intercede

MyID Authentication Server

High availability, Load balancing and Redundancy for MyID MFA

Product Version: 5.0

Publication date: February 2024

Call us on: +44 (0)1455 558 111 (UK & EMEA)
+1 408 706 2866 (US)
Email us: info@intercede.com

Intercede Ltd, Lutterworth Hall, St. Mary's Road, Lutterworth, Leicestershire, LE17 4PS, United Kingdom
UK Tel: +44 (0)1455 558 111 US Tel: +1 888 646 6943 email: info@intercede.com web: www.intercede.com

www.intercede.com | info@intercede.com | +44(0)1455 558 111| +1 888 646 6943

Table of Contents

Introduction

> **Note**
> MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly.
> The term 'Authlogics' may still appear in certain areas of the product.

This document has been created to show how MyID Multi-factor Authentication can be made to highly available, load-balanced and redundant based on the various agents authenticating to the MyID servers.

For Enterprise environments, Intercede recommend that at least 2 MyID Servers are deployed within an environment however, more than 2 servers can be deployed as required.

Furthermore, when the enterprise is spread over numerous geographic locations, we recommend that each location has its own MyID Authentication Server deployments so that authentication requests are sent over potentially slow WAN links and processed locally

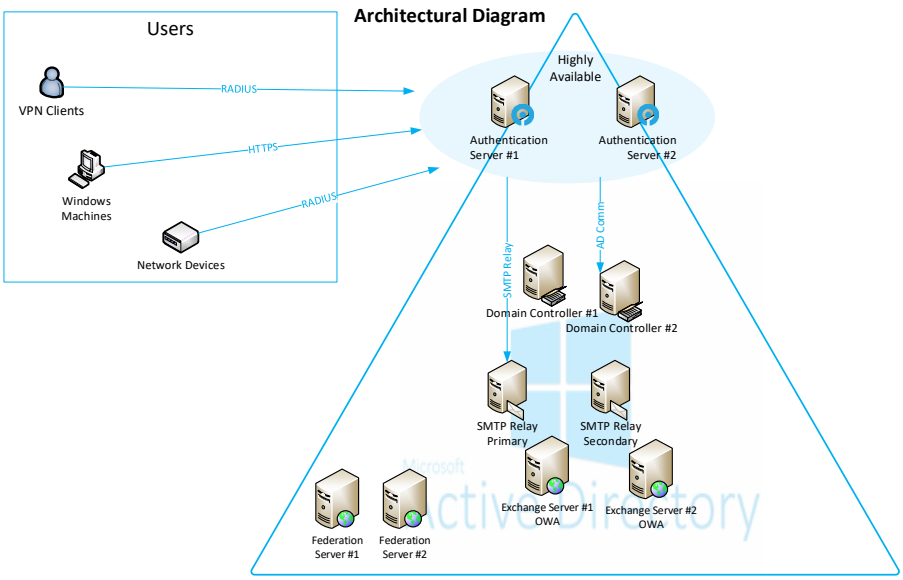
The MyID Database is Active Directory

MyID utilises the existing Active Directory database as the underlying user account database; with no schema extensions. As such, 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, an install of a new MyID server, with the private key of the original certificate, will be able to access the user and settings from the Active Directory with no loss of data.

Architecture

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



Agents

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 AD forest. When attempting an authentication request, WDA will query Active Directory to determine the names of all deployed MyID servers. Once WDA knows what MyID servers are registered within AD, WDA will then poll the MyID servers to determine which server has the fastest response time.

As soon as the first MyID server responds, the authentication request will be sent to the that MyID Authentication Server. If one of the registered MyID Server is not available, the other registered serves will respond and authentication requests will only be passed to these servers. If no servers are available then WDA will work offline.

With this functionality, WDA is natively Active-Active highly available and network load-balancing is not required. WDA determines which servers are accessible and the server which responds the quickest will be used to process the authentication request. This is also useful if PC's move between different offices to ensure the local Authentication Server is used.

MyID Exchange Agent

As with the Windows Desktop Agent, the MyID Exchange Agent is also designed to be automatically highly available as soon as more than one MyID Authentication Server is deployed within the AD forest. When attempting an authentication request, the Exchange Agent will query Active Directory and request the server names of all deployed MyID servers. MyID Exchange Agent will poll the registered MyID Authentication Server and will determine each server's availability.

MyID Exchange Server agent will then send the authentication requests to the first responding server thus satisfying both high-availability, redundancy and load-balancing natively in an Active-Active manner.

MyID ADFS Agent

The MyID ADFS Agent is also designed to be automatically highly available as soon as more than one MyID Authentication Server is deployed within the AD forest. When attempting an authentication request, MyID ADFS Agent will query Active Directory and request the server names of all deployed MyID servers. MyID ADFS Agent will poll the registered MyID Authentication Server and will determine each server's availability.

MyID ADFS Agent will then send the authentication requests to the first responding server thus satisfying both high-availability, redundancy and load-balancing natively in an Active-Active manner.

