SurePassID RADIUS Server Guide

SurePassID Authentication Server 2025

SurePassID, Corp.

360 Central Avenue

First Central Tower

Suite 800

St. Petersburg, FL 33701

USA

+1 (888) 200-8144

www.surepassid.com

Table of Contents

Table of Figures

Introduction

This document outlines the installation and configuration processes for the SurePassID RADIUS Server in order to address your organization's security requirements. The aim of this guide is to serve as a comprehensive reference for system administrators.

This guide provides information on the following topics:

- **What is SurePassID RADIUS Server?**
    - A brief introduction to the SurePassID RADIUS Server and how it can help you get the most out of the SurePassID authentication system.
- **Installing and Configuring SurePassID RADIUS Server**
    - Detailed explanations for installing, configuring and maintaining the SurePassID RADIUS Server.

Other SurePassID Guides

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

- SurePassID LDAP Installation Guide.pdf
- SurePassID Postman Guide.pdf
- SurePassID Server Install Guide.pdf
- SurePassID Google Authenticator Guide.pdf
- SurePassID Mobile Authenticator Guide.pdf
- SurePassID ServicePass User Guide.pdf
- SurePassID Swagger Guide.pdf
- SurePassID Windows Logon MFA Guide.pdf
- SurePassID ServicePass Install Guide.pdf
- SurePassID Mobile Connector Install Guide.pdf
- SurePassID SEIM Guide.pdf
- SurePassID FreeRADIUS Guide.pdf
- SurePassID Administration Guide.pdf
- SurePassID ADFS Installation Guide.pdf
- SurePassID O365 SSO Identity Provider Installation Guide.pdf
- SurePassID Desktop Authenticator Guide.pdf
- SurePassID Directory Sync Guide.pdf
- SurePassID Linux PAM.pdf

What is the SurePassID RADIUS Server?

The SurePassID RADIUS is a system service that allows SurePassID to authenticate users from any RADIUS-compliant system such as Microsoft Universal Access Gateway, VPN devices (Cisco, Sonic Wall, etc.), TACACS+, Wi-Fi Access points, etc.

Security

RADIUS Server requires TLS 1.2 or TLS 1.3 for transport security.

System Logging

RADIUS Server maintains its own system log files to store critical information. The system logs help you troubleshoot and repair any issues the system might encounter during daily operations.

Installing the RADIUS Server

The SurePassID RADIUS Server installs the RADIUS Server components. After the SurePassID RADIUS Server is installed, you can configure the RADIUS component using the **Configuration Manager** app that will be installed as part of the installation.

Note: If you require RADIUS support for Linux systems you need to install and configure the SurePassID FreeRADIUS plug-in.

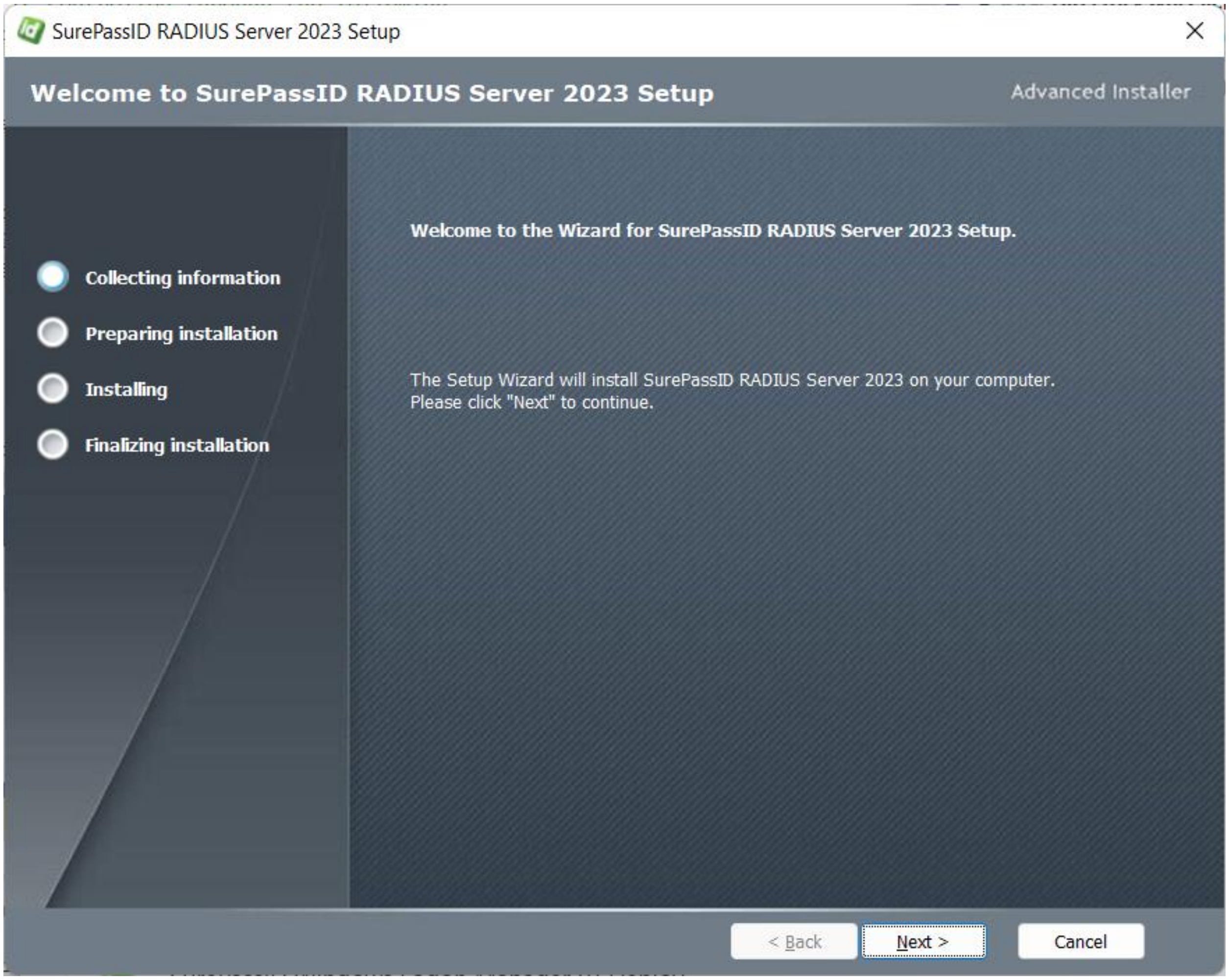
To install the RADIUS Server, you must first download and unzip the installer from here:

https://downloads.surepassid.com/RS/SPRS.zip

The installer and application are digitally signed by SurePassID. You must verify that as part of the installation.

After downloading the file unzip, unzip the file and run the msi installer file.

Then you will see the installation screen. Follow the steps to install product.


SurePassID RADIUS Server 2023 Setup

Welcome to SurePassID RADIUS Server 2023 Setup

Welcome to the Wizard for SurePassID RADIUS Server 2023 Setup.

The Setup Wizard will install SurePassID RADIUS Server 2023 on your computer.
Please click "Next" to continue.

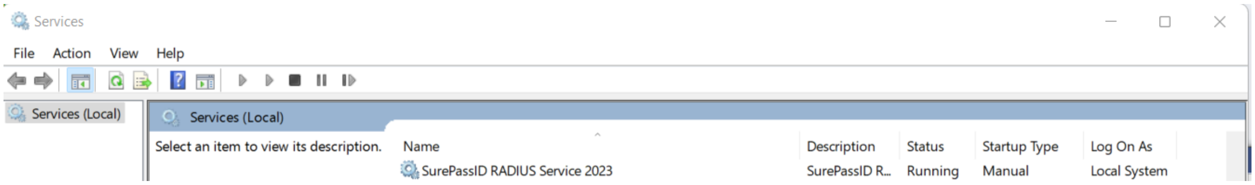
Follow the prompts until you get to the **User Access Control screen.**

<u>You must verify that the publisher is SurePassID Corp. If not, then press the No button.</u>

When you press the **Yes** button the RADIUS Server will be installed.

When installation is complete, you will see the final screen that indicates that the SurePassID RADIUS Server has now been installed and click the ***Finish*** button.

As part of the installation the SurePassID RADIUS server is installed as a Windows service as shown below:



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
SurePassID RADIUS Service 2023	SurePassID R...	Running	Manual	Local System

Installed RADIUS Service

By default, this service is installed in a non-running state as shown below. This allows you to configure the service and then start it **only** when you plan to use it. When you plan to use the SurePassID RADIUS Service, you should set the service to start automatically if you are ready to use it.

For production or testing, set the service to start automatically when the system restarts, and click the **Start** button to start the service now and click **OK** to save your changes.

Supported RADIUS Systems

The **RADIUS Server** can be integrated with most appliances (virtual and physical) and software systems that support RADIUS standards for authentication. We've verified compatibility with a wide variety of vendors and devices. Here is just a short list:

- Barracuda SSL VPN
- Cisco ACS / ISE / ISR / Catalyst / SSH Network Device Access / IPSec VPN / ASA
- Citrix ACS NetScaler Gateway including XenDesktop & XenApp
- F5 Networks BIG-IP VPN
- Juniper and Pulse Secure SSL VPN
- Microsoft NPS
- Palo Alto Global Protect, IPSEC and SSL VPN
- SonicWALL TZ, NSA, SMA, SRA, etc.
- VMware View
- VPN Routers and NAS (Linksys, ASUS, etc.)
- Web Application Firewalls (WAF)
- TACACS+ devices (Cisco ICE)

The SurePassID RADIUS Server only requires that the RADIUS compliant system (VPN, Firewall, etc.) use the PAP protocol for communication.

Configuring the RADIUS Server

The **RADIUS Server** allows you to add two-factor authentication (two-step authentication) to any system that supports RADIUS.

The server supports the following RADIUS features:

- **Challenge Response** – The user can be challenged for many different credentials. Most of the time, the challenge will be to provide a One-Time Password after successfully entering a valid username and password. Some RADIUS devices (such as VPNs (Virtual Private Network)) only support single-factor authentication. Two-factor authentication can still be used by appending the One-Time Password to the user's password.
- **Proxy Server Chaining** – In RADIUS authentication, there can often be multiple RADIUS servers as part of the authentication process.

The **RADIUS Server** supports the following directories for single-factor (username and password) authentication:

- **Active Directory** – For tight integration with existing enterprise Identity Management Systems
- **SurePassID Directory** – For use with other cloud systems or external users that are not part of the existing enterprise Active Directory Forest.
- **LDAP Directory** – For companies that use an LDAP directory such as Unix and Linux systems.

The **RADIUS Server** only authenticates pass codes and allows the VPN client to perform the first factor of authentication (LDAP, AD (Active Directory), local, etc.) or participate in more sophisticated authentication strategies such as Citrix nFactor.

The **RADIUS Server** supports sending One Time Passcode (OTP) to the user. The user will concatenate the OTP code after the password unless the user chooses challenge response. The choices are:

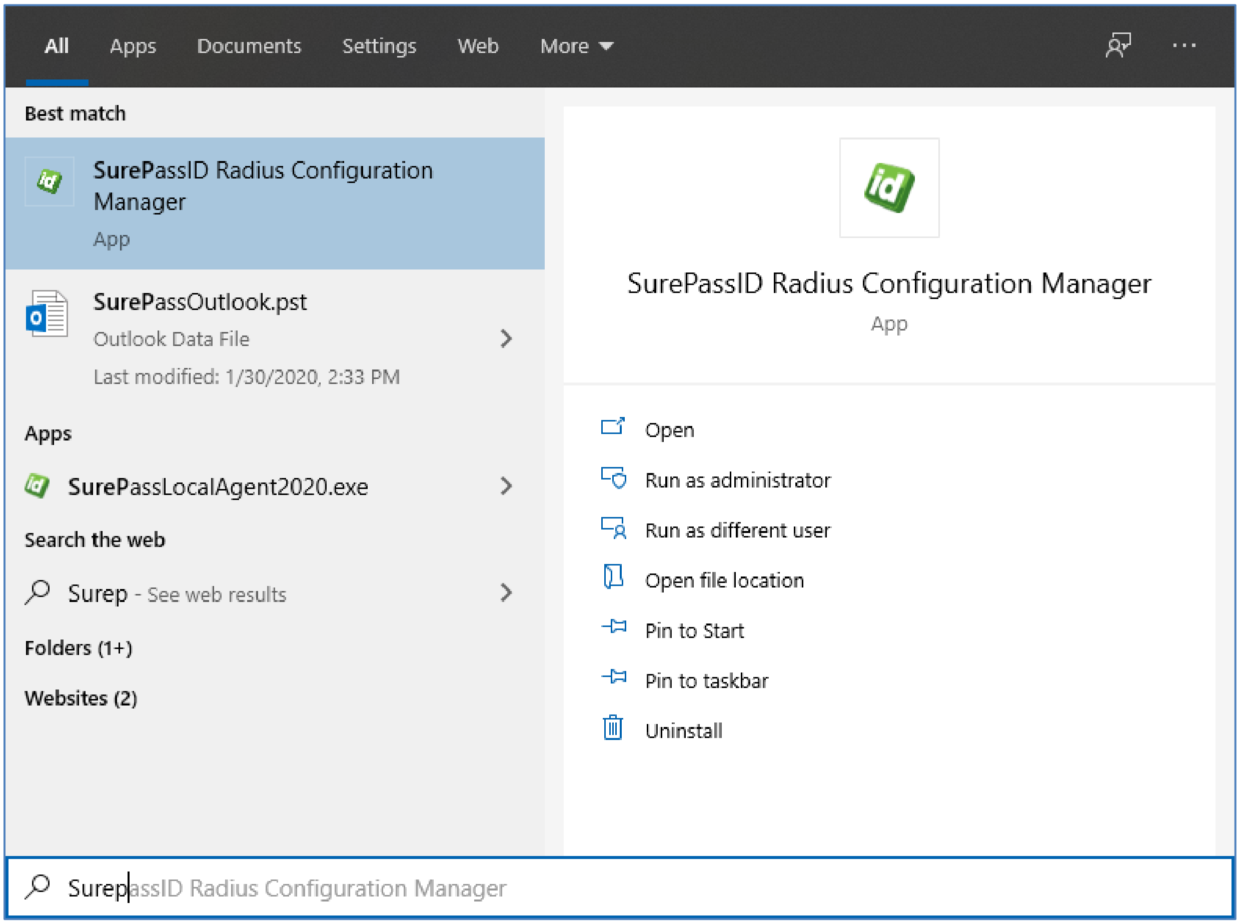
- **SMS Code** – An OTP code is sent via SMS text to the user.
- **Voice Code** – A call is made to the user providing them with an OTP code with a human voice.
- **Email Code** – An email is sent to the user which contains an OTP. This code is concatenated after the user's password.

The **RADIUS Server** also supports pushing authentication requests to the user's phone. If the user accepts the request, the user is allowed to login with just username and password. The choices are:

- **Push Authentication** – Send a message to the SurePassID Mobile Authenticator App to confirm or reject authentication.
- **IVR (Interactive Voice Response) Authentication** – Call the user's phone (including land lines) let them confirm or reject authentication with their keypad.
- **SMS Question** – Push a question is sent to the user's mobile device via SMS text asking the user to confirm or reject authentication with their keypad system.

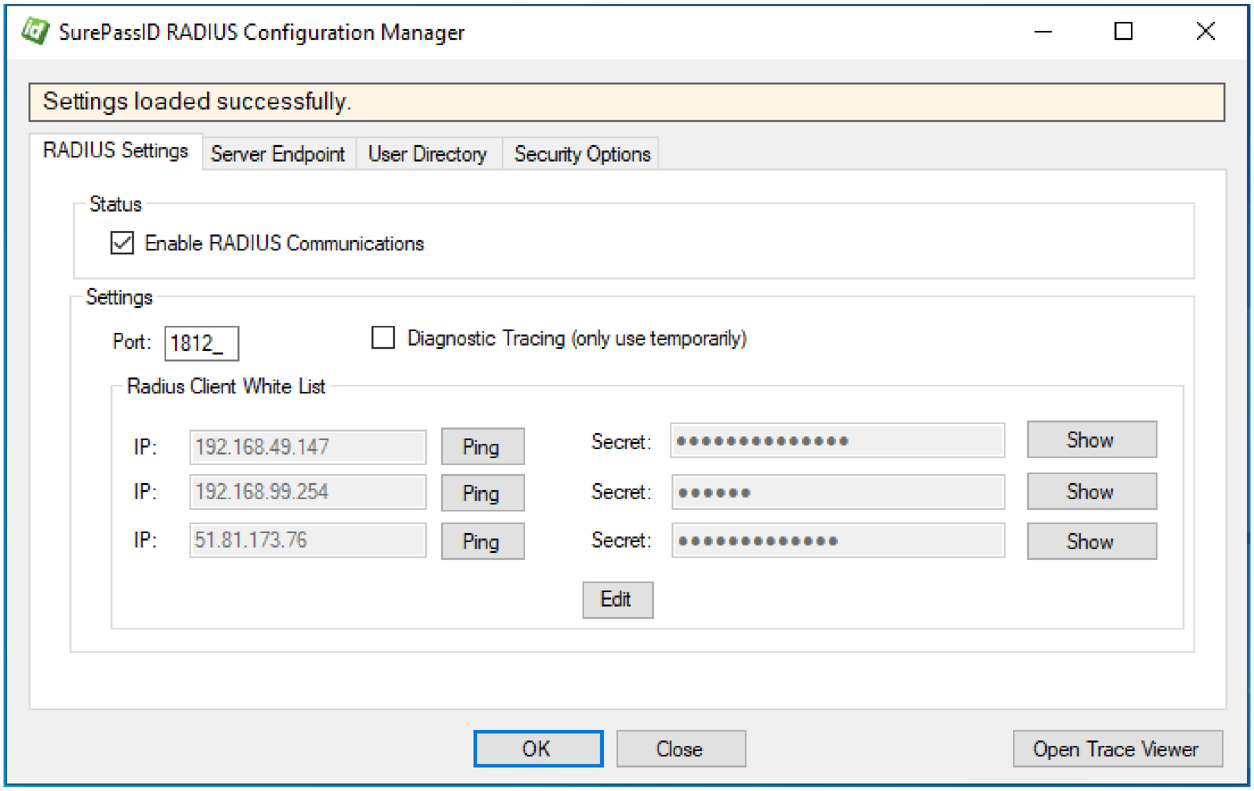
HINT: All messages sent to the user can be tailored to your company's needs in the SurePassID portal using the Customize SMS Messages and Customize Email Messages menus.

The **SurePassID RADIUS Configuration Manager** application is used to configure the RADIUS and Directory Authentication Services. To configure the services, select **SurePassID RADIUS Configuration Manager** from the Windows Start menu as shown below:



Start Configuration Application

SurePassID RADIUS Configuration Manager



SurePassID RADIUS Configuration Manager

Settings loaded successfully.

Status

☑ Enable RADIUS Communications

Settings

Port: 1812_

□ Diagnostic Tracing (only use temporarily)

Radius Client White List

IP: 192.168.49.147 Secret: ••••••••••••••

IP: 192.168.99.254 Secret: ••••••

IP: 51.81.173.76 Secret: •••••••••••••

RADIUS Settings

The application has four folder tabs. These tabs are:

- **RADIUS Settings** – Configuration settings for the SurePassID RADIUS Server specific.
- **Server Endpoint** - Configuration settings for identifying your SurePassID account.
- **User Directory** - Configuration for User Directory settings
- **Security Options** - Configuration for Permitted MFA Methods, User Active Directory Security Groups, and Additional Options.

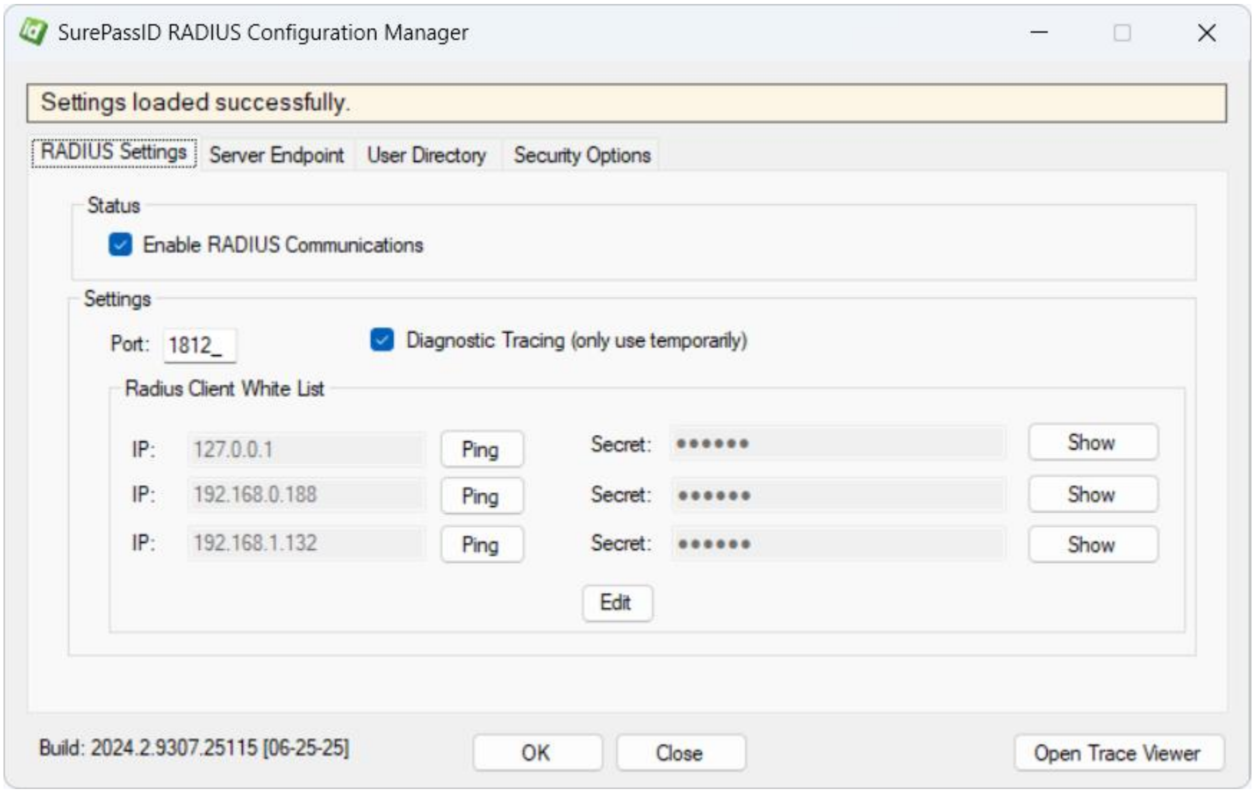
The **RADIUS Settings** tab has the following fields:

- **Enable RADIUS Communications** – Check this box to enable the RADIUS server.
- **Port** – The UDP port that the RADIUS server will listen on. The default value is 1812; the standard RADIUS authentication port.

- **Diagnostic Tracing** – This option should only be checked when you are actively troubleshooting an issue. Leaving this option checked negatively impacts performance and accumulating large amounts of system data can create a potential security issue. All tracing info will be placed in the following folder:

  C:\Program Files (x86)\SurePassID Corp\SurePassID RADIUS Server 2023\Trace

- **RADIUS Client Whitelist** – The first three RADIUS devices that are permitted to communicate with the SurePassID RADIUS service.
  - **IP (Intellectual Property)** – The IP of address of the RADIUS client device
  - **Secret** – The shared secret on the RADIUS client device.
- **Edit Button** – Add, update or remove a RADIUS client from the whitelist. Only RADIUS clients on the whitelist can make requests to the **RADIUS Server.** Each RADIUS client is identified by its IP address and the shared secret used between the RADIUS applications (RADIUS client). Requests from RADIUS clients that are not on the whitelist will be rejected.



SurePassID RADIUS Configuration Manager

Settings loaded successfully.

Status

☑ Enable RADIUS Communications

Settings

Port: 1812_

☑ Diagnostic Tracing (only use temporarily)

Radius Client White List

IP: 127.0.0.1 Secret: ●●●●●●

IP: 192.168.0.188 Secret: ●●●●●●

IP: 192.168.1.132 Secret: ●●●●●●

Build: 2024.2.9307.25115 [06-25-25]

Server Endpoint

The **Server Endpoint** tab has the following fields:

- **Endpoint URL** – The SurePassID authentication Endpoint URL. In most cases, you will not need to change this unless you are using a custom SurePassID installation. The values are:
    - **sandbox** – The SurePassID sandbox cloud system.
    - **prod** – The SurePassID production cloud system.
    - **on premises system** – On-premises or custom installation of the SurePassID MFA server. The format of this parameter is usually:

https://<surepassid_server>/AuthServer/REST/OATH/OATHServer.aspx

- **Test Server Connection button** – This button will verify that this server has connectivity to the SurePassID server using TLS (port 443). If this fails, then steps must be taken to determine where the connection fails. Common problems are (1) port 443 is not open in the firewall or TLS is not configured correctly, (2) the SurePassID Endpoint URL is invalid or not able to accept TLS requests, (3) no TCPIP connectivity, (4) other problems that require trouble shooting.

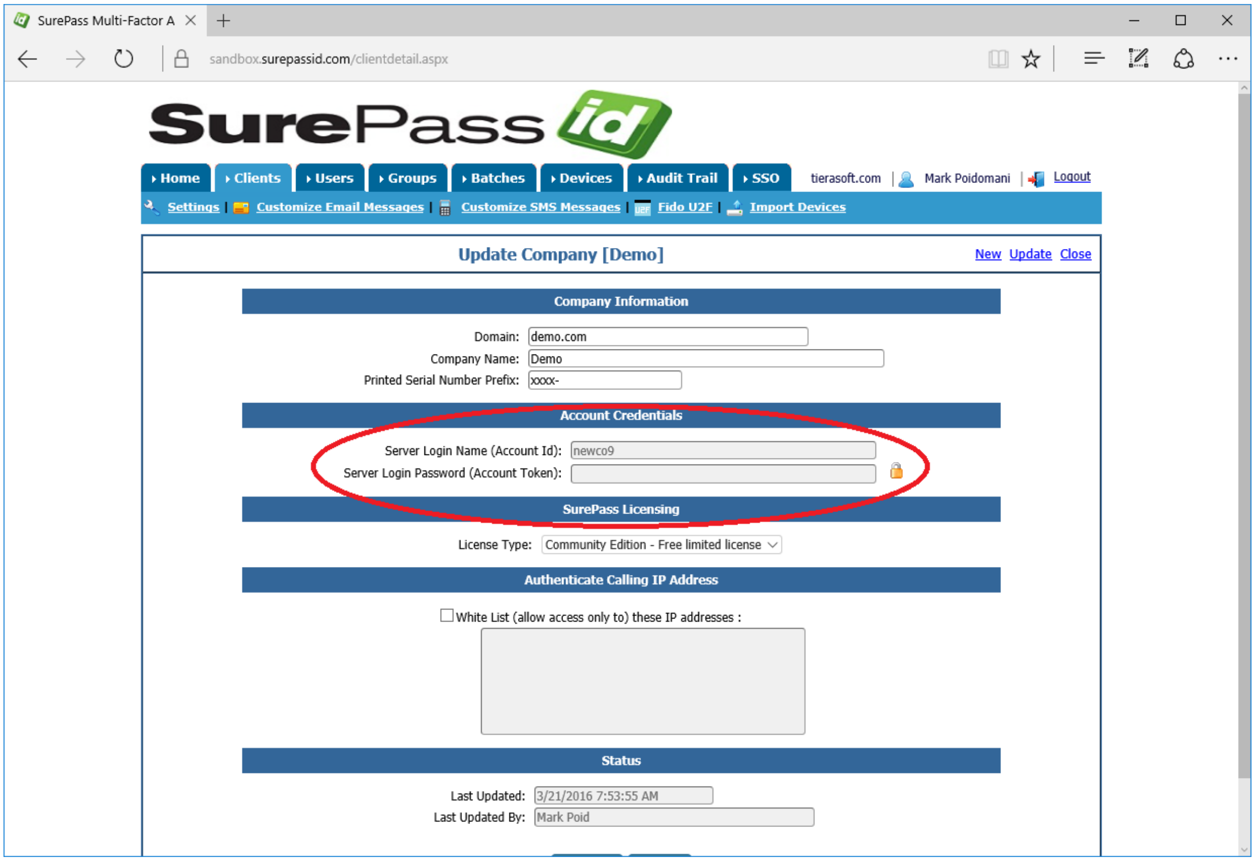
  NOTE: Although it is not recommended, for initial testing the system can be configured for port 80 communications removing the TLS requirement. This requires changes to both the **RADIUS Server** configuration and the SurePassID server. Contact SurePassID technical support (support@surepassid.com) for instructions.
- **Server Login Name** – The login name for your SurePassID account.
- **Server Login Password** – The login password for your SurePassID account.
- **Test Server Credentials Button** – This button will verify that the Server Login Name and Server Login Password are correct.

  IMPORTANT: Before trying this, make sure you have successfully connected to the server via pressing the **Test Server Connection Button**.
- **Open Trace Viewer Button** – This button will display the **RADIUS Server** trace log. This can be useful for verifying initial system connectivity, trouble-shooting system configuration, login failures, and performance related issues.

The **Server Login Name** and **Server Login Password** can be retrieved from your SurePassID account as shown in the next section.

Using the RADIUS Server App with SurePassID MFA Server

If you are using an older version of SurePassID MFA server, you will see the following info for your account as shown below.



Update Company [Demo]

Company Information

Domain: demo.com
Company Name: Demo
Printed Serial Number Prefix: xxxx-

Account Credentials

Server Login Name (Account Id): newco9
Server Login Password (Account Token):

SurePass Licensing

License Type: Community Edition - Free limited license

Authenticate Calling IP Address

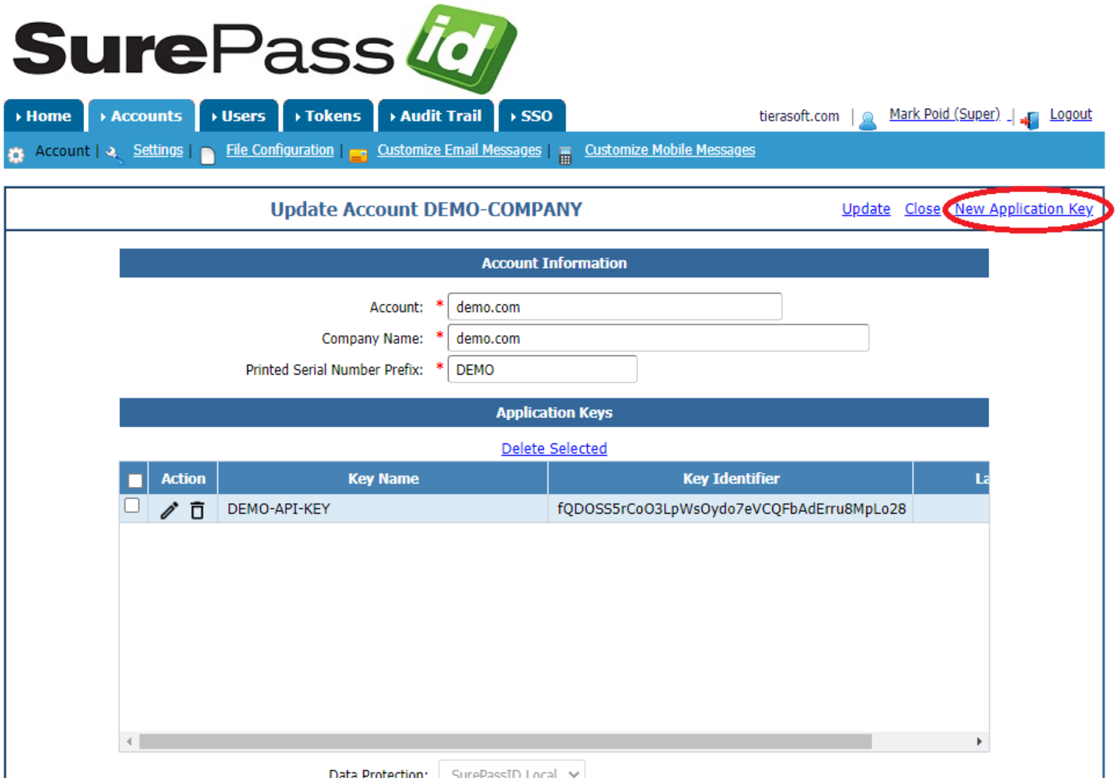
□ White List (allow access only to) these IP addresses :

Status

Last Updated: 3/21/2016 7:53:55 AM
Last Updated By: Mark Poid

SurePassID Legacy Account Settings

If you are using the latest version of SurePassID you will see the following info for your account:



Update Account DEMO-COMPANY

Account Information

Account: *	demo.com
Company Name: *	demo.com
Printed Serial Number Prefix: *	DEMO

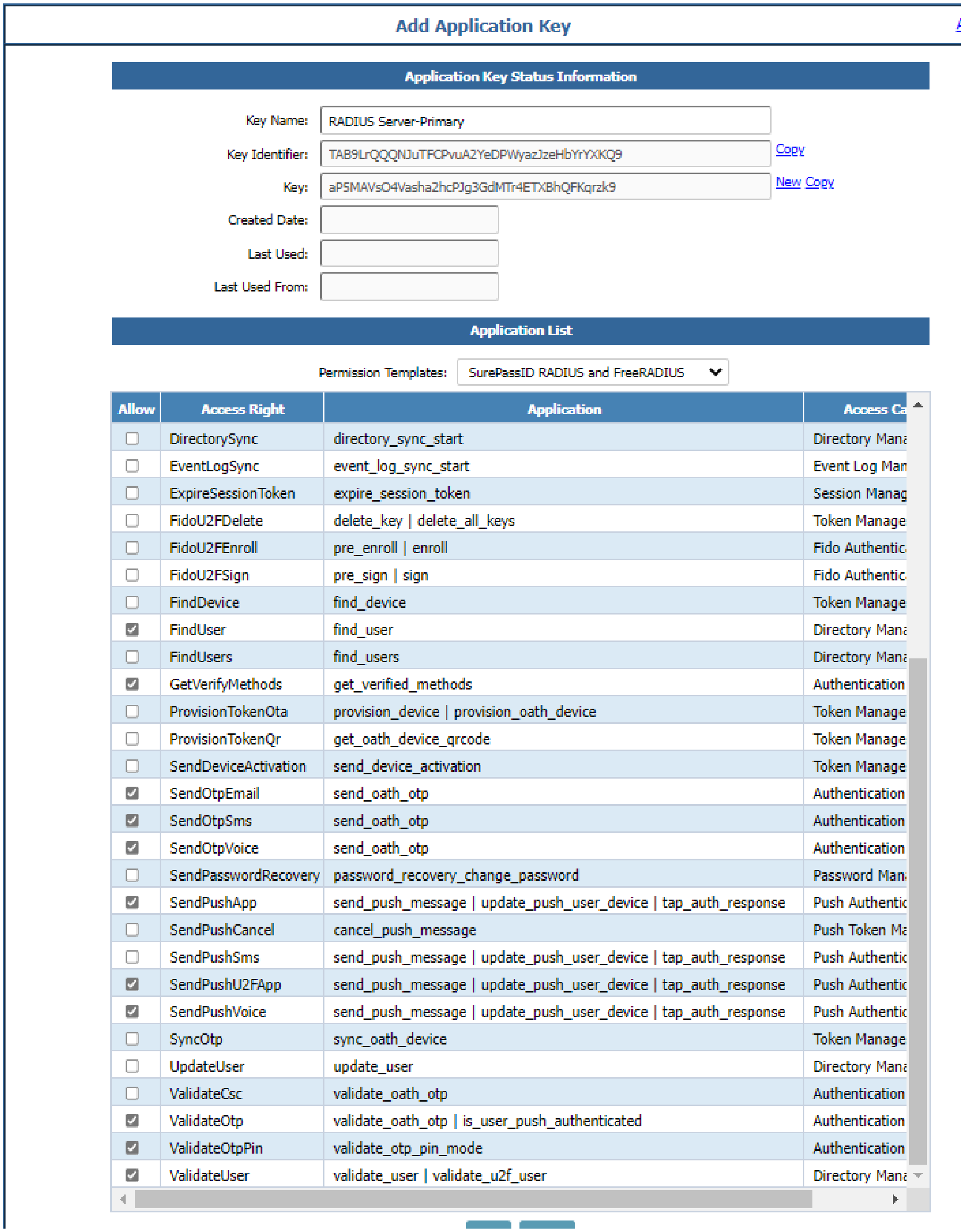
Application Keys

□	Action	Key Name	Key Identifier	La
□	✎ 🗑	DEMO-API-KEY	fQDOSS5rCoO3LpWsOydo7eVCQFbAdErru8MpLo28	

Data Protection: SurePassID Local

SurePassID API Key Settings

All application requests to the MFA Server require an **Application Key**. To create a new **Application Key** just for **RADIUS Server** (recommended) click the **New Application Key** link and see the form below:



Add Application Key

Application Key Status Information

Key Name:	RADIUS Server-Primary
Key Identifier:	TAB9LrQQQNJuTFCPvuA2YeDPWyazJzeHbYrYXKQ9 Copy
Key:	aP5MAVsO4Vasha2hcPJg3GdMTr4ETXBhQFKqrzk9 New Copy
Created Date:	
Last Used:	
Last Used From:	

Application List

Permission Templates: SurePassID RADIUS and FreeRADIUS

Allow	Access Right	Application	Access Ca
☐	DirectorySync	directory_sync_start	Directory Mana
☐	EventLogSync	event_log_sync_start	Event Log Man
☐	ExpireSessionToken	expire_session_token	Session Manag
☐	FidoU2FDelete	delete_key | delete_all_keys	Token Manage
☐	FidoU2FEnroll	pre_enroll | enroll	Fido Authentic
☐	FidoU2FSign	pre_sign | sign	Fido Authentic
☐	FindDevice	find_device	Token Manage
☑	FindUser	find_user	Directory Mana
☐	FindUsers	find_users	Directory Mana
☑	GetVerifyMethods	get_verified_methods	Authentication
☐	ProvisionTokenOta	provision_device | provision_oath_device	Token Manage
☐	ProvisionTokenQr	get_oath_device_qrcode	Token Manage
☐	SendDeviceActivation	send_device_activation	Token Manage
☑	SendOtpEmail	send_oath_otp	Authentication
☑	SendOtpSms	send_oath_otp	Authentication
☑	SendOtpVoice	send_oath_otp	Authentication
☐	SendPasswordRecovery	password_recovery_change_password	Password Mana
☑	SendPushApp	send_push_message | update_push_user_device | tap_auth_response	Push Authentic
☐	SendPushCancel	cancel_push_message	Push Token Ma
☐	SendPushSms	send_push_message | update_push_user_device | tap_auth_response	Push Authentic
☑	SendPushU2FApp	send_push_message | update_push_user_device | tap_auth_response	Push Authentic
☑	SendPushVoice	send_push_message | update_push_user_device | tap_auth_response	Push Authentic
☐	SyncOtp	sync_oath_device	Token Manage
☐	UpdateUser	update_user	Directory Mana
☐	ValidateCsc	validate_oath_otp	Authentication
☑	ValidateOtp	validate_oath_otp | is_user_push_authenticated	Authentication
☑	ValidateOtpPin	validate_otp_pin_mode	Authentication
☑	ValidateUser	validate_user | validate_u2f_user	Directory Mana

The **Key Name** is the friendly name to identify this key. It is not used for any security purposes. For instance, you could name it **Dir Sync Key**.

Select the **SurePassID RADIUS and FreeRADIUS** from the **Permissions Templates** drop down list.

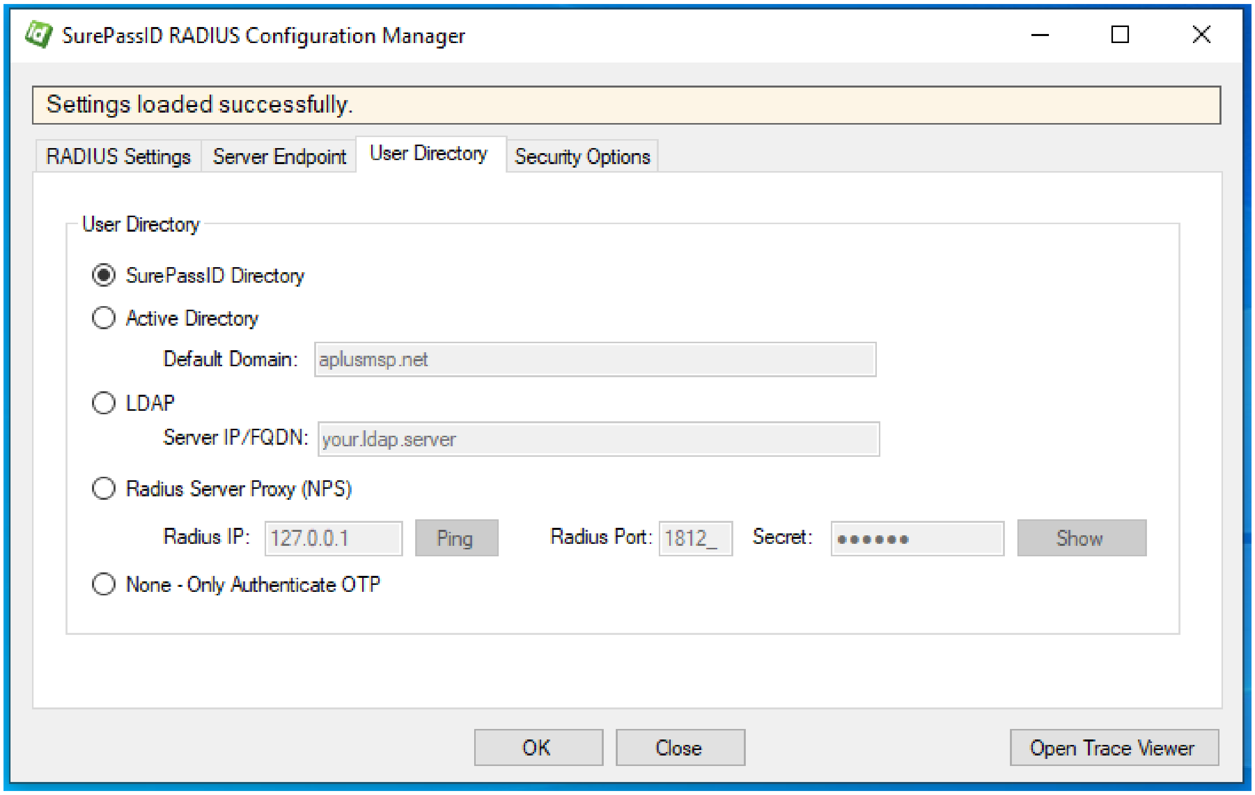
The **Key Identifier** parameter is the **Server Login Name** and the **Key** parameter is the **Server Login Password.**

Copy **Key Identifier** and **Key** for later use when configuring **RADIUS Server**. One you click the **Add** button the **Key** will no longer be viewable. If you forget the **Key**, you can delete this **Application Key** and add a new one.

Press the **Add** button to save the Api Key.

Caution: Deleting an **Application Key** prevents applications using it from accessing the MFA Server. It cannot be restored; a new key must be generated and updated in the application.

User Directory tab has the following fields:



SurePassID RADIUS Configuration Manager

Settings loaded successfully.

User Directory

● SurePassID Directory

○ Active Directory

Default Domain: aplusmsp.net

○ LDAP

Server IP/FQDN: your.ldap.server

○ Radius Server Proxy (NPS)

Radius IP: 127.0.0.1 Radius Port: 1812_ Secret: ●●●●●●

○ None - Only Authenticate OTP

User Directory

- **User Directory** – Check the appropriate User Directory to validate the user's name and password.
  - **SurePassID Directory** – Check this box to use the SurePassID directory
  - **Active Directory** – Check this box to use Active Directory.

        - **Default Domain** - You can specify the default domain for all users. Leaving this field blank will default to the current domain of the RADIUS server.

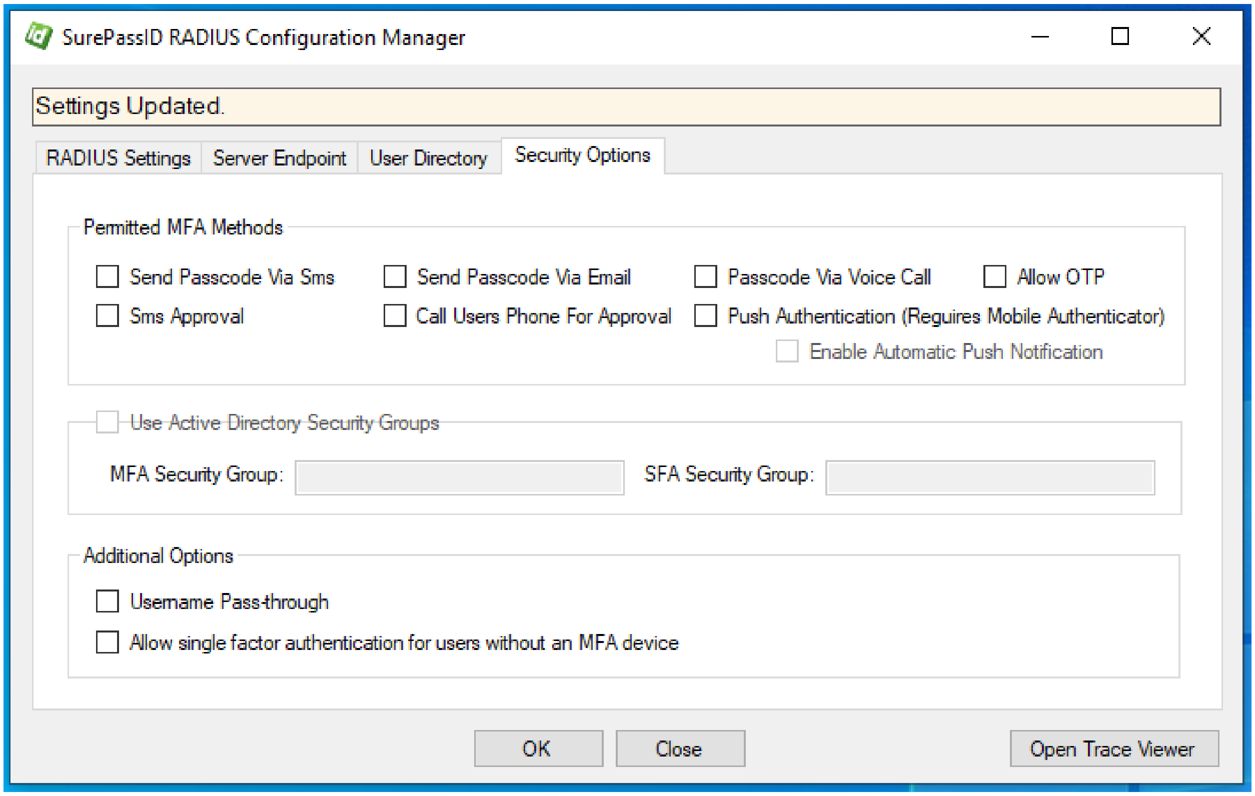
          NOTE: For enterprises that have multiple domains, users can override the default domain when logging in by entering their username in the form of **domain/username** or **username@domain**.

    - **LDAP** – Check this box to use an LDAP directory.
        - **Server IP/FQDN** – You must enter the IP or Fully Qualified Domain Name (FQDN) of the LDAP server
    - **None – Only authenticate OTP** – Check this box to instruct the RADIUS Server to only check the OTP. This means the RADIUS client (VPN/firewall/etc.) will validate the username locally or with some external directory such as Active Directory/LDAP first and then prompt the user for the OTP and send it to RADIUS Server for validation.

After making changes, you can start the **RADIUS Server** windows service**.** If the service is already running the **RADIUS Server** will automatically pick up the changes.

NOTE: When authenticating users, the username (without domain information if present) entered at RADIUS login must be defined in the SurePassID directory regardless of the **User Directory** selected.

The **Security Options** tab has the following fields:



Settings Updated.

Permitted MFA Methods

□ Send Passcode Via Sms
□ Send Passcode Via Email
□ Passcode Via Voice Call
□ Allow OTP
□ Sms Approval
□ Call Users Phone For Approval
□ Push Authentication (Requires Mobile Authenticator)
□ Enable Automatic Push Notification

□ Use Active Directory Security Groups

MFA Security Group:

SFA Security Group:

Additional Options

□ Username Pass-through
□ Allow single factor authentication for users without an MFA device

Security Options

- **Permitted MFA Methods** – Select the MFA methods your users can use to login. <u>If you do not select an MFA method users will not be able to login.</u>
    - **Send Passcode Via SMS** - One time passcode is sent to the user's mobile phone via an SMS text message. The user enters that code.
    - **Send Passcode Via Email** - One time passcode is sent to the user's email. The user enters that code.
    - **Passcode Via Voice Call** – The user receives a phone call, and the one-time passcode is spoken to the user. The user enters that code.
    - **Allow OTP** - The user enters OTP from the mobile authenticator application with password.
    - **SMS Approval** – A question is sent to the user's mobile phone via an SMS text message. The user accepts login or refuses the request.
    - **Call Users Phone for Approval -** The user receives a phone call and is asked a question. The user either answers the question to approve the login request or declines it.

    - **Push Authentication (Requires Mobile Authenticator)** - The user receives a push notification on their mobile phone. The user accepts to login or refuses the notification request.
    - **Enable Automatic Push Notification** - This option will get enabled when user selects **Push Authentication** MFA method. After the user enters a valid username and password, they will automatically be sent a push.

- **User Active Directory Security Groups** - This option will get enabled when user selects Active Directory from the User Directory tab.
    - **MFA Security Group** – You can mention MFA user's security group name. The users from the mentioned group will be allowed to connect to the RADIUS server.
    - **SFA Security Group** – You can mention SFA user's security group name. The users from the mentioned group will be allowed to connect to the RADIUS server.

  If both groups are mentioned, then users that do not belong to any of the above groups will not be allowed access to RADIUS server.
- **Allow single-factor authentication for users without a two-factor device** – Check this box if you will have some users logging in that will not have a two-factor authentication token. Users who are assigned a two-factor authentication token must provide the second factor of authentication.
- **Username Pass-through** - Check this box when AD username normalization is not needed.

Configuring RADIUS Clients

Once the SurePassID **RADIUS Server** is configured and running. You need to configure your RADIUS clients to use it for secure authentication.

When configuring the RADIUS clients' settings, there are specific parameters that are important to the SurePassID **RADIUS Server**.

RADIUS Server IP – Set this IP to the SurePassID **RADIUS Server** IP. Make sure that the IP of the RADIUS client is in the SurePassID **RADIUS Server** whitelist.

RADIUS Server Port - Set this port to 1812 which is the standard for RADIUS authentication. This RADIUS client must use the same port.

RADIUS Secret – This is the shared secret assigned to each whitelist RADIUS client IP in the SurePassID **RADIUS Server**. When the RADIUS client does not have the correct secret that matches its IP, then the SurePassID RADIUS Server will reject access.

RADIUS Authentication Protocol – The typical default is PAP. If the option is offered by the RADIUS client, select PAP. Selecting any other option will not work.

Secondary Authentication – Most RADIUS clients allow you to select primary and secondary authentication methods. We suggest you consider all factors that might occur and prevent your RADIUS client from connecting to the primary RADIUS server (SurePassID **RADIUS Server**) such as internal network outages, external network outage, VM (Virtual Machines) issues, etc. and pick a secondary method that eliminates these potential bottle necks so that a limited number of users can authenticate and access the system remotely in times of need. The SurePassID **RADIUS Server** can be deployed as a load balancer. You can configure multiple instances of the SurePassID RADIUS Server on multiple servers for fault tolerance and additional scalability.

Timeouts and Retries

We recommend a RADIUS authentication timeout of 10 seconds and 3 retries if you are using hard/soft tokens.

Out of band authentication such as sending an email, SMS, or push authentication can take time for the user to respond, and you do not want your users to get cut-off before they authenticate and then retry. Depending on your network latency, authentication methods and SurePassID MFA Server installation options (cloud vs. on-premises) this timing can vary. We recommend a minimum RADIUS timeout of 30 seconds and zero retries as a starting point. You can always make this longer or shorter depending on your needs.

SurePassID natively supports out of band timeouts. This is required for systems that do not have timeouts like RADIUS. This timeout value is specified in the SurePassID admin portal. It is important that your RADIUS timeout value is greater than SurePassID mobile timeout by 5 seconds. This variance is to account for the RADIUS authentication overhead.

If you have any additional questions, please call or email support@surepassid.com for assistance.

Fortinet Notes

Most VPN appliances let you configure the default timeout value using their user interface. This is not the case for the Fortinet. The Fortinet appliance has a default timeout of 5 seconds, which will fail for anything other than OTP passcode authentication. The timeout can be increased only using the Fortinet Command Line Interface (CLI) as described be below:

The following global changes need to be made to the FortiGate as per FortiGate Forum RADIUS Time-Out | Fortinet Technical Discussion Forums:

CLI:

```
config system global
 set remoteauthtimeout <seconds>
 end
```

The following changes need to be made to each SurePassID RADIUS server on the FortiGate as documented in the FortiGate Forum Repeated RADIUS Requests | Fortinet Technical Discussion Forums:

```
config user radius
 edit <radius_server_name>
 set timeout <seconds>
```

We recommend you start with <seconds> = 30. We recommend setting the SurePassID Mobile notifications setting to match the <seconds>.

Configuring Your Proxy Server

If your company uses a proxy server to monitor outbound traffic from your network to the cloud or your SurePassID MFA on-prem server, you will need to configure the RADIUS Server to use that proxy. Follow these steps:

a. Edit SurePassRadiusServerService.exe.config located in the same folder as SurePassRadiusServerService.exe.
b. You will need to make the following changes under the <configuration> element add the following xml.

```
<system.net>
<defaultProxy enabled="true" useDefaultCredentials="true">
<proxy proxyaddress="http://myproxy:80"
        usesystemdefault="true"
        bypassonlocal="true"
        autoDetect="true" />
</defaultProxy>
</system.net>
```

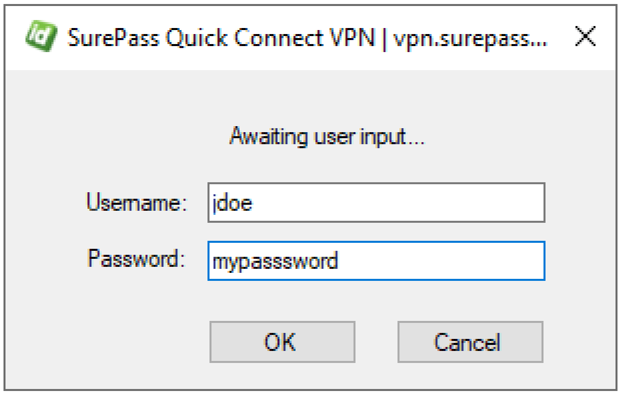
c. You need to modify myproxy:80 to your proxy server:port. Do not remove the leading http://.
d. Restart the **SurePassID RADIUS Server**.

VPN End-User Login Overview & Examples

Example 1 – Login Using Single-Factor

Logging into your VPN with single-factor authentication is a fairly straight forward and legacy process that requires only the username and password. Typically, you follow these steps:

1. Start VPN client software
2. Enter username
3. Enter password



SurePass Quick Connect VPN | vpn.surepass...

Awaiting user input...

Username: jdoe

Password: mypassword

Single-Factor VPN Login

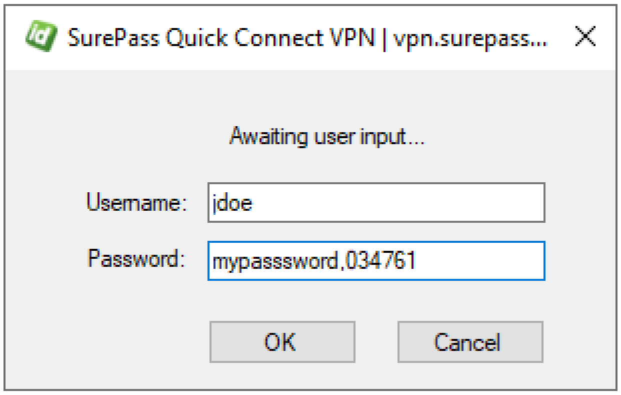
4. Press **OK** to login

When you use two-factor authentication, the process changes slightly because you will need to enter the second factor code in addition to the username and password.

Example 2 – Login Using Code from Hard or Soft Token

You will follow these steps if you have a device that displays a second factor code such as a hard token (OTP display smart card, key fob, etc.) or a soft token (SurePassID desktop token, mobile OTP apps such as Google Authenticator, Nymi Companion App, etc.)

1. Start VPN client software
2. Enter username
3. Enter password and concatenate the second factor code that is displayed from the device. In this example, the number displayed on the device is 034761 as show below:



SurePass Quick Connect VPN | vpn.surepass...

Awaiting user input...

Username: jdoe

Password: mypasssword,034761

Two-Factor Authentication with Token

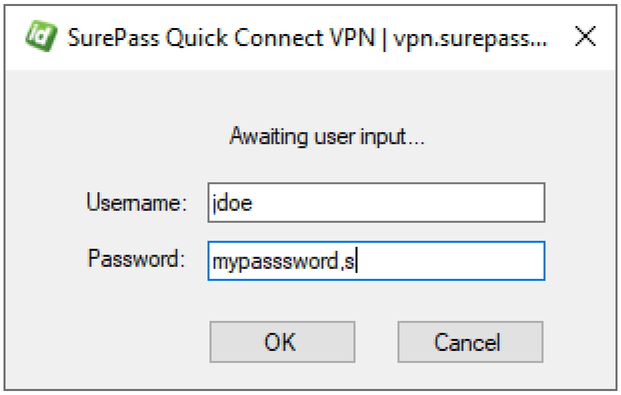
4. Press **OK** to login.

Example 3 – Login Using Sending OTP via SMS, Email or Voice Code

You will follow these steps if you want to have a second factor code sent to you via SMS Text, Voice Call, or Email:

1. Start VPN client software.
2. Enter username.
3. Enter your password followed by a method to send yourself a passcode to login.

    - Enter **s, 0,** or **SENDSMS** to have a code sent via text to your cell phone.


SurePass Quick Connect VPN | vpn.surepass...

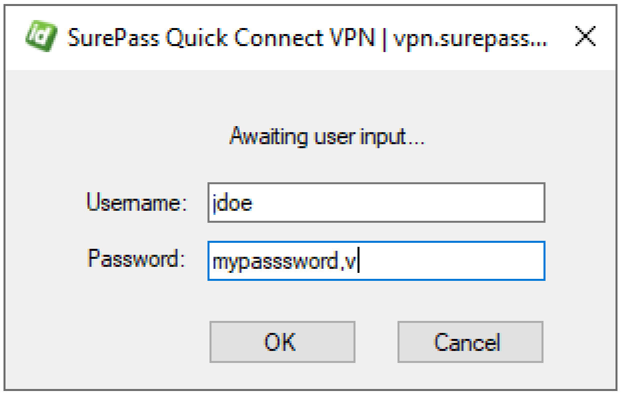
Awaiting user input...

Username: jdoe

Password: mypasssword,s

Two-Factor Authentication with SMS Text Code

- Enter **v**, **2, or SENDVOICE** to have an automated voice call made to your cell phone that will tell you a code.


SurePass Quick Connect VPN | vpn.surepass...

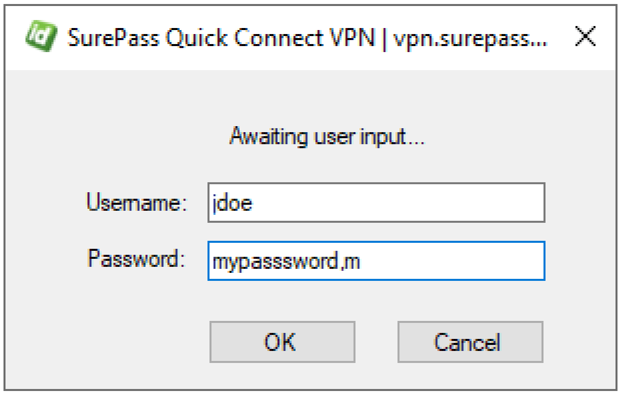
Awaiting user input...

Username: jdoe

Password: mypasssword,v

Two-Factor Authentication with Voice Call

- Enter **m,** 1, or **SENDEMAIL** to have a passcode sent via email.



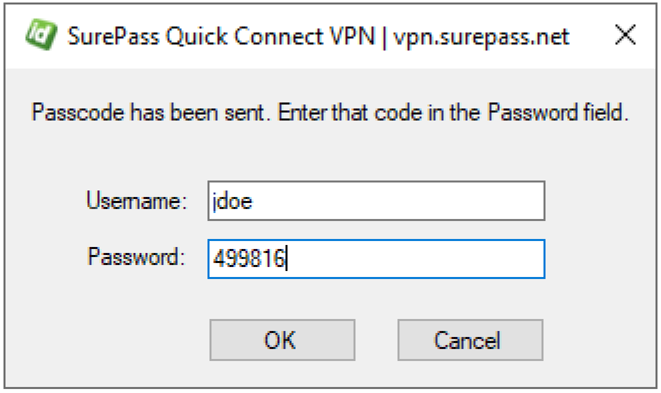
Awaiting user input...

Username: jdoe

Password: mypasssword,m

Two-Factor Authentication with Email

4. If your VPN supports RADIUS challenge/response, then you will receive the following message. Enter your code in the password field.

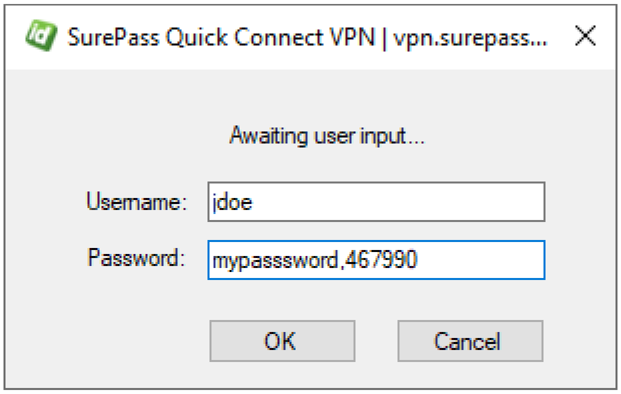


Passcode has been sent. Enter that code in the Password field.

Username: jdoe

Password: 499816

5. If your VPN does not support challenge response, then enter the password followed by a comma, followed by the code you have just received (no spaces after the password).



Awaiting user input...

Username: jdoe

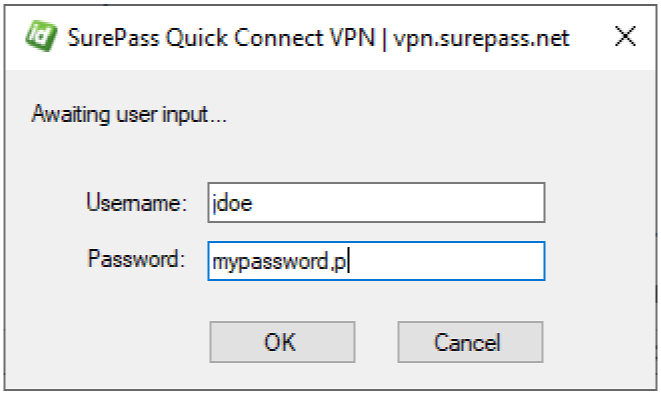
Password: mypasssword,467990

6. In either case press **OK** to login.

Example 4 – Login Using SMS Question

You will follow these steps if you want to secure yourself via an SMS approval question and not have to enter a code.

1. Start VPN client software.
2. Enter username.
3. Enter your password followed by a comma, and **p, ??,** or **PUSHSMS** to have an approval question sent via SMS text to your phone number on your account. You only need to reply to **y** or **yes** (not case sensitive) to the text message to have the second factor authenticated. If you did not request to be authenticated, you can respond with any other answer (such as **n** or **no**) and access will be denied.



SurePass Quick Connect VPN | vpn.surepass.net

Awaiting user input...

Username: jdoe

Password: mypassword,p

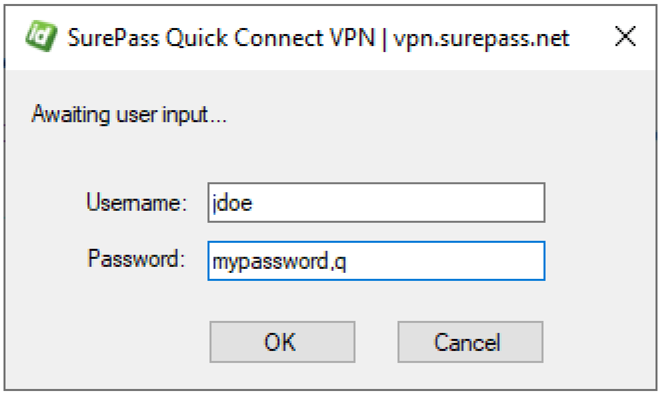
Two-Factor Authentication with SMS Question

4. Press **OK** to send a login question.
5. Wait for the question to be delivered via SMS to your mobile device.
6. Reply Yes (or Y) to the question to allow you to login in.
7. Wait for confirmation from the server that you have been authenticated on your phone.
8. You will be logged in without further action.

Example 5 – Login Using Push Authentication

You will follow these steps if you want to secure yourself via a push notification question and not have to enter a code. This authentication method requires that you have registered your token with SurePassID Mobile Authenticator and your account/token was configured for push notifications.

1. Start VPN client software.
2. Enter username.
3. Enter your password followed by a comma, and **q,?** or **PUSHAPPQUESTION** in the passcode to have a push notification request sent to your phone.



Awaiting user input...

Username: jdoe

Password: mypassword,q

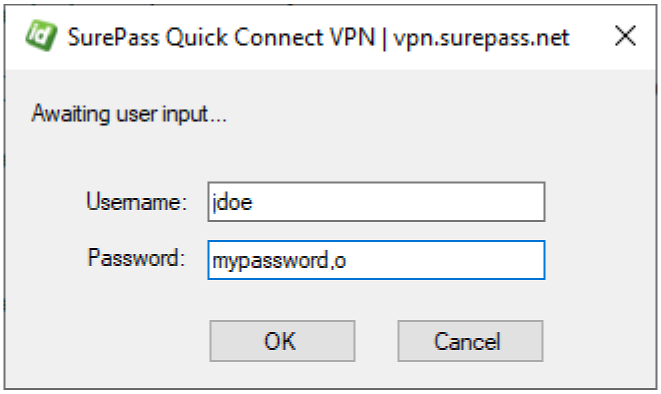
Two-Factor Authentication with Push Notification

4. Wait for the push notification question to be delivered to your mobile device.
5. On your mobile click **Authenticate** to approve the request or click **Cancel** to disallow the request.
6. If you clicked **Authenticate** you will be logged in without further action.

Example 6 – Login Using Push Voice Call

You will follow these steps if you want to secure yourself via a voice call notification. You will not have to enter a code. This requires that your account has been configured for to allows phone call to be made to your phone number

1. Start VPN client software.
2. Enter username.
3. Enter your password followed by a comma, and **o (the letter), #** or **PUSHVOICE** in the passcode to have a push notification request sent to your phone.


SurePass Quick Connect VPN | vpn.surepass.net

Awaiting user input...

Username: jdoe

Password: mypassword,o

Two-Factor Authentication with Voice Call Notification

4. Wait for the call on your phone.
5. Answer the call, listen to the message and take the required actions to allow or deny the request.
6. Wait for confirmation on your phone you have been authenticated on your phone and hang up.
7. You will be logged in without further action.