtime during certificate changes.

2.2.1 Setting up end-customer domain names

MyID MFA uses the following logic when constructing URLs for end-customer domain names:

`<server-host><server-domain-with-no-dots>:<multi-domain-name-with-no-dots>`

Where:

- `<server-host>` is the IdP Host.
- `<server-domain-with-no-dots>` is the IdP Domain without dots.
- `<multi-domain-name-with-no-dots>` is an end-customer domain from your **Multiple DNS Domains** list.

You must therefore internally configure the end-customer domains to fit this format.

This is particularly required when integrating with Entra to provide authentication to Microsoft 365, as that requires a unique Entity ID for each Microsoft tenant.

2.3 Self Service Portal properties

If you plan to offer the Self Service Portal to end customers, on the **Settings** tab of the Self Service Portal Properties dialog, update the URL to your main DNS entry point for MSP customers. This is the **Authority URI** that you set in section *2.2*, *Application properties*.

3 Windows Desktop Agent Integration for MSPs

3.1 Design and deployment scenarios

As MSPs do not have access to Group or Local Policies, you must directly use registry key editing to set these settings. The location on each machine of the Windows Desktop Agent Group Policy registry keys to edit is:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Authlogics\Windows Desktop Agent
```

For information on the available Group Policy settings, see the *Configuring the MyID Windows Desktop Agent* section in the ***Windows Desktop Agent Integration Guide***.

To get the registry key name and the data representing the of each value of each group policy, change them on a local machine. You can then either automate the copying of your local registry key changes, or you can use a registry editor to look at the changes to make on each machine.

3.2 Allowing duplicate names

As a Managed Service Provider, if you have a centrally hosted MyID MFA and PSM server, you may need to cater for duplicate names:

- You may need to support duplicate Active Directory domain names if two organizations use the same domain name.
- You may need to support multiple workgroup-based computers with the same computer name.

The Windows Desktop Agent supports multiple domain and computer names by allowing you to substitute the names with a GUID, an ID that is guaranteed to be unique.

3.2.1 Allowing duplicate Active Directory domain names

To allow duplicate Active Directory domain names, create the following registry value on the client PC:

```
HKLM\SOFTWARE\Policies\Authlogics\Windows Desktop Agent\MspEnableUniqueDomainId
```

Accepted values:

- `0` – disabled.
- `1` – enabled.

When you enable this value, the Windows Desktop Agent associates each Active Directory domain name with a unique GUID, and replaces the Active Directory domain name with the relevant GUID when sending logon requests to the server. The Windows Desktop Agent obtains the GUID from the Active Directory configuration automatically.

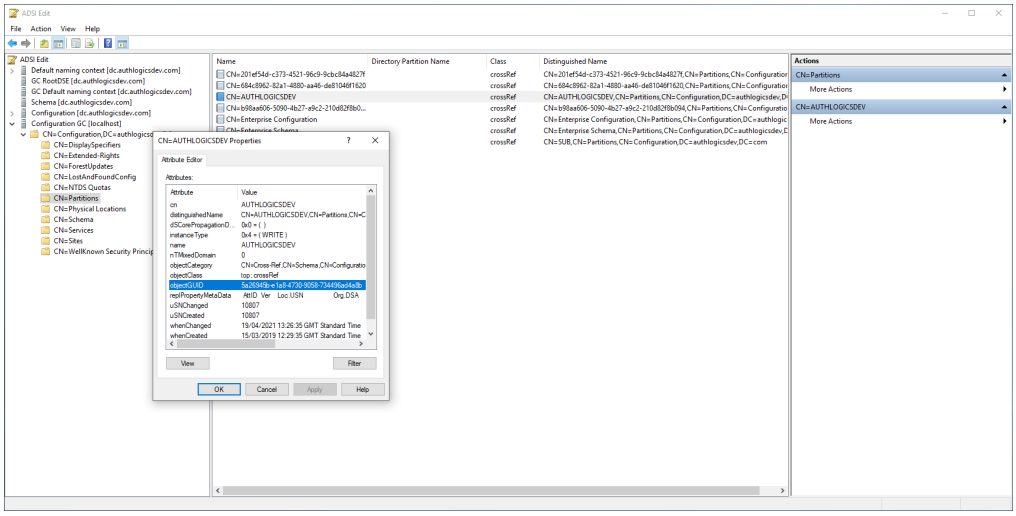
Note: This setting is in the `Policies` section of the registry, but is not visible in the Group Policy Template.

To complete the setup of allowing duplicate Active Directory domain names, you must also:

1. Get the GUID from the Active Directory Configuration Partition.

   This is available in all Global Catalog servers and is named:

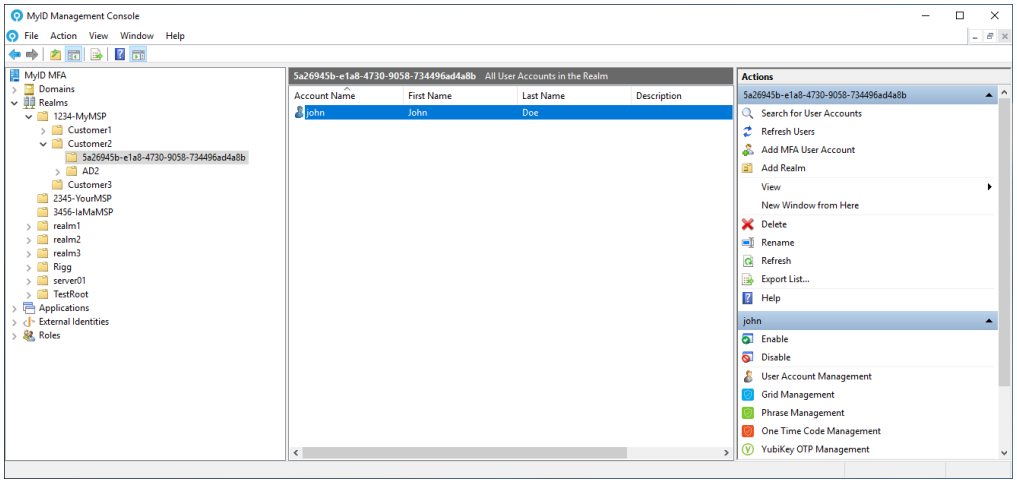
   `objectGUID`



2. On the authentication server, in the MyID Management console:

   a. Create a realm with the name of the Active Directory domain name GUID.

   b. Within the new realm, create the external users associated with the computer associated with that Active Directory domain name GUID.



3.2.2 Allowing duplicate computer names

To allow duplicate computer names, create the following registry keys on the client PC:

- `HKLM\SOFTWARE\Policies\Authlogics\Windows Desktop Agent\MspUniqueIdKeyName`

  Accepted value:

  - A path to the registry key where you have stored a unique GUID.

- `HKLM\SOFTWARE\Policies\Authlogics\Windows Desktop Agent\MspUniqueIdKeyValue`

  Accepted value:

  - The name of the registry value within the above key where you have stored a unique GUID.

Note: These settings are in the `Policies` section of the registry, but are not visible in the Group Policy Template.

For example, if you have stored a GUID in the following registry value:

`HKEY_LOCAL_MACHINE\SOFTWARE\SoftwareName\Subfolder\DeviceGuid`

Set the following key values:

- `MspUniqueIdKeyName` = `"HKEY_LOCAL_MACHINE\SOFTWARE\SoftwareName\Subfolder"`
- `MspUniqueIdKeyValue` = `"DeviceGuid"`

When enabled, the Windows Desktop Agent associates the name of each computer with the unique GUID provided by the `MspUniqueIdKeyName` and `MspUniqueIdKeyValue` registry settings, and replaces the computer's name with this GUID when sending logon requests to the server.

For example, if you have a PC with the name `mypc`, with users `jane` and `susan`, if you set the following in the PC registry:

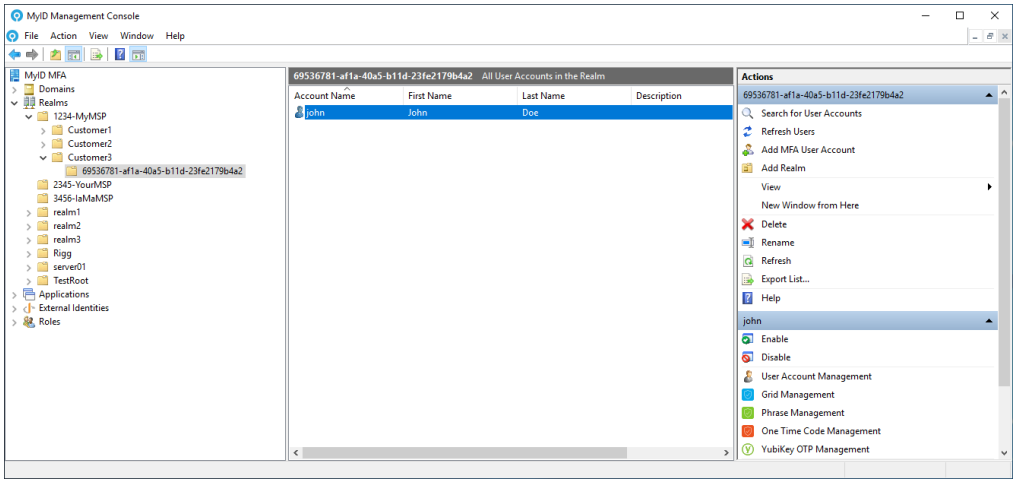
```
[HKEY_LOCAL_MACHINE\SOFTWARE\SoftwareName\Subfolder]
"DeviceGuid "="723ea5f0-e796-4507-9234-ac35d9bc37e0"
```

when the Windows Desktop Agent sends logon requests to the server, it makes the following substitutions:

- `mypc\jane` becomes `723ea5f0-e796-4507-9234-ac35d9bc37e0\jane`
- `mypc\susan` becomes `723ea5f0-e796-4507-9234-ac35d9bc37e0\susan`

To complete the setup of allowing duplicate computer names, in the MyID Management console on the authentication server, you must also:

1. Create a realm with the name of the computer name GUID.
2. Within the new realm, create the external users associated with the computer associated with that computer name GUID.



4 Federation with Microsoft 365 for MSPs

4.1 Multi-domain configuration

As an MSP, it is essential that you enable multi-domain configuration, as each customer has a unique domain name. For information on enabling multi-domain configuration, see the *Enable multi-domain federation using PowerShell* section in the ***Federation with Microsoft 365*** guide.

You can use the sample PowerShell scripts, or you can call the Microsoft Graph APIs and Authentication Server Rest APIs directly from MSP application logic.

4.2 Federation without directory synchronization

As MSP customers who use Entra ID synchronize with their own existing Active Directory domain if they have one, or else just use a Workgroup of Entra ID directly, there is no opportunity to use the Microsoft directory synchronization tool to link the Entra ID tenant to the MFA directory.