MyID RADIUS Server

Every deployed MyID Authentication Server deployed within the environment is a RADIUS Server. They are available to be accept RADIUS authentication requests from RADIUS clients, e.g. from VPN solutions like Palo Alto, Cisco Server , F5, Citrix and Linux Servers. MyID leverages the Microsoft Network Policy Server role for processing RADIUS server authentication.

> ***Note***
> ***Ensure that all the MyID RADIUS Servers have the appropriate RADIUS clients configured within the Network Policy Server. Please refer to the MyID Authentication Server for more information.***

High availability, load-balancing and redundancy can be achieved in multiple ways. Below is a description of these mechanisms.

Active-Passive

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

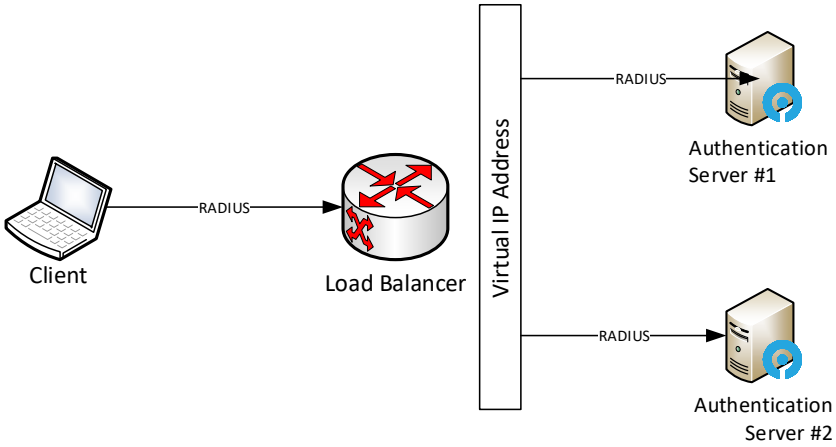
In this scenario, MyID Server #1 will be configured as the Primary RADIUS Server and MyID Server #2 as the Secondary RADIUS Server. When configured in this manner, the RADIUS client will send authentication requests to the Primary RADIUS Server. Should this server not be available, then the client will fall-over to the Secondary Server for authentication request processing.

Active-Active

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

The load balancer will create a Virtual IP Address and forward the RADIUS protocols UDP ports1645 and 1812. RADIUS clients will pass RADIUS authentication requests to this virtual IP address. The load-balancer will then determine the MyID Server availability and pass the authentication request to the appropriate server for processing.

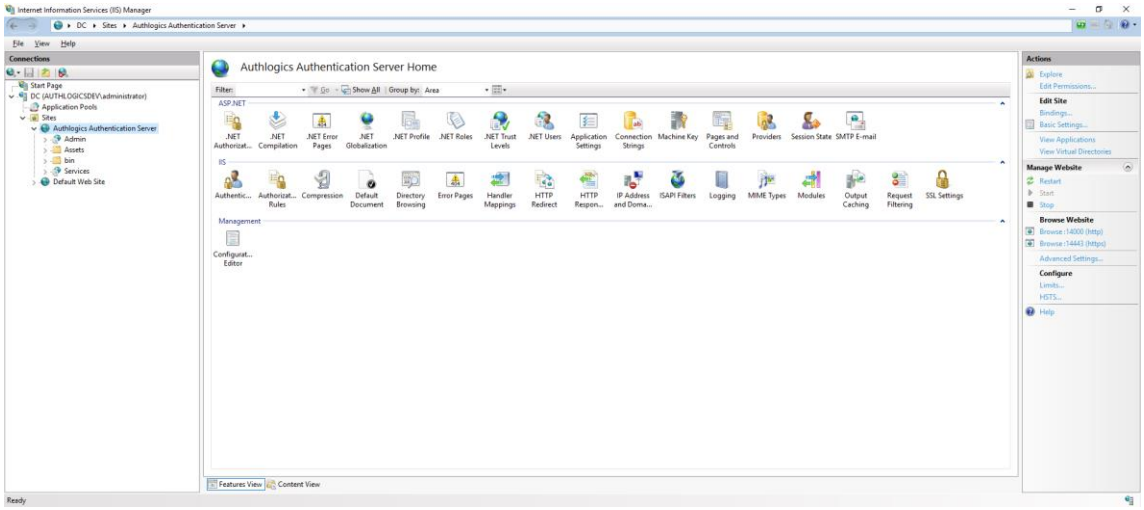
The following diagram depicts this scenario.



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. These services are web sites and services published on the Authentication Server's Internet Information Services (IIS) instance under the site MyID **Authentication Server.**

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



In order to load balance these services and make them highly available and redundant, a hardware or software load-balancer will need to be implemented and reverse proxy these protocols.

The following services are published on MyID Authentication Servers:

- Self-Service Portal - **"https://server.authlogicsdemo.com:14443/".**
- Web operator console - **"https://server.authlogicsdemo.com:14443/admin".**
- Web Service APIs -**"https://server.authlogicsdemo.com:14443/services/api".**

The following diagram shows the infrastructure: