

# SurePass

## SurePassID Administration Guide

SurePassID Authentication Server 23.1



© 2013-2023 SurePassID, Corp. All rights reserved. Protected by patents pending. SurePassID, the SurePassID logo and design, and Secure SSO are registered trademarks or trademarks of SurePassID, Corp. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

**SurePassID, Corp.**

360 Central Avenue

First Central Tower

Suite 800

St. Petersburg, FL 33701

USA

+1 (888) 200-8144

[www.surepassid.com](http://www.surepassid.com)

## Table of Contents

Table of Figures .....	3
About the SurePassID Administration Guide.....	5
SurePassID System Installation Options.....	5
What is SurePassID System Configuration?.....	6
Configuring System Settings .....	7
SurePassID Login .....	7
SurePassID Administration Navigation.....	9
<b>Home Folder .....</b>	<b>11</b>
Account.....	12
Settings.....	13
Customize Email Settings .....	16
Customize Mobile Settings.....	17
FIDO U2F Settings .....	19
Users Folder .....	22
Managing Users .....	23
Managing Users Groups .....	25
Importing Users .....	29
Member of Group .....	39
<b>Tokens Folder.....</b>	<b>40</b>
Managing Token Groups.....	43
Check One Time Passcode .....	45
Create Temporary Passcode .....	45
Synchronizing Token.....	46
Importing Hard Tokens.....	50
<b>Audit Trail Folder .....</b>	<b>54</b>
<b>SSO (Single Sign-On) Folder .....</b>	<b>58</b>
Configuring SSO Apps .....	60
Configuring SSO Policies.....	64
Configuring SSO Roles.....	66

## Table of Figures

SurePassID Login .....	9
------------------------	---

SurePassID Login – Enter One Time Passcode .....	10
SurePassID Page Structure .....	11
SurePassID Home tab .....	13
SurePassID Account sub-form .....	14
SurePassID Settings .....	16
SurePassID SMS Messages .....	21
SurePassID Email Messages.....	19
SurePassID FIDO U2F Facets .....	22
SurePassID Users tab .....	24
SurePassID User Detail .....	26
SurePassID User Group List .....	28
SurePassID User Group Detail .....	29
SurePassID Import Users from CSV File – Select Import File .....	32
SurePassID Import Users Active Directory/LDAP – Select Import File .....	33
SurePassID Import Users Active Directory/LDAP – Load Groups .....	34
SurePassID Import Users Active Directory/LDAP – Select Groups .....	35
SurePassID Import Users – Map Fields .....	35
SurePassID Import Users – Select Options .....	37
SurePassID Import Users – Import Results .....	39
SurePassID Member Of Group .....	40
SurePassID Tokens tab .....	42
SurePassID Token Group Folder .....	44
SurePassID Token Group Detail .....	46
SurePassID Token Detail .....	48
SurePassID Check One-Time Passcode .....	48
SurePassID Create Temporary Passcode .....	49
SurePassID Synchronize Token .....	49
SurePassID Import Tokens – Specify File .....	53
SurePassID Import Tokens – Map Fields .....	55
SurePassID Import Tokens – Select Options .....	56
SurePassID Import Tokens – Import Results .....	57
SurePassID Audit Trail Folder .....	59
SurePassID SSO Configuration Folder .....	61
SurePassID SSO SAML 2.0 Configuration Form .....	64
SurePassID SSO Web Configuration Form .....	65
SurePassID SSO Policy List .....	67
SurePassID SSO Policy Form .....	68
SurePassID SSO Role List .....	69
SurePassID SSO Role Form .....	70

## About the SurePassID Administration Guide

This guide explains how to administer the SurePassID authentication system and how it may be configured to meet your organization's security needs. The purpose of this guide is to provide a reference for system administrators of the system.

This Guide provides information on the following topics:

- **What is SurePassID System Configuration?**
  - A brief introduction to configuring the SurePassID authentication system.
- **Configuring System Settings** ○ Explanations of how to tailor your SurePassID account configuration of users, tokens, audit trail logging, Secure Single Sign-On, and general system operations.

---

### Other SurePassID Guides

---

The SurePassID Administration Guide has the following companion guides that provide additional detail on specific topics for SurePassID:

- Getting Started Guide
- SurePassID Programmer API Guide
- SurePassID Local Agent Guide
- Glossary

## SurePassID System Installation Options

SurePassID Authentication Server is available as a multi-tenant cloud version that runs on Azure or Amazon EC2 or as a server-based application that is installed on your servers. The product is functionally equivalent with a few differences.

- The system can be deployed in the possible configurations.
  - **SurePassID Cloud Version**– You license a tenant in the SurePassID managed multi-tenant cloud version running on Windows Azure. This is a highly scalable/highly available environment.

- **SurePassID Server Version** – The system is a single tenant solution installed on your servers (or in your cloud instance such as Windows Azure or Amazon EC2) and is managed by you.
  - **SurePassID Server Multi-Tenant Edition** - The system is a multitenant solution installed on your servers or in the cloud and is managed by you. You can create and manage tenants in the system. Perfect for very large enterprises that need segregated instances for different parts of the organization. Also great for Managed Service Providers who want to offer the system to their clients as a paid managed service.
- The cloud version supports SurePassID Directory or Azure Active Directory only. The server version also supports traditional Active Directory.
  - The cloud version supports SurePassID key management which is implemented in a software container and optionally uses Amazon Cloud Hardware Security Module (HSM). The server version also supports an HSM for key management.

## What is SurePassID System Configuration?

The SurePassID System Configuration folder is used to manage all aspects of the SurePassID system. The System Configuration folder allows the system to:


- Set system-wide security parameters.
- Set system-wide configuration parameters such as e-mail, SMS, FIDO, messages, system customization, Active Directory, One-Time Passcode lifetimes, etc.
- Add, update, delete and import users into the system.
- Add update, delete, and import tokens into the system.
- Define SSO roles and profiles
- Operate and maintain the system.
- Resolve situations that require your attention.
- Review the audit log.

## Configuring System Settings

To configure the system, you first need to login to the system. Follow the instructions below to login to the system.

### SurePassID Login

Enter the SurePassID URL into your browser and you will be presented with the following login form:

**SurePass** 

---

Login

Account:

Username:

Password:

[Login](#)

[Forgot Password?](#)

---

© 1999-2021 SurePassId Corp. All rights reserved.  
[Terms Of Use](#)

### SurePassID Login

Enter your **Domain**, **Username** and **Password** and press the **Login** button. If your credentials are accepted, you will be presented with the following two-factor form:



## Login

Complete your login using a second factor.

Account:

Username:

One Time Passcode (OTP):

Verify OTP

2FA Options:



[Forgot Password?](#)

© 1999-2021 SurePassId Corp. All rights reserved.

[Terms Of Use](#)

**HINT:** You can bookmark the login server URL with domain and username specified so that these fields are prefilled for you. The format is:

**`https://<surepassid_installation>/?d=<domain_name>&u=<username>`**







For example, if you are using the community version of SurePassID, your company domain is **spman.com** and your username is **JJJameson**, you would bookmark:

**`https://sandbox.surepassid.com/?d=spman.com&u=JJJameson`**




## SurePassID Login – Enter One Time Passcode

You will need to securely login to your account using a two-factor authentication method. One such method is to use a One Time Passcode (OTP). These are the following passcode choices:

- View a passcode on a token (hardware or mobile) assigned to your account.
- Click the  to receive a temporary passcode via Email.
- Click the  to receive temporary passcode via SMS.
- Click the  to receive a temporary passcode via voice call.
- Click the  to receive an SMS authentication request.
- Click the  to have an authentication request pushed to your mobile device.
- Click the  to receive an authentication request via phone call to your mobile device.

Enter the passcode into the **One Time Passcode (OTP)** field and press the **Verify OTP** button.

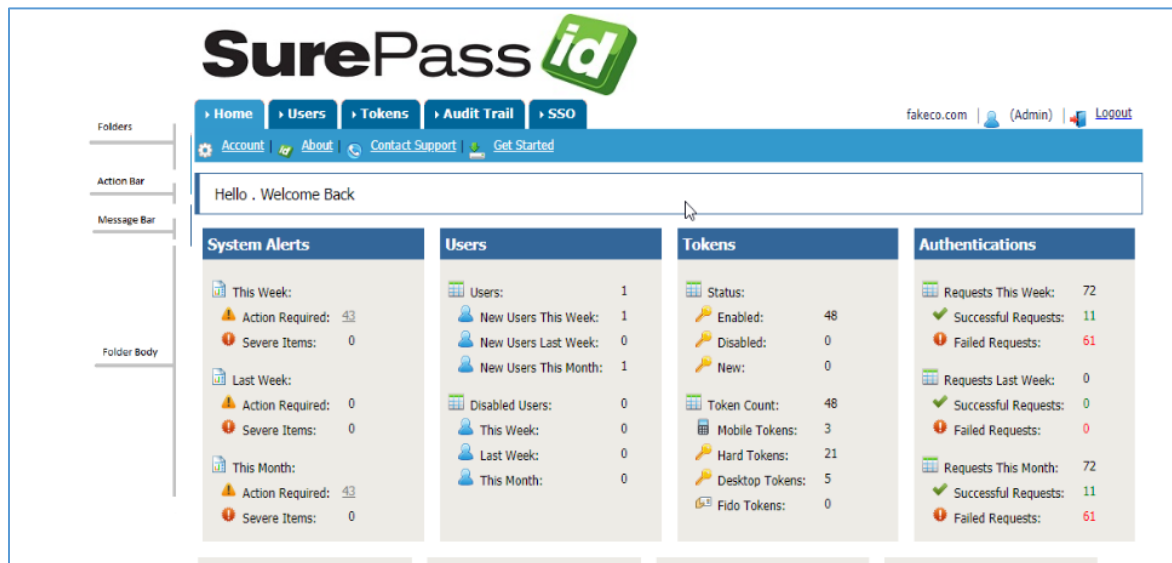
Alternatively, you can click the  to send a push notification question to the user's phone. The user confirms or denies access on their phone to allow or deny access to the system and then presses the **Approve** button and the SurePassID Home form will be displayed.

You can also login with a FIDO U2F token if it is already registered to SurePassID and you are using a FIDO U2F certified web browser such as Chrome or Firefox.

Just insert your U2F token, wait for the token to blink, and then press the button on the token. If the token is valid for your account, the SurePassID Home form will be displayed. If the login fails, you can click the **Verify U2F** button to reattempt U2F authentication.

## ***SurePassID Administration Navigation***

All forms in the system follow a common format containing the following sections:



## SurePassID Page Structure

The sections are:

- **Folders** – The folders section is used to organize information in an intuitive manner.
- The system currently has the following main folders:
  - **Home** – Displays the system dashboard and manages account profile and system configuration settings. Help documentation is also available on the Home page.
  - **Users** – Manages the users defined in the system
  - **Tokens** – Manages the tokens that are defined in the system.
  - **Audit Trail** – System log and audit trail
  - **SSO** – Secure Single Sign-On settings
- **Action Bar** - The action bar displays the available actions beneath the currently selected folder and provides links to sub-functions.
- **Message Bar** - Displays informative messages to the user based on the user's actions.
- **Folder Body** - The information in the currently selected folder/action.

## Home Folder

The Home form displays the system dashboard. The dashboard highlights system alerts and statistics. The hyperlinks associated with system alerts allow the system administrator to quickly review and take the appropriate action to clear the alert.

The following functions are available in the Home action bar:

- **Account**
- **About**
- **Contact Support**
- **Documents**
- **Downloads**

The screenshot displays the SurePassID Home dashboard. At the top, the SurePassID logo is visible. Below the logo is a navigation bar with tabs for Home, Users, Tokens, Audit Trail, and SSO. To the right of the navigation bar, the user is logged in as Admin, and there is a Logout button. Below the navigation bar is a welcome message: "Hello . Welcome Back". The dashboard is divided into four main sections: System Alerts, Users, Tokens, and Authentications. Each section contains a list of metrics and statistics.

