

# ServicePass Installation Guide

SurePassID Authentication Server 2021



SurePassID ServicePass Installation Guide Revision: 01012020.1

You can find the most up-to-date technical documentation at:

http://www.surepassid.com/resources

The SurePassID web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

support@surepassid.com

©2013- 2020 SurePassID, Inc. 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, Inc. 13750 W. Colonial Drive Winter Garden, FL 34787 www.surepassid.com



# **Table of Contents**

About SurePassID ServicePass	. 4
What is SurePassID ServicePass?	. 5
Prerequisites	6
System Security	7
User Security	7
Database	7
Internet Information Server	8
Post Configuration Steps	8
Installing and Configuring ServicePass	. 9
Customizing the System	14
Web.config	14
Notification Messages	16
Notification Message Customization	16
Default Language	17



## About SurePassID ServicePass

This guide explains how to install and configure SurePassID ServicePass Self-Service Portal (SSP). The purpose of this guide is to provide a reference for system administrators.

This guide provides information on the following topics:

- What is SurePassID ServicePass?
  - A brief introduction to the ServicePass
- Installing and Configuring ServicePass
  - Detailed explanations for installing ServicePass

#### Other SurePassID Guides

ServicePass has the following companion guides that provide additional detail on specific topics for SurePassID:

- Server API Guide
- FIDO U2F Mobile API Guide
- <u>System Administration Guide</u>
- Local Agent Guide
  - High performance Radius Server
  - Windows Event Log Integration
  - Active Directory Synchronization
- Desktop OTP Authenticator Guide
- <u>Google Authenticator Guide</u>
- Windows Login Authentication Guide



## What is SurePassID ServicePass?

SurePassID ServicePass is a web based self-service portal that allows users to manage their One-Time Password (OTP), Card Security Codes (dynamic CVx) and FIDO U2F security tokens. ServicePass is delivered in both an out-of-the-box installable image that allows for simple stylistic changes such as CSS style sheets and corporate logo's. It also serves as an open source solution that can be completely customized and enhanced for virtually any support situation.

ServicePass offers users all the functionality they need to manage their strong authentication tokens, eliminating the costs associated with help desk calls. ServicePass uses the <u>SurePassID API's</u> (REST and Windows WCF) allowing for complete integration into existing intranet, extranet and internet enterprise service desk applications while serving as the foundation for newly developed self-service applications.



Below is a high level architectural view.

This document focuses on the areas in the green boxes.



## Prerequisites

SurePassID Server can be installed on the following Windows versions:

- Windows Server 2012 All versions
- Windows Server 2016 All versions
- Windows 7 Professional & Ultimate
- Windows 8 Professional & Ultimate
- Windows 10

#### **Supported Tokens**

ServicePass supports all the security tokens that SurePassID Server supports:

Soft Tokens:

- SurePassID Mobile Authenticator (OATH & dCVV)
- SurePassID Desktop Authenticator
- SurePassID Push OTP Technologies (SMS, Email, SMS challenge response, U2F)
- Mobile OTP
- SurePassID Google Authenticator
- SurePassID FIDO U2F Virtual Devices

#### Hard Tokens:

- SurePassID TapID
- SurePassID Display Card
- SurePassID TapID Treo
- SurePassID OTP Key FOB
- OATH compatible device

#### Self-Service Functions

ServicePass offers all the functionality users need to manage their soft and hardware tokens. The ServicePass provides the following capabilities:

- Token Activation & Registration
- Token Synchronization
- Lost Token Disablement and Re-Issuance
- Automated Notifications
- Password Reset
- SurePassID API Advanced features



• Integration into 3<sup>rd</sup> Party applications

### System Security

SurePassID ServicePass <u>does not</u> install with any certificates for SSL. You must configure ServicePass (IIS web app) for SSL using corporate certificates for production or create self-signed certificates for testing.

It is recommended that ServicePass is configured to communicate to the SurePassID Authentication Server using transport level security (https) on a specific port (see Customizing the System section). <u>The firewall should be configured to only allow communications on that port from the ServicePass server IP.</u>

The ServicePass configuration file can limit the types of REST API requests that will be permitted. It is important that you only allow the requests that your mobile app supports.

For ultra-secure operations, ServicePass can be daisy chained across many servers.

It is recommended that you follow security best practices for deploying mobile applications.

#### User Security

ServicePass is delivered as a secure system. Users accessing ServicePass are required to provide their Windows Active Directory, LDAP or SurePassID username and password. By default, ServicePass also requires two factor authentication for access to the self-service portal. The reason for this is simple:

# Adding/modifying a security token requires absolute proofing of the individual. Username and password alone are insufficient.

In situations where the user's two factor authentication token has not been issued (or not functioning properly) ServicePass can send a passcode to the user via email, SMS or SMS challenge response to securely authenticate the user.

For certain applications such as intranet portals, this can be turned off.

#### Database

The system does not require any database access.



## Request Logging

The system does support request logging. Logging captures the payload and IP of the requesting application. By default the logs will be persisted in the local file in the local file system. Alternatively, they can be sent to the Windows Event Log for persistence, trouble shooting or further analysis.

#### Internet Information Server

The Windows server must have the IIS feature enabled.

## Post Configuration Steps

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

- Set up TLS for the ServicePass IIS virtual directory.
- Rename the ServicePass IIS virtual directory to something that conforms to your standards.
- Update DNS (internal or external depending on the use) to allow for access to the ServicePass via A record or CNAME.
- Customize the web.config file as per the <u>Customizing the System section</u>
- 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



## Installing and Configuring ServicePass

SurePassID ServicePass is distributed as a Windows msi installer file (ServicePass2017.exe) located in a zip file (SPPASS.ZIP).

After downloading and unzipping **SPPASS.ZIP** locate the file **ServicePass2017.exe** file, copy the file to the appropriate Windows server (if not already there) and run **ServicePass2017** to install the system. The following window will be displayed.

User Account Control	×	
Do you want to allow this app to make changes to your device?		
<b>Ore Passid Service</b>	Pass 2017	
Verified publisher: SurePassID Corp. File origin: Hard drive on this computer		
Show more details		
Yes	No	

Click Yes.





#### Click Next.

Q SurePassId ServicePass 2017 Setup	_		×
Select Installation Folder			
This is the folder where SurePassId ServicePass 2017 will be installed.			Ë
To install in this folder, dick "Next". To install to a different folder, ent "Browse".	er it belov	w or click	
Eolder:			
C:\Program Files (x86)\SurePassID Corp\SurePassId ServicePass $ \smallsetminus $	Br		
Advanced Installer			
< <u>B</u> ack <u>N</u> ext >		Cance	el

Click Next.





#### Click Install.

🦉 SurePassId Se	rvicePass 2017 Setup	×
Installing Su	ırePassId ServicePass 2017	51
Please wai take sever	it while the Setup Wizard installs SurePassId ServicePass 2017. This may ral minutes.	
Status:	Installing new services	
Advanced Installer		
	< <u>B</u> ack <u>N</u> ext > Cancel	

You will see files being installed and IIS being configured. When completed, you will see:





Click Finish. ServicePass will be started and you will see the following screen:



Sure Pass (2) Service Pass Portal		
Welcome to the ServicePass self-service portal.	S It appears the system has not been configured yet and will not function properely until you make a few minor changes. Please check out the install guide and check the section of configuration.	
The portal will allow you to manage all of your security tokens. First you must login to your account. Start by entering your username and password and pressing the Login button.	Login   Username:   Password:   Login Forgot Password?	
	© 1999-2017 SurePassId Corp. All rights reserved.	

This screen informs you that the system is installed and ready and needs to be customized before it can be used. Once you customize the system, this message will no longer appear. The next section will provide you with the information you need to customize the system to use your instance of SurePassID Authentication Server and specify default functionality for your user base.



# **Customizing the System**

When installation is completed, you will have fully functioning system, however, it cannot properly service requests until you configure and tailor the system to your company's requirements.

Customizations are made in the **web.config** file located in the root folder of the SurePass installation. Local customizations are made by each tenant using the SurePassID Admin portal.

## 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 suit 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:

Parameter	Description	
Server.RESTEndPoint	The SurePassID server endpoint that will process all ServicePass	
	requests.	
	<ul> <li>Sandbox – SurePassID cloud sandbox</li> </ul>	
	<ul> <li>Prod – SurePassID production cloud system</li> </ul>	
	Use the SurePassID on-premises url	
Server.CompanyAccount	Your account in the SurePassID Authentication server. Only	
	used if Server.AllowSubDomains = FALSE.	
Server.CompanyAccountKey	Your account key in the SurePassID Authentication server. Only	
	used if Server.AllowSubDomains = FALSE.	
Server.Company_ <url>_Account</url>	Maps a URL to a SurePassID tenant account. Only used if	
	Server.AllowSubDomains = TRUE. Substitute <url> with the URL</url>	
	that points to ServicePass.	
Server.Company_ <url>_Key</url>	Maps a URL to a SurePassID tenant account key. Only used if	
	Server.AllowSubDomains = TRUE. Substitute <url> with the URL</url>	
	that points to ServicePass.	
Server.AllowSubDomains	TRUE – ServicePass will map a URL to a specific SurePassID MFA	
	server tenant. One of more Server.Company_ <url>_Account and</url>	
	Server.Company_ <url>_Key pairs must be defined.</url>	
	FALSE – Ignore the URL and always you Server.CompanyAccount	
	and Server.CompanyAccountKey to identity the SurePassID MFA	
	server tenant	

### <configuration><appsettings> keys



SurePassID Authentication server. The log output is stored in the Trace subfolder of the installation folder.           Server.2FARequired         D=Zfa mandatory. User can use sms, email, or push notification if they do not have a token assigned to them yet. 1=no Zfa, single factor only 2=2fa required if the user has a token assigned to them. If not, single factor is okay. Good for intranet.           Server.AppId         FIDO U2F AppIC. This will be the viri of the ServicePassID DNS name or the FIDO U2F Facet URL.           Server.PushRelyingPartyAppAuthURL         When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.           Server. EdgeHeaderKey         The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to on the meader.           Server. DefaultFromEmailAddress         Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.           Server.DefaultFromEmailName         Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.           Server.DefaultFromEmailName         Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.           Server.DefaultFromEmailName         Optional: Email FROM name when sending email notifications, overriding the values are: • FIDO U2F - Any FIDO U2F token           Server.DefaultFromEmailName         Optional: Email FROM name when sending email notif	Server.Trace	Logs all activity that passes from the ServicePass to the
Iter Trace subfolder of the installation folder.           Server.2FARequired         0=2fa mandatory. User can use sms, email, or push notification if they do not have a token assigned to them yet. 1=no 2fa, single factor is okay. Good for intranet.           Server.AppId         FIDO U2F AppId. This will be the url of the ServicePassID DNS name or the FIDO U2F Facet URL.           Server.PushRelyingPartyAppAuthURL         When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.           Server. EdgeHeaderKey         The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.           Server. EdgeHeaderValue         The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.           Server. EdgeHeaderValue         The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.           Server. EdgeHeaderValue         The custom header value that will be sent to SurePassID Server.           Server.DefaultFromEmailName         Optional: Email FROM ame when sending email notifications, overriding the values in the SurePassID Server.           Server.DefaultFromEmailName         Optional: Email FROM anderesusID appID rec token		SurePassID Authentication server. The log output is stored in
Server.2FARequired       0=2fa mandatory. User can use sms, email, or push notification if they do not have a token assigned to them yet.         1=no 2fa, single factor only       2=2fa required if the user has a token assigned to them. If not, single factor is okay. Good for intranet.         Server.Appid       FIDO U2F Appid. This will be the url of the ServicePassID DNS name or the FIDO U2F Facet URL.         Server.PushRelyingPartyAppAuthURL       When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.         Server. EdgeHeaderKey       The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.         Server. EdgeHeaderValue       The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server.DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the surePassID Server.         Server.DefaultFromEmailName       Optio		the <b>Trace</b> subfolder of the installation folder.
if they do not have a token assigned to them yet.         1=no 2(a, single factor not)         2=2fa required if the user has a token assigned to them. If not, single factor is okay, Good for intranet.         Server.Appid       FIDO U2F Appl. This will be the url of the ServicePassID DNS name or the FIDO U2F Facet URL.         Server.PushRelyingPartyAppAuthURL       When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.         Server. EdgeHeaderKey       The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server. DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM address wenthen sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEromEmailName       Format of email notifications sent to the user (forgot password and password change, etc.) .         in thrd - send in thrufforations       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         FIDOUZE Pany FIDO U2F token	Server.2FARequired	0=2fa mandatory. User can use sms, email, or push notification
1=no 2fa, single factor only         2=2fa required if the user has a token assigned to them. If not, single factor is okay. Good for intranet.         Server.Appid       FIDO U2F Appid. This will be the url of the ServicePassID DNS name or the FIDO U2F Facet URL.         Server.PushRelyingPartyAppAuthURL       When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.         Server. EdgeHeaderKey       The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server.DefaultFromEmailAddress       Optional: Email FROM andere when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM fame when users register a new FIDO token to their account. Values are:         Server.DefaultEmailFormat       Format of email notifications sent to the user forgot password and password thange, etc.).         Server.DefaultNewSoftToken       The default FIDO		if they do not have a token assigned to them yet.
2=2fa required if the user has a token assigned to them. If not, single factor is okay, Good for intranet.         Server.Appld       FIDO U2F Appld. This will be the url of the ServicePassID DNS name or the FIOO U2F Facet URL.         Server.PushRelyingPartyAppAuthURL       When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.         Server. EdgeHeaderKey       The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse prox/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse prox/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server.DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.) .         Server.DefaultEmailFormat       The default FIDO U2F token type when users register a new FIDD token to their account. Values are:         FIDOU2F - Any FIDO U2F token       The OATH token type when user adds a new soft token to their account. Values are:         Server.DefaultNewSoftToken <td< td=""><td></td><td>1=no 2fa, single factor only</td></td<>		1=no 2fa, single factor only
single factor is okay. Good for intranet.           Server.Appid         FIDO U2F Appid. This will be the url of the ServicePassID DNS name or the FIDO U2F Facet URL.           Server.PushRelyingPartyAppAuthURL         When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.           Server. EdgeHeaderKey         The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.           Server. EdgeHeaderValue         The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.           Server.DefaultFromEmailAddress         Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.           Server.DefaultFromEmailName         Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.           Server.DefaultEmailFormat         Format of email notifications sent to the user (forgot password and password change, etc.).           Server.DefaultEmailFormat         Format of email notifications sent to the user segister a new FIDO token to their account. Values are:		2=2fa required if the user has a token assigned to them. If not,
Server.AppId       FIDD U2F AppId. This will be the url of the ServicePassID DNS name or the FIDD U2F Facet URL.         Server.PushRelyingPartyAppAuthURL       When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.         Server. EdgeHeaderKey       The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server.DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.) .         Server.DefaultEmailFormat       The default FIDD U2F token type when users register a new FIDD token to their account. Values are:         Server.DefaultNewSoftToken       The default FIDD U2F token type when users token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.ActivateSPMobileURL<		single factor is okay. Good for intranet.
name or the FIDD U2F Facet URL.           Server.PushRelyingPartyAppAuthURL         When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.           Server. EdgeHeaderKey         The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.           Server. EdgeHeaderValue         The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.           Server. DefaultFromEmailAddress         Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.           Server.DefaultFromEmailName         Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.           Server.DefaultEmailFormat         Format of email notifications sent to the user (forgot password and password change, etc.).           Server.DefaultEweWU2FToken         The default FIDO U2F token type when users register a new FIDO token to their account. Values are:           Server.DefaultNewSoftToken         The OATH token type when user adds a new soft token to their account. Values are:           Server.DefaultNewSoftToken         The OATH token type when user adds a new soft token to their account. Values are:           Server.ActivateSPMobileURL         The URL that is a server endpoint for o	Server.Appld	FIDO U2F AppId. This will be the url of the ServicePassID DNS
Server.PushRelyingPartyAppAuthURL       When the user requests a push question sent to their mobile to login, this is what will be displayed in the message as the requesting system.         Server. EdgeHeaderKey       The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server. DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the surePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.) .         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.ActivateSPMobileURL       The UATH that is a server endpoint for over the air activations. The form is https://serverendpointb.cathen.app.         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:		name or the FIDO U2F Facet URL.
login, this is what will be displayed in the message as the requesting system.         Server. EdgeHeaderKey       The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server. DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https://serverendpoint/sothen app.         Server.DefaultNewSoftToken       The URL that is a server endpoint for over the air activations. The form is https://serverendpoints/sothen app.         Server.ActivateSPMobileURL       The URL that is a server endpoint	Server.PushRelyingPartyAppAuthURL	When the user requests a push question sent to their mobile to
Server. EdgeHeaderKey       The custom header name that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a come header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server. DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https://cserver endpoint/cost-ota-provision/ where <serverendpoint>/csst-ota-provision/ where <serverendpoint>/s a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint</serverendpoint></serverendpoint>		login, this is what will be displayed in the message as the
Server. EdgeHeaderKey       The custom header name that will be sent to SurePassID MFA         server. The value can be tested at any edge reverse proxy/load       balancer such to confirm trusted the traffic is from a trusted         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA         Server. DefaultFromEmailAddress       Optional: Email FROM address when sending email         Server.DefaultFromEmailName       Optional: Email FROM address when sending email         Server.DefaultFromEmailName       Optional: Email FROM name when sending email         Server.DefaultEromEmailName       Optional: Email FROM name when sending email         Server.DefaultEromEmailName       Optional: Email FROM name when sending email         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.DefaultNewSoftToken       The URL that is a server endpoint for over the air activations. The form is https://sserverendpoints/oath-ota provision/ where <serverendpoints a="" api="" auth="" connector="" endpoint="" mobile="" or="" server="" ss="" surepassid="" surepassid<="" td=""><td></td><td>requesting system.</td></serverendpoints>		requesting system.
server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.           Server. EdgeHeaderValue         The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.           Server. DefaultFromEmailAddress         Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.           Server. DefaultFromEmailName         Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.           Server.DefaultEmailFormat         Format of email notifications sent to the user (forgot password and password change, etc.).           Server.DefaultNewU2FToken         The default FIDO U2F token type when users register a new FIDO token to their account. Values are: • FIDOU2F – Any FIDO U2F token           Server.DefaultNewU2FToken         The OATH token type when user adds a new soft token to their account. Values are: • DesktopAuthenticator - SurePassID desktop token • GoogleAuthenticator - Google Authenticator token           Server.ActivateSPMobileURL         The URL that is a server endpoint for over the air activations. The form is https://sserverendpoint/s a SurePassID Auth Server endpoint or SurePassID Mubile API connector endpoint           Allow.TokenDisable         TRUE – Allow user to add soft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account. <td>Server. EdgeHeaderKey</td> <td>The custom header name that will be sent to SurePassID MFA</td>	Server. EdgeHeaderKey	The custom header name that will be sent to SurePassID MFA
balancer such to confirm trusted the traffic is from a trusted endpoint. Leave blank to not send a custom header.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server.DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:		server. The value can be tested at any edge reverse proxy/load
endpoint.       Leave blank to not send a custom header.         Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA server. The value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server.DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https://cserverendpoints/oath-ota-provision/ where cserverendpoints /s a SurePassID Authenticator token         Allow.SoftToken       TRUE – Allow user to ads oft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to adsoft tokens that are already assigned to their account.		balancer such to confirm trusted the traffic is from a trusted
Server. EdgeHeaderValue       The custom header value that will be sent to SurePassID MFA         server. The value can be tested at any edge reverse proxy/load       balancer such to confirm trusted the traffic is from a trusted         Server.DefaultFromEmailAddress       Optional: Email FROM address when sending email         Notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications,         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The default FIDO U2F token type when users register a new of token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https://serverendpoints/oath-ota-provision/ where cserverendpoints is a SurePassID Auth Server endpoint or S		endpoint. Leave blank to not send a custom header.
Server. The Value can be tested at any edge reverse proxy/load balancer such to confirm trusted the traffic is from a trusted endpoint.         Server.DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https://serverendpoints/oath-ota-provision/ where <serverendpoints a="" account.<="" and="" api="" auth="" connector="" endpoint="" is="" mobile="" or="" server="" serversion="" surepassid="" surger="" td="" their="" to="" wassigned="">         Allow.TokenDisable       TRUE – Allow user to adds oft tokens to their account FALSE – Users cannot disable their tokens         Allow.TokenDisable       TRUE – Allow user to disable their tokens</serverendpoints>	Server. EdgeHeaderValue	The custom header value that will be sent to SurePassID MFA
balancer such to contirm trusted the traffic is from a trusted endpoint.         Server.DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are: • FIDO U2F – Any FIDO U2F token         Server.DefaultNewU2FToken       The OATH token type when users register a new FIDO token to their account. Values are: • Treo- SurePassID TapID Treo token         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are: • DesktopAuthenticator - Google Authenticator token • GoogleAuthenticator Mobile – SurePassID authenticator soft token app.         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https://serverendpoint>/oath-ota-provision/ where <serverendpoint> is a SurePassID Authenticacount FALSE – Users can only activate soft tokens to their account.         Allow.SoftTokenCreation       TRUE – Allow user to adds oft tokens to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens FALSE – Users can only activate soft tokens to their account.</serverendpoint>		server. The value can be tested at any edge reverse proxy/load
Server.DefaultFromEmailAddress       Optional: Email FROM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.) .         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.) .         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https://cserverendpoints/oath-ota-provision/ where <serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE – Allow user to ads oft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens         FALSE – Users can only activate soft tokens that are already assigned to their account.       FALSE – Users can only activate soft tokens that are already assigne</serverendpoint>		balancer such to confirm trusted the traffic is from a trusted
Server.DefaultPromemailAddress       Optional: Email RFOM address when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultErromEmailName       Optional: Email RFOM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.) .         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https:// <serverendpoints oath-ota-provision="" where<br=""><serverendpoints a="" auth="" endpoint="" is="" or<br="" server="" surepassid="">SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE – Allow user to disable their tokens         Allow.TokenDisable       TRUE – Allow user to disable their tokens         Allow.TokenDisable       TRUE – Allow user to disable their tokens         Allow.TokenDisable       TRUE – Allow user to disable their tokens</serverendpoints></serverendpoints>		endpoint.
Server.DefaultFromEmailName       Optional: Email FROM name when sending email notifications, overriding the values in the SurePassID Server.         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.) . <ul> <li>html – send in html format</li> <li>text – send in plain text format</li> <li>text – send in plain text format</li> </ul> Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are: <ul> <li>FIDOU2F – Any FIDO U2F token</li> <li>The OATH token type when user segister a new FIDO token to their account. Values are:             <ul> <li>FIDOU2F – Any FIDO U2F token</li> <li>The OATH token type when user segister to their account. Values are:             <ul> <li>DesktopAuthenticator – SurePassID desktop token</li> <li>GoogleAuthenticator – Google Authenticator token</li> <li>SurePassIDAuthenticator Mobile – SurePassID authenticator soft token app.</li> </ul> </li> <li>Server.ActivateSPMobileURL</li> <li>The URL that is a server endpoint for over the air activations. The form is https://cserverendpoints/oath-ota-provision/ where <serverendpoints a="" api="" auth="" connector="" endpoint="" endpoint<="" is="" li="" mobile="" or="" server="" surepassid=""> <li>Allow.SoftToken</li> <li>TRUE – Allow user to ads oft tokens to their account FALSE – Users cannot disable their tokens</li> <li>Allow.TokenDisable</li> <li>TRUE – Allow user to enable their tokens</li> <li>Allow user to enable their tokens</li> </serverendpoints></li></ul></li></ul>	Server.DelauteromemanAddress	optional: Email FROM address when sending email
Server.DefaultProlifemativative       Optional: Entail Provide and password and password change, etc.).         Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         •       html – send in html format         •       text – send in plain text format         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         •       FIDOUZF – Any FIDO U2F token         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         •       DesktopAuthenticator – SurePassID desktop token         •       GogleAuthenticator – SurePassID desktop token         •       Server.ActivateSPMobileURL         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https://serverendpoints/oath-ota-provision/ where <serverendpoints a="" auth="" authber="" endpoint="" endpoint<="" is="" or="" server="" surepassid="" td="">         Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account FALSE – Users cannot disable their tokens         Allow.TokenDisable       TRUE – Allow user to disable their tokens         Allow.TokenEnable       TRUE – Allow user to disable their tokens</serverendpoints>	Sonuer DefaultFromEmailName	Optional Empil EPOM name when conding amail patifications
Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         •       html – send in html format         •       text – send in plain text format         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         •       FIDOU2F – Any FIDO U2F token         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         •       DesktopAuthenticator - SurePassID desktop token         •       GoogleAuthenticator - Google Authenticator token         •       Server.ActivateSPMobileURL         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https:// <serverendpoint>/oath-ota-provision/ where         SurePassID Mobile API Connector endpoint       TRUE – Allow user to add soft tokens to their account         Allow.TokenDisable       TRUE – Allow user to disable their tokens         Allow.TokenDisable       TRUE – Allow user to cannot disable their tokens</serverendpoint>	Server.Delauteromemaniname	Optional: Email FROM name when sending email notifications,
Server.DefaultEmailFormat       Format of email notifications sent to the user (forgot password and password change, etc.).         •       html – send in html format         •       text – send in plain text format         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are:         •       FIDOU2F – Any FIDO U2F token         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         •       DesktopAuthenticator - SurePassID desktop token         •       GoogleAuthenticator - Google Authenticator token         •       SurePassIDAuthenticator of token app.         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https:// <serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint         Allow.SoftToken       TRUE – Allow user to add soft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to enable their tokens         Allow.TokenDisable       TRUE – Allow user to enable their tokens</serverendpoint>		overhuing the values in the surerassid server.
and password change, etc.).       • html – send in html format         • text – send in plain text format         Server.DefaultNewU2FToken         The default FIDO U2F token type when users register a new         FIDO token to their account. Values are:         • FIDOU2F – Any FIDO U2F token         Server.DefaultNewSoftToken         Server.DefaultNewSoftToken         The OATH token type when user adds a new soft token to their account. Values are:         • DesktopAuthenticator - SurePassID desktop token         • GoogleAuthenticator - Google Authenticator token         • SurePassIDAuthenticator of token app.         Server.ActivateSPMobileURL         The URL that is a server endpoint for over the air activations. The form is https:// <serverendpoint>/oath-ota-provision/ where         - serverendpoint&gt; is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens         Allow.TokenEnable       TRUE – Allow user to enable their tokens</serverendpoint>	Server.DefaultEmailFormat	Format of email notifications sent to the user (forgot password
•       html – send in html format         •       text – send in plain text format         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new FIDO token to their account. Values are: <ul> <li>•</li> <li>FIDOU2F – Any FIDO U2F token</li> <li>•</li> <li>Freo- SurePassID TapID Treo token</li> </ul> Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are: <ul> <li>•</li> <li>DesktopAuthenticator - SurePassID desktop token</li> <li>•</li> <li>GoogleAuthenticator - Google Authenticator token</li> <li>•</li> <li>SurePassIDAuthenticator Mobile – SurePassID authenticator soft token app.</li> </ul> Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is <a cserverendpoint="" href="https://cserverendpoint&gt;/oath-ota-provision/where&lt;/a&gt; &lt;a href=" https:="">/oath-ota-provision/where</a> <a cserverendpoint="" href="https://cserverendpoint&gt;/oath-ota-provision/where&lt;/a&gt; &lt;a href=" htttps:="">/oath-ota-provision/where</a> <a< td=""><td></td><td>and password change, etc.) .</td></a<>		and password change, etc.) .
• text – send in plain text format         Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new         FIDO token to their account. Values are:       • FIDOU2F – Any FIDO U2F token         • Treo- SurePassID TapID Treo token       • Treo- SurePassID TapID Treo token         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         • DesktopAuthenticator - SurePassID desktop token       • GoogleAuthenticator - Google Authenticator token         • SurePassIDAuthenticator - Google Authenticator token       • SurePassIDAuthenticator soft token app.         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is <a href="https://serverendpoint&gt;/oath-ota-provision/">https://serverendpoint&gt;/oath-ota-provision/</a> where <a href="https://serverendpoint&gt;" serverendpoint"="">server endpoint or SurePassID Mobile API Connector endpoint</a> Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account         FALSE – Users can only activate soft tokens that are already assigned to their account.       TRUE – Allow user to disable their tokens         Allow.TokenDisable       TRUE – Allow user to enable their tokens         Allow.TokenEnable       TRUE – Allow user to penable their tokens		<ul> <li>html – send in html format</li> </ul>
Server.DefaultNewU2FToken       The default FIDO U2F token type when users register a new         FIDO token to their account. Values are:       •         •       FIDOU2F – Any FIDO U2F token         •       Treo- SurePassID TapID Treo token         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         •       DesktopAuthenticator - SurePassID desktop token         •       GoogleAuthenticator - Google Authenticator token         •       SurePassIDAuthenticator Mobile – SurePassID authenticator soft token app.         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is https://serverendpoints/oath-ota-provision/ where <serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account         FALSE – Users cannot disable their tokens       FALSE – Users cannot disable their tokens         Allow.TokenDisable       TRUE – Allow user to adisable their tokens         FALSE – Users cannot disable their tokens       FALSE – Users cannot disable their tokens</serverendpoint>		<ul> <li>text – send in plain text format</li> </ul>
Server.DefaultNewU2FTokenThe default FIDO U2F token type when users register a new FIDO token to their account. Values are: 		
FIDO token to their account. Values are:• FIDOU2F – Any FIDO U2F token• Treo- SurePassID TapID Treo tokenServer.DefaultNewSoftTokenThe OATH token type when user adds a new soft token to their account. Values are:• DesktopAuthenticator - SurePassID desktop token• GoogleAuthenticator – Google Authenticator token• SurePassIDAuthenticator – Google Authenticator token• SurePassIDAuthenticator of token app.Server.ActivateSPMobileURLThe URL that is a server endpoint for over the air activations. The form is <a href="https://serverendpoint&gt;/oath-ota-provision/">https://serverendpoint&gt;/oath-ota-provision/</a> where <serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpointAllow.SoftTokenCreationTRUE – Allow user to add soft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account.Allow.TokenDisableTRUE – Allow user to disable their tokens FALSE – Users cannot disable their tokensAllow.TokenEnableTRUE – Allow user to enable their tokens</serverendpoint>	Server.DefaultNewU2FToken	The default FIDO U2F token type when users register a new
• FIDOU2F – Any FIDO U2F token         • Treo- SurePassID TapID Treo token         Server.DefaultNewSoftToken         The OATH token type when user adds a new soft token to their account. Values are:         • DesktopAuthenticator - SurePassID desktop token         • GoogleAuthenticator - Google Authenticator token         • SurePassIDAuthenticator - Google Authenticator token         • SurePassIDAuthenticator of token app.         Server.ActivateSPMobileURL         The URL that is a server endpoint for over the air activations. The form is <a href="https://serverendpoints/oath-ota-provision/">https://serverendpoints/oath-ota-provision/</a> where <a href="https://serverendpoints/oath-ota-provision/">server.ActivateSPMobileURL         Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account         FALSE – Users can only activate soft tokens that are already assigned to their account.       TRUE – Allow user to disable their tokens         Allow.TokenDisable       TRUE – Allow user to disable their tokens         Allow.TokenEnable       TRUE – Allow user to enable their tokens</a>		FIDO token to their account. Values are:
• Treo- SurePassID TapID Treo token         Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are: <ul> <li>DesktopAuthenticator - SurePassID desktop token</li> <li>GoogleAuthenticator - Google Authenticator token</li> <li>SurePassIDAuthenticatorMobile – SurePassID</li> <li>authenticator soft token app.</li> </ul> Server.ActivateSPMobileURL           Server.ActivateSPMobileURL         The URL that is a server endpoint for over the air activations. The form is <a href="https://serverendpoint">https://serverendpoint&gt;/oath-ota-provision/</a> where <serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint           Allow.SoftTokenCreation         TRUE – Allow user to add soft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account.           Allow.TokenDisable         TRUE – Allow user to disable their tokens FALSE – Users cannot disable their tokens           Allow.TokenDisable         TRUE – Allow user to enable their tokens</serverendpoint>		<ul> <li>FIDOU2F – Any FIDO U2F token</li> </ul>
Server.DefaultNewSoftToken       The OATH token type when user adds a new soft token to their account. Values are:         • DesktopAuthenticator - SurePassID desktop token         • GoogleAuthenticator - Google Authenticator token         • SurePassIDAuthenticator Mobile - SurePassID         authenticator soft token app.         Server.ActivateSPMobileURL         The URL that is a server endpoint for over the air activations. The form is <a href="https://serverendpoints/oath-ota-provision/">https://serverendpoints/oath-ota-provision/</a> where <serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE - Allow user to add soft tokens to their account fALSE - Users can only activate soft tokens         Allow.TokenDisable       TRUE - Allow user to disable their tokens         Allow.TokenEnable       TRUE - Allow user to enable their tokens</serverendpoint>		Treo- SurePassID TapID Treo token
Allow.TokenDisable     TRUE – Allow user to enable their tokens	Server.DefaultNewSoftToken	The OATH token type when user adds a new soft token to their
GoogleAuthenticator – Google Authenticator token     GoogleAuthenticator – Google Authenticator token     SurePassIDAuthenticatorMobile – SurePassID     authenticator soft token app.     Server.ActivateSPMobileURL     The URL that is a server endpoint for over the air activations. The     form is https:// <serverendpoint>/oath-ota-provision/ where     <serverendpoint> is a SurePassID Auth Server endpoint or     SurePassID Mobile API Connector endpoint     Allow.SoftTokenCreation     TRUE – Allow user to add soft tokens to their account     FALSE – Users can only activate soft tokens that are already     assigned to their account.     Allow.TokenDisable     TRUE – Allow user to disable their tokens     FALSE – Users cannot disable their tokens     FALSE – Users cannot disable their tokens     FALSE – Users cannot disable their tokens</serverendpoint></serverendpoint>		DesktonAuthenticator - SurePassID deskton token
SurePassIDAuthenticator Mobile – SurePassID     authenticator soft token app. Server.ActivateSPMobileURL The URL that is a server endpoint for over the air activations. The form is https:// <serverendpoint>/oath-ota-provision/ where <serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint Allow.SoftTokenCreation TRUE – Allow user to add soft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account. Allow.TokenDisable TRUE – Allow user to disable their tokens FALSE – Users cannot disable their tokens Allow.TokenEnable TRUE – Allow user to enable their tokens</serverendpoint></serverendpoint>		GoogleAuthenticator – Google Authenticator token
authenticator soft token app.         Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is <a href="https://serverendpoints/oath-ota-provision/">https://serverendpoints/oath-ota-provision/</a> where <serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens FALSE – Users cannot disable their tokens         Allow.TokenEnable       TRUE – Allow user to enable their tokens</serverendpoint>		SurePassIDAuthenticatorMobile – SurePassID
Server.ActivateSPMobileURL       The URL that is a server endpoint for over the air activations. The form is <a href="https://serverendpoint&gt;/oath-ota-provision/">https://serverendpoint&gt;/oath-ota-provision/</a> where <serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens FALSE – Users cannot disable their tokens         Allow.TokenEnable       TRUE – Allow user to enable their tokens</serverendpoint>		authenticator soft token app.
form is https:// <serverendpoint>/oath-ota-provision/ where         <serverendpoint> is a SurePassID Auth Server endpoint or         SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account         FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens         FALSE – Users cannot disable their tokens         FALSE – Users cannot disable their tokens         FALSE – Users cannot disable their tokens</serverendpoint></serverendpoint>	Server.ActivateSPMobileURL	The URL that is a server endpoint for over the air activations. The
<serverendpoint> is a SurePassID Auth Server endpoint or SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens FALSE – Users cannot disable their tokens         Allow.TokenEnable       TRUE – Allow user to enable their tokens</serverendpoint>		form is <u>https://<serverendpoint>/oath-ota-provision/</serverendpoint></u> where
SurePassID Mobile API Connector endpoint         Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account         FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens         FALSE – Users cannot disable their tokens		<serverendpoint> is a SurePassID Auth Server endpoint or</serverendpoint>
Allow.SoftTokenCreation       TRUE – Allow user to add soft tokens to their account         FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens         FALSE – Users cannot disable their tokens         FALSE – Allow user to enable their tokens		SurePassID Mobile API Connector endpoint
FALSE – Users can only activate soft tokens that are already assigned to their account.         Allow.TokenDisable       TRUE – Allow user to disable their tokens         FALSE – Users cannot disable their tokens         Allow.TokenEnable       TRUE – Allow user to enable their tokens	Allow.SoftTokenCreation	TRUE – Allow user to add soft tokens to their account
Allow.TokenDisable     TRUE – Allow user to disable their tokens       Allow.TokenEnable     TRUE – Allow user to enable their tokens		FALSE – Users can only activate soft tokens that are already
Allow.TokenEnable TRUE – Allow user to disable their tokens FALSE – Users cannot disable their tokens TRUE – Allow user to enable their tokens		assigned to their account.
Allow TokenEnable TRUE – Allow user to enable their tokens	Allow. I oken Disable	I KUE – Allow user to disable their tokens
	Allow TokenEnable	TRUE - Allow user to enable their takens
FALSE – Users cannot enable their tokens		FALSE – Users cannot enable their tokens



Allow.TokenDelete	TRUE – Allow user to delete their tokens FALSE – Users cannot delete their tokens
Server.DefaultNewSoftTokenOtpType	<ul> <li>The soft token One Time Passcode type. Values are:</li> <li>OATH Event</li> <li>OATH Time</li> <li>CardSecurityCodeEvent</li> <li>CardSecurityCodeTime</li> </ul>
Server.DefaultNewSoftTokenOtpWindow	The default windows size for the One Time Passcode. For default value is 30.
Server.DefaultNewSoftTokenOtpDriftUnit	The default windows size for time based the Time based One Time PasscodesThe default value is 3.
Allow.OfflineToken	TRUE – Allow user to add offline soft tokens to their account FALSE – User cannot add offline soft tokens to their account.
Allow.U2FTokenCreation	TRUE – Allow user to add Fido U2F tokens to their account FALSE – User cannot add Fido U2F tokens to their account.
Server.DirectoryEndpointType	The directory that will be used for first factor authentication. AD = ActiveDirecoty SP= SurePassID

## Notification Messages

When users require password recovery, ServicePass will send them a recovery notification email with instructions on how to reset their password. The password recovery process is slightly different based on which directory type SurePassID Authentication Server is configure for. Below are the behaviors for the supported directory options:

- SurePassID Directory, Active Directory:
  - The user is sent a recovery email.
  - The email contains a recovery link
  - The user clicks the recovery link
  - The user is presented with a web form to allow a change to his/her password.
  - The user is sent an email to alert him/her the account password has been changed.
- LDAP, Azure AD:
  - The user is sent a recovery email.
  - The email body provides the steps the user must follow to reset the password, such as, call help desk, etc.

## Notification Message Customization

ServicePass is delivered with predefined emails for password recovery and password change notification. The predefined emails are meant to be sent as



html email but you can change this by setting the **Server.DefaultEmailFormat** option as defined in the <u>Customize the System</u> section.

You can optionally set the FROM email address (e.g. <u>support@yourco.com</u>) and email name (e.g. Support) in the notification by changing the **Server.DefaultFromEmailAddress** and **Server.DefaultFromEmailName** configuration values respectively. The email address that you use <u>must be a valid</u> <u>email account</u> for your SMTP server. The SMTP server that SurePassID Authentication Server uses is defined in the SurePassID Authentication Server **Customize Email Settings** section.

The pre-defined emails are located in the ServicePass install sub-folder named account\_setup. These files are:

- forgot\_password\_subject.txt Forgot password email subject
- forgot\_password\_body.txt Forgot password email body
- pw\_change\_subject.txt Password changed email subject
- pw\_change\_body.txt Password changed email body

## Default Language

The system ships with a 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.

There are only a few instances when the system will provide the user with a web page. To make these pages culturally friendly you will need to update the language file.

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 to match the user's language.

If you would like to change the English text of the messages you can modify the **settings.resx** file located in **App\_GlobalResources** folder located under the root installation folder. This is the language file for the default culture. To add additional cultures you will need copy the existing **settings.resx** to **settings.xx-yy.resx** where xx is the language and yy is the dialect. For example, is en-us is for the United States, en-gb is for Great Britain, fr-fr is France and fr-ca is Canada, etc.). The system will automatically change to the match the default language that is currently selected in the user's browser.

