SurePassID Authentication Server Install Guide for Windows Servers

SurePassID Authentication Service 23.1

Table of Contents

SurePassID, Corp.
360 Central Avenue
First Central Tower
Suite 800
St. Petersburg, FL 33701
USA
+1 (888) 200-8144
www.surepassid.com

Table of Figures

About this Guide

This guide explains how install and configure the SurePassID Authentication 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 Universal Server?**
  - A brief introduction to the SurePassID Authentication Server for Windows Servers.
- **Installing and Configuring SurePassID Authentication Server**
  - Detailed explanations for installing the SurePassID Authentication 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 Universal Server:

- 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 Authentication Server?

The SurePassID Authentication 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 (Amazon Web Services).

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 provided default license file is for a single tenant-only system to reduce the amount of configuration required for small or single company installation. If you are a large company or 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 oversite, eliminate disparate authentication systems, consolidate support activities, and create recurring revenue streams.

Prerequisites

SurePassID Authentication Server can be installed on the following Windows versions:

- **Windows 2016** – All versions
- **Windows 2019** – All versions
- **Windows 2022** – All versions
- **Windows 10, 11**
- **Windows 10**
- **SQL Server 2016, 2017, 2019, 2022** – Any version

Deployment Environments

In addition to being installed on your on-premises system, the Authentication Server can also be installed on public and private clouds like AWS GovCloud or Azure, Azure GCC and Azure GCC High. The Authentication Server can also be installed as an Azure App Service.

General Security Considerations

Although the SurePassID Authentication Server can be installed inside the behind the corporate firewall, outside the firewall or in the DMZ, the system should **never** be installed in the DMZ or outside your internal corporate firewall. In most situations the only external network access that might be required of the Authentication Server is from mobile phones (SurePassID Authenticator initial provisioning soft tokens or for push authentication from public networks).

To support mobile phones, an application gateway (and optional Web Application Firewall) and/or reverse proxy should always be the external endpoint for mobile phone requests. Those products can use HTTP tunnelling and other methods to eventually get the request/response from the Universal Server. We strongly suggest you consult your network and security engineers to use best practice methods for setting this up.

Although SurePassID Authentication Server is a software product it can be installed and operated in the DMZ or outside the corporate firewall. **It is very strongly recommended that it is installed behind your corporate firewall** for security reasons. Your network engineer can help with this.

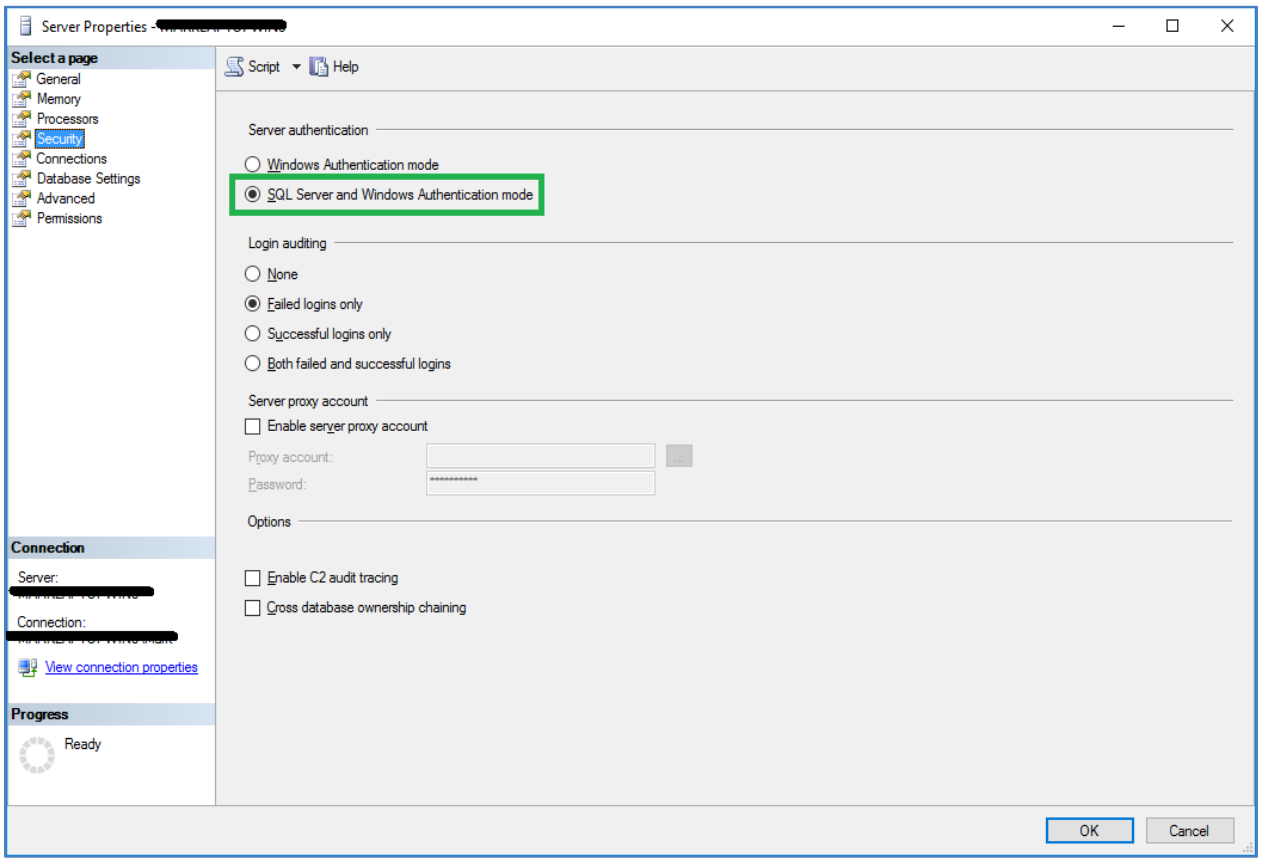
Database

SurePassID Authentication Server requires a SQL Server database. You can use any SQL Server 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), you should enable SQL Server authentication and Windows authentication for the initial installation. After you are up and running you can always disable SQL Server Authentication later.

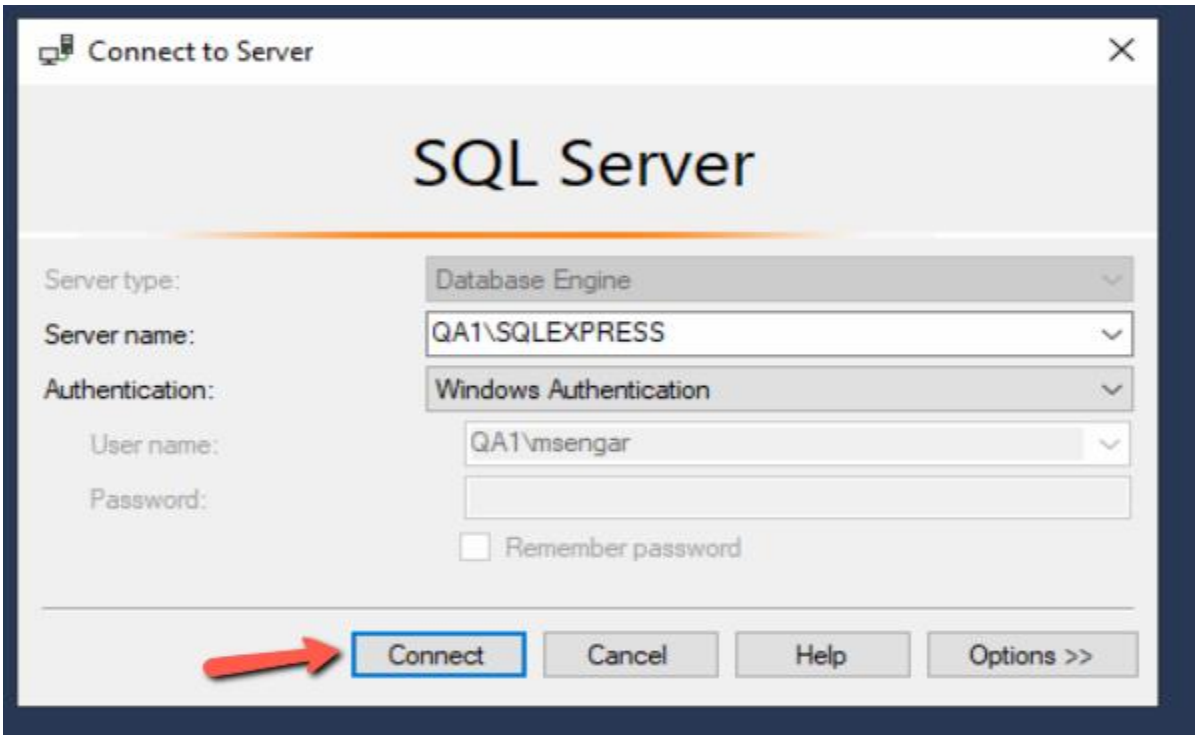
Start SQL Server Management Studio, right click on the server, select **Properties** menu. The following form will be displayed. Verify the security setting as shown below:



SQL Server Authentication Settings

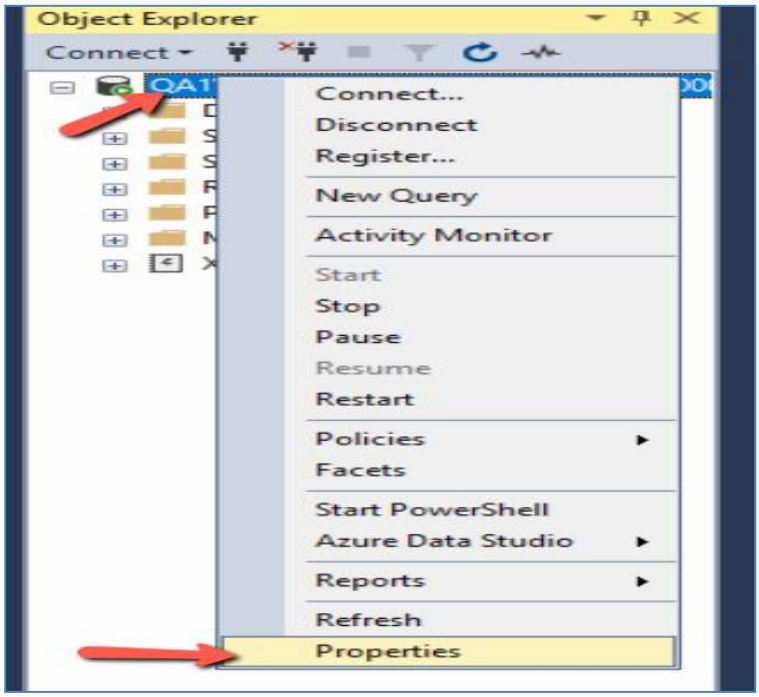
If **Windows Authentication mode** is selected, follow the steps below to enable SQL Server and Windows Authentication mode**.**

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



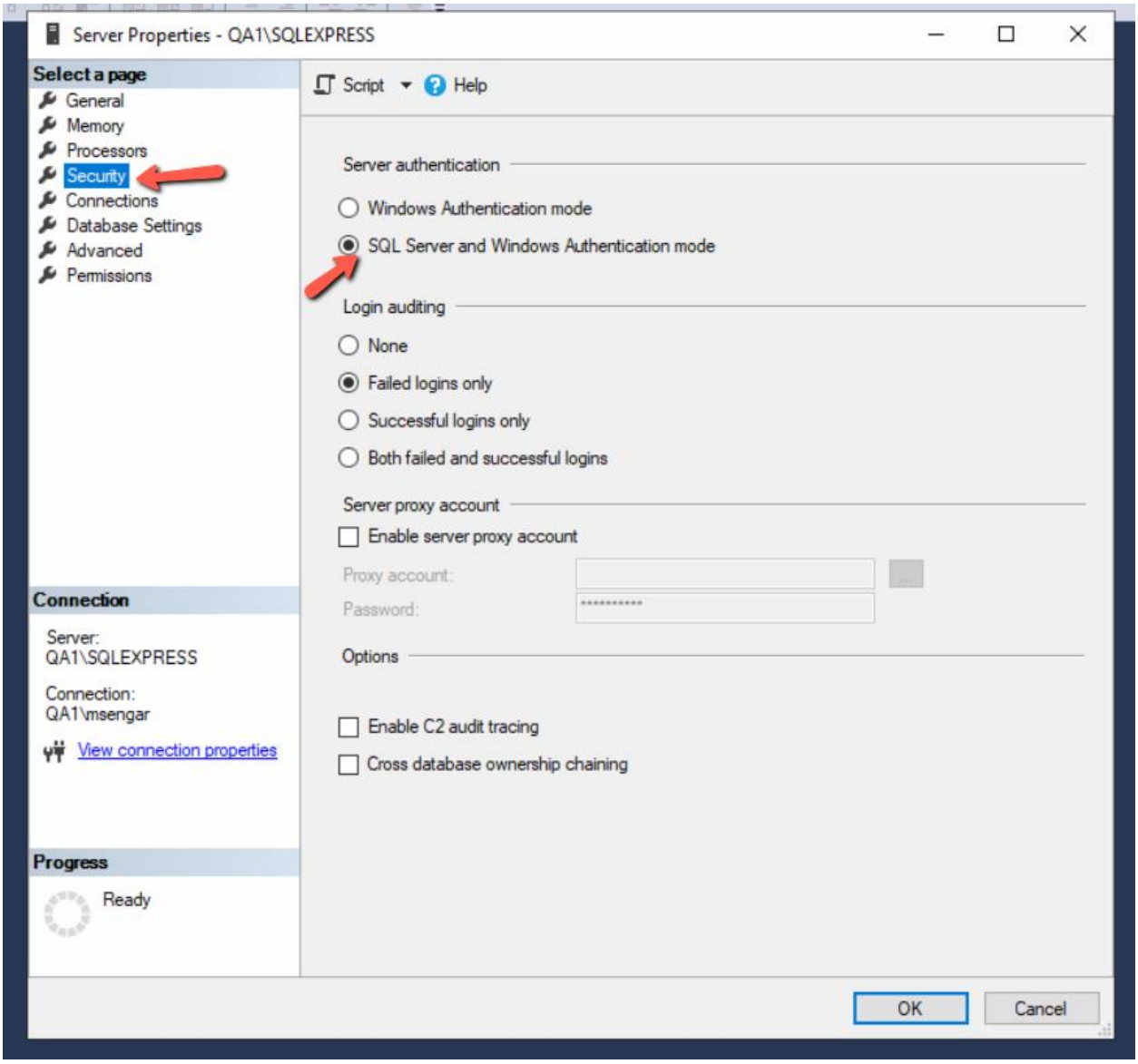
Connect to SQL Server

Right click on the SQL Server and select Properties.

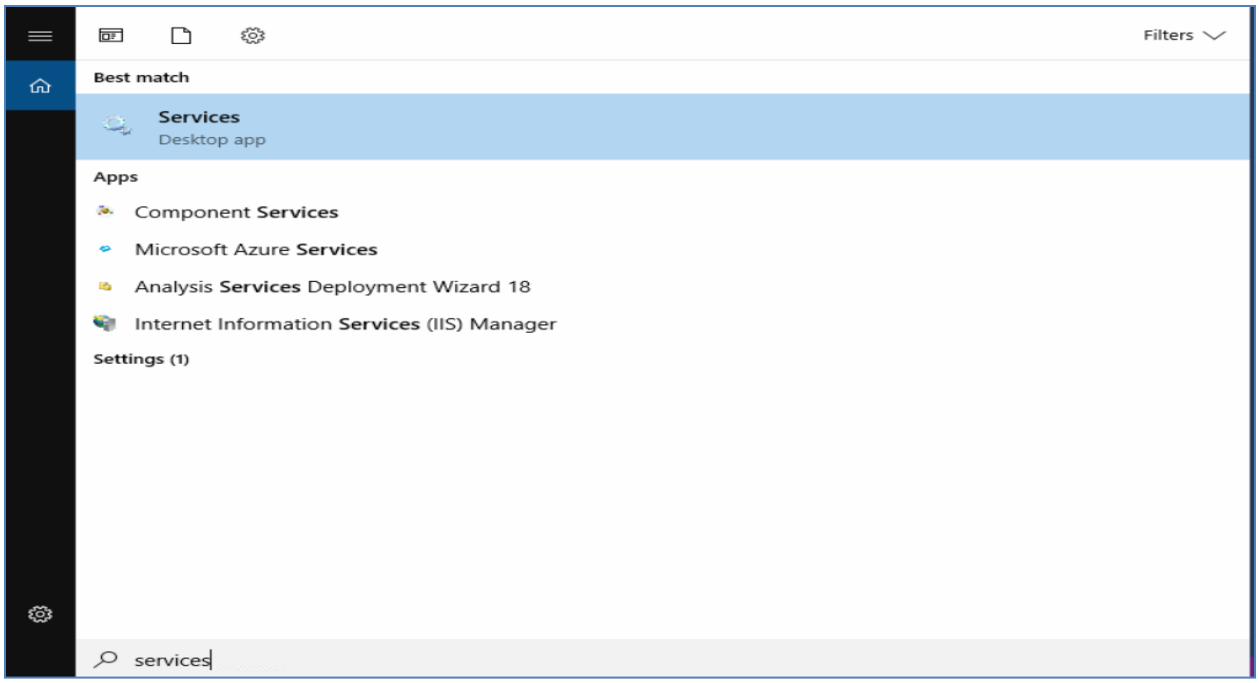


SQL Server Properties

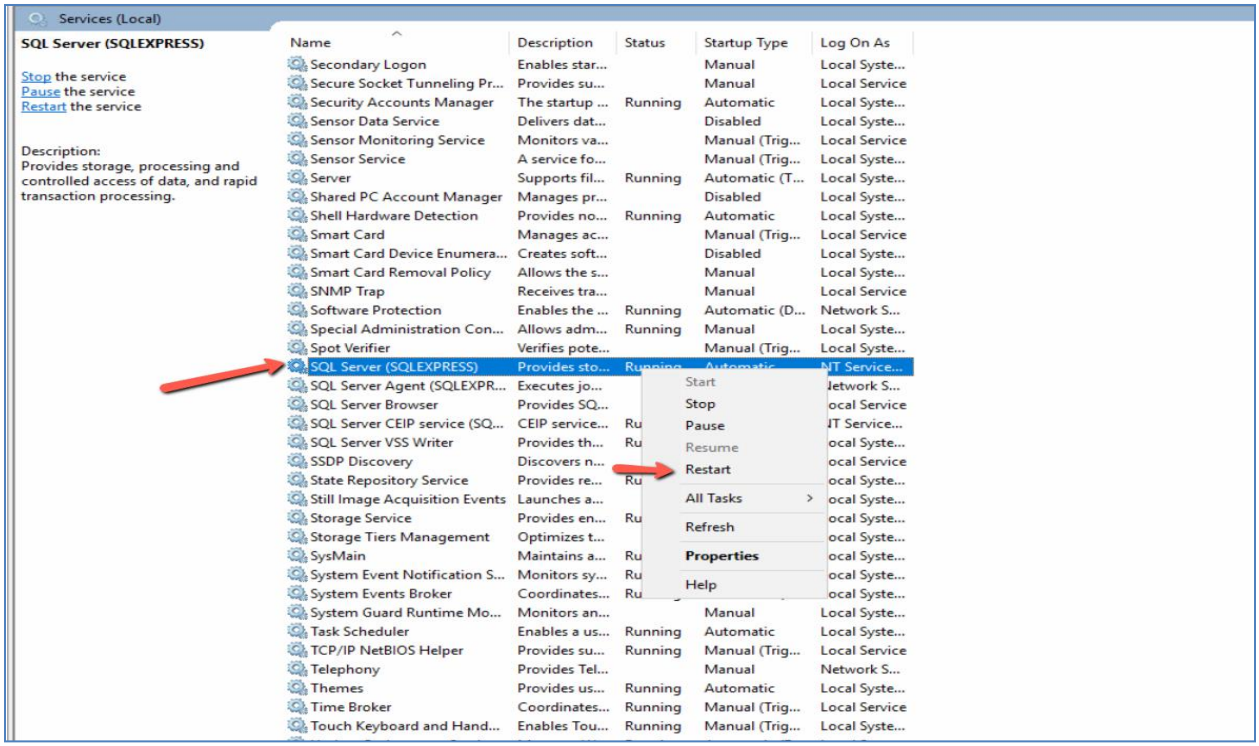
Select **Security** and then Select **SQL Server and Windows Authentication mode**



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.

SMTP

The SurePassID Authentication Server supports the use of email for many things such as password recovery, password change notifications, production user rollout/set-up notifications, etc. If you use these features, you will need an SMTP account. Your system administrator can help with this.

SMS

The SurePassID Authentication Server supports the use of SMS for many things such as password recovery, password change notifications, SMS push notifications, IVR push notifications, production user rollout/set-up notifications, etc. The system supports Twilio as an SMS provider. You can register for a free Twilio account here.

.NET Framework

The SurePassID Authentication Server uses Microsoft .NET Framework 4.8 and must be installed on your server. More info and downloads can be found here.

The .NET Core Hosting Bundle

The SurePassID Authentication Server uses Microsoft .NET Core and must be installed on your server. More info and downloads can be found here.

Transport Level Security (TLS)

SurePassID Authentication Server for Windows Servers by default does not install with any trusted certificates for SSL (Secure Socket Layers). It is recommended that you configure the SurePassID Authentication Server (IIS web app) TLS bindings. Your system admins shoud be able to provide you with trusted certs that can be used to bind TLS to SurePassID Universal server.

Since procuring these certs can take a while, the SurePassID Authentication Server ships with a PowerShell script **create_selfsigned_iis_certs.ps1** (located in the Tools folder) that can create the certs for the system, place them in the Personal (My) certificate store of the Local Machine, and in the in the Trusted Roots certificate store allowing the system to operate with TLS. The PowerShell script must be run **as Administrator** and creates the following two certs:

- SurePassID MfaServer Server Cert for local.surepassid2023.com

- SurePassID Fido2 Server Cert for local.surepassidfido2023.com

If you will be using the SAMl2 IdP, there is an additional script in the Tools folder (create_saml2_selfsigned_iis_cert.ps) to create the SAML2 IdP certificate for local.saml2.surepassid2023.com.

This should be considered a temporary solution for setting up the system and testing until you procure your own certs signed with a trusted Certificate Authority (CA).

SurePassID Authentication Server and additional components currently support TLS 1.2 and TLS 1.3. If you are uncertain what TLS version your windows server supports, contact your system administrator to make sure you support either of these TLS versions.

Internet Information Server

The Windows server must have the IIS feature enabled using the Windows Server Manager. If you send emails using the IIS virtual SMTP server (not recommended), you must ensure that feature is installed too.

After installation, the Authentication Server will install two IIS sites:

- local.surepassid2023.com – The main Authentication Server portal and system.
- local.surepassidfido2023.com – The Fido2 passwordless (webauthn) server.
- Local.saml2.surepassid2023.com – The SAML2 IdP for on-premesis application. By default this IIS site is stopped. If you plan to use the SAML2 IdP you should start the service. If you have not intention of using the SAMl2 Idp, you can delete the site from IIS.

All IIS sites will be configured, but it will be up to you to bind certificates to port 443 after the system (see Transport Level Security section prior) has been installed as post installation configuration step that will be discussed in the next section.

Internal DNS Considerations

Authentication Server applications such as the RADIUS Server, Windows Login Manager, SIEM (Security Information Event Management), etc. to request services the Authentication Server you need to configure DNS on your internal network. This can be done by adding:

- One DNS (A) record for local.surepassid2023.com that points to the Authentication Server IP.
- One DNS (A) record for local.surepassidfido2023.com that points to the Authentication Server IP.
- OPtionally, one DNS (A) record for local.saml2.surepassidfido2023.com that points to the SAml2 IdP.

Another option (not a great one) is to update the **hosts** file on the Authentication Server windows server specifying the IP of the Authentication Server and the host name.

To do this edit host file in **C:\Windows\System32\drivers\etc** path and open (you will need administrator privileges to save it), add the highlighted (in green) lines below changing 192.168.1.174 to your server IP, and save it.

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host
# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost

192.168.1.174 pa1.spass.mysurepassid.com
192.168.1.174 local.surepassid2023.com
192.168.1.174 local.surepassidfido2023.com
192.168.1.174 local.surepassid2022.saml2idp.com
```

Edit Hosts file

The downsize approach to this method is that the hosts file will need to be updated on any server that has a SurePassID application like the RADIUS Server.

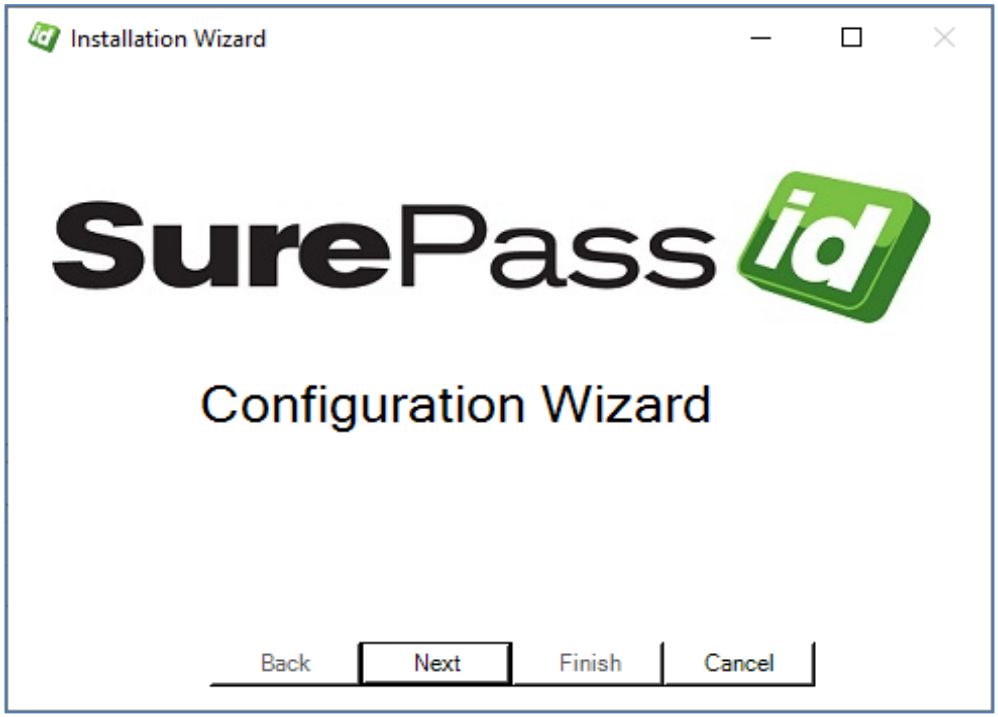
Software Installation

The SurePassID Authentication 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.

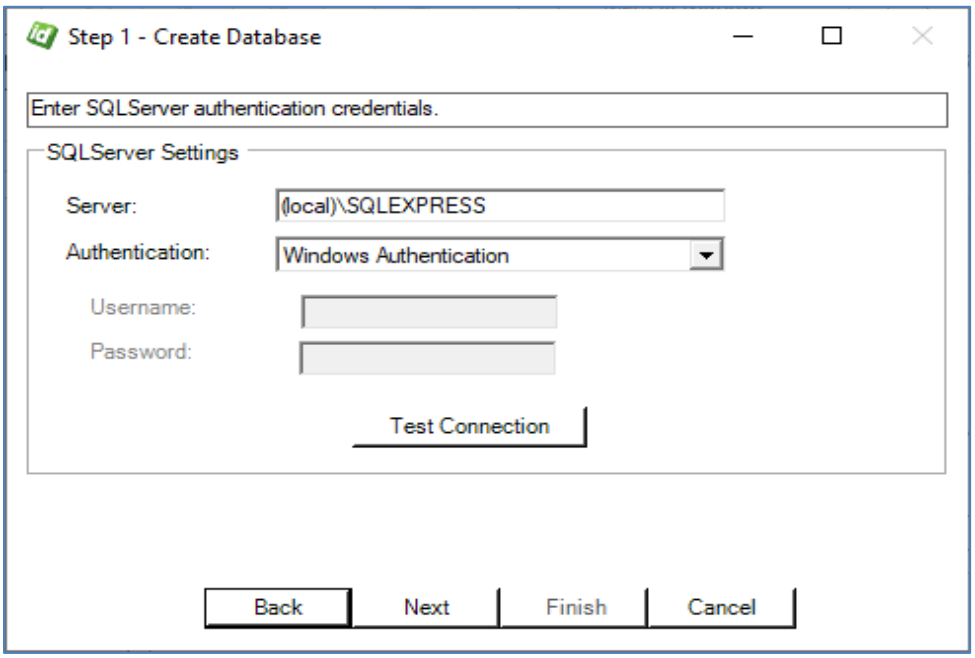
1. Creates the SurePassID SQL Server database.
2. Creates the SurePassID database schema.
3. Creates all the strong AES256 encryption keys to keep sensitive data in the database secret.
4. Create the SurePassID Administrator account so you can log into the system after configuration is complete.
5. Set 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:

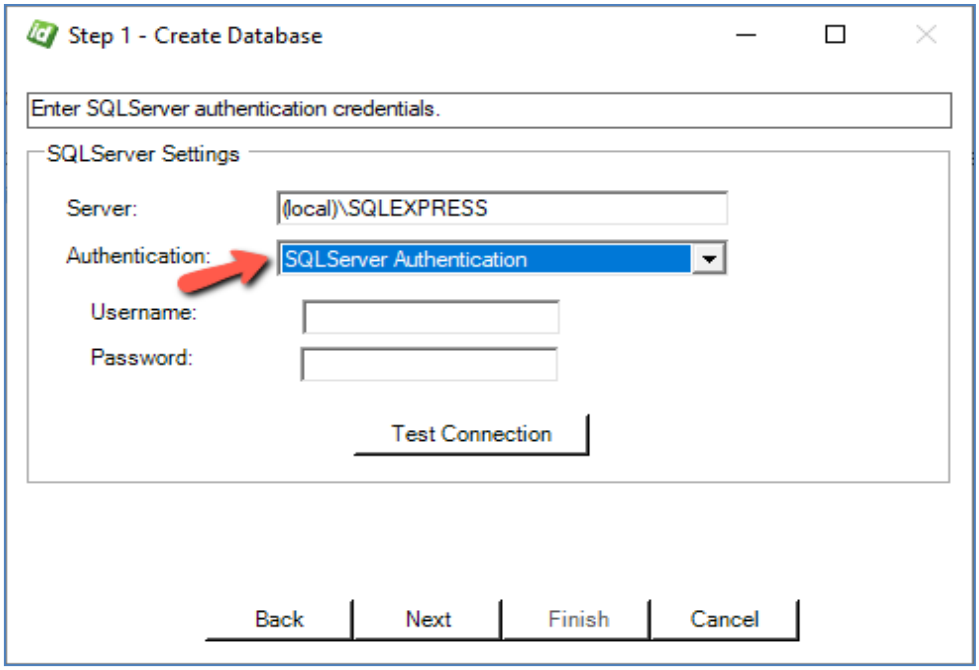


Start Configuration Wizard

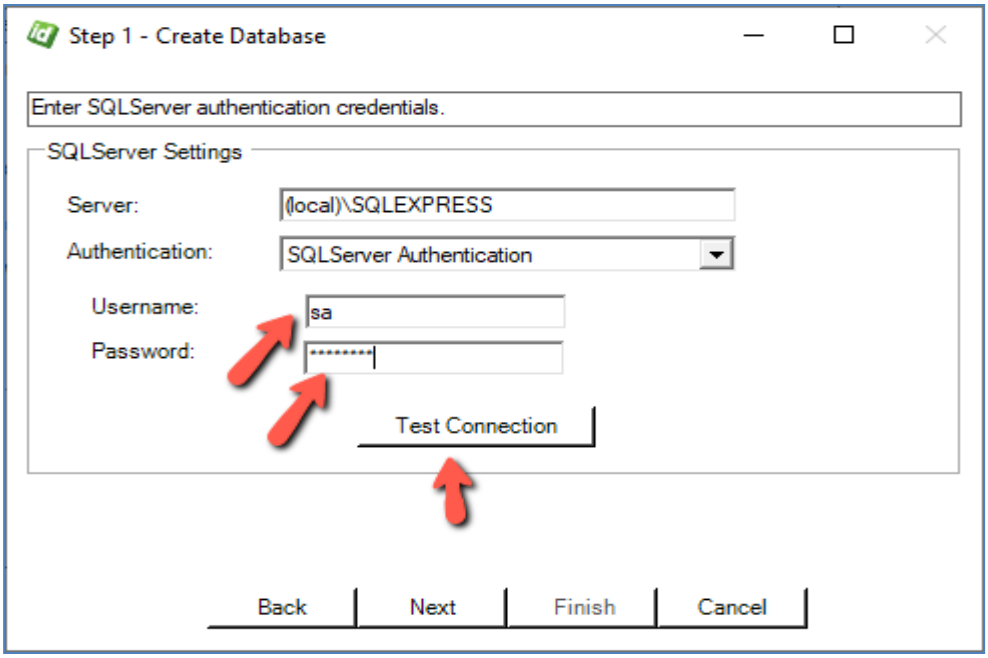
Click the ***Next*** button to test connectivity to the database.
You can use Windows Authentication or SQL server authentication for testing connectivity and the install. However, by default SQL Server Authentication must be enabled to start the SurePassID Administration portal.



Step 1 - Test Windows Authentication



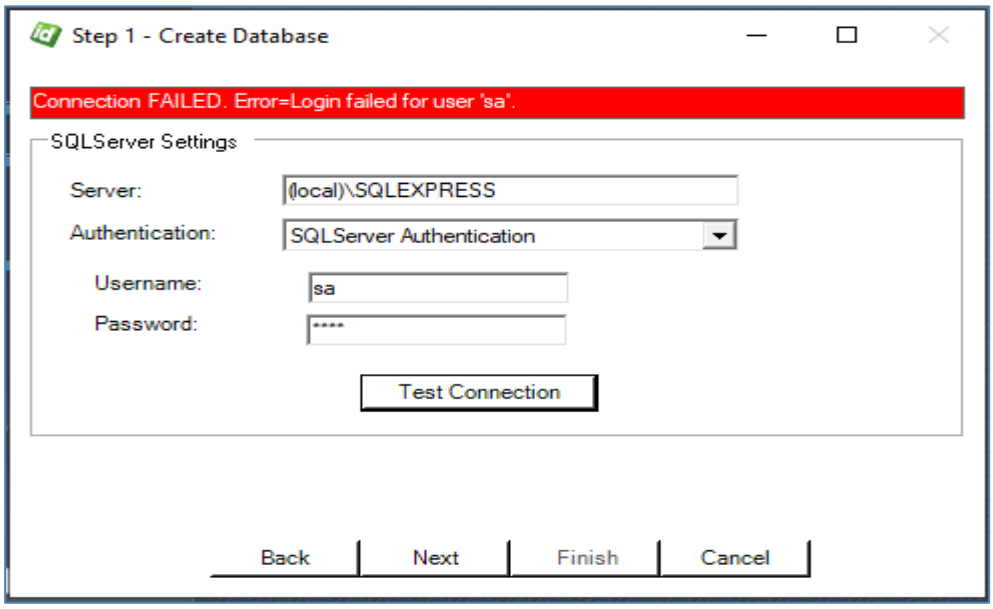
Step 1 - Test SQL Server Authentication



Step 1 – Test Connection

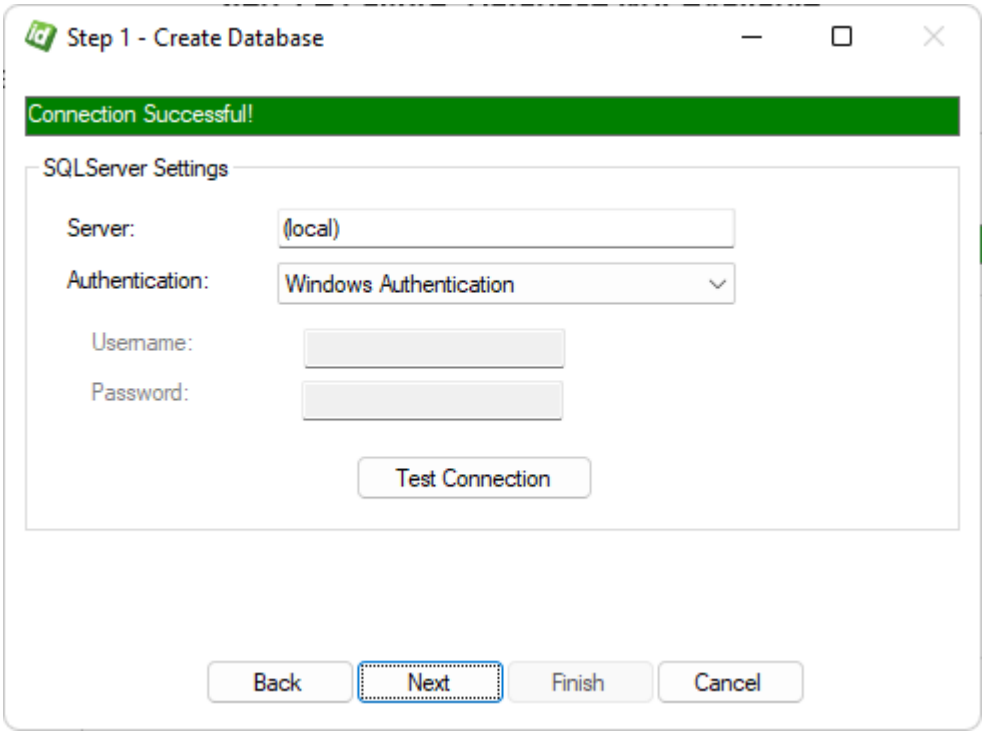
If you have the connection details for your SQL Server database, you can enter them now. If you are not sure you can accept all of the defaults and click the **Test Connection** button.

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.



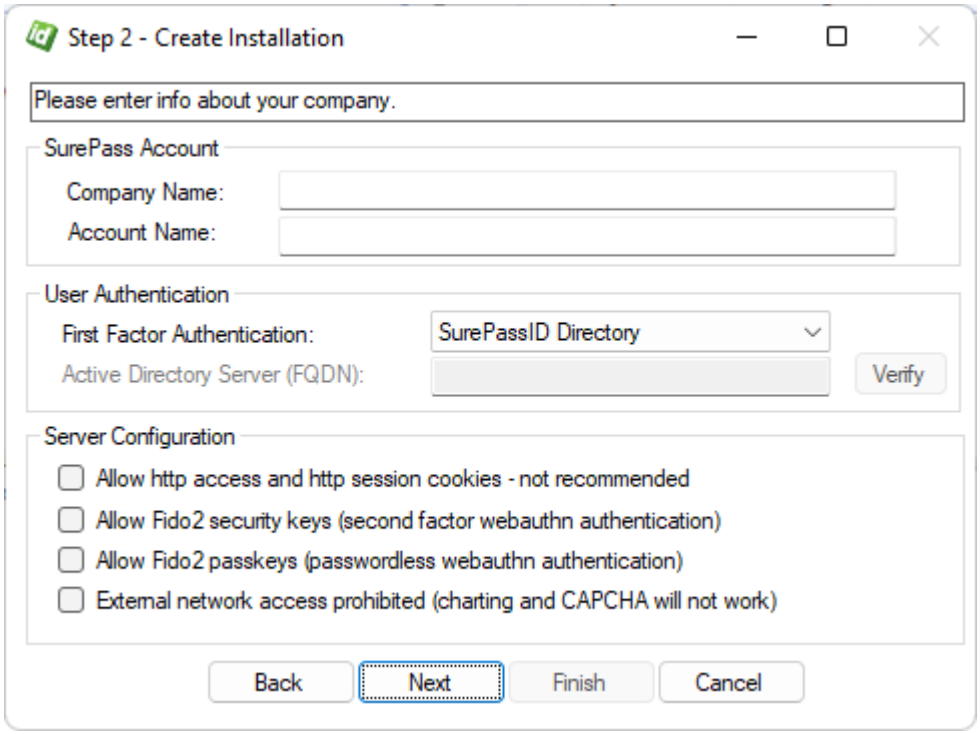
Step 1 – Failure: Database Not Available

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



Step 1 – Success: Database Is Available

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



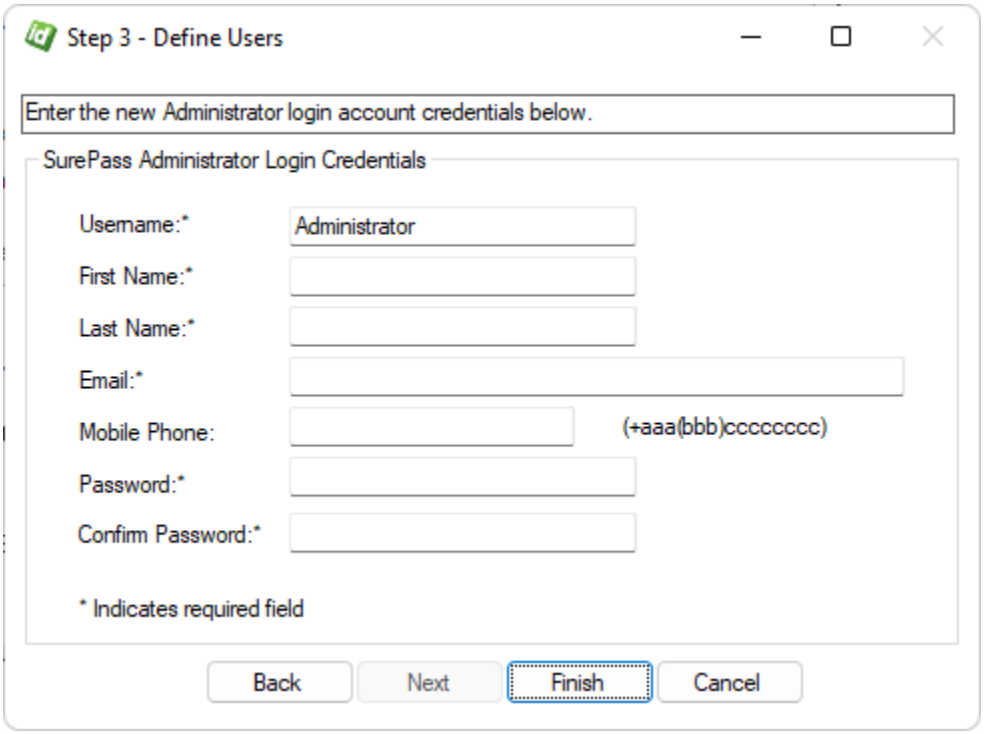
Step 2 – Create Installation

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 is appropriate. You can change this later, but you will need it for initial login to the system.
- **First Factor Authentication** – SurePassID authenticates users via username 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 **Factor Authentication,** then you will need to enter the Active Directory Domain Controller fully qualified domain name or IP address.
- **Verify Button** – Click this button to verify connectivity to Active Directory.
- **Allow http access and http session cookies - not recommended* –** Only use this if instructed by technical support. Checking this option opens your system to compromise.
- **Allow Fido2 security keys (second factor webauthn authentication) *** – Check this is you want to allow your Fido2 (or other webauthn compliant tokens) to be permitted for second factor authentication.
- **Allow Fido2 passkeys (passwordless webauthn authentication)*** - Check this is you want to allow your Fido2 (or other webauthn compliant tokens) to be permitted for passwordless authentication.
- **External network access prohibited (charting and CAPCHA will not work) *** - Check this if you are using the system in an environment where no Internet access is available such as

*These options can be changed after installation if required.

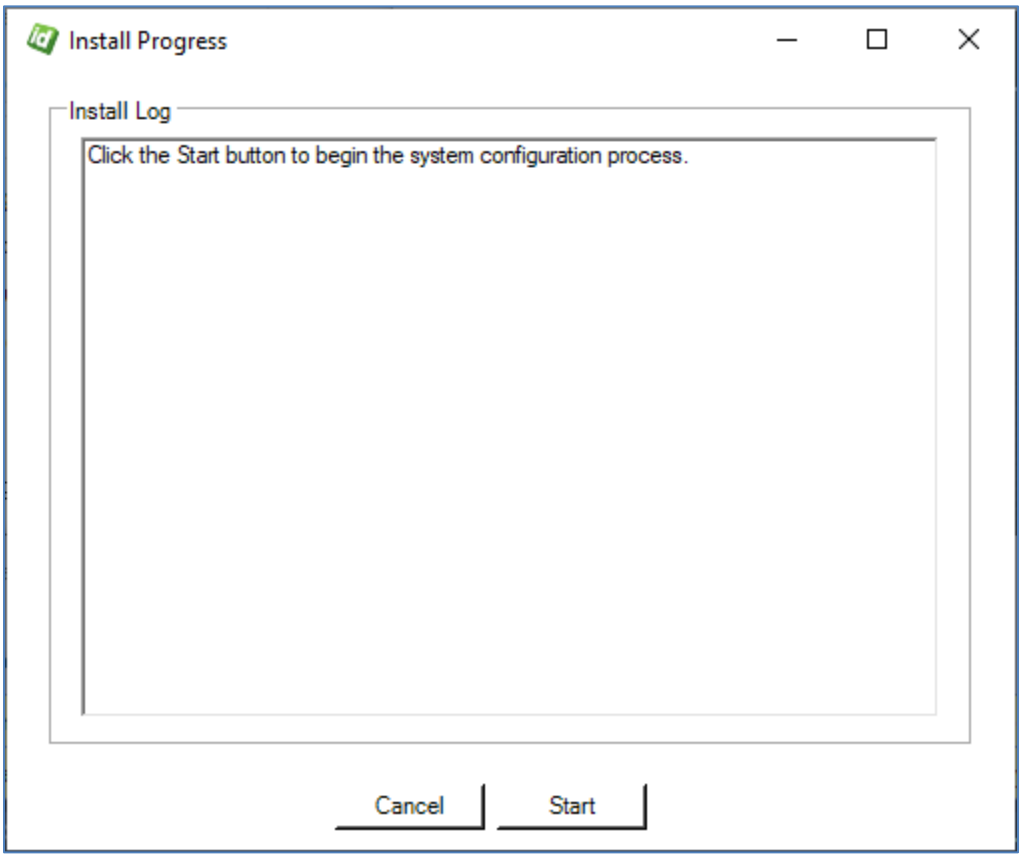
Press the ***Next*** button. You will see the following window.



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.

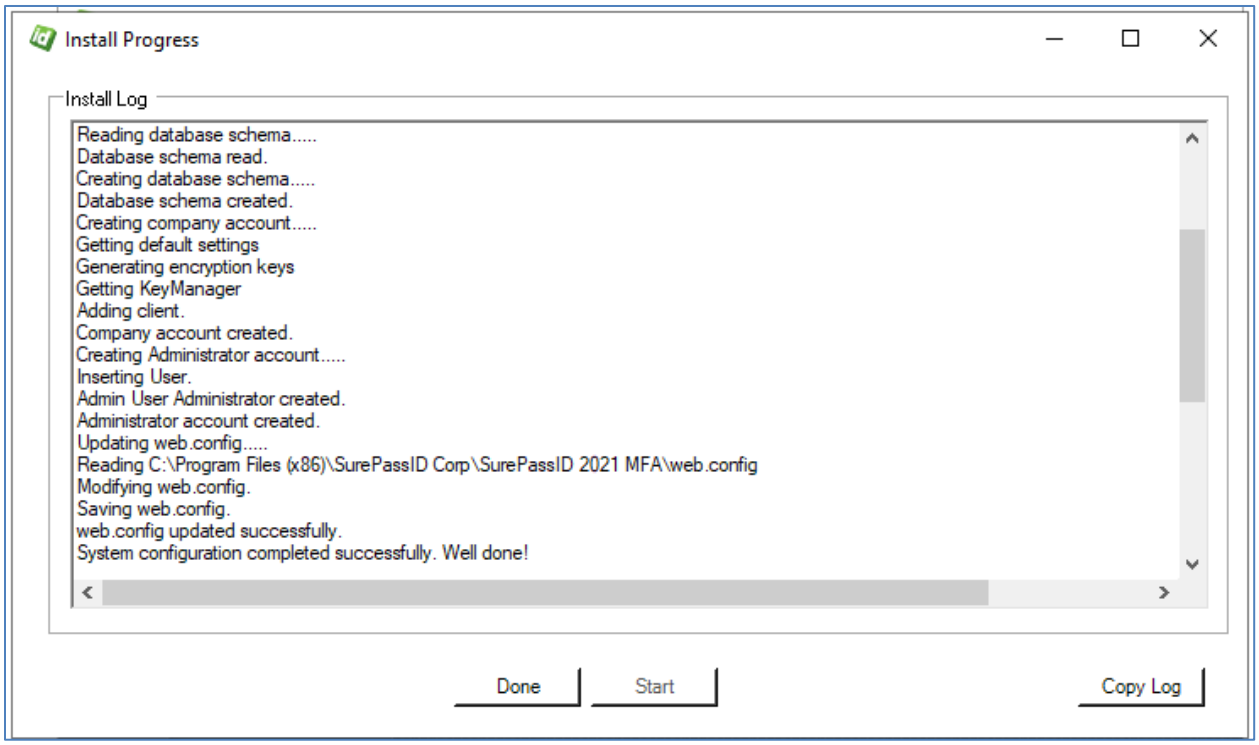
Press the ***Finish*** button to start the configuration process. You will see the following window.



Step 4 – Start Account Database Set-up

Press the ***Start*** button.

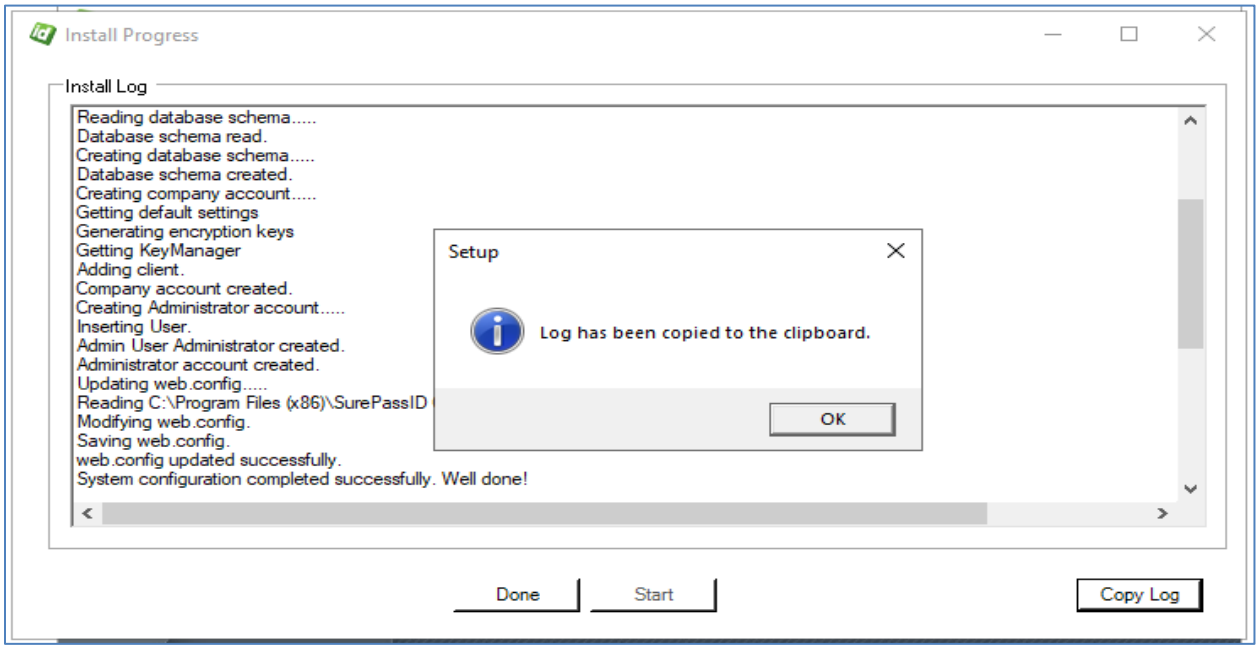
When the configuration process is done, you will be presented with an installation log and results shown below.



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 troubleshoot any errors more effectively 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

Post Installation 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 Authentication Server portal ships with MFA turned off for the Administration portal. You need to turn MFA on after you set up the administrators with MFA device, set up push notifications, or enable Fido devices. To turn on MFA, set:

  <configuration><appsettings> System.IgnoreLogin2FactorAuth = false

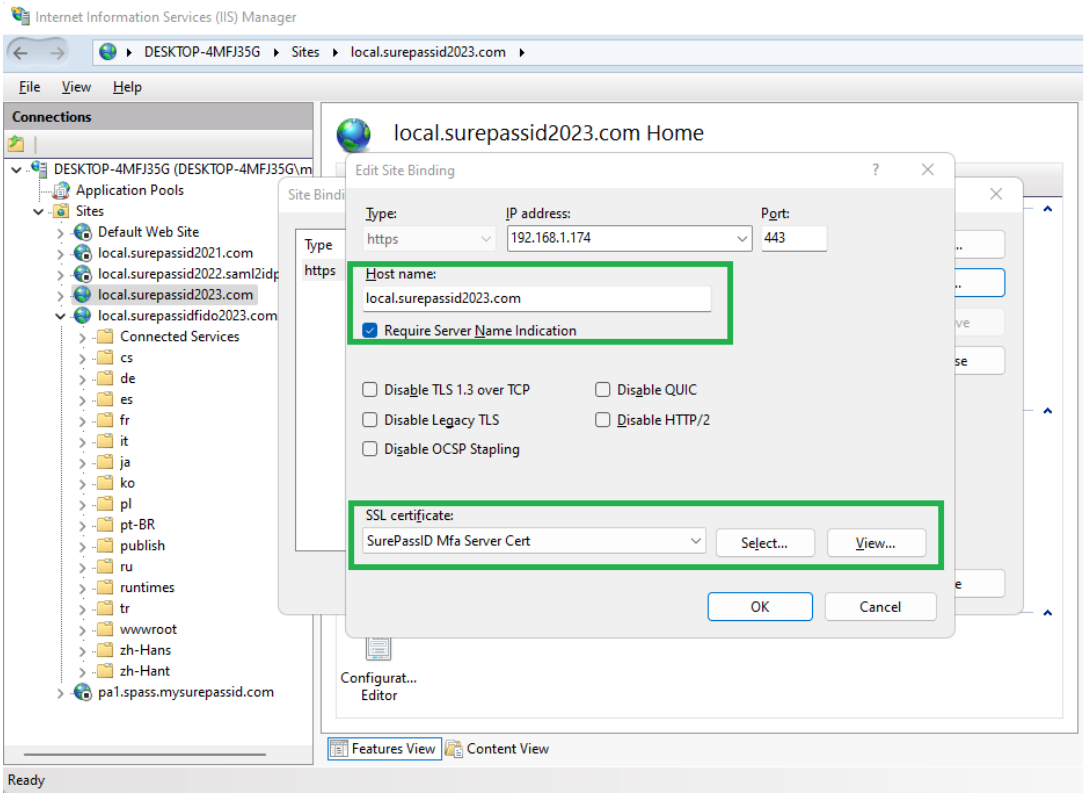
  in the web.config file. More on this below.

- 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:

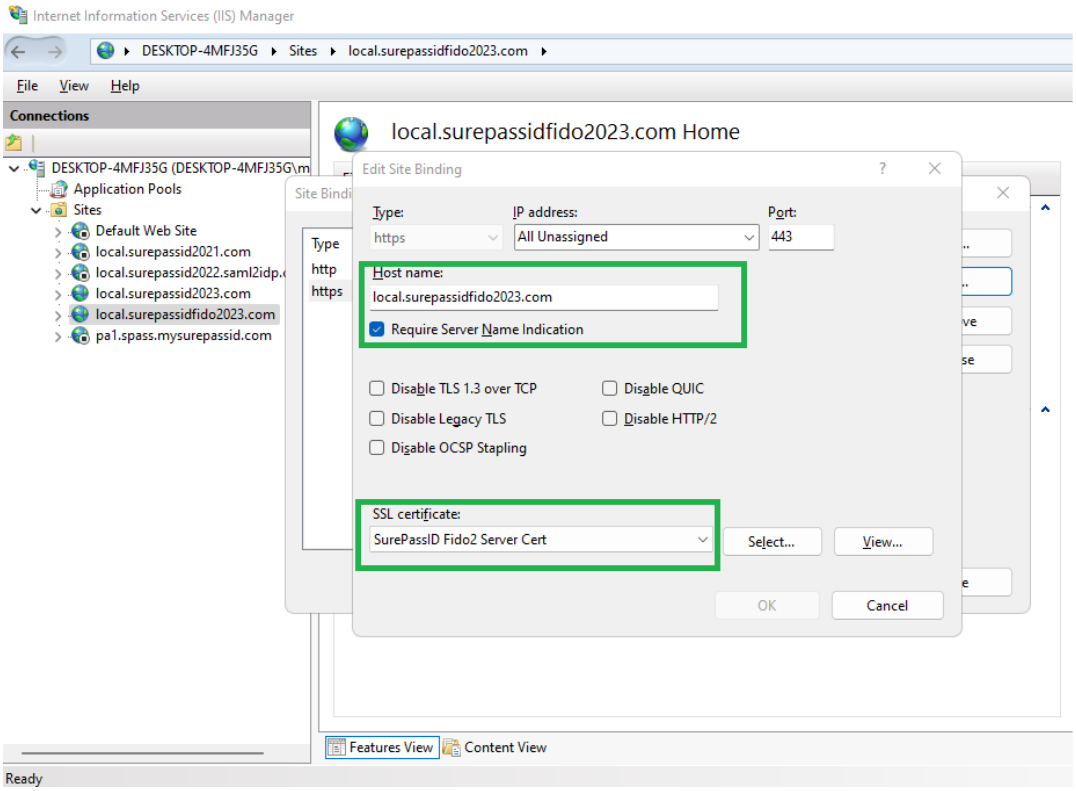
  https://msdn.microsoft.com/en-us/library/zhhddkxy(v=vs.140).aspx

IIS Setting Site Bindings

Since both DNS records will point to the same IP, IIS will need to know what IIS site to access when receiving requests for each unique URL. This is done in the site bindings for each IIS site using the host header (requesting URL) and the certificate that matches (make sure you check **Require Server Name Indication**). For instance, the binding for local.surepassid2023.com with the self-signed certs would be:



For instance, the binding for local.surepassidfido2023.com with the self-signed certs would be:



Changing Authentication Server URL

You can change this site names and the URLS that are used to meet your company standards. To do that you will need to:

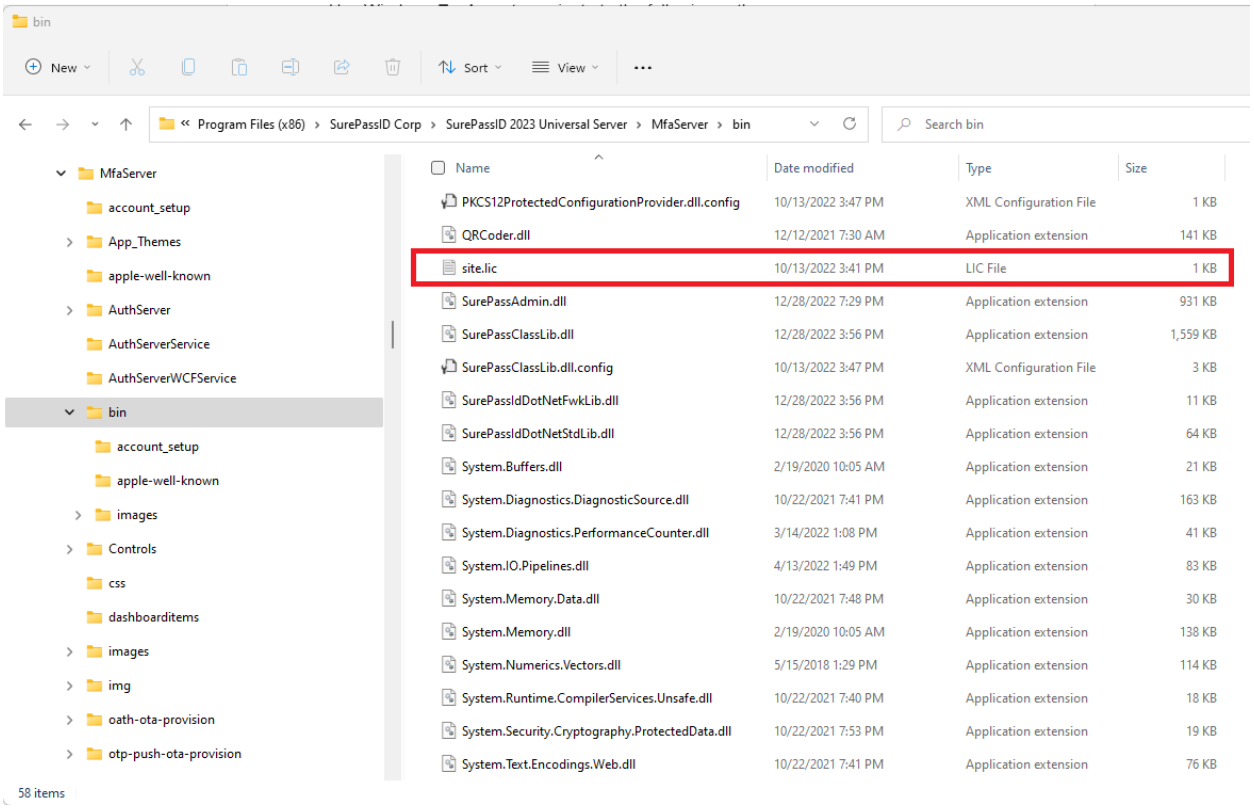
- Create/procure new certificates with the new URL
- Configure DNS (A) record to have the new URL point to the Authentication Server IP
- Set the IIS binding to set the new certificates to the URL as shown in previous section

Copying License File

Use Windows **Explorer** to navigate to the following path:

C:\Program Files (x86)\SurePassID Corp\SurePassID 2023 MFA\MfaServer\bin

and replace the site.lic (as shown below) file with the license file you have been provided by your SurePassID customer service representative.



Add License File

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 affect 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 Authentication Server
Support.HelpCompanyName	The name of the company. Used for white labeling the SurePassID platform. E.g. Johns Universal 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 requests will come from. You can get this from the Twilio account portal.
System.AllowPortalSingleFactorLogin	Allows single factor login to the admin portal. **true**=allow single factor (username + password) to access the system. **false**= require multi-factor authentication to access the system. Strongly recommended.

Server.ExternalNetworksProhibited	Allows or prevents the server from reaching out to the internet for certain functions like charting, CAPCHA, etc. **true**=do not allow external access to the Internet. **false**=allow access to the Internet. For air gapped systems set to true.

<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

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 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:

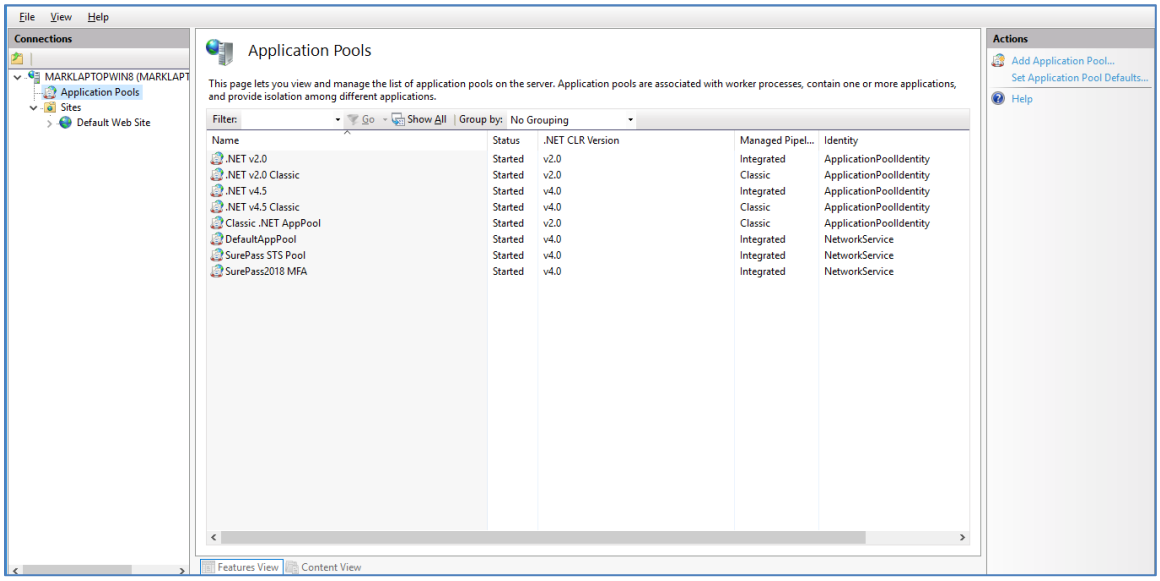
1. Provide a language centric experience to your users across cultural boundaries.
2. Change any constant field/message in the system.

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.

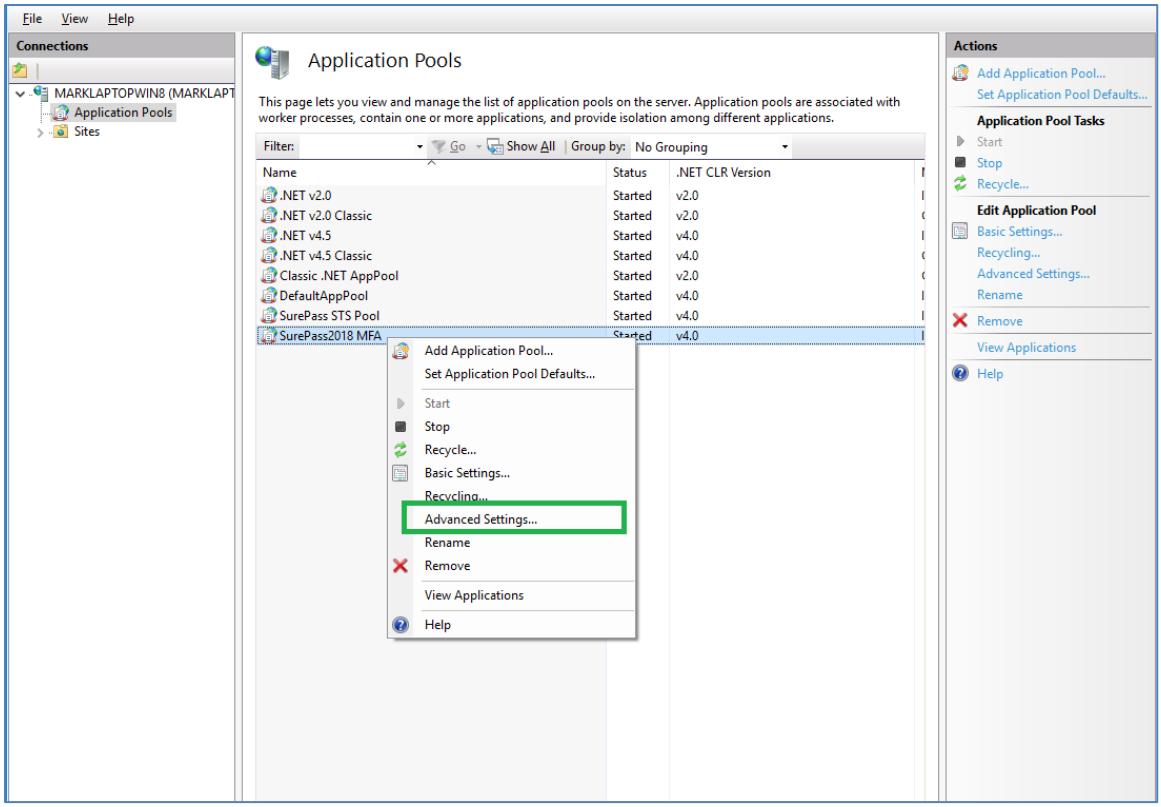
SurePassID Portal Session Timeout

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:

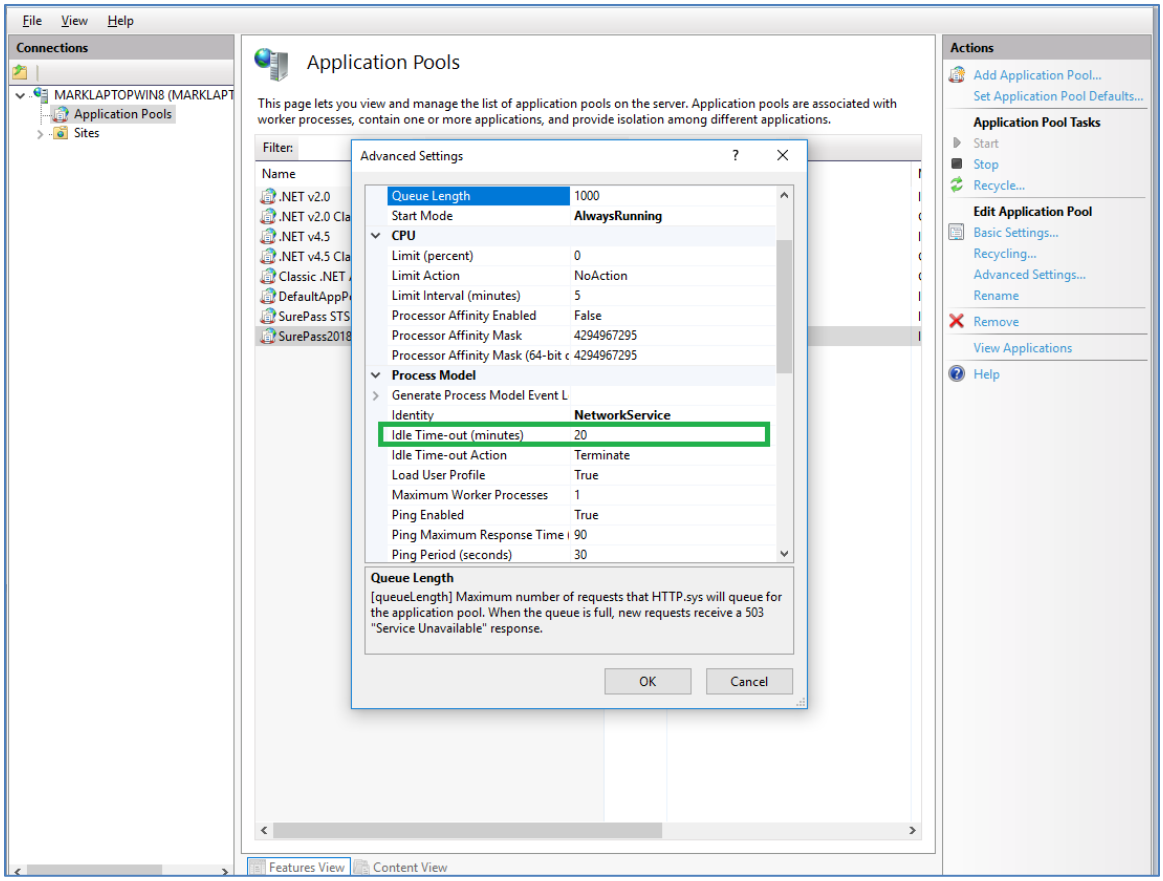
Start Internet Information Services (IIS) on the web server that SurePassID is installed on and right click **Application Pools** in the tree.



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



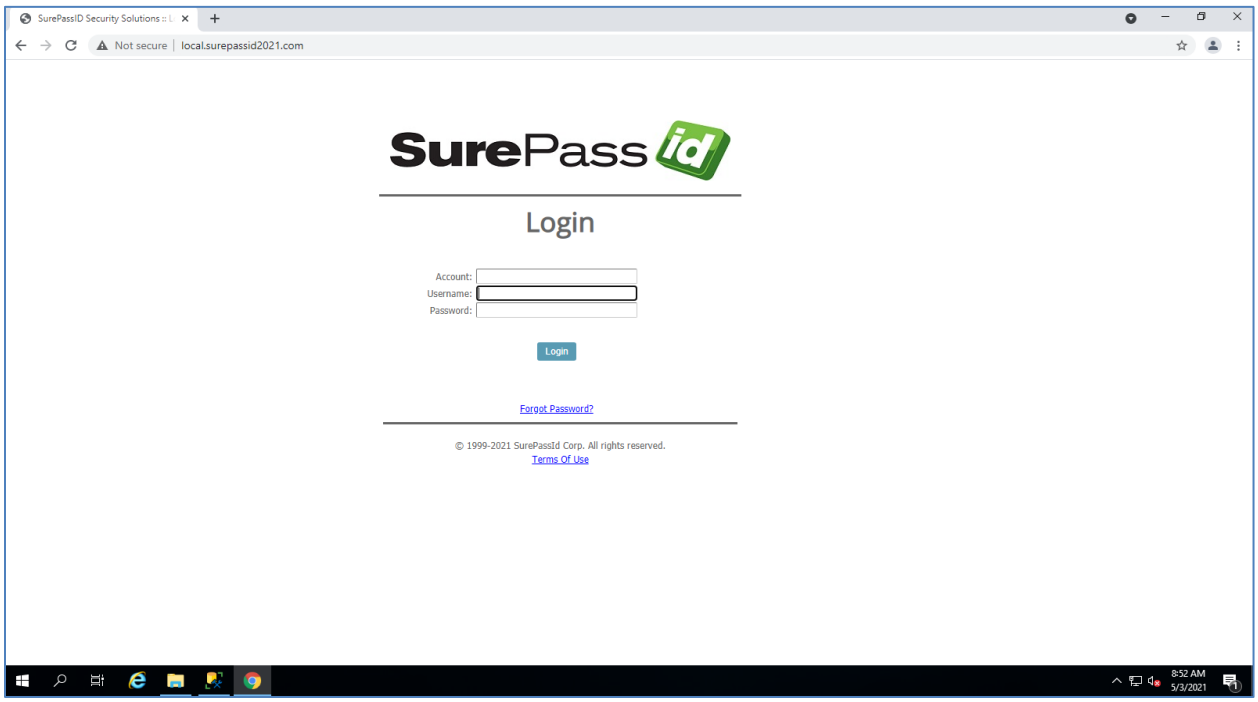
Right click on **SurePass2021MFA** and select Advanced Settings.



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.

Start the System

To login to SurePassID Universal Server, you can enter the following into a browser on the local machine http://local.SurePassID2023.com and you will see the following window:



Authentication Server 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.

High Availability Considerations and Capabilities

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

To that end the Authentication Server supports the following scalability and high availability capabilities.

Load Balancing

Load balancers make it possible to scale applications and create high availability services quickly and easily. 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 Authentication Server was designed to be load balanced and offers these features and characteristics:

- Each authentication request to the Authentication Server is atomic; there is no session state. This allows an unlimited number of Authentication Server instances to run behind one or many load balancers and provides the load balancer with the best options for request distribution.
- One or more load balancers can be set up in a single data center servicing multiple Authentication Server instances.
- Load balancers can also be geographically located to the user's request location for performance.
- An SurePassID Authentication 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 Universal 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 Authentication 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 Authentication Server supports all versions of Microsoft SQL Server editions:

- Enterprise
- Standard
- Web
- Express

The Authentication Server is designed to leverage all high availability capabilities 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 exceptionally large enterprises we recommend SQL Server Enterprise. Both editions have dozens of high availability options but the 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 (Information Technology) staff and no downtime to your users.

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

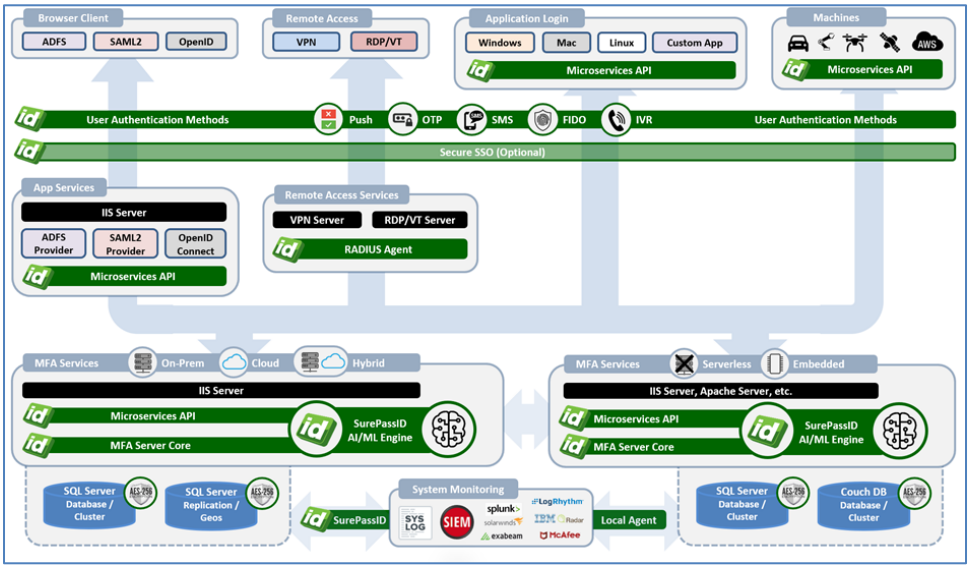
Single/Multiple Datacenter Architecture

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

Below is a single data center diagram of the overall Authentication 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 many Authentication Server configurations possible based on your requirements and constraints. Our technical experts can work with you to design an Authentication 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 our server-based products are designed for high availability and scalability. The brief 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 Authentication Server API