System Alerts	Users	Tokens	Authentications
<b>This Week:</b> Action Required: 43 Severe Items: 0	<b>Users:</b> 1 New Users This Week: 1 New Users Last Week: 0 New Users This Month: 1	<b>Status:</b> Enabled: 48 Disabled: 0 New: 0	<b>Requests This Week:</b> 72 Successful Requests: 11 Failed Requests: 61
<b>Last Week:</b> Action Required: 0 Severe Items: 0	<b>Disabled Users:</b> 0 This Week: 0 Last Week: 0 This Month: 0	<b>Token Count:</b> 48 Mobile Tokens: 3 Hard Tokens: 21 Desktop Tokens: 5 Fido Tokens: 0	<b>Requests Last Week:</b> 0 Successful Requests: 0 Failed Requests: 0
<b>This Month:</b> Action Required: 43 Severe Items: 0			<b>Requests This Month:</b> 72 Successful Requests: 11 Failed Requests: 61

### SurePassID Home tab

## Account



Clicking **Account** displays the following form:

The image shows the 'Update Account' form. At the top, it has the 'SurePass id' logo and a navigation menu similar to the first screenshot. Below the navigation is a sub-header 'Update Account' with links for 'New', 'Update', and 'Close'. The form is divided into several sections: 1. 'Account Information' with fields for 'Account' (fakeco.com), 'Company Name' (Fake\_Company), and 'Printed Serial Number Prefix' (FAKE). 2. 'Account Credentials' with 'Server Login Name (Account Id)' (newco9), 'Server Login Password (Account Token)' (with a 'Show' link), and 'Data Protection' (None). 3. 'SurePassID Licensing' with a 'License Type' dropdown set to 'Community Edition - Free limited license'. 4. 'Authenticate Calling IP Address' with a checkbox for 'White List (allow access only to) these IP addresses' and an empty text area. 5. 'MFA Options For Portal Login' with checkboxes for 'Send Sms Otp', 'Send Email Otp', 'Voice Otp', 'Push Sms Question', 'Push Question To App', and 'Call My Phone'. 6. 'Status' with 'Last Updated' (5/19/2021 8:20:28 AM) and 'Last Updated By' (Mark Poid). At the bottom are 'Update' and 'Close' buttons.

### SurePassID Account sub-form

The Account form has the following fields:

- **Account** – Domain name associated with this account
- **Company Name** – Name of the company
- **Printed Serial Number Prefix** – The prefix applied to all soft Tokens created by SurePassID. This is required for OATH compliance.
- **Server Login Name (Account Id):** – The name that is used when making requests to the authentication server using the SDK and API.
- **Server Login Password (Account Token):**– The password that is used when making requests to the authentication server using external applications such as API, Radius server, Forms Event Log Sync, Active Directory Sync, etc. This field should be kept private.
- **License Type** – The type of license for your account.
- **White List (allow access only to) these IP addresses** – The list of IP addresses from which the server will allow requests. IP address white list entries can be full IP addresses, or they can contain wild cards. Wild cards are specified as a partial IP address that is used as a prefix mask. The server will only allow requests for IP addresses that have the prefix. For example, setting an IP white list entry as 209.055. will prevent access from any IP addresses that do not start with 209.055.

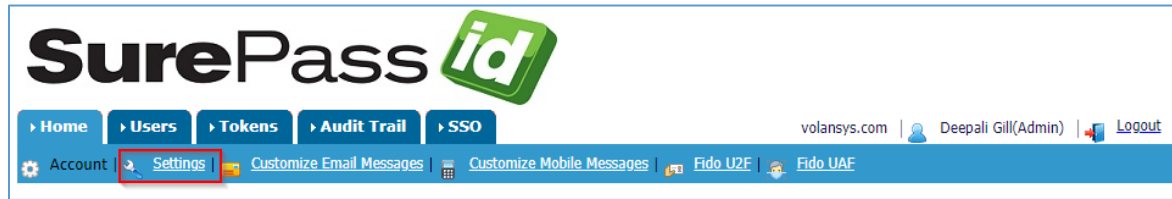
**Note:** We recommend using X509 certificates and firewall rules as the primary method from limiting access. However, for companies that cannot use X509 certificates, this is the recommended way to limit access.

**Note:** For SurePassID enabled mobile apps, we offer the SurePassID Proxy which can filter out public traffic and use a TLS tunnel to the server

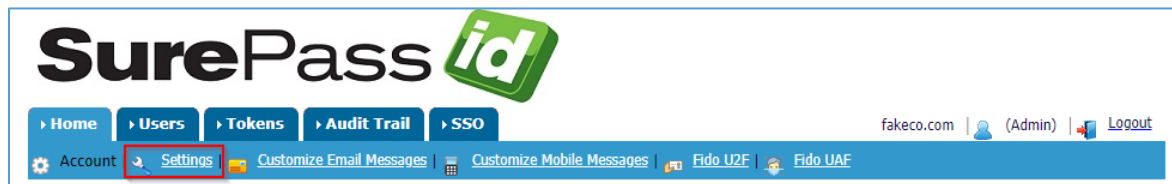
**Last Updated** – The date the settings were last updated.

- **MFA Options for Portal Login** – Admin can select one or more MFA options that will be visible to users while logging into Tenant SurePassID account.
- **Last Updated By** – The last user to update the settings.

## Settings



Clicking **Settings** displays the following form:



### SurePassID Settings

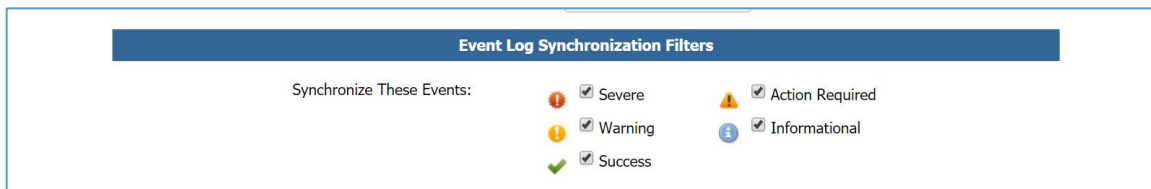
The form has the following fields:

- **Maximum Users Licensed** – Maximum number of users licensed to use the system.
- **Maximum Tokens Licensed** – Maximum number of tokens that can be used in the system.
- **Account Expiration Date** – The date this account will expire and will no longer accept authentication requests.
- **Time Zone** – Time zone for this company.
- **Current Culture** – Current culture for the web browser. This is the language file that will be used for this user.
- **Allowable Failed OTP Validations Per Token** – The maximum number of invalid OTPs allowed before the token status is changed to disabled. Disabled tokens cannot be used until they are manually enabled by the system administrator.
- **Account Password Expiration** – The interval used to time the expiration of passwords.
- **Mobile notifications are valid for** – The time frame (minutes & seconds) for which an SMS passcode is valid.
- **Email OTP is valid for** – The time frame (minutes & seconds) for which an Email passcode is valid.
- **Temporary OTP is valid for** – The time frame (minutes & seconds) for which a temporary passcode is valid. Temporary OTPs are given to users that need access but might not have their authentication token.

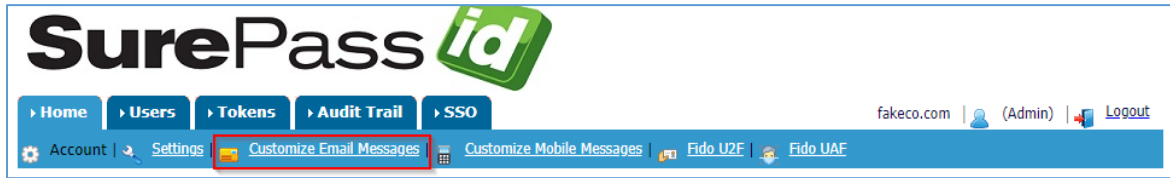
Temporary OTPs are given to the user by the admin or self-service API or portal for a single-use login.

- **User Authentication Method** – The method SurePassID will use to verify the user’s first factor (username and password). Options are:
  - **SurePassID (SD)** – SurePassID directory (cloud and server versions)
  - **Active Directory (AD)** – Microsoft Active Directory (server version only)
  - **Azure Active Directory (AZAD)** – Microsoft Azure Active Directory (cloud and server versions)
- **Event Log Synchronization Filters** – Event Log Synchronization (ELS) is the process of securely pulling SurePassID audit trail events and storing them in the Forms event log or a Linux syslog. Event Log Synchronization Filters specifies the SurePassID event types that are eligible to be pulled. The ELS application is installed on your servers and is a component of the SurePassID Local Agent.
- **Synchronize These Events** – Specify the allowable Event types for synchronization.

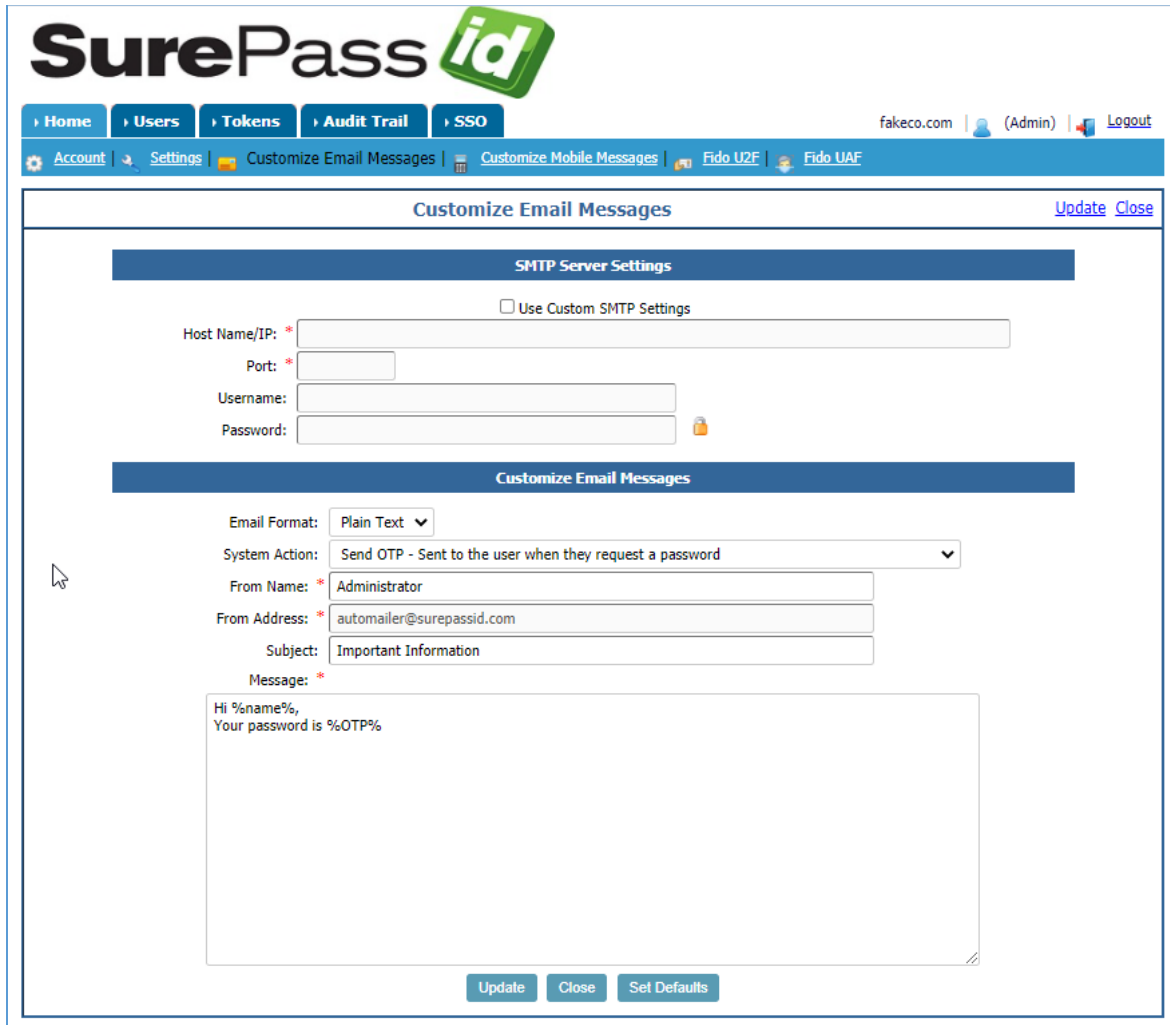
Options for the types of events that can be synced to the Windows event log are shown here:



## Customize Email Settings



Clicking **Customize Email Messages** displays the following form:

The screenshot shows the 'Customize Email Messages' form. It is divided into two main sections: 'SMTP Server Settings' and 'Customize Email Messages'.  
**SMTP Server Settings:**  
- A checkbox labeled 'Use Custom SMTP Settings' is present.  
- Fields for 'Host Name/IP:', 'Port:', 'Username:', and 'Password:' are provided.  
**Customize Email Messages:**  
- 'Email Format:' is set to 'Plain Text'.  
- 'System Action:' is set to 'Send OTP - Sent to the user when they request a password'.  
- 'From Name:' is 'Administrator'.  
- 'From Address:' is 'automailer@surepassid.com'.  
- 'Subject:' is 'Important Information'.  
- 'Message:' field contains the text: 'Hi %name%,  
Your password is %OTP%'.  
At the bottom of the form are buttons for 'Update', 'Close', and 'Set Defaults'. The top right of the form has 'Update' and 'Close' links.

### SurePassID Email Messages

The form has the following fields:

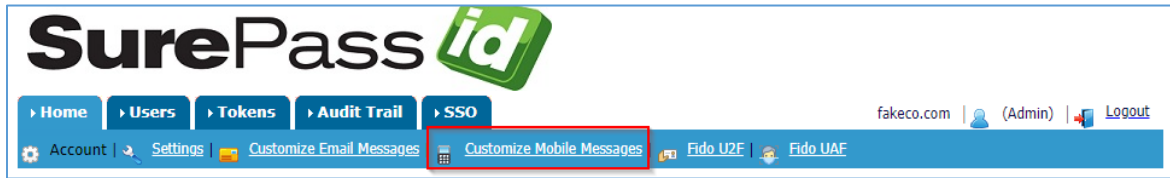
- **Use Custom SMTP Settings** – By default the installation-wide server is determined by the system administrator. Alternatively, you can override



those settings and use your own SMTP server. Check with your system administrator for the following settings:

- **Host Name/IP** – The host name or IP address of your SMTP server.
- **Port** – The SMTP server port. Usually this is port 25 but it can also be port 587 for more secure operations.
- **Username** – The username of the account that will be used to authenticate to the SMTP server.
- **Password** – The password for the **Username** account that will be used to authenticate to the SMTP server.
- **Email Format** – You can choose to send the email in plain text or HTML format.
- **System Action** – Select the system event for the email settings. These can be for token activation, user enrollment, etc.
- **From Name** – Email name.
- **From Address** – Email address.
- **Subject** – Email subject
- **Message** – Email message body that will be sent. The message supports the use of dynamic place holder. Dynamic placeholders are replaced with real-time values that are available based on the system action.

## ***Customize Mobile Settings***



Clicking **Customize Mobile Messages** displays the following form:

**Customize Mobile Messages** [Update](#) [Close](#)

SMS Provider	Twilio	
Account SID:	*****5ea8f7f2923	
Auth Token:	*****eb245374fbf	
From Phone Number:	+1(727)800-3526	
Activating a mobile token:	The device code for your account is: %deviceid%	<a href="#">Set Default</a>
Sending One Time Passcode:	Hi <name/>, Your password is <otp/>. Use this verification code to access your account.	<a href="#">Set Default</a>
Challenge question for push authentication:	App: <appname/><crlf/>Account: <account/><crlf/>Reason: <reason/><crlf/><crlf/>Is requesting access. Reply Y to allow	<a href="#">Set Default</a>
Voice message to send user:	Press # to approve access. Press 3 to cancel	<a href="#">Set Default</a>
Voice message when user is approved access:	Access is granted	<a href="#">Set Default</a>
Voice message when user is denied access:	Access is denied	<a href="#">Set Default</a>

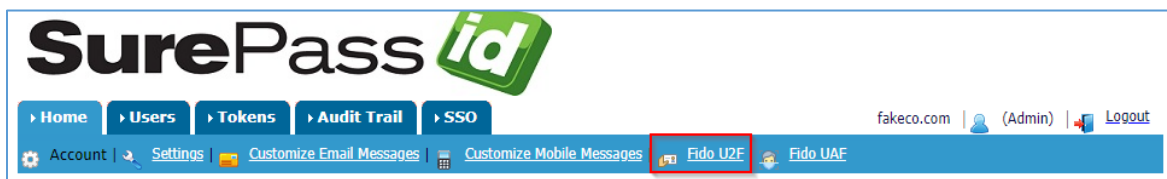
[Update](#) [Close](#)

## SurePassID Mobile Messages

The form has the following fields:

- **SMS Provider** – The SMS provider that will send the SMS message. Currently only Twilio is supported. You must obtain your own company Twilio account in order to configure this feature.
- **Account SID** – The Twilio SID for your account.
- **Auth Token** – The Twilio Auth Token for your account.
- **From Phone Number** – The Twilio phone number associated with your account.
- **Activating a mobile token**– Message sent to the user for activating a mobile token such as Google Authenticator soft token or SurePassID Authenticator soft token.
- **Sending One Time Passcode** – Message sent to the user when a passcode is requested.
- **Challenge question for push authentication:** Challenge question sent to the user for push authentication.
- **Voice message to send user:** The voice prompt to use when requesting authentication via IVR.
- **Voice message when user is approved access:** The voice prompt to use when the request for approval is granted via IVR.
- **Voice message when user is denied access:** The voice prompt to use when the request for approval is denied via IVR.

## ***FIDO U2F Settings***



Clicking **FIDO U2F** displays the following form:

The image shows the 'FIDO U2F Settings' form. At the top, it has the SurePass ID logo and navigation menu. Below the navigation bar, the title 'FIDO U2F Settings' is centered, with a 'Close' link on the right. The form contains a 'Fido AppId:' dropdown menu, a 'Delete AppId' button, and an 'Add AppId' button followed by an input field. Below this is a table with two columns: 'Action' and 'Allowable Apps (U2F Facets)'. The 'Action' column contains an 'Edit' link. The 'Allowable Apps (U2F Facets)' column is currently empty. At the bottom left, it says '1 page(s): [1]'. At the bottom center, there is a 'Save Changes' button.

### SurePassID FIDO U2F Facets

The form has the following fields:

- **FIDO AppId** – The currently selected FIDO U2F AppId.
- **Allowable Apps (U2F Facets)** – The allowable facets for the currently selected FIDO AppId. Facets are typically required when you want many different websites/mobile apps to share the same base AppId. See the FIDO U2F documentation for more Info.

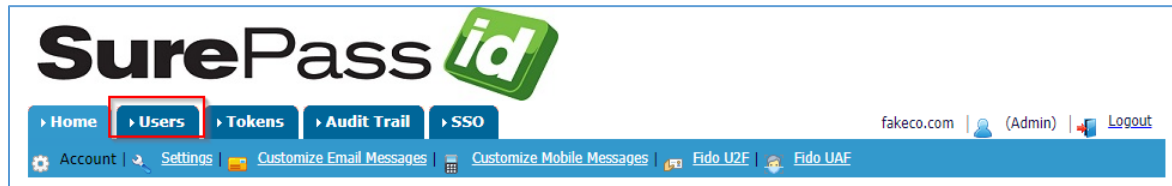
Click the **Delete AppId** button to delete the currently selected **FIDO AppId**.

Click the **Add AppId** button to add a new **FIDO AppId**.

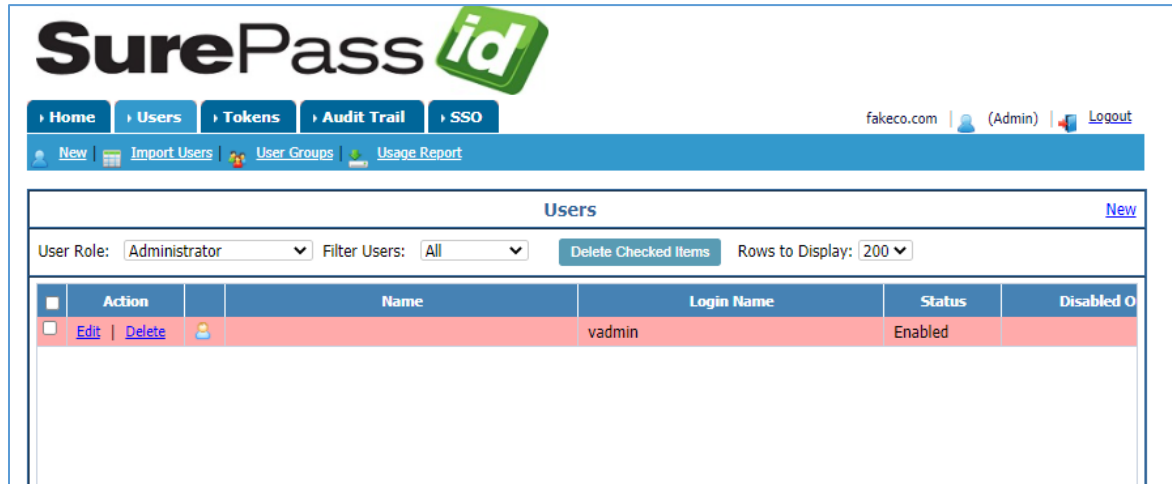
Click the **Save Changes** button to save the **Allowable Apps (U2F Facets)** that have been specified for the current **FIDO AppId**.



## Users Folder



Selecting the **Users** folder shows the User List form:



The following functions are available in the User action bar:

- **New**
- **Import Users**
- **User Groups**
- **Usage Report**

### SurePassID Users tab

The User List Form has two distinct sections. The first section is the User Filter Section, where you can search for a specific user or users based on several different search criteria. The second section, the User List Section, allows you to perform actions on specific users and only displays the users that meet the search criteria specified in the Users Filter Section.

The User Filter Section parameters are:

- **User** – Search for users whose names begins with, is, or contains a specific value.
- **Delete Checked Items** – Press this button to delete users in Users List Section that have the checkbox column checked.

The actions you can take on each user are:

- **Edit** – Edit the user.

The Users folder has the following action bar functions:

- **New** – Add a new user to the system.
- **Import Users** – Import users into the system.
- **User Groups** – Create collections of users.
- **Usage Report** – Creates a CSV file report of relevant user information.

## ***Managing Users***

When you edit or add a new user the following form will be displayed:

The screenshot shows the 'Update vadmin' form in the SurePassID administration interface. The form is divided into several sections: Login Credentials, User Credentials, User Time Zone, User Role, Secure SSO Settings, and Status. At the bottom, there is a 'Tokens' table showing a single token for the user.

**Update vadmin** [New](#) [Update](#) [Close](#) [Email Login Info](#) [Password/PIN Reset](#)

**Login Credentials**

User Name: \* vadmin Password: [ ]

**User Credentials**

First Name: [ ] Last Name: [ ]  
 Email: deepali.gill@volansystech.com Mobile Phone: [ ] [Test Sms](#) [Test Call](#)

**User Time Zone**

Time Zone: (UTC-08:00) Pacific Time (US & Canada) ▼

**User Role**

Super Administrator  
 Administrator  
 Helpdesk  
 User - No portal access

**Secure SSO Settings**

Mobile Activation Code: Nk3afk0954-anCyLg0Kq8-wo5VoT3Dx6 Mobile Activation Date: [ ]  
 Mobile 2FA Options: No 2FA - Single factor login is ok ▼ SSO Identity: vadmin

**Status**

Status: Enabled ▼

[Update](#) [Close](#)

**Tokens** [Add New Soft Token](#)

Action	Serial Number	User Defined Name	Status	Token Type	Last OTP Validation	Created
<a href="#">Edit</a>   <a href="#">Delete</a>	xxxx-00000048	Token48	Enabled	SurePassID Authenticator Token		Time

## SurePassID User Detail

The following fields are displayed on the User Detail Form:

- **User Name** – The user’s login name.
- **Password** – The user’s login password.
- **First Name** – The user’s first name.
- **Last Name** – The user’s last name.
- **Email** – The user’s email address.
- **Mobile Phone** – If the user is to receive SMS notifications (such as token activations) this field must be the user’s mobile phone number.



- **User Time Zone** – The user’s time zone.
- **User Role** – Created User can be assigned a role of Super Administrator/ Administrator/Helpdesk/User-No Portal access.
- **Secure SSO Mobile Activation Code** – Used by SurePassID Secure SSO mobile app to identify this user.
- **Secure SSO Mobile Activation Date** – The date SurePassID Secure SSO mobile app was activated by this user from their mobile token. If the field is blank the account has not been configured.
- **Secure Mobile 2FA Option** – The level of two-factor authentication security for this user when they login through the SecureSSO mobile app. The choices are:
  - **No Two Factor** – Single factor (username & password) authentication is sufficient to authenticate the user.
  - **Require 2FA** – User can only login if they have a two factor authentication token assigned to their account.
  - **2FA Not Mandatory** – If the user has a two factor authentication token they must use that token to login. If the user does not have a two factor authentication token then the user is permitted to login with single factor (username & password) only.
- **SSO Identity** – When users login into a SAML2 app, the app itself (the relying partner) requests SurePassID (identity provider) to provide the user’s identity (account) that the SAML2 app should use. The SurePassID admin can set-up an account that uses the user’s email, username, or SSO Identity. If SSO Identity is chosen, then this field represents this user’s identity to the SAML2 app.
- **Status** – The status of the account. Accounts can be enabled or disabled.
- **Disabled On** – The date the user account was disabled.
- **Tokens** – The Tokens assigned to this user. If this user will be set up as an Admin (Admin Privilege checked) they will need to have a token assigned to him/her or they will not gain access.

After entering the information about the user, click the **Update** button to update the user or the **Add** button to add the user. You can also press the Email Login Info link in the page header to send the SurePassID login credentials to the user.

## ***Managing Users Groups***

In large enterprises with many users it is advantageous to group users with common relationships so that they can be easily managed.

SurePassID uses its directory to store all things related to strong authentication. Certain data elements that SurePassID requires are stored in other directories such as Active Directory or LDAP.

SurePassID cloud can be configured to sync the directory with a Windows Azure Active Directory. SurePassID cloud does not have direct access to Active Directory (AD) or the LDAP directory that are behind a company's firewall but you can still sync with the Active Directory by using the Directory Sync component of the SurePassID Local Agent.

Directory Sync is an app that can periodically push Active Directory/LDAP changes to SurePassID. Check out the SurePassID Local Agent Guide for information on how to install and setup.

To manage user groups, select **User Groups** from the action bar on the **Users** folder as shown below:



### SurePassID User Groups List

Selecting **New** allows you to create a new user group.

Selecting **Edit** or **Delete** next to a group allows you to modify or delete an existing user group.

The screenshot shows the SurePass ID web application interface. At the top left is the SurePass ID logo. The navigation menu includes Home, Users, Tokens, Audit Trail, and SSO. The user is logged in as Admin on fakeco.com. A 'New' button is visible. The main content area is titled 'User Groups' and contains a table with the following data:

Action	Group Name	Description:	Users In Group
<a href="#">Edit</a>   <a href="#">Delete</a>	Sample Group	Test data	0

**SurePassID User Group Detail**

The following fields are displayed on the Update User Group Form:

The screenshot shows the 'Update User Group' interface in the SurePass ID system. At the top, there is a navigation bar with links for Home, Users, Tokens, Audit Trail, and SSO. The user is logged in as M Stein. The main form contains the following fields:

- Group Name: Sample User Group
- Description: An example
- Map To AD Group: (empty)
- Azure AD Endpoint: (empty)
- Users in Group: 0

Below the form are buttons for Update, Close, and Synchronize. A table titled 'Members Of This Group' is displayed below the form, showing the following data:

	Login Name	Name	Status
<input type="checkbox"/>	mstein	M Stein	Enabled
<input type="checkbox"/>	markpoid@tierasoft.com	Mark Poid	Enabled

- **Action** – Edit / Delete to modify an existing group or delete same.
- **Group Name** – The user group name.
- **Description** – The description of the group.
- **Map To AD Group**– The AD group to link to this group. This can also be an AD filter.
- **Azure AD Endpoint** – The Azure AD Endpoint information. A concatenation of property values.
- **Users in Group** – A count of the users in the group.
- **Members Of This Group** – The users that are part of this group.

After you have set the fields, click the **Add/Update** button to save your changes.

You can press the **Synchronize** button to synchronize SurePassID with AD.

SurePassID only synchronizes username (SAM Account), mobile phone, and email. *SurePassID does not synchronize the user password field.*

## ***Importing Users***

SurePassID cloud uses its own user directory by default. SurePassID cloud can be configured to use a Windows Azure Active Directory as the user directory as well. SurePassID cloud does not have direct access to Active Directory (AD) or the LDAP directory that are behind a company's firewall but provides two methods for importing and synchronizing users from Active Directory:

- **Importing users from CSV file** – Initial or incremental loading
- **SurePassID Active Directory Sync** – Power shell app that runs on your server.

Another option is to use SurePassID server which can access Active Directory.

**TIP: You can export user information from both AD and LDAP directories to a .csv and then import the information into SurePassID.**

Importing users is a multi-step process. Below are the following steps to import users into the system.

1. **Select the import file.**
2. **Map the fields in the import file to SurePassID directory fields.**
3. **Select options for the import.**
4. **Import the users and review the results.**

The system supports the importing of both hard tokens and soft tokens which are defined as follows:

- **Hard Tokens** – Hard Tokens are physical devices such as display cards, key fobs, USB devices, and smart cards. Hard tokens are imported into the system by using **Import Tokens** menu in the **Tokens** folder. Hard tokens are identified by a printed serial number on the hard token. Hard tokens have secret keys that are embedded in the token when they are manufactured and usually cannot be changed. You can assign hard tokens (using printed serial numbers on them) that have already been imported into the system.
- **Soft Tokens** – These are virtual devices that can be installed (or emulated) on existing hardware equipment such as mobile apps, windows apps, and desktop apps. When you import users, the system can create the soft tokens, assign them to the user and optionally send the user an

email or SMS to configure them. This allows you to add a large number of users with very little administrative effort.

**Tip:** FIDO U2F hard tokens (that only support FIDO U2F) are treated as soft tokens because they have no secret keys specific to the hard token itself.

You can import users from csv files or directly from Active Directory/LDAP.

*Importing directly from Active Directory/LDAP is only available when you are using the on premise server version.*

To start the import wizard, select **Import Users** from the action bar on the **Users** folder as shown below:



And the following form is displayed:

## SurePassID Import Users From CSV File – Select Import File

Before you can import users you must first create the import file. You can create the CSV import file on several ways:

- Manually create the file with user information.
- If you are using the cloud version, you can export Active Directory users with Powershell.

```
Get-ADUser -Filter * -Properties * | Select-Object -Property Surname,
GivenName, SamAccountName, MobilePhone, EmailAddress | Sort-
Object -Property Name | ConvertTo-CSV
```

- You can also use the csvde.exe utility to export users. For example:

```
csvde -f exported_users.csv -r objectClass=user -l sn, givenName,
sAMAccountName, mobile, mail
```

In the **Import Source** field, select **Import from text file (.txt, .csv)** then press the **Browse** button and select the file (\*.txt, \*.csv) file to import. The file must be in a comma separated format.

If you are running the server version, you can import from Active Directory/LDAP by selecting Import from Active Directory/LDAP in the **Import Source** drop down list as show below.

The screenshot shows the SurePassID web interface. At the top, there is a navigation bar with links for Home, Users, Tokens, Audit Trail, and SSO. Below this is a secondary navigation bar with links for New, Import Users, User Groups, and Usage Report. The main content area is titled 'Import Users (Step 1 - Specify File)'. It contains the following form fields:

- Import Source:** A dropdown menu set to 'Import from Active Directory/LDAP'.
- Directory Server (FQDN)/IP Address:** A text input field containing 'sptieradc.tierasoft.com'.
- Directory Filters:** A dropdown menu set to 'All directory users' with a link for 'Add AD Group Filters'.
- Directory Filter:** A text input field containing the LDAP search filter '(&(objectCategory=person)(objectclass=user))'.
- Directory Username:** A text input field containing 'administrator'.
- Directory Password:** A text input field with masked characters (dots).

At the bottom of the form, there are two buttons: 'Next' and 'Close'.

## SurePassID Import Users Active Directory/LDAP – Select Import File

You will see the following form fields:

- **Import Source** – The source used for the import, file or AD/LDAP.
- **Directory Server** – FQDN/IP Address – The directory server address using Fully Qualified Domain Name or IP address.
- **Directory Search Filters** – By default you will see two dropdown list items.
  - All directory users
  - Custom directory search query – Custom craft your own directory search filter and enter it into the Directory Search Filter.

When you select a filter from the drop-down list, the **Directory Filter** will be updated with the actual LDAP search filter.

- **Directory Search Filter** – The RFC2254 LDAP directory search filter that will be used to select the users to be imported. You can always tailor this to meet your needs. This value will be retained in SurePassID with the directory group that will be created in Step 3 of the import allowing you to manually synchronize the directory later and keeps a history of where the users where imported from.
- **Directory Username & Password** – Depending on your security configurations, this is the directory where you need to authenticate.

When you press the **Add AD Group Filters** link, the system will add all the existing Active Directory groups to the Directory Filter.



**SurePass id**

Home Users Tokens Audit Trail SSO

tierasoft.com Admin User Logout

New Import Users User Groups Usage Report

### Import Users (Step 1 - Specify File)

Import Source: Import from Active Directory/LDAP

Directory Server (FQDN)/IP Address: sptieradc.tierasoft.com

Directory Filters: All directory users [Add AD Group Filters](#)

Directory Filter: (&(objectCategory=person)(objectclass=user))

Directory Username: administrator

Directory Password: .....

Next Close

## SurePassID Import Users Active Directory/LDAP – Load Groups

You can import users in structured groups that map to your enterprise structure as shown below.

**SurePass id**

Home Users Tokens Audit Trail SSO

tierasoft.com Admin User Logout

New Import Users User Groups Usage Report

Active Directory group search filters have been updated. Please select the Directory Filters: dropdown list to select available filters.

### Import Users (Step 1 - Specify File)

Import Source: Import from Active Directory/LDAP

Directory Server (FQDN)/IP Address: sptieradc.tierasoft.com

Directory Filters: Access Control Assistance Operators [Add AD Group Filters](#)

Directory Filter: Access Control Assistance Operators

- Account Operators
- Administrators
- All directory users
- Allowed RODC Password Replication Group
- Backup Operators
- Cert Publishers
- Certificate Service DCOM Access
- Cloneable Domain Controllers
- Cryptographic Operators
- Custom directory search query
- Denied RODC Password Replication Group
- Distributed COM Users
- DnsAdmins
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users

© 1999-2018 SurePass ID 200-8144

## SurePassID Import Users Active Directory/LDAP – Select Groups

SurePassID will retain this group structure for you so that Active Directory group structure will be preserved in SurePassID.

Regardless of how or from where you import users, press the **Next** button to continue to the second step of the wizard to define the field mapping for the data fields in the import file as shown below:

The import file has 2 record(s). Each record has 5 columns.

### Import Users (Step 2 - Map Fields)

**User Import Preview**

Column 1	Column 2	Column 3	Column 4	Column 5
ava.jade	Ava	Jade	ava.jade@xyzsample.com	+91(711)1234567
cynthia.williams	Cynthia	Williams	cynthia.williams@xyzsample.com	+91(711)1234567

Ignore first record in the import file:

**Map Import Data**

Column 1: Login Username  
Column 2: First Name  
Column 3: Last Name  
Column 4: Email  
Column 5: Mobile Phone

Next Close

## SurePassID Import Users – Map Fields

The **User Import Preview** section displays the columns of data in the import file. The **Map Import Data** section allows you to map the import data columns to the corresponding SurePassID field. You can map import data columns to the following fields in SurePassID:

- **Login User Name** – User’s login name.
- **First Name** – User’s first name.
- **Last Name** – User’s last name.
- **Email** – The email of the user. This must be a valid email address.
- **Mobile Phone** – User’s cell phone. This is required if the user wants to receive passcodes via SMS, or voice call. The format is:

+aaa(bbb)cccccccc where aaa is country code, bbb is area code and cccccccc is the local number. For example. US: +1(800)200-8411 UK: +44(0)20 1234 5678.

- **Serial Number** – The serial number of the token that is assigned to this user. (When using import from file)
- **PIN** – The PIN for this user. Only used for Time and PIN based passcodes. (When using import from file)

After you have set the fields you plan to map, click the **Next** button and the **Import Users (Select Options)** form is displayed:

**Tip:** When importing users that will be assigned a hard token the token import file can include the serial number of the token that will be assigned to the user provided you have imported the hard tokens into the system first.

**SurePassID**

Home Users Tokens Audit Trail SSO fakeco.com (Admin) Logout

New Import Users User Groups Usage Report

### Import Users (Step 3 - Select Options)

#### Create Soft Tokens

Token Type: SurePassID Authenticator Token

OTP Type: Time (Oath)

OTP Length: 6 Digits

OTP Window Size: 30

Authenticator Usage: OTP Authentication Only

Mobile Setup Verification: No mobile user verification

User Group: not assigned  Create Group

#### Send Account & Token Notification Options

Send notifications to the user

Send user account login details

Send token setup instructions

Send the notification via: Email

#### Import Options

Merge existing users

Import the good records even if some records have errors

Import Close

## SurePassID Import Users – Select Options

Select from the following options for importing users:

**SurePass id**

Home Users Tokens Audit Trail SSO

fakeco.com (Admin) Logout

New Import Users User Groups Usage Report

### Import Users (Step 3 - Select Options)

#### Create Soft Tokens

Token Type: SurePassID Authenticator Token

OTP Type: Desktop Token

OTP Length: Fido Token

OTP Window Size: Google Authenticator Compliant

Authenticator Usage: None - Just import the users for now.

Mobile Setup Verification: Nymi Band

User Group: SMS Token

Send Account & Token Notification Options

Send notifications to the user

Send user account login details

Send token setup instructions

Send the notification via: Email

#### Import Options

Merge existing users

Import the good records even if some records have errors

Import Close

**Token Type** – The type of token for soft Tokens. The choices are:

- Desktop Token
- FIDO Token
- Google Authenticator Token
- None - Just import the users for now.
- Nymi Band
- SMS Token
- SurePassID Authenticator Token
- Voice Message OTP

The following parameters **OTP Type**, **OTP Length**, **OTP Form** and **Send token activation email to each user** are grayed and not available if you select a token type of **None - Just import the users for now**.

- **OTP Type** – The type of the One-Time Password:
- Time (OATH)

- Event (OATH)
- Time + PIN (OATH)
- Challenge Response (OATH)
- **OTP Length** – The length of the One-Time Password:
  - 3 Digits (CSC Visa/MC)
  - 4 Digits (CSC Amex)
  - 6 Digits
  - 8 Digits
  - 10 Digits
- **OTP Window Size** – For Event (OATH/OATH) this parameter specifies the rolling window of the passcode. The typical value is 30. For Time (OATH/OATH), Time + PIN, and Challenge Response (OATH/OATH) this parameter specifies the number of rolling time periods of the passcode time units in seconds. The typical value is 30 seconds.
- **User Group** – Assign the users to an existing group.
- **Create Group** – Check this box to assign the users to a new group. Enter the name of the new group.
- **Send notifications to the user (options below)**
- **Send user account login details** – If you check this option, the system will send the user (if an email is specified for the user) directions on how to download and configure the soft token.
- **Send token setup instructions** - If you check this option the system will send the user (if an email is specified for the user) directions on how to install and activate their token.
- **Merge existing users** – Update existing user information if user already exists. If the imported user does not exist, it will be added. The SurePassID Login name is used to match the imported user data against existing users.
- **Import the good records even if some records have errors** – By default, if the system encounters errors during the import, all the imported records are backed out. If you check this box, the system will commit all the successfully imported records and ignore the bad records.

When ready, click the **Import** button and the Import process will begin. When the import has finished, the following form will be displayed.

Home | Users | Tokens | Audit Trail | SSO

fakeco.com | (Admin) | Logout

New | Import Users | User Groups | Usage Report

All (2) user records were added.

### Import Users Results

#### Import Summary

Import Started: 3:54:23 AM  
 Import Completed: 3:54:23 AM  
 Import File Name: import\_users1.csv  
 Total records in file: 2  
 Total records added: 2  
 Total records updated: 0  
 Total records with errors: 0  
 Email send errors: 0  
 Emails not sent (no address): 0  
 Emails sent: 0

Close

#### Import Log

Record Number	Result	Name	Serial Number	Additional Info	Notification Status
1	User Added	Ava Jade	FAKE00000051		
2	User Added	Cynthia Williams	FAKE00000052		

## SurePassID Import Users – Import Results

The form is broken down into the Import Summary and Import Log Detail sections. The Import Summary shows the following information:

- Import Started
- Import Completed
- Import File Name
- Total records in the file
- Total records added
- Total records updated
- Total records with errors
- Email send errors
- Emails not sent (no address)
- Emails sent

The Import Log Detail shows the status of each import record and how it was processed by the system. If an error was detected, then it is noted in the **Result** and **Additional Info** column.

## Member of Group

Selecting Member of Group as shown below will show all the groups the user is a member of.



Displays the following form:



## Tokens Folder

Selecting the **Tokens** folder shows the **Tokens List** form. The **Tokens List** form displays all the tokens that are defined in the system as shown below:

Action	Serial Number	User Defined Name	Status	Token Type	User
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	xxxx-12345		Enabled	Desktop Token	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	xxxx-000000001		Enabled	Desktop Token	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	NCHE10006006		Enabled	Desktop Token	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	NCHE10006010		Enabled	Desktop Token	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	NCHE10006007		Enabled	Desktop Token	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	80254361		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	80254370		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	80254364		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	ICT-10005745		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	ICT-10006744		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	ICT-10006750		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	TPT-10000154		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	ICT-10005270		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	PASS10001001		Enabled	Matrix Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	PASS10001000		Enabled	Matrix Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	PASS10001003		Enabled	Matrix Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	PASS10001004		Enabled	Matrix Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	TPT-00000149		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	TPT-00000150		Enabled	SurePassID OTP Display Card	<not assigned>
<a href="#">Edit</a>   <a href="#">Delete</a>   <a href="#">Check</a>	TPT-00000152		Enabled	SurePassID OTP Display Card	<not assigned>

### SurePassID Tokens Tab

The **Token List Form** has two sections. The **Tokens Filter Section** allows you to search for specific tokens. The second section, the **Tokens List Section**, allows you to perform actions on specific tokens that meet the search criteria specified in the **Token Filter Section**.

The Token filters are:

- **Token Group** – Filter tokens from a specific group of tokens. (A pull-down menu will list the available groups)



- **Token Type** – Filter tokens based on token type. (A pull-down menu will list the available token types)
- **Token Status** – Filter tokens based on status. (Assigned or Unassigned)
- **Serial Number (Any, Begins With, Is, Contains)** – Filter tokens that have a serial number with a particular value or portion of a value.
- **User (Any, Begins With, Is, Contains)** – Filter tokens that have an assigned user that includes a particular value or portion of a value in Login Name, First Name, or Last Name.
- **Rows to Display** – Choose the number of rows to show on screen.

The actions you can take on each token are:

- **Edit** – Edit a token.
- **Delete** – Delete a token.
- **Check** – Verify a passcode for a token.

The folder has the following action bar:

- **New** – Add a new soft token.
- **Import Hard Tokens** – Import hard tokens.
- **Token Groups** – Import & create Tokens with Group options.
- **Token Usage Report** – Creates a CSV report file showing: Token Serial Number, Secret Key Expiration, Activation Date, Username, StatusDisplay, DeviceTypeDisplay, OTPTTypeDisplay, Last OTP Date

Token Groups are a logical way of grouping physical tokens. You do not have to use token groups, but it has the following advantages when managing large numbers of tokens in your system:

- **Token Import** – Deleting a token group can delete all the Tokens in the token group. This is significant if:
  - You import a group of tokens and make a mistake (such as setting one of the import options incorrectly), you can easily remove all those tokens by deleting the token group and importing them again.
  - It is time to decommission groups of old tokens, you know all the tokens in that token group and users that are assigned to them.
- **Token Decommission** – If there is a problem with a Token Group of tokens, or the tokens are reaching the end of their life you can easily identify the users that will need to have replacement. When the replacements arrive, you can easily assign the existing users new tokens and delete the old Token Group's tokens.

- **Token Manufacturer Management** – Placing all tokens from a particular manufacturer order into a Token Group allows you to easily view all tokens for that manufacturer in case you need to obsolete or discontinue the manufacturer.
- **Token Type Management** – Placing a batch of tokens in a Token Group allows you to easily view all tokens in service for a particular type of token.

**TIP:** Certain system functions such as Token Import can automatically create a new Token Group; all the imported tokens are placed in that token group.

The screenshot shows the SurePass ID web application interface. At the top, there is a navigation bar with links for Home, Users, Tokens, Audit Trail, and SSO. The user is logged in as Admin. Below the navigation bar, there is a 'New' button. The main content area is titled 'Token Groups' and contains a table with the following data:

Action	Description	Tokens	Created On	Last Updated	Last U
<a href="#">Edit</a>   <a href="#">Delete</a>	Batch created as part of device import.	2	1/25/2010 3:18:06 PM	1/25/2010 3:18:06 PM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Batch created as part of device import.	1	1/26/2010 4:07:05 AM	1/26/2010 4:07:05 AM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Batch created as part of device import.	3	5/10/2010 4:28:01 AM	5/10/2010 4:28:01 AM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Batch created as part of device import.	2	5/13/2010 9:10:18 AM	5/13/2010 9:10:18 AM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Batch created as part of device import.	1	5/17/2010 2:57:57 PM	5/17/2010 2:57:57 PM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Batch created as part of device import.	1	9/3/2010 2:46:04 AM	9/3/2010 2:46:04 AM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Imported Display Card for OCTA Demo	1	10/1/2010 5:07:36 AM	10/1/2010 5:11:04 AM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Imported Demo Matrix Cards for OCTA Demo	4	10/1/2010 5:08:42 AM	10/1/2010 5:10:34 AM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Batch created as part of device import.	3	10/8/2010 10:27:18 AM	10/8/2010 10:27:18 AM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Batch created as part of device import.	12	11/27/2010 2:58:21 AM	11/27/2010 2:58:21 AM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Batch created as part of device import.	13	11/27/2010 3:00:02 AM	11/27/2010 3:00:02 AM	Mark Poid
<a href="#">Edit</a>   <a href="#">Delete</a>	Token Group created as part of user import.	2	5/20/2021 3:46:36 AM	5/20/2021 3:46:36 AM	
<a href="#">Edit</a>   <a href="#">Delete</a>	Token Group created as part of user import.	2	5/20/2021 3:54:23 AM	5/20/2021 3:54:23 AM	

At the bottom of the table, there is a pagination control showing '1 page(s): [1]'.

### SurePassID Token Group Folder

The **Token Groups** folder has the following action bar:

- **New** – Add a new token group

The actions you can take on each token group are:

- **Edit** – Edit the token group.
- **Delete** – Delete the token group.

## Managing Token Groups

When you edit or add a new token group, the following form will be displayed:

The screenshot shows the 'Update Token Group' form in the SurePassID interface. The form has the following fields:

- Description: Batch created as part of device import.
- Notes: (Empty text area)
- Tokens In Group: 2
- Created On: 1/25/2010 3:18:06 PM
- Last Updated On: 1/25/2010 3:18:06 PM
- Last Updated By: Mark Poid

Buttons for 'Update' and 'Close' are located below the form fields.

Below the form is a table titled 'Tokens' with the following data:

Action	Serial Number	User Defined Name	Status	Token Type	Last OTP Validation	
<a href="#">Edit</a>   <a href="#">Delete</a>	NCHE10006006		Enabled	Desktop Token	1/25/2010 6:37:59 PM	T
<a href="#">Edit</a>   <a href="#">Delete</a>	NCHE10006010		Enabled	Desktop Token		T

### SurePassID Token Group Detail

The following fields are displayed on the Token Group Detail Form:

- **Description** – A descriptive name for this token group.
- **Notes** – Detail information about this token group.
- **Tokens In Group** – The number of tokens in this group.
- **Created On** – The date this token group was created.
- **Last Updated On** – The date this token group was last updated.
- **Last Updated By** – The last user to update this token group.
- **Tokens** – The Tokens assigned to this token group.

After entering the information about the token group, press the **Update** button to update the token group or the **Add** button to add the Token Group.

## Managing Tokens

When you edit or add a new token, the following form will be displayed:

**SurePass id**

Home Users Tokens Audit Trail SSO fakeco.com (Admin) Logout

New Import Hard Tokens Token Groups Token Usage Report

This token is new. It must be enabled or activated by the user before it can be used.

**Add Token** [New](#) [Add](#) [Close](#)

**Token Information**

Token Group: None

Token Type: SurePassID Authenticator Token

Assigned To:

Printed Serial Number: FAKE00000053

User Defined Token Name:

Internal Serial Number: 00000053

Status: Enabled

Provision Expiration Date: 05/22/2021

Authenticator Usage: OTP Authentication Only

Maximum Uses: 999999999

Mobile Setup Verification: No mobile user verification

Manufacturer: SurePassID

**One Time Passcode Settings**

OTP Type: Time (Oath)

OTP Length: 6 Digits

Time Step (secs.): 30

Time Drift (time step units): 3

Starting Time [T0] (secs.): 0

Add Close

## SurePassID Token Detail

**SurePass id**

Home Users Tokens Audit Trail SSO fakeco.com (Admin) Logout

New Import Hard Tokens Token Groups Token Usage Report

This token is enabled.

**Update Token** [New](#) [Update](#) [Close](#) [Reset Token](#) [Share Token](#)

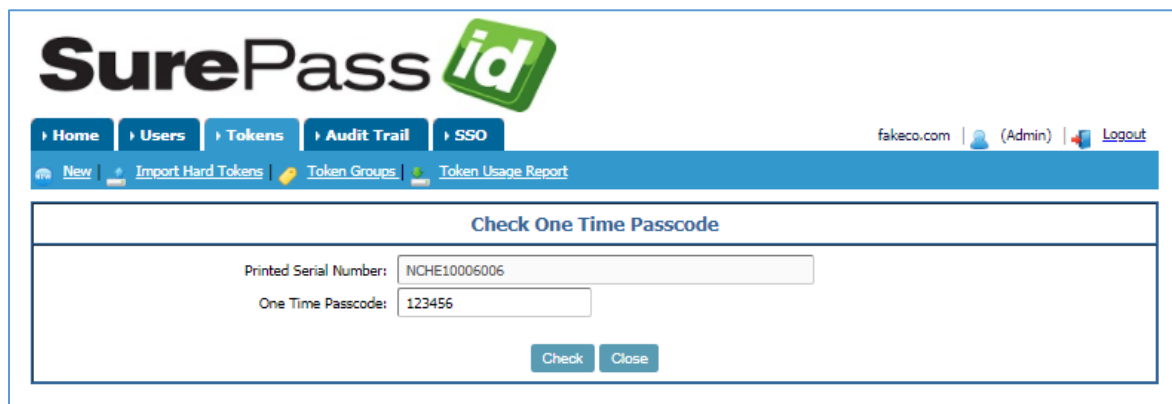
Check OTP Create Temporary Passcode Synchronize

The following buttons are displayed on the top of the Token Detail form:

- **Check OTP** – Checks an OTP for validity.
- **Create Temporary Password** – Displays a form to create a temporary OTP for this token. The lifetime for this OTP is governed by the **Temporary OTP is valid for** setting as part of System settings.
- **Synchronize** – Displays a form to synchronize physical Tokens with the authentication server.
- **Filter Assign To List** – Filter the **Assigned To** list.

### ***Check One Time Passcode***

Pressing the **Check OTP** button displays the following form:



The screenshot shows the SurePassID web interface. At the top, there is a navigation bar with tabs for Home, Users, Tokens, Audit Trail, and SSO. The user is logged in as Admin on fakeco.com. Below the navigation bar, there is a sub-header for 'Check One Time Passcode'. The form contains two input fields: 'Printed Serial Number' with the value 'NCHE10006006' and 'One Time Passcode' with the value '123456'. Below the fields are 'Check' and 'Close' buttons.

### **SurePassID Check One-Time Passcode**

Enter the one-time passcode into the **One-Time Passcode** field and click the **Check** button. The form will display the results of the check. To close the form, press the **Close** button.

### ***Create Temporary Passcode***

Clicking the **Create Temporary Passcode** button displays the following form:

### SurePassID Create Temporary Passcode

Enter the minutes and seconds for the temporary password and press the **Create Passcode** button. The form will be updated to display the temporary OTP. To close the form, press the **Close** button.

### Synchronizing Token

Pressing the **Synchronize** button displays the following form:

### SurePassID Synchronize Token

Enter the time period into **Time Window To Search** field and the One-Time Passcode from the token and click the **Synchronize** button. The form will display the results of the synchronize process. To close the form, press the **Close** button.

The following buttons are displayed on the Token Detail form




- **Token Group** – The token group this token is assigned to.
- **Token Type** – The system soft tokens and hard tokens.

The following soft tokens are supported:

- Desktop Token ○ FIDO Token ○ Google Authenticator Token (OATH/OATH compatible soft tokens)
- Nymi Band ○ SurePassID Authenticator Token (includes Dynamic CVx) ○ SurePassID TapID™ ○ Voice Message OTP

The following hard tokens are supported:

- SurePassID FOB and all OATH/OATH compatible hard tokens
- SurePassID OTP Display Card
- SurePassID TapID™ Treo / Yubikey Neo
- SurePassID OneCard
- SurePassID Dynamic CVx Card

- **Assigned To** – The user the token is assigned to.
- **Printed Serial Number** – The serial number printed on the token.
- **Serial Number** – Internal serial number.
- **Status** – The status of the token. The status can be New, Enabled or Disabled. When soft Tokens are created or hard Tokens are imported, they are set to a status of New. Tokens cannot be used unless they are enabled. Tokens become disabled by the administrator or automatically disabled if the token has exceeded the maximum failed authentication requests.
- **Expiration Date** – The date this token expires and will no longer be valid. Useful for part time, seasonal, contract workers, and consultants.
- **Token Id** – The unique ID for the token. Can be used to manually add a token to an authenticator app. (The following options are visible if the token has not yet been activated) ○ Click the  to send the user a token activation email ○ Click the  to send the user a token activation SMS.
  - Click the  to display the activation QR code.

- **Authenticator Usage** – Options for OTP auth only or both OTP auth and push. (requires use our push enabled authenticator app on a mobile device)
- **Maximum Uses** – The maximum number of times the token can be used before it is disabled.
- **OTP Activation Date** – The date the token was activated by the user. If the token is a soft token and is eligible for activation or re-activation (reactivation is only allowed for a token that has not already been authenticated to SurePassID) several icons will be visible to the right of the **Token Id**.
- **Mobile Setup Verification** – Choose whether the mobile user is required to verify the activation of a new token by logging into the system with their userid / password or not.
- **Manufacturer** – The manufacturer of the token.
- **OTP Type** – The type of the One-Time Password:
  - Event (OATH)
  - Time (OATH)
  - Time + PIN Based (OATH)
  - Challenge Response (OATH)
  - Card Security Code (CSC) Event
  - Card Security Code (CSC) Time
- **OTP Length** – The length of the One-Time Password:
  - 3 Digits (CSC Visa/MC)
  - 4 Digits (CSC Amex)
  - 6 Digits
  - 8 Digits
  - 10 Digits
- **Time Step (OTP Window Size)** – For Event (OATH) this parameter specifies the rolling window of the passcode. The typical value is 30 (events). This allows for inadvertent OTP events such as showing someone an OTP card or accidental presses. For Time (OATH), Time + PIN, and Challenge Response (OATH) this parameter specifies the number of rolling time periods of the passcode time units in seconds. The typical value is 30 seconds.
- **PIN** – The PIN for this token.
- **Time Drift (time step units)** – The initial time drift (in seconds) for a timebased token. Not used for event-based tokens.
- **Starting Time [T0] (secs.)** – The starting time for the time-based counter.



- **Current Time Counter** – The sliding parameter that is adjusting for realtime clock drift.
- **Last Validation** – The time the last OTP was authenticated for this token.
- **Failed Token Requests** – The current number of failed OTPs for this token.

## Importing Hard Tokens

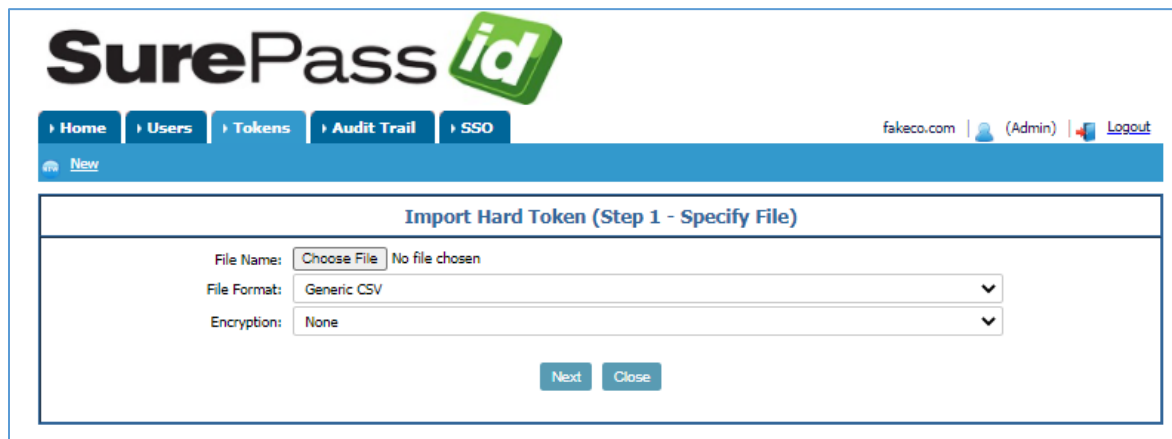
Physical Tokens such as display cards, key fobs, and SurePassID TapID™ are manufactured and programmed at external factories. The secret information stored in those tokens must be imported into the SurePassID authentication server. This secret information is securely provided with the physical tokens (not in the same package of course!) and referred to as a “seed file” or “key container” file.

Importing Tokens is a multi-step process. Below are the following steps to import tokens into the system.

1. **Select the import seed file**
2. **Map the fields in the import file to SurePassID fields**
3. **Select the option for the import**
4. **Import the tokens and review the results**

**Tip:** FIDO U2F hard tokens (that only support FIDO U2F) are treated as soft tokens because they have no secret keys specific to the hard token itself that need to be imported.

To start the hard token import wizard, select **Import Hard Token** from the action bar on the **Tokens** folder or any other forms in the system where you can see the **Import Hard Tokens** action and the following form is displayed:



The screenshot shows the SurePassID web application interface. At the top, there is a navigation bar with links for Home, Users, Tokens, Audit Trail, and SSO. The user is logged in as Admin. The main content area displays the 'Import Hard Token (Step 1 - Specify File)' form. The form has three input fields: 'File Name' with a 'Choose File' button and 'No file chosen' text; 'File Format' with a dropdown menu set to 'Generic CSV'; and 'Encryption' with a dropdown menu set to 'None'. At the bottom of the form are 'Next' and 'Close' buttons.

### SurePassID Import Tokens – Specify File

The first step in the process is to click the Browse button and select the import file.

- **File Name** – Press the **Browse** button and select the import file. After selecting the import file, you need to specify the following items:

- **File Format** – Select one of the following options based on the format of the import file:
  - Generic CSV
  - OATH 1.2 PSKC
- **Encryption** – Select the encryption format of the import CSV file. The system assumes zero trailing padding.
  - None
  - AES-128
  - AES-192
  - AES-256
  - PBE-AES-128
  - PBE-AES-192
  - PBE-AES-256

Once all the fields are specified, press the **Next** button to start the import process. If you selected **Generic CSV**, the Import Field mapping form will be shown:

The import file has 6 record(s). Each record has 2 column(s).

### Import Hard Token (Step 2 - Map Fields)

Sample Data From Import File

Column 1:	Column 2:
Serial#	Secret Key (Hex)
3358200011429	227CA26037FDF5EC3CDC648AB7AD16FBF1C00F21
3358200001039	16E8083CE35A4A9C4655AF0BDF68FBA99639F33
3358200012078	90AEE61762854D119EC10B0AB6D1E2FB68C44DFE
3358200012184	F44053B1CC2AEEE4069BF4C629B5C5FB79839ADD
3358200001005	433987C71BDEDC7BFACDC449480CEFBA79E30CE

Ignore first record in the import file:

### Map Import Data

Column 1: Printed Serial Number

Column 2: Secret Key (Hex)

Next Close

## SurePassID Import Tokens – Map Fields

The top of the form has the **Sample Data From Import File** section that gives you a preview of the data in the import file. The bottom half of the form has the **Map Import Data** section that allows the token to map each column of the import file to a SurePassID field.

Review each column in the **Map Import Data** section and select the corresponding SurePassID field. You can map the following fields to SurePassID:

- **RFID Tag**
- **Serial Number**
- **Maximum Number Of Uses**
- **Secret Key (Hex)**
- **Secret Key (Base64)**
- **Starting Counter T0**
- **Expiration Date**

After you have set the fields you plan to map, click the **Next** button and the Import Options form is displayed:

The screenshot shows the SurePassID web application interface. At the top, there is a navigation bar with links for Home, Users, Tokens, Audit Trail, and SSO. The user is logged in as Admin. The main content area is titled "Import Hard Tokens (Step 3 - Select Options)". The form contains the following fields:

- Manufacturer: SurePassID (dropdown)
- Token Type: SurePassID FOB Token (dropdown)
- OTP Type: Time (Oath) (dropdown)
- OTP HMAC Hash: SHA1 (dropdown)
- OTP Length: 6 Digits (dropdown)
- Time Step (secs.): 30 (input field)
- Time Drift (time step units): 3 (input field)
- Status: Enabled (dropdown)
- Notes: (large text area)

At the bottom of the form, there are two buttons: "Import" and "Close".

### SurePassID Import Tokens – Select Options

Select the following options for creating soft Tokens (credentials) for the Tokens being imported:

- **Manufacturer** – The vendor that manufactured the token.
- **Token Type** – The token type.
- **OTP Type** – The type of passcode the token displays.
- **OTP Length** – The number of digits the token displays.
- **OTP Window Size / Time Step** – For even-based tokens, the event counter window. For time-based tokens the number of seconds of each time step/time period. This is usually 30 or 60 seconds.
- **Time Drift** – The initial time drift (in seconds) for a time-based token. Not used for event-based tokens.
- **Notes** – Important information related to this import.

When ready, click the **Import** button and the import process will begin. When the import has finished, the following form will be displayed.

The screenshot shows the SurePass ID web interface. At the top, there is a navigation bar with links for Home, Users, Tokens, Audit Trail, and SSO. The user is logged in as Admin. A green banner at the top of the main content area displays the message: "All (5) records were imported successfully." Below this is a section titled "Import Results". Inside this section, there is a sub-section titled "Import Summary" which contains the following information:

- Import Status: All token records (5) were added.
- Import File Name: TOTP\_ImportToken.csv
- Records in import file: 6
- Total tokens in file: 6
- Tokens added: 5
- Tokens with errors: 0

Below the summary is a "Close" button. At the bottom of the "Import Results" section is an "Import Error Log" table with the following data:

Record Number	Result	Serial Number	Additional Info
1	Token added	3358200011429	
2	Token added	3358200001039	
3	Token added	3358200012078	
4	Token added	3358200012184	
5	Token added	3358200001005	

## SurePassID Import Tokens – Import Results

The form is broken down into the Import Summary and Import Log Detail sections. The Import Summary shows the following information:

- **Import Status**
- **Import File Name**
- **Records in import file**
- **Total tokens in file**
- **Tokens added**
- **Tokens with errors**

The Import Log Detail shows the status of each import record and how it was processed by the system. If an error was detected, then it is noted in the Result and Additional Info column.

## Audit Trail Folder

The Audit Trail folder allows you to view all the operations that take place in the system. Each operation that takes place in the system is referred to as an audit log item. Reviewing the audit log can be useful in the following ways:

1. Trouble- shooting connectivity problems with external Tokens such as VPN issues.
2. Reviewing who is accessing the system and what they are doing.
3. Reviewing who is trying to access the system but failing.
4. Addressing conditions that require your attention.
5. Trouble-shooting problems when developing new applications with the Software Development Kit.

All audit log items fall into one of the following categories:

1. **Success**
2. **Warning**
3. **Informational**
4. **Action Required**
5. **System Error**

Selecting the Audit Trail folder shows the Audits List form. The Audits List form displays all the audit log items defined in the system as shown below:

**Audit Trail**

Filter Users: All Request: Any Severity: Any

Start Date: 5/20/2021 End Date: 5/20/2021 Delete Checked Items Rows to Display: 20

	User	Login Name	Date	Request	Result Message
<input type="checkbox"/>		vadmin	05/20/2021 04:09:46.900	Temporary OTP	OTP [TEMPOTP] [152923] created for [NCHE
<input type="checkbox"/>		vadmin	05/20/2021 04:07:41.207	Admin Audit (Update)	Token NCHE10006006 has been modified.
<input type="checkbox"/>		vadmin	05/20/2021 03:47:29.617	Admin Audit (New)	Group Test data [From Account:] has not bee
<input type="checkbox"/>		vadmin	05/20/2021 03:28:55.907	Admin Login	User has logged into the system.[110.226.16.
<input type="checkbox"/>		vadmin	05/20/2021 03:28:55.900	Request Push Auth	PUSH [APP QUESTION] OK
<input type="checkbox"/>		vadmin	05/20/2021 03:28:55.897	OTP Validation	Your account has expired on 8/6/2013 1:01:0
<input type="checkbox"/>	None		05/20/2021 03:28:55.597	Send Push Message	Authentication Id [sxJJ8-OFvR3-KkPM3] is inv
<input type="checkbox"/>	None		05/20/2021 03:28:55.483	Send Push Message	Authentication Id [sxJJ8-OFvR3-KkPM3] is inv
<input type="checkbox"/>	None		05/20/2021 03:28:55.477	Send Push Message	Authentication Id [sxJJ8-OFvR3-KkPM3] is inv
<input type="checkbox"/>		vadmin	05/20/2021 03:28:54.967	Send Push Message	The authentication message cannot be cance
<input type="checkbox"/>		vadmin	05/20/2021 03:28:54.960	Send Push Message	Authentication Id [sxJJ8-OFvR3-KkPM3] has t
<input type="checkbox"/>		vadmin	05/20/2021 03:28:54.890	OTP Validation	Your account has expired on 8/6/2013 1:01:0
<input type="checkbox"/>		vadmin	05/20/2021 03:28:53.893	OTP Validation	Your account has expired on 8/6/2013 1:01:0
<input type="checkbox"/>		vadmin	05/20/2021 03:28:52.907	OTP Validation	Your account has expired on 8/6/2013 1:01:0
<input type="checkbox"/>		vadmin	05/20/2021 03:28:51.897	OTP Validation	Your account has expired on 8/6/2013 1:01:0
<input type="checkbox"/>		vadmin	05/20/2021 03:28:50.893	OTP Validation	Your account has expired on 8/6/2013 1:01:0
<input type="checkbox"/>		vadmin	05/20/2021 03:28:49.897	OTP Validation	Your account has expired on 8/6/2013 1:01:0
<input type="checkbox"/>		vadmin	05/20/2021 03:28:48.890	OTP Validation	Your account has expired on 8/6/2013 1:01:0
<input type="checkbox"/>		vadmin	05/20/2021 03:28:47.903	OTP Validation	Your account has expired on 8/6/2013 1:01:0
<input type="checkbox"/>		vadmin	05/20/2021 03:28:46.893	OTP Validation	Your account has expired on 8/6/2013 1:01:0

2 page(s): [1] 2

### SurePassID Audit Trail Folder

The Audit List Form has two distinct sections. The first section is the Audit Filter Section where you can search for specific audit log items based on several different search criteria. The second section, the Audits List Section, allows you to perform actions on specific audit log items and only displays the audit log items that meet the search criteria specified in the Audit Filter Section.

The Audits folder has the following action bar:

- **Export Audit Log** – Export the audit log.
- **Delete These Log Items** – Deletes the log items that are part of the current Audit Filter Selection.
- **Empty Log** – Deletes the complete audit log.
- **Refresh** – Refresh the Audit List Section.

The Audit Filter Section parameters are:



- **Audit Type** – Filter by request type.
- **Request** – Filter by request.
- **Severity** – Filter for a specific severity.
- **Start Date** – The start date for audit log items.
- **End Date** – The end date for audit log items.
- **Delete Checked Items** – Click this button to delete all the audit log items that are checked in the Audit List Section.
- **Rows to Display** – Select the number of rows to be displayed on screen.

## SSO (Single Sign-On) Folder

The SSO folder allows you to configure and manage all the identity management and access control for your SAML 2.0-based SSO applications, such as Google Apps, Salesforce.com, and hundreds of others. The SurePassID SSO Identity Manager uses this configuration information to control access to your SSO applications regardless of the platform they are running on. SurePassID SSO runs on every internet-connected token that has a web browser.

Alternatively, the SurePassID SSO mobile app can be used to run your SSO apps from a native mobile app developed for Android, Apple and Blackberry phones. The SurePassID SSO mobile app integrates with BYOD and MDM providers to make deploying, provisioning and removals of apps a breeze.

SurePassID SSO is a role and policy based system. You can configure different users to have specific roles within the organization and associate those roles with access policies on a product by product basis, locking down your apps.

SurePassID ships with over 50 applications preloaded. However, there might be a need to add a new SAML 2.0 app that comes on the market, or your company might develop their own SAML 2.0 app. SurePassID can support these apps by allowing you to add new SAML 2.0 apps that are only visible to your company.

When you select the SSO Folder you will see the SSO configuration folder shown below:

The screenshot displays the 'Update Single Sign On (SSO) Settings' page in the SurePass ID administration console. The page is divided into three main sections: SSO Settings, Authentication Settings, and SSO Applications Available.

**SSO Settings:** This section contains several configuration options, all currently set to 'Disabled':

- SSO Login Support: Disabled
- User without a credential can login with only username and password: Disabled
- Users can change their password: Disabled
- Your logo url for SSO login form: (empty text field)
- SurePassID Identity Provider URL: <https://cloudsso.yourdomain.com/?d=tierasoft.com>
- SSO Public Certificate (.cer): Download Certificate | Show Certificate

**Authentication Settings:** This section includes:

- Secure Authentication Server: SurePassID

**SSO Applications Available:** This section features a table with columns for Action, Select Your SSO Apps, Login Method, and Policies. The table lists various applications with checkboxes for selection and a 'Policies' count of 0 for each.

Action	Select Your SSO Apps	Login Method	Policies
<input type="checkbox"/>	Google Apps	SAML2	0
<input type="checkbox"/>	GMail	SAML2	0
<input type="checkbox"/>	Google Docs	SAML2	0
<input type="checkbox"/>	Google Calendar	SAML2	0
<input type="checkbox"/>	SalesForce.com	SAML2	0
<input type="checkbox"/>	Zen Desk	SAML2	0
<input type="checkbox"/>	SugarCRM	SAML2	0
<input type="checkbox"/>	WebEx	SAML2	0
<input type="checkbox"/>	Accellion	SAML2	0
<input type="checkbox"/>	Atlassian JIRA Windows	SAML2	0
<input type="checkbox"/>	Atlassian JIRA Linux	SAML2	0

At the bottom of the table, there are 'Update' and 'Close' buttons.

## SurePassID SSO Configuration Folder

The following functions are available in the action bar:

- **Policies**
- **Roles**
- **Manage SSO Apps** (if you are a Super Admin)

The following fields are displayed in the SSO configuration folder:

- **SSO Login Support** – Globally turn SSO support on or off.
- **User without a credential...** – Allow users without two-factor authentication credentials to login to the system with single factor authentication (username and password).

- **Users can change their password** – Only supported for some SAML2 apps. Also, this field is ignored if Active Directory support is enabled.
- **You logo for SSO login form** – Customize the SSO login form with your company's logo. Enter the entire URL of your company logo such as <http://www.yourcompany.com/logo.gif>.
- **SurePassID Identity Provider URL** – The URL you provide to your users to login into SurePassID and have access to all of their SSO apps.
- **SSO Public Certificate (.cer)** – Options for downloading the certificate and show the certificate.
- **Secure Authentication Server** – Select your two-factor authentication server. SurePassID is the default but you can select popular legacy two factor authentication systems such as RSA, Vasco, Entrust, etc.
- **SSO Application List** – Check all the SSO apps that your company plans to use. After the form has been updated, you will then be able to configure each of those apps. Click the **New Custom App** link in the header to add your own SAML 2.0 app.

After making your selections, you can click the **Update** button to save your changes.

To configure each SSO app, click the **Configure** link next to the app.

## **Configuring SSO Apps**

When you press the **Configure** link on the SSO Configuration form, you can specify the configuration for that application. SurePassID will try to plug in the correct values for the fields, but you can always modify them based on the service provider app such as Google Apps, Salesforce.com, etc. If the application is a SAML 2.0 app, the following form will be displayed:

**SurePassID SAML2 Settings ( Identity Provider)**

App Name:

SAML2 Issuer:

SAML2 Subject Data Store:

SAML2 Subject Field:

Assertion Is Valid For: Hours:  Minutes:  Seconds:

**Application SAML2 Settings (Service Provider)**

SAML2 Issuer:

Assertion Consumer Service URL:

Audience URI:

How To Start App:

Login URL:

Logout URL:

**SAML2 Attributes**

Action	Attribute Name	Attribute Value
<a href="#">Edit</a>		

## SurePassID SSO SAML 2.0 Configuration Form

The following fields are displayed on the Configure SSO SAML 2.0 form:

- **SurePassID SAML2 Settings (Identity Provider)**
  - **App Name** – The SAML2 application name.
  - **SAML2 Issuer** – The SurePassID Identity Provider Issuer identification. The value needs to match the Identity Provider Issuer identification specified at the service provider SAML2 configuration settings.
  - **SAML2 Subject Data Store** – The only option for now is SurePassID.

- **SAML2 Subject Field** – This is the login name that will be sent to service provider for access after SurePassID authenticates the system. This needs to match what the service provider expects. The choices are:
    - **Email** – The user’s Email.
    - **Username** – The user’s Login Name.
    - **SSO Username** – The user’s SSO ID.
  - **Assertion Valid For** – The time that the SAML2 assertion is good for. Some service providers ignore this value and others will force the user to re-login when assertion is no longer valid.
  - **Application SAML2 Setting (Service Provider)** ○ **SAML2 Issuer** – This is the identification of the service provider that will make the request for access from SurePassID.
    - **Assertion Consumer Service URL** – The service provider URL that will accept the SAML2 assertion from SurePassID identity provider.
    - **Audience URI** – The service provider audience that this request is designated for.
    - **How To Start App** – SAML2 apps are usually designed to be initiated by the identity provider, service provider or both. This field specifies which one the service provider supports.
    - **Login URL** – The URL to login the user to the service provider. Not often needed.
    - **Logout URL** – The URL to logout the user from the service provider.
  - **SAML2 Attributes** – Additional SAML2 Attributes (name value pairs) that will be sent to the Service provider with the SAML2 assertion.
- If the application is a web form app, the following form will be displayed:

The screenshot shows the 'Add WebForm SSO App' configuration page in the SurePass ID administration interface. The page has a blue header with the SurePass ID logo and navigation links: Home, Users, Tokens, Audit Trail, SSO, Policies, and Roles. The user is logged in as 'Admin User'.

The main content area is titled 'Add WebForm SSO App' and contains a section for 'Web Form Login Settings'. The settings include:

- Login Web Form Type: Web Form POST (dropdown menu)
- App Name: (text input field)
- <form> name= and id= : myForm (text input field)
- Login Web Form URL: (text input field)

Below the settings is a table with the following data:

Action	Attribute Name	Attribute Value
<a href="#">Edit</a>	username	html_form_tag_user_username
<a href="#">Edit</a>	password	html_form_tag_user_password
<a href="#">Edit</a>		

At the bottom of the table are three buttons: Add, Close, and Show HTML Preview.

## SurePassID SSO Web Configuration Form

The following fields are displayed on the Configure SSO Web form:

- **Login Web Form Type**
  - **Web Form POST** – The web form login page supports the POST method.
  - **Web Form GET** – The web form login page supports the GET method.
- **App Name** – The application name.
- **<form> name= and id=** – Only valid for web forms that support the POST method. This is the name of the form that is created and posted to.
- **Login Web Form URL** – The web form URL that supports the login process.
- **Additional Parameters** – Additional parameter that will be part of the web form login process. For apps that support the POST method app, these parameters will be added to the form that is POSTed. For web form GET method apps, these parameters will be added to the GET request.

After making your selections, click the **Update** button to save your changes.

## Configuring SSO Policies

SurePassID allows you to configure different SSO use policies. These policies can then limit access to company resources such as applications, location, and time.

The SSO Policy List form displays all the policies defined to the system and allows you to copy, delete, update and add profiles as shown below:



The screenshot shows the SurePassID web application interface. At the top left is the SurePassID logo. Below it is a navigation menu with buttons for Home, Users, Tokens, Audit Trail, and SSO. On the right side of the navigation bar, there is a user profile for 'Admin User' and a Logout button. Below the navigation bar, there are tabs for Policies and Roles. The main content area is titled 'SSO Policies' and contains a table with three columns: Action, Policy Name, and Policy Violation Action. The table is currently empty. At the bottom left of the table area, it says '0 page(s): [1]'. There is a 'New' link in the top right corner of the table area.

### SurePassID SSO Policy List

The actions you can take on each policy are:

- **New** – Add a new policy to the system.
- **Edit** – Edit an existing policy.
- **Delete** – Delete an existing policy.
- **Copy** – Copy an existing policy.

Select the appropriate action and the SSO Policy Form will be shown as below:



**SurePass id**

Home | Users | Tokens | Audit Trail | SSO | tiersoft.com | Admin User | Logout

New Policy | Policies | Roles

### Add SSO Policy

[New](#) [Add](#) [Close](#)

#### Policy Settings

Policy Name:

Policy Violation Action: Enforce - Policy violations will prevent access and logged.

#### Time Restriction Policy

Day of the Week	Access Type	Start Time	End Time
Monday	Not Permitted Access	09:00 AM	05:00 PM
Tuesday	Not Permitted Access	09:00 AM	05:00 PM
Wednesday	Not Permitted Access	09:00 AM	05:00 PM
Thursday	Not Permitted Access	09:00 AM	05:00 PM
Friday	Not Permitted Access	09:00 AM	05:00 PM
Saturday	Not Permitted Access	09:00 AM	05:00 PM
Sunday	Not Permitted Access	09:00 AM	05:00 PM

#### Access IP Restriction Policy

Limit access to only these IP addresses

#### App and Roles Restrictions

Assign Apps	Assign Roles
<input type="checkbox"/> Google Apps <input type="checkbox"/> Gmail	

## SurePassID SSO Policy Form

The following fields are displayed on the Configure SSO App form:

### □ SurePassID SAML2 Settings (Identity Provider) ○

**Policy Name** – The name of this policy.

- **Policy Violation Action** – The action the system will take when someone violates a policy rule. Choices are:
  - **Log** – User is permitted access but the violation is logged in the audit trail.
  - **Enforce** – User is **not** permitted access and the violation is logged in the audit trail.
  - **Ignore** – User is permitted access and the policy is ignored.


- **Time Restriction Policy** – Set the allowable times that this policy will be used.
- **Access IP Policy** – You have two choices:
  - Allow access from any IP.
  - Limit access to only these IP addresses - Specify the allowable IP addresses for this policy. You can use wildcards for each IP address by limiting the trailing octets. You can also use multiple IP addresses by specifying a different IP address on each line.
- **App and Role Restrictions** – Specify the apps and roles that are bound to this policy.


Click the **Add** or **Update** button to save your policy settings.

## ***Configuring SSO Roles***

SurePassID allows you to configure roles for a set of users. These roles can then be applied to policies that you have defined in the system.

The SSO Role list displays all the roles defined to the system and allows you to copy, delete, update and add profiles as shown below:

**SurePass** 

[Home](#) | [Users](#) | [Tokens](#) | [Audit Trail](#) | [SSO](#)
tierasoft.com |  Admin User |  Logout

[Roles](#) | [Policies](#)

**SSO Roles** [New](#)

Action	Role Name	Description
<a href="#">Edit</a>   <a href="#">Copy</a>   <a href="#">Delete</a>	Test role	

1 page(s): [1]

### SurePassID SSO Role List

The actions you can take on each role are:

- **New** – Add a new role.
- **Edit** – Edit an existing role.
- **Delete** – Delete an existing role.
- **Copy** – Copy an existing role.

Select the appropriate action and the SSO Role Form will be shown as below:

**SurePass id**

Home Users Tokens Audit Trail SSO

tierasoft.com Admin User Logout

Update Role Policies Roles

**Update Role [Test role]** [New](#) [Update](#) [Close](#)

**Role Settings**

Role Name:

Role Description:

**Users In This Role**

<input type="checkbox"/>	Members Of This Role	Login Name	Status
<input checked="" type="checkbox"/>	Admin User	Administrator	Enabled
<input checked="" type="checkbox"/>	Admin User	Administrator1	Enabled
<input checked="" type="checkbox"/>	Matthew Stein	matt.stein1	Enabled
<input checked="" type="checkbox"/>	Matthew Stein	matt.stein	Enabled

### SurePassID SSO Role Form

The following fields are displayed on the SSO Role form:

- **Role Name** – The name of this role.
- **Role Description** – Short description of this role.
- **User In This Role** – Select the users that are in this role.

Click the **Add** or **Update** button to save your role settings.