MyID MFA and PSM

Version 5.0.7

High Availability and Load Balancing Guide

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

Copyright

Conventions

- 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 and to indicate references to other sections within the current document:

  For example:
  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and Italic*** 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 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

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.

You can configure MyID Multi-Factor Authentication to be highly available, load-balanced, and redundant, based on browsers and various agents authenticating to the MyID servers.

For Enterprise environments, Intercede recommends that you deploy at least two MyID Authentication Servers within an environment; however, you can deploy more than two servers if required.

If the enterprise is spread over numerous geographic locations, Intercede recommends that each location has its own MyID Authentication Server deployments so that authentication requests are not sent over potentially slow WAN links, and are instead processed locally.

Note: Before you install additional Authentication Servers, ensure that the Authentication Server and Identity Provider Signing certificates, with their private keys, have been imported onto the new Authentication Server before starting the installation.

1.1 Change history

Version	Description
IMP2051-01	Reformatted and released with MyID MFA and PSM version 5.0.7. Added information about ensuring high availability for the identity provider and other services.

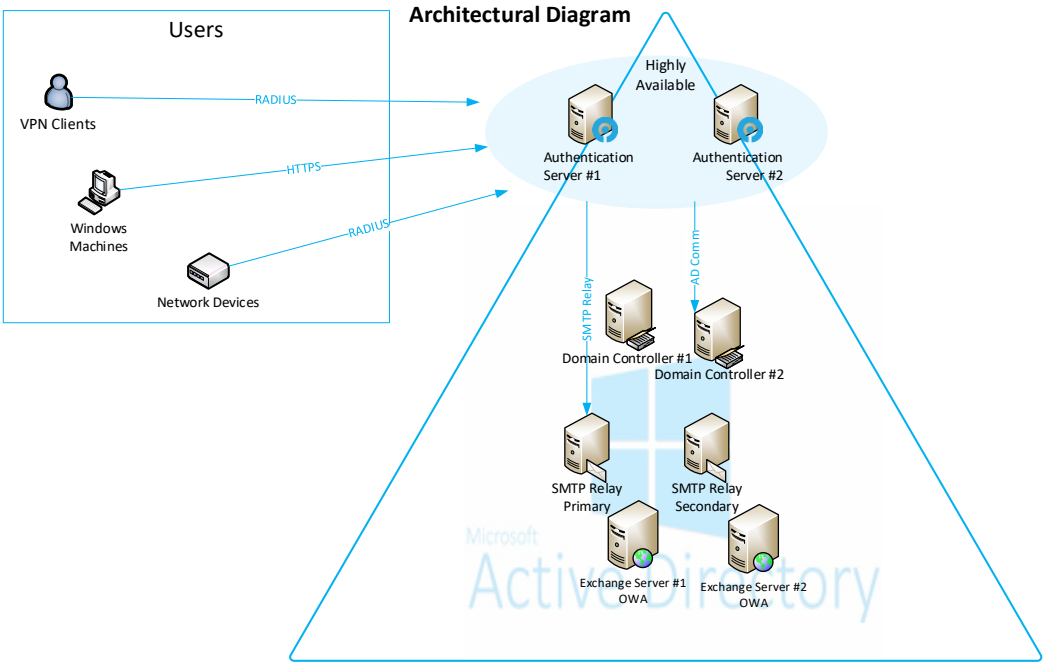
1.2 MyID MFA uses Active Directory as a database

MyID uses the existing Active Directory database as the underlying user account database with no schema extensions; in environments where there are multiple Domain Controllers, the MyID settings and user information is automatically replicated to the multiple deployed Domain Controllers.

For recovery purposes, a fresh installation of a MyID MFA and PSM server that has the private key of the original certificate can access the user and settings from the Active Directory with no loss of data.

1.3 Architecture

The following higher-level architecture diagram depicts a typical MyID deployment showing the various clients attaching to the MyID servers:



2 Agents

2.1 MyID Windows Desktop Agent

The MyID Windows Desktop Agent (WDA) is designed for high availability as soon as more than one MyID Authentication Server is installed within the Active Directory forest. It determines which servers are accessible and the server which responds the quickest is used to process the authentication request.

To do this, when attempting an authentication request, the WDA queries the Active Directory to determine the names of all deployed MyID Authentication Servers. Once WDA knows what MyID Authentication Servers are registered within Active Directory, WDA polls the MyID servers to determine which server has the fastest response time. The WDA sends the authentication request to the first MyID Authentication Server to respond.

If you are moving PCs between offices, this can be useful, as it ensures that the *local* authentication server is used.

If there are registered MyID Authentication Servers that are not available, the authentication requests are passed only to the registered servers that respond. If no servers are available, the WDA works offline.

With this functionality, WDA is natively Active-Active highly available and network load-balancing is not required.

2.2 MyID Exchange Agent

The MyID Exchange Agent is designed to be automatically highly available as soon as more than one MyID Authentication Server is deployed within the Active Directory forest. When attempting an authentication request, the Exchange Agent queries Active Directory and requests the server names of all deployed MyID servers. MyID Exchange Agent then polls the registered MyID Authentication Servers and determines each server's availability.

The MyID Exchange Agent then sends the authentication requests to the first responding server; this satisfies high-availability, redundancy, and load-balancing natively in an Active-Active manner.

2.3 MyID ADFS Agent

The MyID ADFS Agent is designed to be automatically highly available as soon as more than one MyID Authentication Server is deployed within the Active Directory forest. When attempting an authentication request, the MyID ADFS Agent queries Active Directory and requests the server names of all deployed MyID servers. The MyID ADFS Agent then polls the registered MyID Authentication Server and determines each server's availability.

The MyID ADFS Agent then sends the authentication requests to the first responding server; this satisfies high-availability, redundancy, and load-balancing natively in an Active-Active manner.

2.4 MyID RADIUS Server

Every MyID Authentication Server is a RADIUS Server. The MyID Authentication Servers can accept RADIUS authentication requests from RADIUS clients; for example, from VPN solutions like Palo Alto, Cisco Server, F5, Citrix, and Linux Servers.

MyID uses the Microsoft Network Policy Server role in Windows for processing RADIUS server authentication.

Note: You must ensure that all the MyID RADIUS Servers have the appropriate RADIUS clients configured within the Network Policy Server. For more information, see the ***MyID Authentication Server*** guide.

You can achieve high availability, load-balancing, and redundancy in multiple ways; for example, Active-Passive or Active-Active.

2.4.1 Active-Passive

This is the most common deployment method. In an Active-Passive deployment method, the configuration of the RADIUS client defines the load-balancing / high-availability by specifying the Primary and Secondary RADIUS servers at the client end.

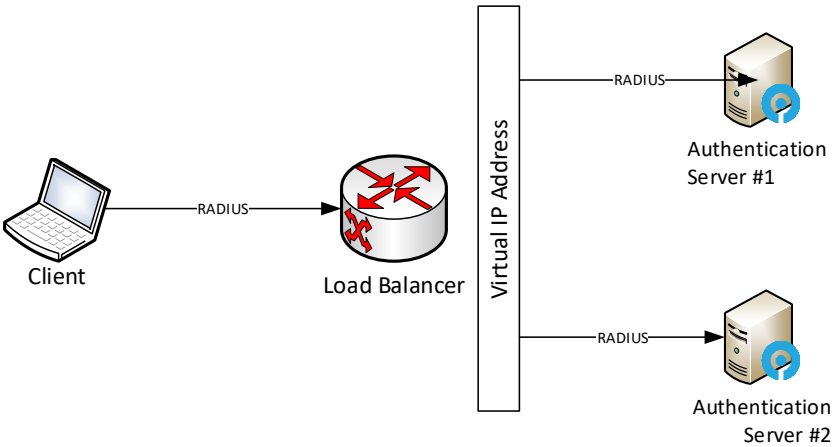
In this scenario, MyID Server #1 is configured as the primary RADIUS server and MyID Server #2 as the secondary RADIUS server. When configured in this manner, the RADIUS client sends authentication requests to the primary RADIUS server. If this server is not available, the client instead uses the Secondary Server for authentication request processing.

2.4.2 Active-Active

To make MyID RADIUS Server highly available in an Active-Active manner, you must share multiple MyID Authentication Servers using a Hardware or Software Load Balancer such as Windows Network Load Balancing (NLB).

The load balancer creates a Virtual IP Address and forwards the RADIUS protocols to UDP ports 1645 or 1812. RADIUS clients pass RADIUS authentication requests to this virtual IP address. The load-balancer then determines the MyID Server availability and passes the authentication request to the appropriate server for processing.

The following diagram depicts this scenario:

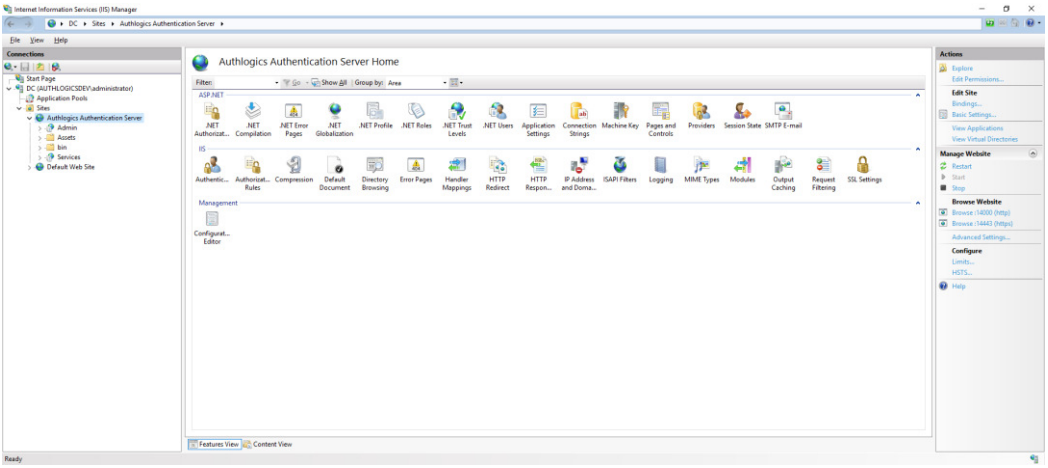


3 MyID Authentication Server services

MyID Authentication Servers are also deployed with specific services; namely, the MyID IdP, Self-Service Portal, Web Operator Console, and Web Service APIs.

You can find these services published as services and web sites on the Authentication Server's Internet Information Services (IIS) instance under the **MyID Authentication Server** site.

By default, these sites are running on the HTTPs protocol bound to port 14443.



To load balance these services and make them highly available and redundant, you must implement a hardware or software load-balancer or reverse proxy.

The following services are published on MyID Authentication Servers:

- Identity Provider
- Self-Service Portal
- Web operator console
- REST APIs

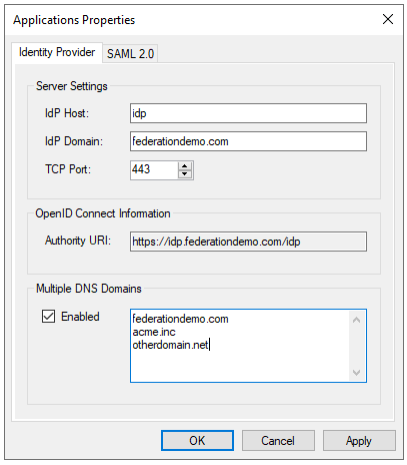
You can load-balance these services and publish them on a virtual DNS / IP Address across multiple servers.

3.1 Identity provider

The provisioned services location is determined on the Applications Properties dialog, on the **Identity Provider** tab.

By default, the IdP URI assumes the DNS name of the first MyID Authentication Server deployed using the address format:

```
https://{IdP Host}.{IdP Domain}:14443/idp
```



You can change the IdP Host name at any time to reflect a virtual DNS host name instead of the first server name. The virtual DNS host name can resolve to a virtual IP address of a load balancer or a round robin DNS entry, for example.

Warning: You can also change the IdP Domain name; however, it has the following impacts:

- Any existing bearer tokens no longer successfully validate, as the issuer is based on the IdP Domain name.
- Any existing FIDO2 passkeys must be re-registered, as the IdP Domain name is the issuing authority for passkeys.

3.2 Additional services

The additional Self Service Portal, Web Operator Console, and Web Services APIs are services that are hosted on the Authentication Server's IIS instance.

Below is a list of the service URIs:

Service	URI
Self Service Portal	`https://{IdP Host}.{IdP Domain}:14443/ssp`
Web Operator Console	`https://{IdP Host}.{IdP Domain}:14443/admin`
Web Service APIs	`https://{IdP Host}.{IdP Domain}:14443/services/api`

These URIs are generated based on the IdP server settings.

The following diagram shows the infrastructure: