Service Provider

Administrator Guide

SafeNet | Authentication SERVICE

Powerful Authentication Management for Service Providers and Enterprises

Version 3.2

Authentication Service Delivery Made EASY™

Copyright © 2012 SafeNet, Inc. All rights reserved.

All attempts have been made to make the information in this document complete and accurate. SafeNet, Inc. is not responsible for any direct or indirect damages or loss of business resulting from inaccuracies or omissions. The specifications contained in this document are subject to change without notice.

SafeNet and SafeNet Authentication Service are either registered with the U.S. Patent and Trademark Office or are trademarks of SafeNet, Inc., and its subsidiaries and affiliates, in the United States and other countries. All other trademarks referenced in this Manual are trademarks of their respective owners.

SafeNet Hardware and/or Software products described in this document may be protected by one or more U.S. Patents, foreign patents, or pending patent applications.

Please contact SafeNet Support for details of FCC Compliance, CE Compliance, and UL Notification.

Support

SafeNet technical support specialists can provide assistance when planning and implementing SafeNet Authentication Service. In addition to aiding in the selection of the appropriate authentication products, SafeNet can suggest deployment procedures that will provide a smooth, simple transition from existing access control systems and a satisfying experience for network users. We can also help you leverage your existing network equipment and systems to maximize your return on investment.

SafeNet works closely with channel partners to offer worldwide Technical Support services. If you purchased this product through a SafeNet channel partner, please contact your partner directly for support needs.

To contact SafeNet Authentication Service support directly:

Europe / EMEA		**North America**	
Freephone:	0800 694 1000 (UK)	Toll Free:	800-307-7042
Telephone:	+44 (0)1276 608 000 (Int'l)	Telephone:	+1 613 599 2441
E-mail:	sassupport@safenet-inc.com	E-mail:	sassupport@safenet-inc.com

Publication History

Date	Description	Revision
2012.08.31	Update for SMS Gateway redundancy	5.1
2012.06.01	Updates reflecting v3.2 release and SafeNet branding changes	5.0
2011.10.31	Updates reflecting v3.1 release	4.0
2011.08.05	Minor formatting repairs	3.0
2011.05.11	Added detail for customizing email messages and using self-service	2.0
2011.04.11	Initial Release	1.0

Contents

Applicability 14
Introduction 14
Purpose of this Guide 14
Audience 14
Terminology 15
Customer Feedback 15
Additional Reading 15
New in Version 3.2 17
Chapter 1 21
SafeNet Authentication Service (SAS, SPE, PCE) 21
Workflow Automation 22
Branding 22
Billing 22
Granular Security Roles and Scope 22
Management UI 24
Service Provider Views 24
Virtual Service Provider Views 24
Subscriber Views 25
Tabs and Modules 25
Management UI Conventions 26
The Virtual Server 27
Chapter 2 28
Dashboard Tab 28
Alerts Module 29
Viewing, Acknowledging and Closing Alerts 30
Subscriber Metrics Module 31
Inventory Module 32
On-boarding Tab 34
Create Account Shortcut 35
Services Module 36

Allocation Module 38
ICE (In Case of Emergency) 40
SMS Credits 40
Using the Allocation Wizard 40
Allocation Wizard for Sale, ICE and SMS transactions 45
Sale Transactions 45
ICE Transactions 45
SMS Credits Transactions 45
Transaction Log 46
De-Allocating an Account's Inventory 47
Deallocating MP-1/SMS Software Tokens and/or Capacity 47
Deallocating Hardware Tokens 49
Create Operator Module 51
Auth Nodes Module 53
Adding an Auth Node 54
Configuring Auth Nodes 56
Sharing and Realms 57
Contacts Module 59
Accounts List 59
Delegation Code Module 61
Using Delegation Codes 61
To generate and activate a delegation code 62
Administration Tab 67
Operational Security Overview 68
Account Management Groups Module 68
Creating Account Management Groups 69
Account Manager Roles Module 70
Creating an Account Management Role 71
Adding or Editing a Role 71
Module Actions 72
Account Manager Maintenance 73
Adding an Account Manager 74

Alert Event Thresholds 76
Role Alert Management 77
Viewing, Acknowledging and Closing Alerts 79
Reports and Billing Management 80
Available Reports Module 81
Customize Report 83
My Customized Reports Module 84
Schedule Report 84
My Scheduled Reports Module 85
My Report Output 85
Custom References 86
Agents and software download URL 86
Documentation download URL 86
Service Notifications 87
RADIUS Server IP Address 88
Account Role Provisioning Rules 89
Auto Remove 90
Virtual Servers Tab 91
Chapter 3 93
Snapshot Tab 94
Authentication Activity Module 94
Authentication Metrics Module 97
Token States Module 98
SMS Credits Module 98
Allocation Module 99
References Module 101
Assignment Tab 102
Creating Users 106
Create User Shortcut 106
Import Users Shortcut 108
LDAP Synchronization 110
LDAP Integration 111

User Detail Module 112
Tokens Module 112
Provision 115
Self-enrollment 116
Provisioning Tasks 117
Editing a Provisioning Task 118
Managing a User's Tokens 118
Managing a Token 120
Suspend 120
Unlock 121
New PIN 122
Resync 123
Initialize 124
Issue 124
Revoke 124
Authentication Metrics Module 125
Authentication Activity Module 125
Access Restrictions Module 126
Group Membership Module 127
RADIUS Attributes 127
SAML Services 128
Tokens Tab 129
Tokens Module 130
Import SafeNet Tokens Module 132
Import Third Party Tokens 133
RADIUS Tokens 133
SecurID Tokens 133
Bulk Assign Third Party Tokens 134
RADIUS Tokens 134
SecurID Tokens 135
OATH Token 135
Initialize Token Module 135

Preparing the KT series token for Initialization 136
Preparing the RB series token for Initialization 136
Groups Tab 137
Group Maintenance 137
Internal and Synchronized Groups 138
Group Maintenance 138
Group Membership Module 139
RADIUS Attribute (Group) Module 140
Set RADIUS Attribute 140
Viewing RADIUS Attributes (Group) 140
Containers 141
Creating Containers 141
Container Members Module 142
Moving Objects 142
Reports Tab 143
Available Reports Module 144
Customize Report 145
My Report List Module 146
Schedule Report 147
My Scheduled Reports Module 148
My Report Output 148
Self-Service Tab 149
Self-Service WSDL API 149
Self-Service Overview 149
Self-service Web Site 150
Self-service Site Appearance 152
Inheritance 152
Module Configuration 153
Languages 153
Authorities 153
Workflow 155
Provisioning Tasks 155

Reporting 155
Configuring Self-service 156
Self-Service Policy Module 156
Set Customization Inherit 157
Configure Self-Service Appearance 157
Configure Self-Service Buttons 158
Configure Self-Service Fonts 159
Configure Self-Service Modules 161
Language Set 161
Self-Service Module Options 162
Default Elements Module 163
Request a Token Module 164
User Type Page 165
Create Account Page 166
Token Type Page 166
Confirmation Page 167
Validation Page 168
User Page 168
Reset PIN Module 171
User Page 171
Select a Token Page 171
Create New PIN Page 172
Server Side PIN Page 172
Confirmation Page 172
Reset PIP Module 173
User Page 173
Select Pattern Page 174
Confirmation Page 174
Resync Token Module 175
User Page 175
Auth Resync Page 176
Time-based Resync Page 176

Challenge Response Page 176
Confirmation Page 177
Sign In Module 178
Authenticate Page 178
Authenticate to Process Page 178
Send Password by Email Page 179
Send Password by SMS Page 180
My Profile Module 180
Select to Proceed Page 180
View my logon statistics 181
View and update my profile 181
Update my security Questions and Answers 182
Question Management Page 182
Question Sets Page 183
Question Assignment 184
Configure Self-Enrollment Pages 184
My Token Request 184
Default/Common Page 185
Software Token Page 185
Custom Token Page 186
Hardware Token Page 186
Password Page 186
Self-Service Authorities Module 187
Configuring Authorities 188
Out of Band Notification 189
Request and Approval Queue Processing 189
Configure Request and Approval Queue Processing 189
Queue Management Module 191
Approval Level 1 192
Approval Level 2 192
Issue 192
Shipping Queue 193

