



SurePassID MFA Server Install Guide for Windows Servers

SurePassID Authentication Server 2021



Table of Contents

Table of Figures.....	3
About this Guide	4
What is the SurePassID MFA Server for Windows?	5
Prerequisites	5
Security.....	6
Database	6
Internet Information Server	12
Post Configuration Steps	12
Installation	13
Customizing the System	22
Web.config.....	23
Default Language.....	25
SurePassID Portal Session Timeout	26
High Availability Considerations and Capabilities	29
Load Balancing.....	29
Data Management High Availability.....	30
Single/Multiple Datacenter Architecture	30
SurePassID Product Family.....	32

© 2013-2020 SurePassID , Corp. All rights reserved. Protected by patents pending. SurePassID , the SurePassID logo and design, and Secure SSO are registered trademarks or trademarks of SurePassID , Corp. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

SurePassID , Corp.
13750 W. Colonial Drive
Winter Garden, FL 34787
+1 (888) 200-8144
www.SurePassID.com

Table of Figures

SQL Server Authentication Settings	7
Connect to SQL Server	8
SQL Server Properties	8
Select Services App	10
Restart SQL Server	11
Start Configuration Wizard	13
Step 1 - Test Windows Authentication	14
Step 1 - Test SQL Server Authentication	14
Step 1 – Test Connection	15
Step 1 – Failure: Database Not Available	16
Step 1 – Success: Database Is Available	16
Step 2 – Create Installation	17
Step 3 – Define SurePassID Admin Account	18
Step 4 – Start Account Database Set-up	18
Step 4 – Start Account Database Completed	19
Step 5 – Copy Log Button	20
Add License File	21
Edit Hosts file	22
SurePassID Login Screen	22
High Availability Architecture	31

About this Guide

This guide explains how install and configure the SurePassID MFA Server in a Windows Server environment. The purpose of this guide is to provide a reference for system administrators.

This guide provides information on the following topics:

- **What is SurePassID MFA Server?**
 - A brief introduction to the SurePassID MFA Server for Windows Servers.
- **Installing and Configuring SurePassID MFA Server**
 - Detailed explanations for installing the SurePassID MFA Server in a Windows Server environment.

Other SurePassID Guides

The Server Install Guide for Windows Servers has the following companion guides that provide additional detail on specific topics for SurePassID MFA Server:

- [Developer API Guide](#)
- [Fido U2F Mobile API Guide](#)
- [System Administration Guide](#)
- [Local Agent Guide](#)
 - High performance Radius Server
 - Windows Event Log Synchronization
 - Active Directory Synchronization
- [Desktop Authenticator Guide](#)
- [Google Authenticator Guide](#)
- [SurePassID Mobile Authenticator Guide](#)
- [Mobile API Connector](#)
- [Windows Credential Provider Guide](#)
- [Self-Service Portal](#)
- [ADFS Installation Guide](#)

What is the SurePassID MFA Server for Windows?

The SurePassID MFA Server for Windows Servers is a complete, fully functional SurePassID multi-factor authentication server that operates on 32-bit or 64-bit Windows servers. The system is distributed as a Windows set-up (msi) install that you run on an existing or new Windows server. The server can be a physical server or a virtualized system running on-premises or on cloud platforms such as Windows Azure or Amazon AWS.

The system supports traditional OATH event-based and time-based One-Time Password (OTP) password authentication, authentication push technologies for mobile devices, and new technologies such as wearables, biometrics, and FIDO (Fast IDentity Online) authentication methods.

The system is by design a multi-tenant system. However, the default license file that is provided is for a single tenant only system to reduce the amount of configuration required for small and or single company installation. If you are a large company, a service provider you might want to consider using the multi-tenant version for the following reasons:

- You might want to partition users by logical group or organizational unit and allow those groups to manage their users while you maintain complete oversight for managing corporate governance, compliance, and group authentication policies based on risk.
- Service providers can partition their customer base, maintain oversight, eliminate disparate authentication systems, consolidate support activities, and create recurring revenue streams.

Prerequisites

SurePassID Server can be installed on the following Windows versions:

- **Windows 2012** – All versions
- **Windows 2016** – All versions
- **Windows 2019** – All versions
- **Windows 10**
- **SQL Server 2016, 2017, 2019** – Any version

Security

SurePassID MFA Server for Windows Servers does not install with any certificates for SSL. It is recommended that you configure the SurePassID application (IIS web app) for TLS using your corporate wild card certificates for production or create self-signed certificates for testing. Optionally the server can be configured to use message level security for a higher level security. Message-level security also requires additional certificate exchange between the server and your client-based applications that support message level security.

SurePassID MFA Server can operate in the DMZ or behind the corporate firewall. **It is very strongly recommended that it is installed behind the firewall** for security reasons.

SurePassID apps can reside inside the firewall, outside the firewall or in the DMZ. These are the only SurePassID components that should be outside the firewall.

Database

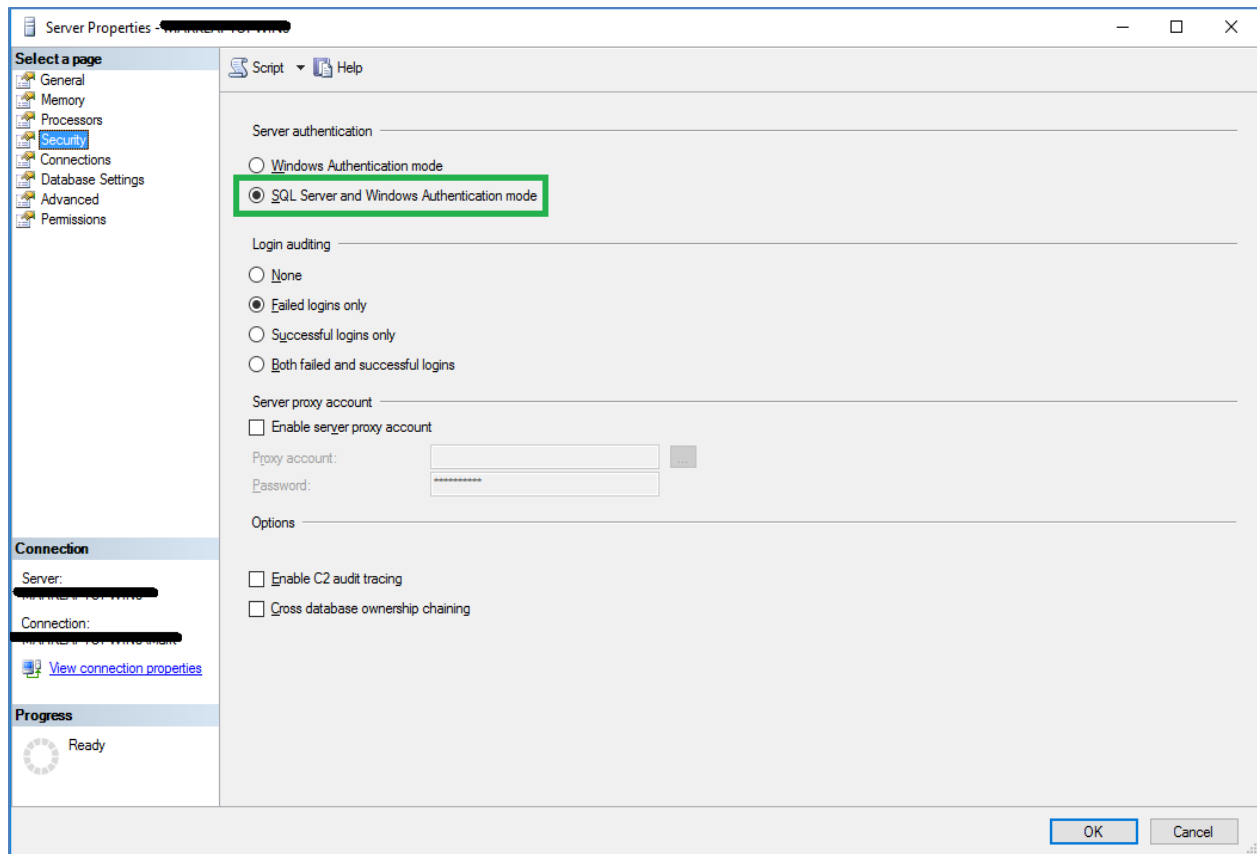
SurePassID Server requires a SQL Server database. You can use SQL Server any version after SQL Server 2014. You can use the Express, Standard or Enterprise editions.

Download SQL Server using the link below:

<https://www.microsoft.com/en-us/sql-server/sql-server-downloads>

Although you can use only Windows Authentication (and or Managed Service Accounts) it is recommended that you enable SQL Server authentication in addition to Windows authentication for the initial install. You can always disable SQL Server Authentication later.

Start SQL Server Management Studio, right click on the server, select **Properties** menu. The following form will be displayed. Verify the security setting as shown below:



SQL Server Authentication Settings

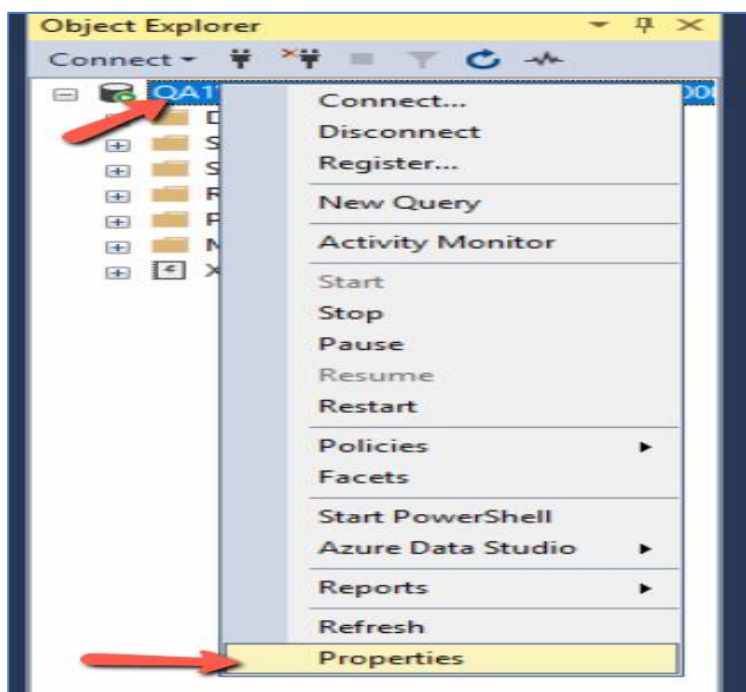
If **Windows Authentication mode** is selected follow the steps below to enable SQL Server and Windows Authentication mode.

Start **SSMS** with login with Windows authentication.



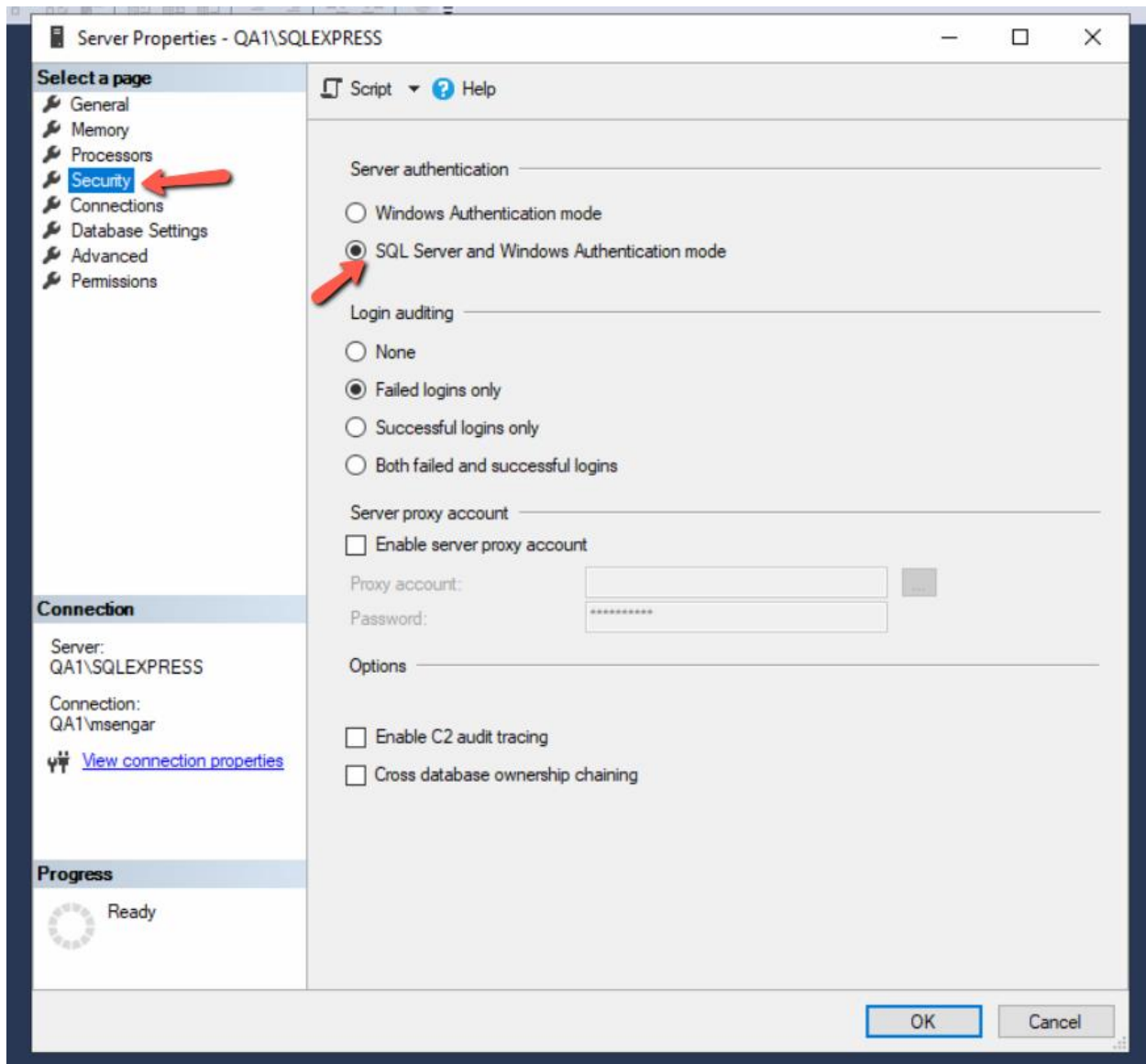
Connect to SQL Server

Right click on the SQL Server and select Properties.

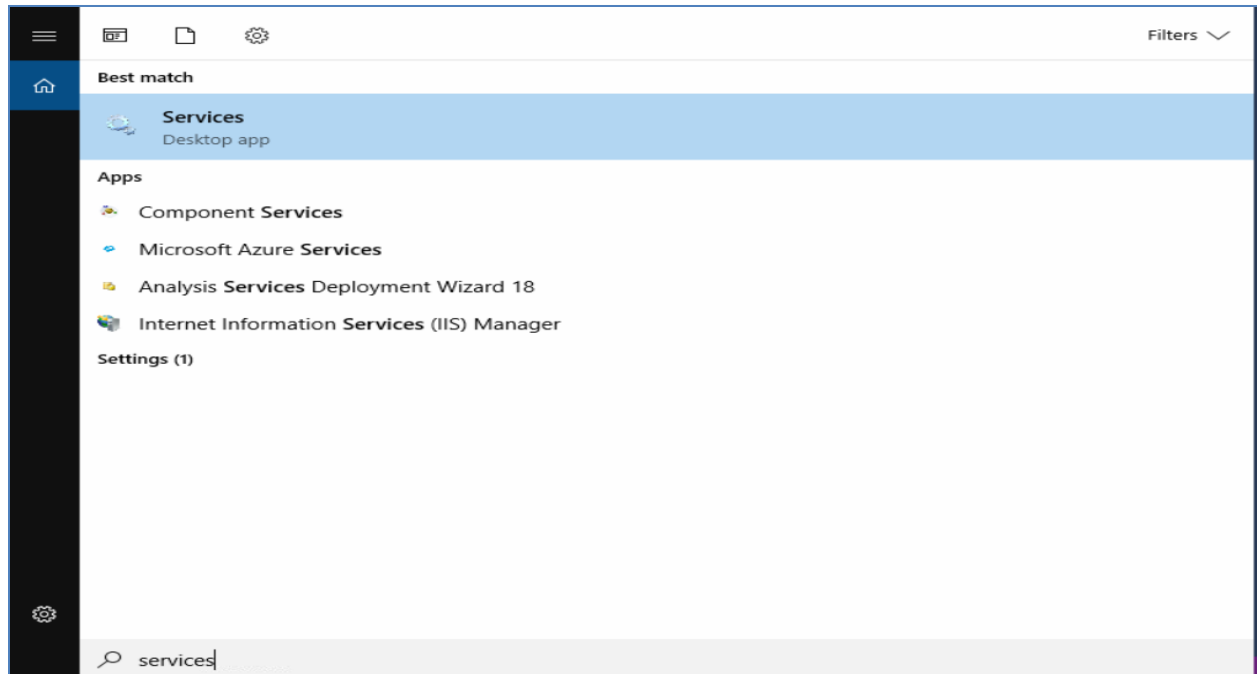


SQL Server Properties

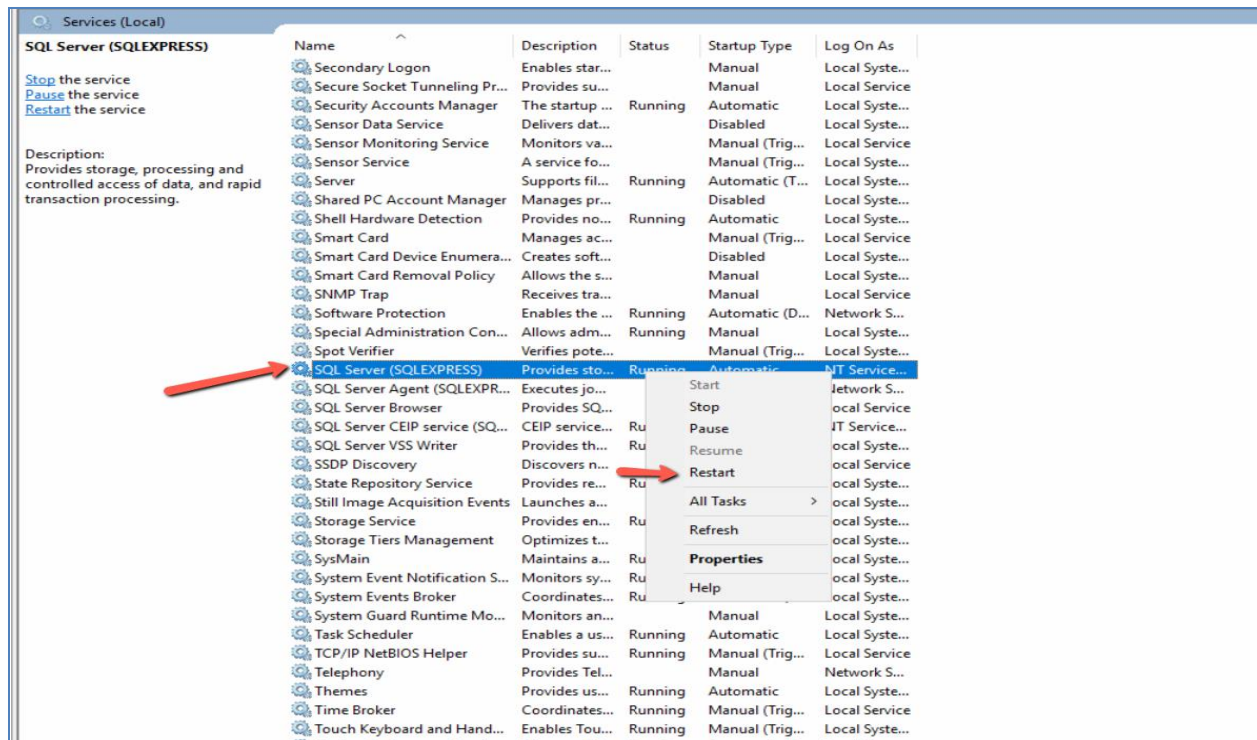
Select **Security** and then Select **SQL Server and Windows Authentication mode**



You must restart SQL Server for the changes to take effect. This can be done from **Services** app on your server as below:



Select Services App



Restart SQL Server

Right click on the SQL Server process and select Restart.

Internet Information Server

The Windows server must have the IIS feature enabled. If you will be sending emails using the IIS virtual SMTP server, you will need to make sure that feature is installed as well.

Post Configuration Steps

It is HIGHLY recommended that you proceed with the following steps after installation:

- Review the **SurePassID Administrators Guide** to get a feel for the system and review the tenant-specific customizations that are available.
- Copy the license file (site.lic) into the \bin folder of the SurePassID installation replacing the existing file.
- The system ships with 2FA turned off for the Administration portal. You need to turn MFA on after you setup the administrators with a 2FA device, set up push notifications, or enable Fido devices. To turn on 2FA, set:
`<configuration><appsettings> System.IgnoreLogin2FactorAuth = false`

in the web.config file. More on this below.

- Set up TLS for the SurePassID portal.
- Customize the web.config file.
- Customize the tenant instance you will be using.
- Protect the web.config file in the root folder of the SurePassID configuration by encrypting it using Aspnet_regiis utility. Detail procedures on how to do this can be found here:

[https://msdn.microsoft.com/en-us/library/zhhddkxy\(v=vs.140\).aspx](https://msdn.microsoft.com/en-us/library/zhhddkxy(v=vs.140).aspx)

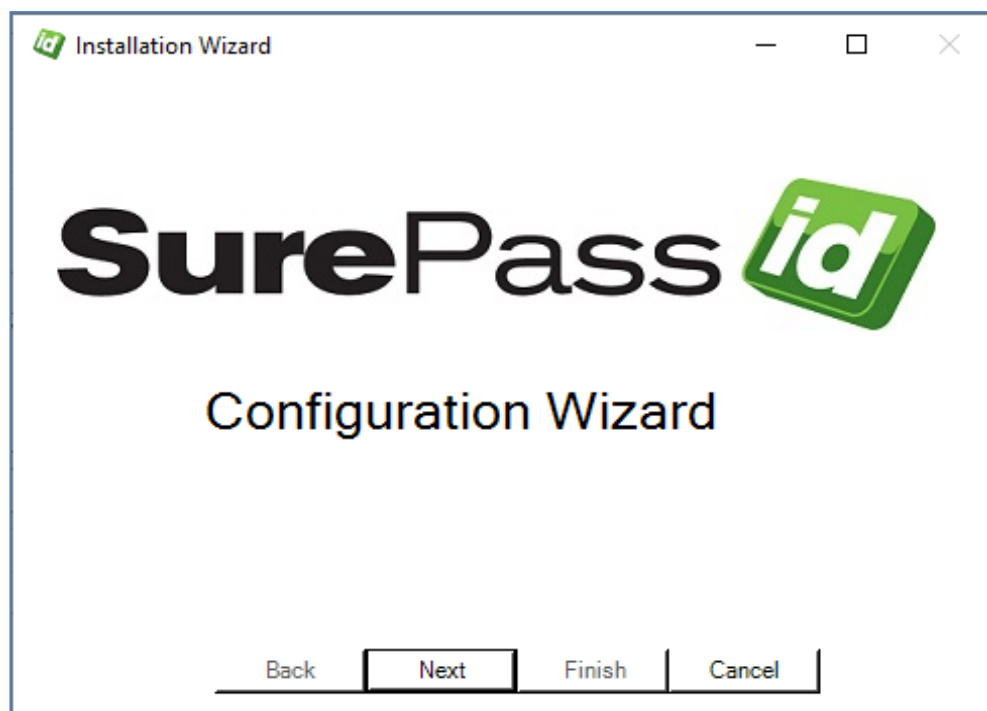
Installation

The SurePassID Server for Windows Servers is distributed as a setup file and an msi file. When you run the setup.exe, the system will be installed in an IIS virtual directory. As part of the system install, the SurePassID Configuration Wizard will start to perform the following functions:

NOTE: You will need an SQL Server admin account for steps 1 and 2.

1. Creates the SurePassID SQL Server database.
2. Creates the SurePassID database schema.
3. Creates all the strong AES256 encryption keys to keep sensitive data in the database secret.
4. Create the SurePassID Administrator account so you can log into the system after configuration is complete.
5. Set the user directory to either SurePassID or Active Directory
6. Optionally, import Active Directory users into SurePassID .

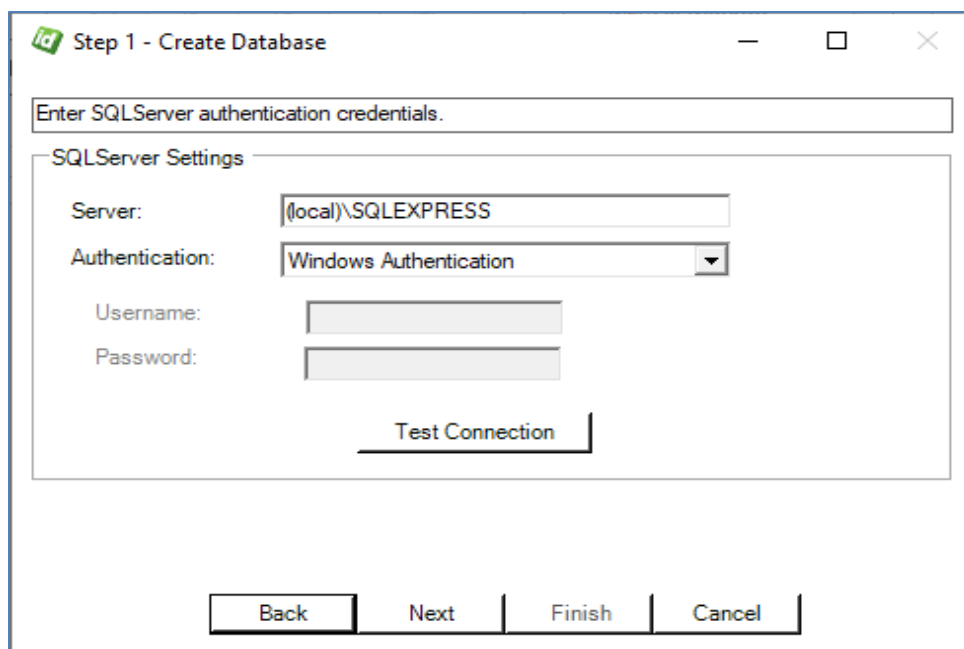
To run the SurePassID Configuration Wizard, run the **SurePassID Setup** icon short cut from the desktop. Once you start the Configuration Wizard you will see the following window:



Start Configuration Wizard

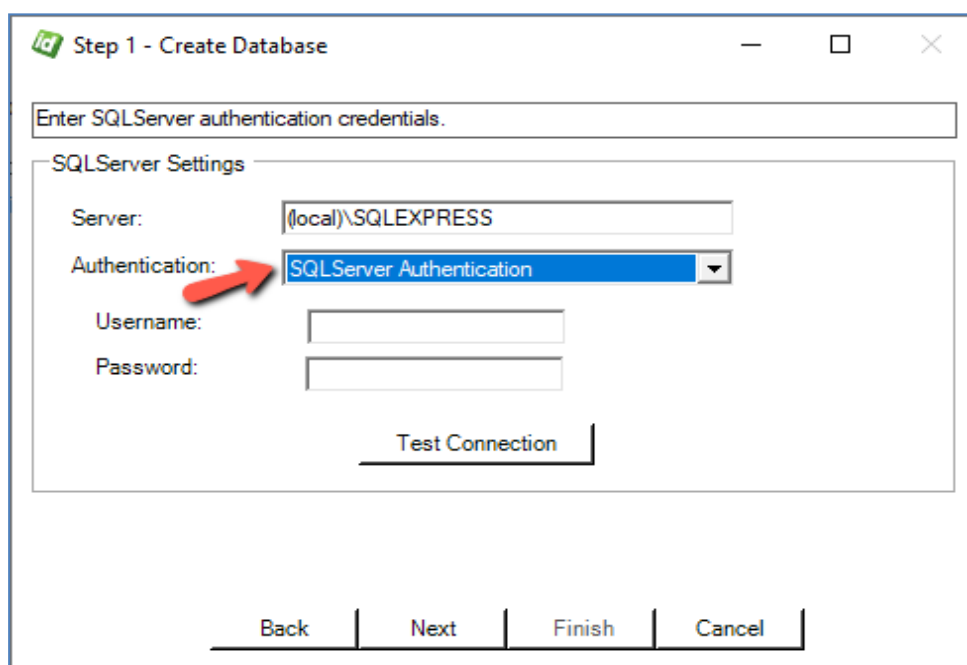
Click the **Next** button to test connectivity to the database.

You can use Windows Authentication or SQL server authentication for testing connectivity and the install. However, by default SQL Server Authentication must be enabled to start the SurePassID Administration portal.



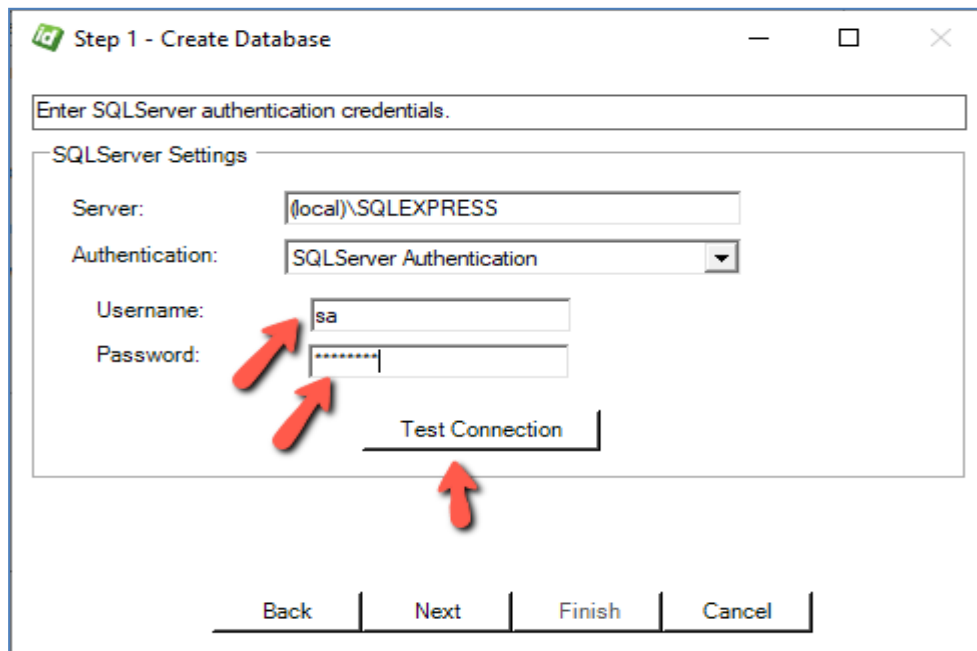
The screenshot shows a window titled "Step 1 - Create Database" with a green "id" logo. At the top is a text box labeled "Enter SQLServer authentication credentials." Below it is a section titled "SQLServer Settings" containing four fields: "Server:" with the value "(local)\SQLEXPRESS", "Authentication:" with a dropdown menu showing "Windows Authentication", "Username:" with an empty text box, and "Password:" with an empty text box. A "Test Connection" button is located below these fields. At the bottom of the window are four buttons: "Back", "Next", "Finish", and "Cancel".

Step 1 - Test Windows Authentication



This screenshot is similar to the previous one, but the "Authentication:" dropdown menu now shows "SQLServer Authentication" selected. A red arrow points to this dropdown menu. The "Server:" field remains "(local)\SQLEXPRESS", and the "Username:" and "Password:" fields are still empty. The "Test Connection" button and the bottom navigation buttons ("Back", "Next", "Finish", "Cancel") are also present.

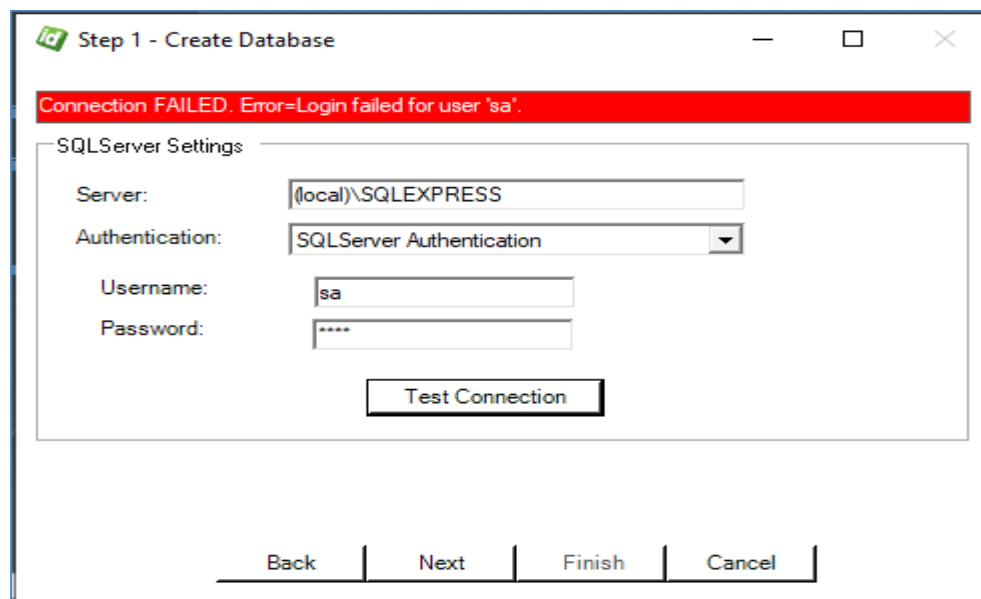
Step 1 - Test SQL Server Authentication



Step 1 – Test Connection

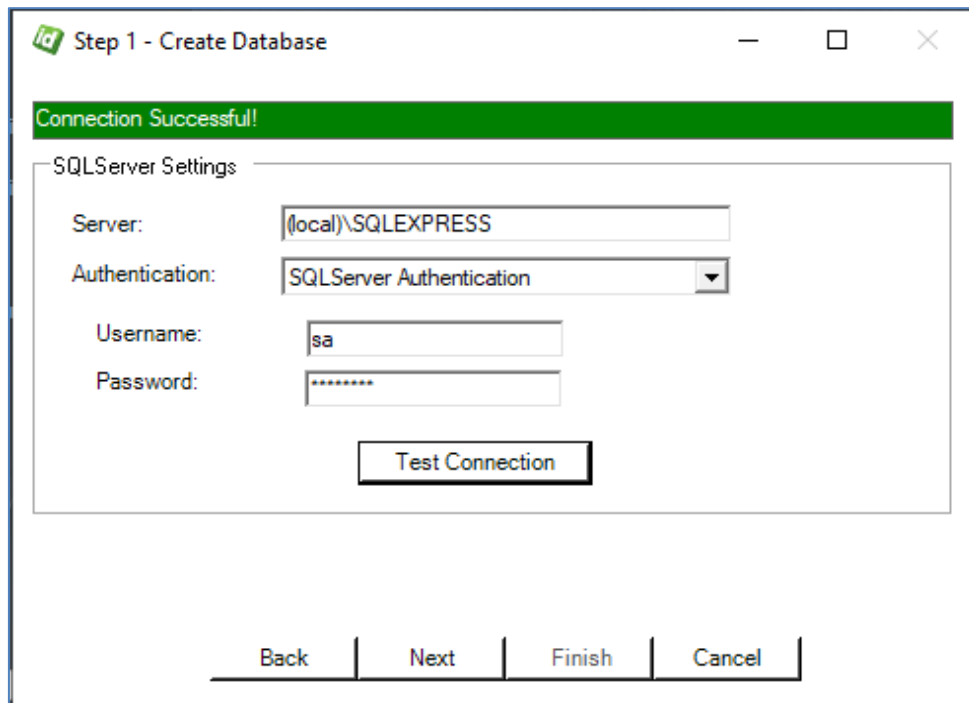
If you have the connection details for your SQL Server database you can enter them now. If you are not sure you can accept all of the defaults and click the **Test Connection** button.

If the connection is not available, you will see the following window and you need to talk to your system administrator and cancel the wizard by pressing the **Cancel** button.



Step 1 – Failure: Database Not Available

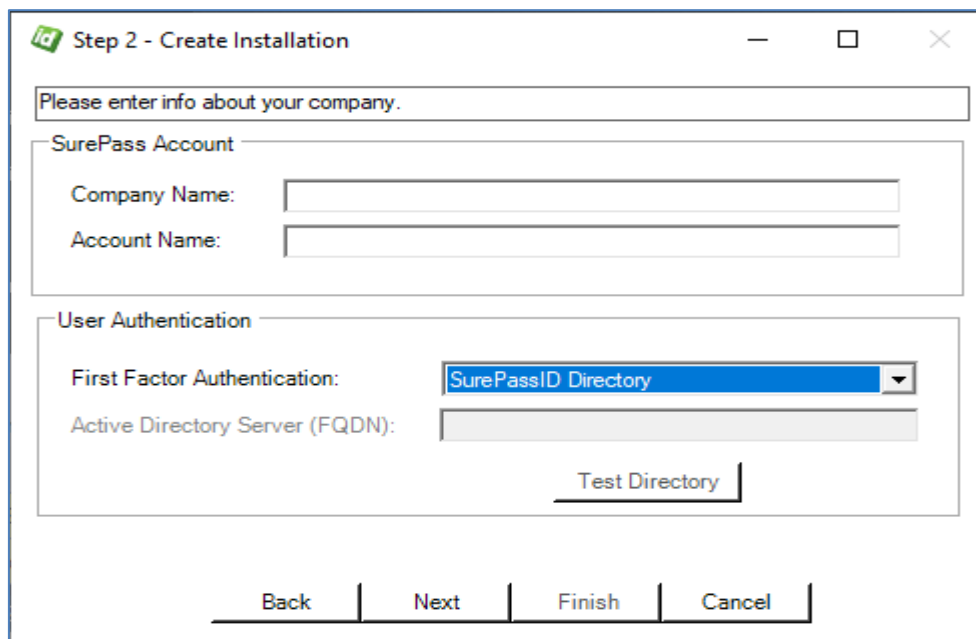
If the connection is available, you will see the following window.



The screenshot shows a window titled "Step 1 - Create Database". At the top, a green banner reads "Connection Successful!". Below this, the "SQLServer Settings" section contains the following fields: "Server:" with the value "(local)\SQLEXPRESS", "Authentication:" with a dropdown menu set to "SQLServer Authentication", "Username:" with the value "sa", and "Password:" with a masked field of seven asterisks. A "Test Connection" button is located below these fields. At the bottom of the window, there are four buttons: "Back", "Next", "Finish", and "Cancel".

Step 1 – Success: Database Is Available

Press the **Next** button. You will see the following window.



The screenshot shows a window titled "Step 2 - Create Installation". At the top, there is a text box with the prompt "Please enter info about your company.". Below this, the "SurePass Account" section contains two text boxes: "Company Name:" and "Account Name:". The "User Authentication" section contains a "First Factor Authentication:" dropdown menu set to "SurePassID Directory" and an "Active Directory Server (FQDN):" text box. A "Test Directory" button is located below these fields. At the bottom of the window, there are four buttons: "Back", "Next", "Finish", and "Cancel".

Step 2 – Create Installation

The **Create Installation** window has the following fields:

- **Company Name** – Your Company name. This will be displayed to users when they log into SurePassID . You can change this later.
- **Domain Name** – The SurePassID domain name associated with this SurePassID account. This is not related to anything outside of SurePassID can be anything you think that is appropriate. You can change this later but you will need it for initial login to the system.
- **First Factor Authentication** – SurePassID first authenticates users via user name and password as the first factor of authentication. SurePassID can authenticate users in its own directory or in Active Directory. You need to select the choice that makes the most sense for your deployment. You must select from the following two options:
 - **SurePassID**
 - **Active Directory**
- **Active Directory FQDN** – If you select Active Directory as your first **First Factor Authentication**, then you will need to enter the Active Directory Domain Controller fully qualified domain name or IP address.
- **Test Button** – Click this button to verify connectivity to Active Directory.

Press the **Next** button. You will see the following window.

Step 3 - Define Users

Enter the new Administrator login account credentials below.

SurePass Administrator Login Credentials

Username:* Administrator

First Name:*

Last Name:*

Email:*

Mobile Phone: (+aaa(bbb)ccccccc)

Password:*

Confirm Password:*

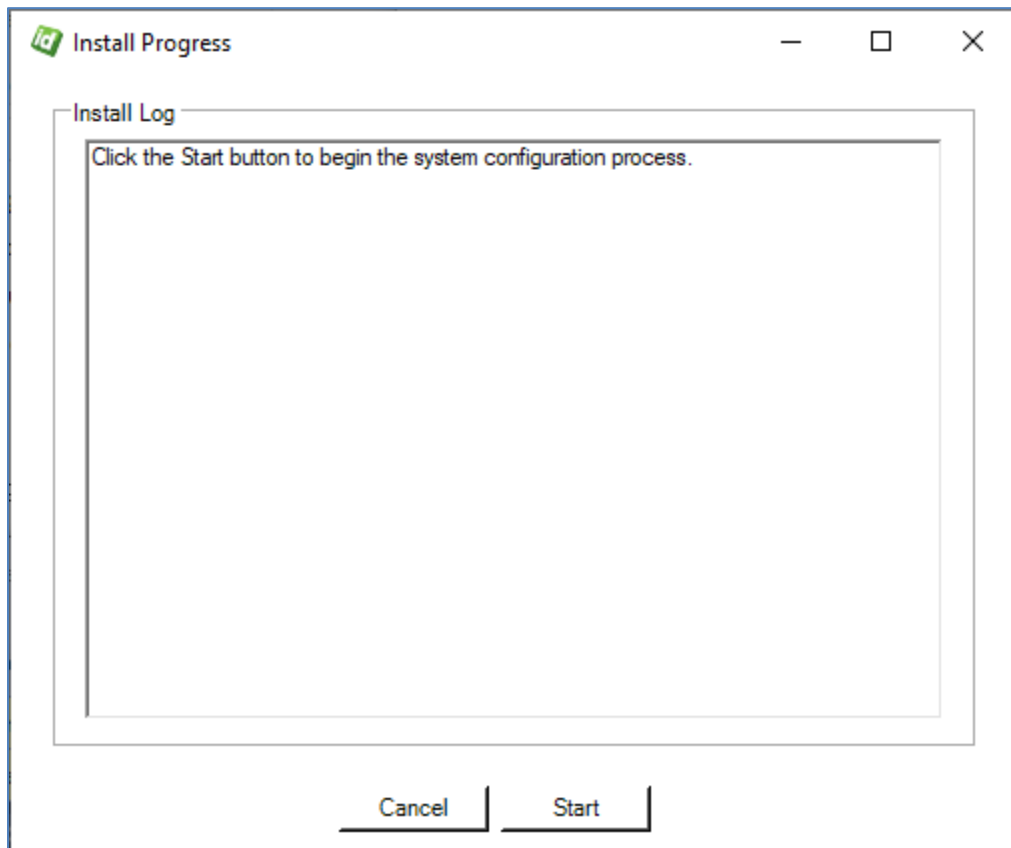
* Indicates required field

Back Next Finish Cancel

Step 3 – Define SurePassID Admin Account

This window allows you to set the user information for the SurePassID Administrator account. You will need to save the **Username** and **Password** to login to SurePassID later.

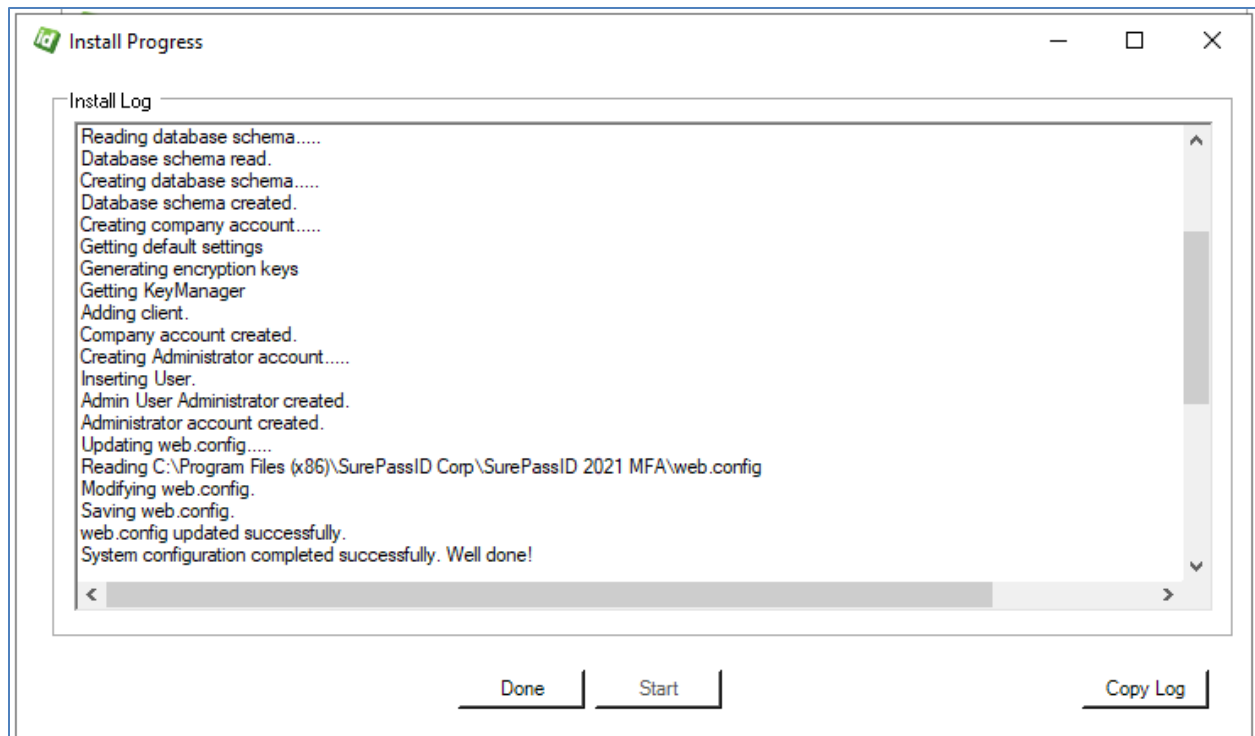
Press the **Finish** button to start the configuration process. You will see the following window.



Step 4 – Start Account Database Set-up

Press the **Start** button.

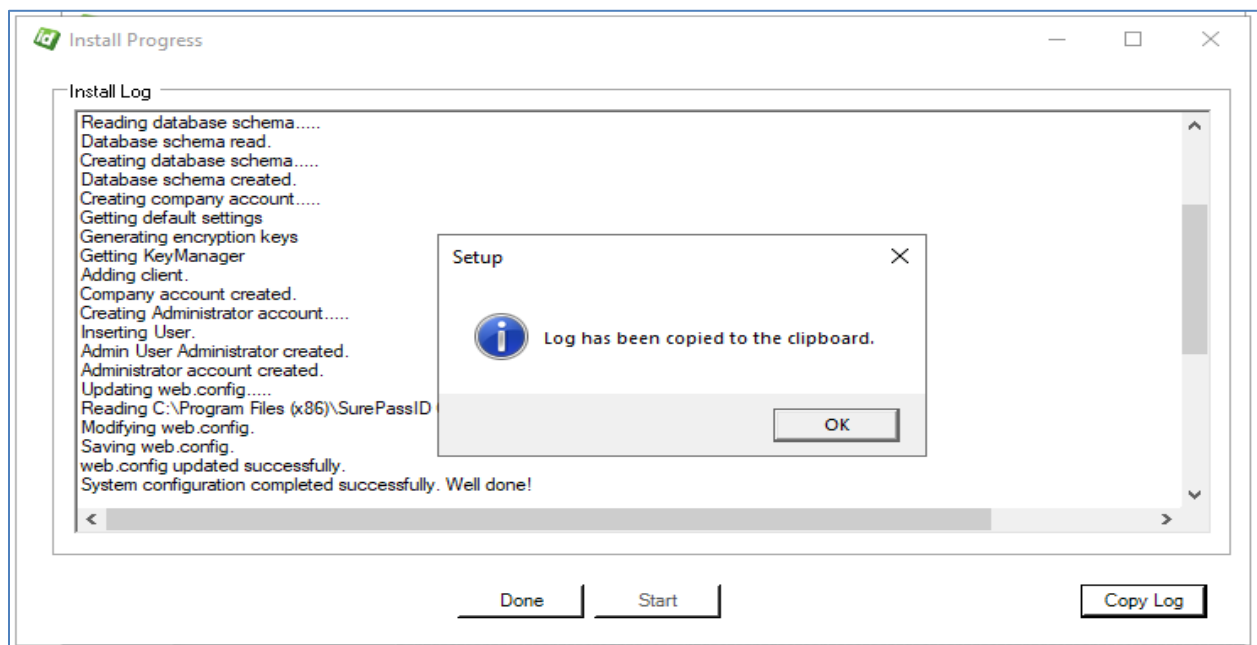
When the configuration process has completed you will be presented with an installation log and results as shown below.



Step 4 – Start Account Database Completed

You can the installation log using the **Copy Log** button. The **Copy Log** button allows the install log to be copied as text to the clipboard to more effectively troubleshoot any errors as well as save login info for future reference.

The log contains the initial system URL and username you have selected for the Administration account.

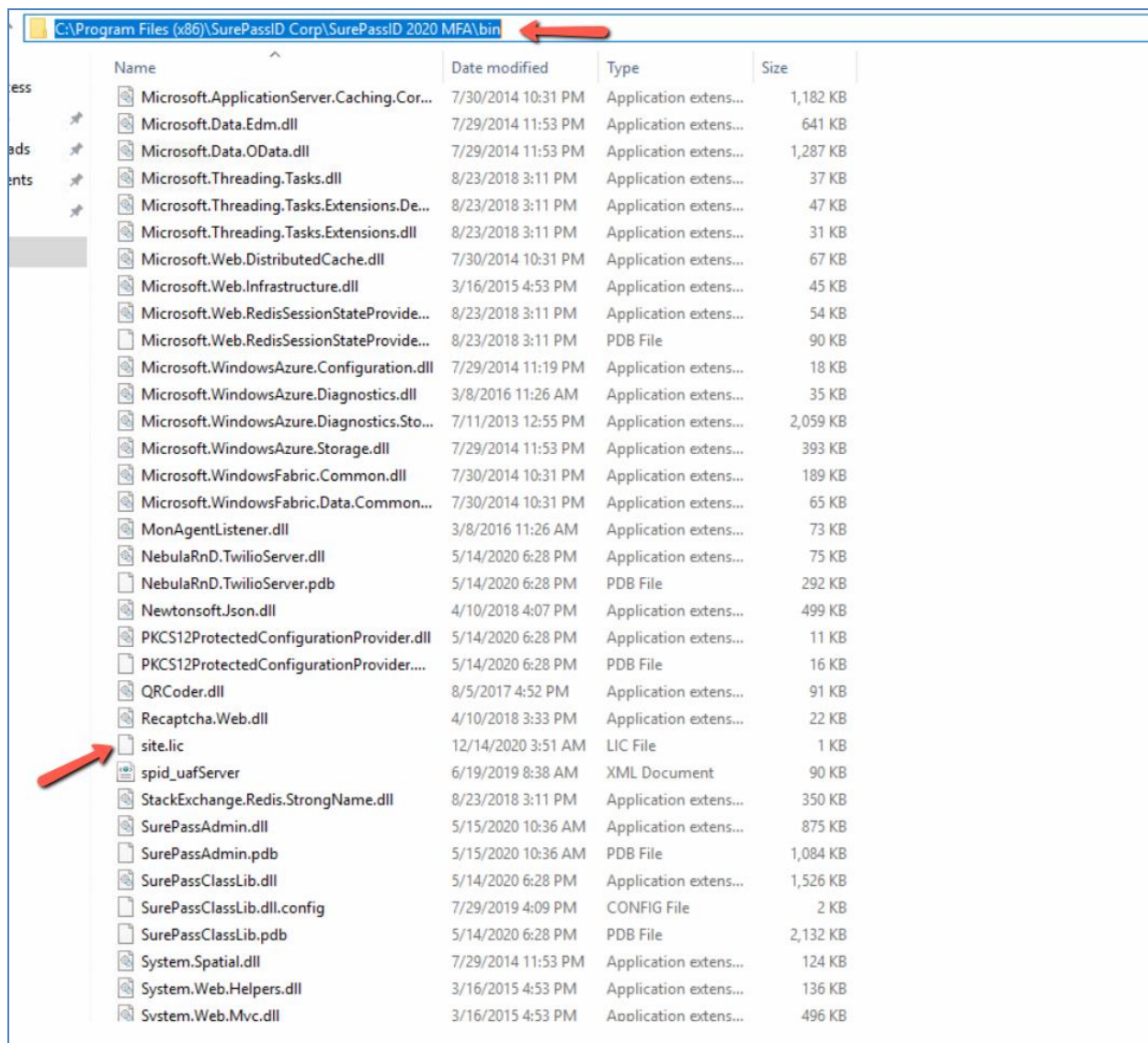


Step 5 – Copy Log Button

After the system is installed use **Explorer** to navigate to the following path:

C:\Program Files (x86)\SurePassID Corp\SurePassID 2020 MFA\bin

and replace the site.lic file with the license file you have been provided by SurePassID .



Name	Date modified	Type	Size
Microsoft.ApplicationServer.Caching.Cor...	7/30/2014 10:31 PM	Application extens...	1,182 KB
Microsoft.Data.Edm.dll	7/29/2014 11:53 PM	Application extens...	641 KB
Microsoft.Data.OData.dll	7/29/2014 11:53 PM	Application extens...	1,287 KB
Microsoft.Threading.Tasks.dll	8/23/2018 3:11 PM	Application extens...	37 KB
Microsoft.Threading.Tasks.Extensions.De...	8/23/2018 3:11 PM	Application extens...	47 KB
Microsoft.Threading.Tasks.Extensions.dll	8/23/2018 3:11 PM	Application extens...	31 KB
Microsoft.Web.DistributedCache.dll	7/30/2014 10:31 PM	Application extens...	67 KB
Microsoft.Web.Infrastructure.dll	3/16/2015 4:53 PM	Application extens...	45 KB
Microsoft.Web.RedisSessionStateProvide...	8/23/2018 3:11 PM	Application extens...	54 KB
Microsoft.Web.RedisSessionStateProvide...	8/23/2018 3:11 PM	PDB File	90 KB
Microsoft.WindowsAzure.Configuration.dll	7/29/2014 11:19 PM	Application extens...	18 KB
Microsoft.WindowsAzure.Diagnostics.dll	3/8/2016 11:26 AM	Application extens...	35 KB
Microsoft.WindowsAzure.Diagnostics.Sto...	7/11/2013 12:55 PM	Application extens...	2,059 KB
Microsoft.WindowsAzure.Storage.dll	7/29/2014 11:53 PM	Application extens...	393 KB
Microsoft.WindowsFabric.Common.dll	7/30/2014 10:31 PM	Application extens...	189 KB
Microsoft.WindowsFabric.Data.Common...	7/30/2014 10:31 PM	Application extens...	65 KB
MonAgentListener.dll	3/8/2016 11:26 AM	Application extens...	73 KB
NebulaRnD.TwilioServer.dll	5/14/2020 6:28 PM	Application extens...	75 KB
NebulaRnD.TwilioServer.pdb	5/14/2020 6:28 PM	PDB File	292 KB
Newtonsoft.Json.dll	4/10/2018 4:07 PM	Application extens...	499 KB
PKCS12ProtectedConfigurationProvider.dll	5/14/2020 6:28 PM	Application extens...	11 KB
PKCS12ProtectedConfigurationProvider....	5/14/2020 6:28 PM	PDB File	16 KB
QRCoder.dll	8/5/2017 4:52 PM	Application extens...	91 KB
Recaptcha.Web.dll	4/10/2018 3:33 PM	Application extens...	22 KB
site.lic	12/14/2020 3:51 AM	LIC File	1 KB
spid_uafServer	6/19/2019 8:38 AM	XML Document	90 KB
StackExchange.Redis.StrongName.dll	8/23/2018 3:11 PM	Application extens...	350 KB
SurePassAdmin.dll	5/15/2020 10:36 AM	Application extens...	875 KB
SurePassAdmin.pdb	5/15/2020 10:36 AM	PDB File	1,084 KB
SurePassClassLib.dll	5/14/2020 6:28 PM	Application extens...	1,526 KB
SurePassClassLib.dll.config	7/29/2019 4:09 PM	CONFIG File	2 KB
SurePassClassLib.pdb	5/14/2020 6:28 PM	PDB File	2,132 KB
System.Spatial.dll	7/29/2014 11:53 PM	Application extens...	124 KB
System.Web.Helpers.dll	3/16/2015 4:53 PM	Application extens...	136 KB
Systen.Web.Mvc.dll	3/16/2015 4:53 PM	Application extens...	496 KB

Add License File

Next navigate to the **C:\Windows\System32\drivers\etc** path and open (with the administrator option) the hosts file and add the following line in the file and save it.

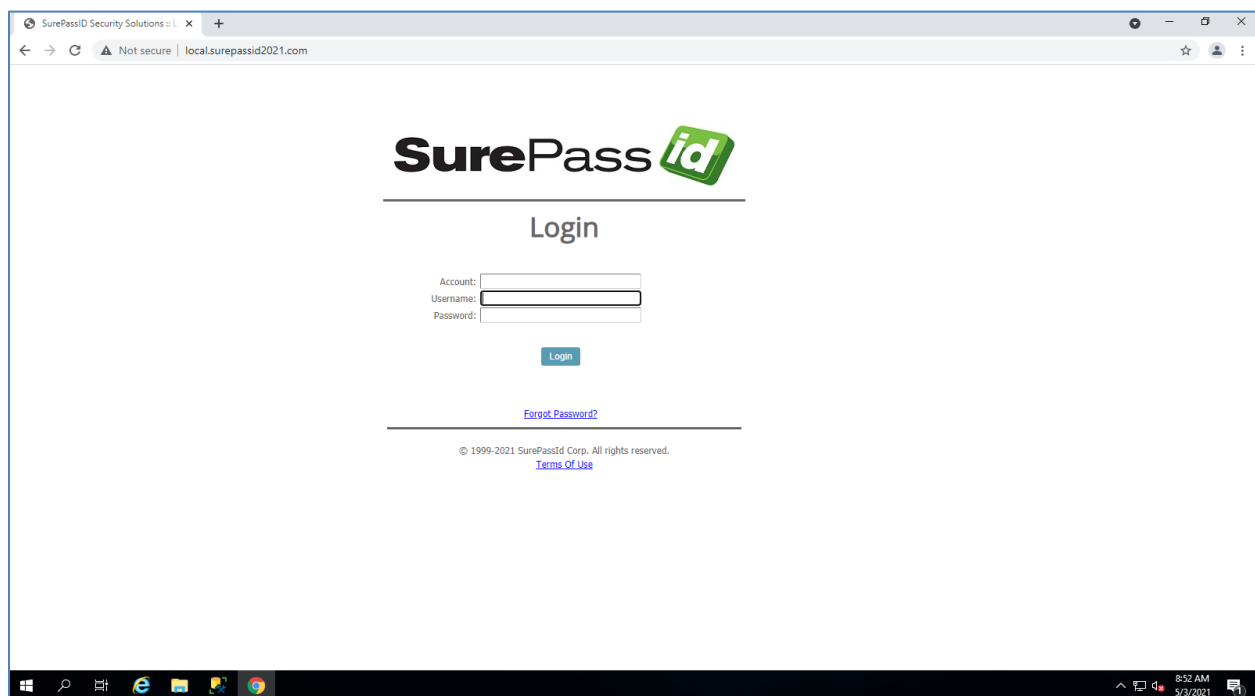
Local IP(127.0.0.1) and local.SurePassID 2021.com (domain name)

Note: Remove any leading # sign in the line.

```
# localhost name resolution is handled within DNS itself.  
#       127.0.0.1       localhost  
#       ::1             localhost  
127.0.0.1       local.surepassid2021.com
```

Edit Hosts file

To login to SurePassID , you can enter the following into a browser on the local machine `http://local.SurePassID 2021.com` and you will see the following window:



SurePassID Login Screen

Enter the **Domain**, **Username** and **Password** that you set as part of the **Configuration Wizard** setup and press the **Login** button to start using the system.

Customizing the System

When installation is completed, you will have a fully functioning authentication system. However, there are certain customizations that you will need to tailor the system to your company's requirements.

There are two types of customizations: global and local. Global customizations are changes that will be seen by every tenant in the system. Local customizations only effect a single tenant. Global customizations are made in the web.config file located in the root folder of the SurePassID installation. Local customizations are made by each tenant using the SurePassID Admin portal.

When SurePassID is installed the portal has multi-factor turned off. This is so that you can log in to the system and configure multi-factor methods for your users and yourself. Before going live you should turn on the multi-factor support. Multi-factor support can be turned on using the **System.IgnoreLogin2FactorAuth** setting in the web.config file as described in the next section.

Web.config

The web.config file is an XML file and is part of the .Net Framework. The file contains global customization settings. Some of the settings are SurePassID specific (**<configuration><appsettings>**) and you should change them to suite your needs. Other settings affect the way that asp .Net operates and you should not change these settings unless you have experience in this area. Some settings you can change and others you should not. If you make a change to web.config that violates the rules of xml syntax, the system will not run and you will receive an error. The table below describes the most notable SurePassID specific settings:

<configuration><appsettings> keys

Key	Description
Authorization.ServerURL	The URL of the Authentication Server
System.IgnoreLogin2FactorAuth	Security for the Admin portal: true = Only single factor required false = 2FA required
Support.ContactFromEmailName	The email name in all emails sent to/from support. E.g. Support
Support.ContactFromEmailAddress	The email name in all emails sent to/from support. E.g. support@company.com
Support.ContactPhone	The phone number that users can call for support.
Support.HelpWebSiteName	The website name for help/forums. E.g. Help Desk
Support.HelpWebSiteURL	The website URL link for help/forums. E.g. https://support.company.com

Support.HelpProductName	The name of the product. Used for white labeling the SurePassID platform. E.g. Johns MFA Server
Support.HelpCompanyName	The name of the company. Used for white labeling the SurePassID platform. E.g. Johns MFA Server
System.DefaultFromEmailAddress	The email name in all emails sent to/from support. E.g. Support
System.DefaultFromEmailName	The email name in all emails sent to/from support. E.g. support@company.com
Server.AppId	The Fido U2F appid for this server. Can be a Fido facet.
ActivateDeviceURL	Device Activation URL. Usually the URL of the Authentication Server/Activate.aspx
System.ActivateSPMobileURL	The SurePassID one tap authentication URL. Usually the URL of the Authentication Server/ oath-ota-provision
System.ExceedTokenUsesWarningOnly	When an OTP is authenticated by the server for an event based token that exceeds the maximum number of uses the OTP validation of the token fails and the condition is logged in the audit log. Setting this value to "true" will allow the authentication to continue and the condition will be logged as only as a warning.
Server.DefaultTokenExpirationIncrementDays	The default numbers of days before a token expires. Expiration is a logical condition that renders the token no longer usable after the number of days expire. This is meant for transient workers (consultants) that will work for some period of time and then no longer need access.
Server.DefaultTotpTokenDriftUnits	The default number of drift time units that are allowed for hard TOTP (time based) tokens.
System.AllowHttp	By default the server allows portal or API access using http for testing and initial setup. It is advisable to setup TLS (IIS certificate) for the server and setting this value to false. true = allow http false = require TLS (https)
System.AllowVpnPinReset	VPN Pin resets allows an administrator to reset a users account and when they log in they can authenticate with their mfa only and set their Pin. The length of the Pin is dictated by System.AllowVpnPinResetPinLength true = allow Vpn Pin reset false = do not allow Vpn Pin reset
System.AllowVpnPinResetPinLength	Length of Pin for Vpn reset.
System.DefaultSMSProvider	The default SMS/IVR call provider. Only Twilio is valid at this time.

System.DefaultSMSAccountId	Your Twilio Account id. You can get this from the Twilio account portal.
System.DefaultSMSAccountToken	Your Twilio Account token. You can get this from the Twilio account portal.
System.DefaultSMSAccountExtra	Your Twilio account phone number that all request will come from. You can get this from the Twilio account portal.

<configuration><system.net><mailSettings><smtp><network>

The system wide default SMTP server for all outbound emails. For multi-tenant environments, such as a Managed Services Provider or multi-divisional enterprise, each Tenant (admins only) can override these parameters using the SurePassID Admin portal.

Details are available at the following URL:

[https://msdn.microsoft.com/en-us/library/w355a94k\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/w355a94k(v=vs.110).aspx)

Default Language

The system ships with a compiled default language file that is based on US English culture (en-US). The system is Unicode based so it can support every possible language including double byte and right to left character sets.

The system will automatically change language to the culture of the user (which is usually set by the underlying operating system) if the appropriate culture (language file) exists for their culture. This has two important uses:

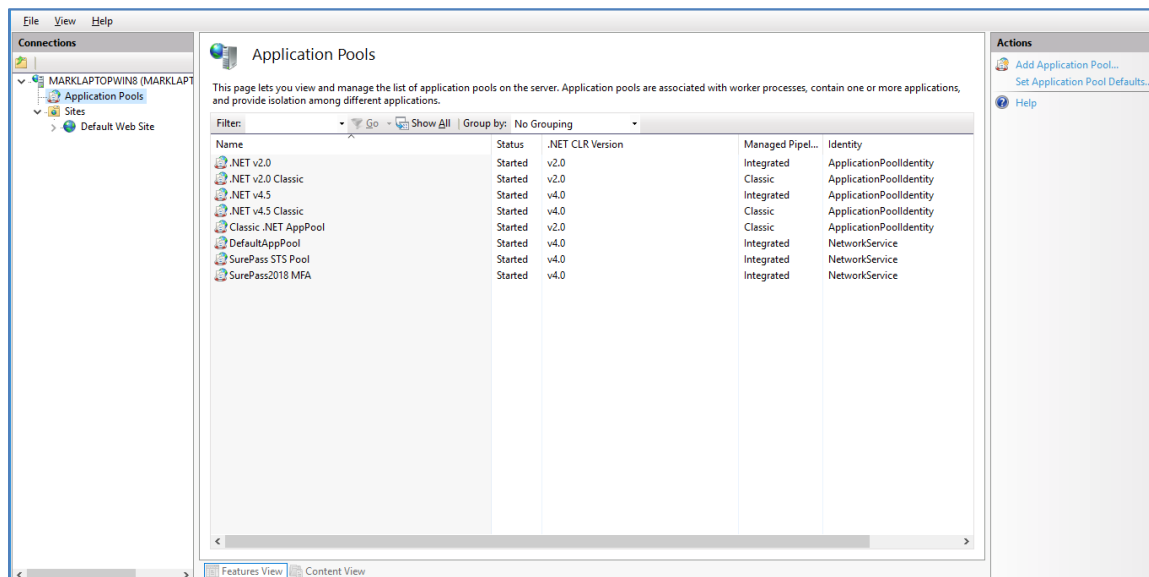
1. Provide a language centric experience to your users across cultural boundaries.
2. Change any constant field/message in the system.

If you would like to add an additional language or change the constants/messages in the existing system, please contact us. We will provide the tools to add your language. This typically takes less than one day.

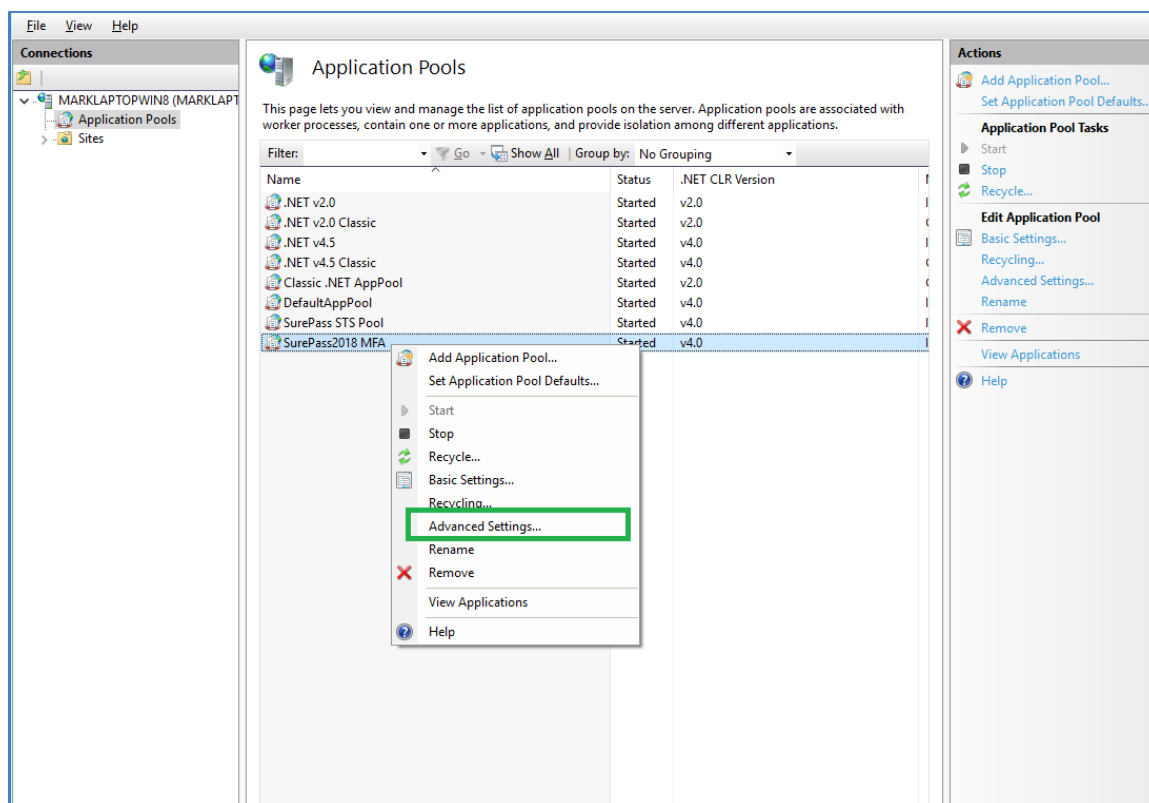
SurePassID Portal Session Timeout

The SurePassID portal ships with a default session timeout of 20 mins. The session timeout determines how long the user interface will be idle before the administrator must re-login. To increase or decrease session time follow the following instructions:

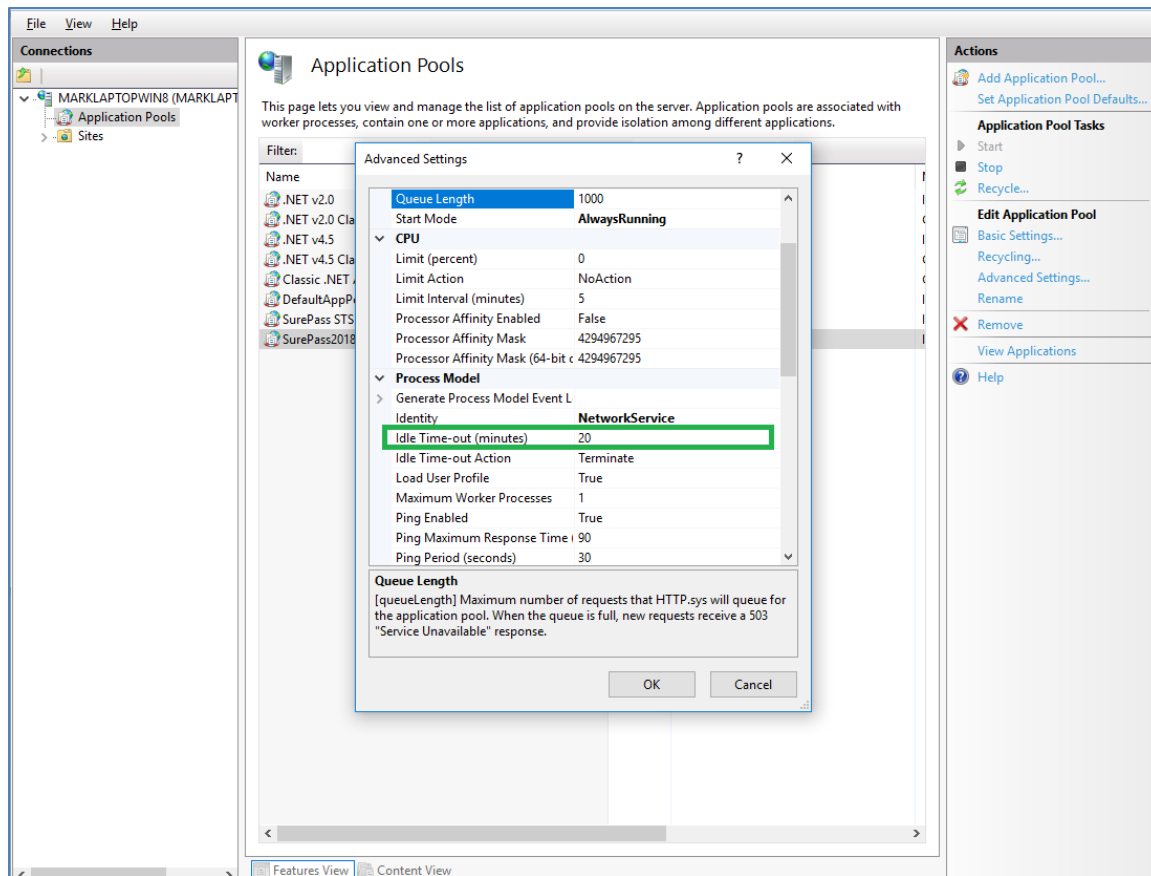
Start Internet Information Services (IIS) on the web server that SurePassID is installed on and right click **Application Pools** in the tree.



Right click on **SurePass2021MFA** and select Advanced Settings.



Right click on **SurePass2021MFA** and select Advanced Settings.



Locate the **Idle Time-out (minutes)** option and change the default time-out value from 20 to the desired number of idle-minutes can pass before the user must login again and click OK.

High Availability Considerations and Capabilities

The MFA server was designed from the very beginning as a highly available and highly scalable product. In fact, the MFA server was the first MFA server to be deployed on Windows Azure in 2014.

To that end the MFA server supports the following scalability and high availability capabilities.

Load Balancing

Load balancers make it possible to quickly and easily scale applications and create high availability services. Load balancer distributes new inbound transactions that arrive at the load balancer's endpoint and distributes the transaction application instances, according to specified rules and health probes.

Load balancing only works with applications that are designed for it. The MFA server was designed to be load balanced and offers these features and characteristics:

- Each authentication request to the MFA server is atomic; there is no session state. This allows an unlimited number of MFA Server instances to run behind one or many load balancers and provides the load balancer the best options for request distribution.
- One or more load balancers can be set up in a single data center servicing multiple MFA server instances.
- Load balancers can also be geographically located to the user's request location for performance.
- An SurePassID MFA server can support any number of load balancing algorithms such as round robin, least active (connections), and geographic to name just a few.
- Virtualization allows MFA servers to be dynamically created and torn down based on system load using products such as VMWare or Hyper-V.
- SurePassID works with load balancers such as F5 BIGIP, Azure Traffic Manager and AWS load balancer.
- Each MFA server provides health check endpoints that can be queried by the load balancer for the current health state of the instance. This allows the load balancer to make intelligent choices for request routing maximizing your resources and providing 99.999 up time and sub-second response time.

Data Management High Availability

The MFA server supports all versions of Microsoft SQL Server editions:

- Enterprise
- Standard
- Web
- Express

The MFA server is designed to leverage all of the high availability capabilities that are available in each edition.

A comprehensive list of high availability capabilities for each SQL Server edition can be found here:

<https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-version-15?view=sql-server-ver15>

For small systems that require high availability we recommend SQL Server Standard. For very large enterprise we recommend SQL Server Enterprise. Both of these edition have dozens of high availability options but most notable are Always On Failover Clustering and many In-memory cache options that are essential for highly available systems.

Always On Failover Clustering provides application and business continuity when a SQL Server instance experiences a hardware or software failure. Always On Failover Clustering provides an environment where there is no noticeable impact to applications and users. If applications are designed poorly, even Always On Failover Clustering might require operator intervention and an application restart negatively impacting your users. If applications are implemented properly the application will automatically reconnect without manual intervention by your IT staff and virtually no downtime to your users.

The MFA server is designed properly and will automatically reconnect to new server cluster when an existing server fails. No manual intervention is required by your IT staff and virtually no downtime to your users.

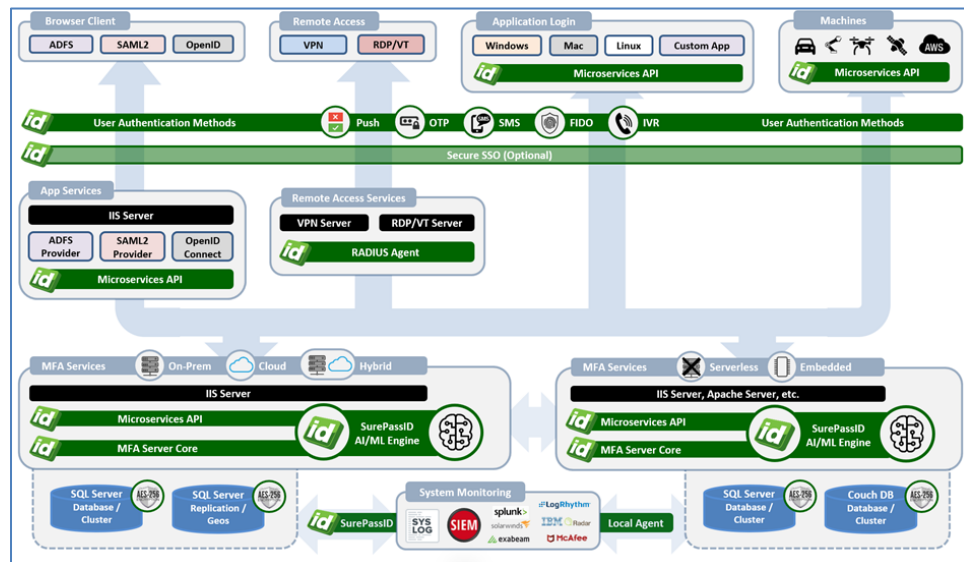
Single/Multiple Datacenter Architecture

Most every IT infrastructure configuration is different, but they all have similar requirements.

Below is a single data center diagram of the overall MFA server architecture based on common IT requirements. It is meant to show the flexibility and a common deployment

architecture for a single data center. However, there are a large number of MFA server configurations possible based on your requirements and constraints. Our technical experts can work with you to design an MFA server configuration that meets your needs.

In addition, this single data center model can be cloned to other data centers that are geographically separate to create a high performance global authentication and identity management platform.



High Availability Architecture

SurePassID Product Family

There are over 15 products in the SurePassID authentication suite. All of our server-based products are designed for high availability and scalability. The short list of products are:

- SurePassID Radius Server (Windows Platforms)
- SurePassID FreeRADIUS (any platform)
- SurePassID Reverse Proxy
- SurePassID OpenID Connect Server
- SurePassID SAML2 IdP
- SurePassID ADFS Adapter
- SurePassID Event Log Sync - Windows Event Log, Splunk, syslog, etc.
- SurePassID User Sync - Sync user information from external directories such as LDAP and Active Directory
- SurePassID MFA Server API