Reporting 193
Operators Tab 195
Internal Operators Module 195
Adding an Internal Operator 196
Assign a Role 197
Assign Scope 197
Access Restrictions 197
Operator E-mail Validation 198
External Operator Module 199
Adding an External Operator Account (Delegation) 201
Modifying and Removing External Operators 203
Policy Tab 204
User Policies Module 204
Account Lockout / Unlock Policy 204
Token Policies Module 205
Token Templates 205
Token Passcode Processing Policy 209
Server-side PIN Policy 210
Temporary Password Policy 212
Synchronization Policy 213
SMS/OTP Policy 214
Token File Creation Policy 215
Allowed Targets Policy 216
MP Token Devices Policy 218
Third Party Authentication Options Policy 218
GrIDsure Method 219
RADIUS Tokens 220
RADIUS Tokens 220
SecurID Tokens 221
Bulk Assign Third Party Tokens 221
RADIUS Tokens 222
Role Management Module 225

Role Management Policy 225
Creating an Operator Role 226
Adding or Editing a Role 226
Module Actions 227
Alert Management Policy 228
External Alert Recipients Policy 230
Event Thresholds 230
Language 232
Automation Policies Module 233
Provisioning Rules 233
Self-enrollment Policy 235
SAML Provisioning Rules 236
Auto Remove 237
Comms Tab 238
Communications Module 238
Custom SMS Settings 239
E-mail Settings 240
Custom E-mail Settings 241
SMS Messages 242
Custom SMS Messages 242
E-Mail Messages 243
Custom E-mail Messages 244
LDAP Sync Server Settings 273
FTP/SFTP/SCP Settings 273
LDAP Module 274
LDAP User Source 274
LDAP/Active Directory Integration 275
Schema Management 276
Authentication Processing Module 278
Pre-authentication Rules 278
Configure Pre-Authentication Rules 279
Agent is 280

Date Restrictions 280
IP 281
LDAP Password Pass Through 281
User is a member of 282
Authentication Agent Settings 282
Remote Service Settings 283
LDAP Sync Agent Settings 283
ICE Activation 284
LDAP Sync Agent Hosts 284
Auth Node Module 285
Configuring Auth Nodes 286
Sharing and Realms 286
SAML Service Providers Module 288
Custom Branding Module 295
Custom Fonts 296
Custom Colours 296
Custom Colours – Logon Page 297
Custom Colours – Management UI 297
Custom Buttons 297
Custom Logo Images 298
Custom Titles 299
Custom Labels 301
Custom Product Name 301

Applicability

The information in this document applies to:

- SafeNet Authentication Service (SAS)
  A cloud authentication service of SafeNet Inc.
- SafeNet Authentication Service – Service Provider Edition (SAS-SPE)
  The software used to build a SafeNet authentication service.
- SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)
  A term used to describe the implementation of SAS-SPE on-premise.

Introduction

Purpose of this Guide

This guide describes the functionality of SafeNet Authentication Service (SAS, SPE and PCE Editions) from the perspective of the Service Provider Account Manager role. It describes all of the process required to:

- On-board accounts including tasks such as service creation, inventory management, workflow automation and management by exception.
- Manage account Virtual Servers.
- Generate audit, compliance, usage and billing reports.
- Use Operational Security to establish Account Manager Roles, Scope and Access Restrictions.
- Brand and customize the service delivered to subscriber accounts.

Readers are encouraged to read this guide in the order in which information is presented as successive chapters often rely on information and concepts presented in prior chapters.

Audience

This guide is intended for SafeNet Authentication Service – Service Provider Administrators, responsible for how managed authentication services are delivered to accounts and for configuring the Service to reflect the Service Provider's internal business processes, Service Level Agreements and management hierarchy.

Terminology

Several terms and their meaning are important to understanding the information presented in this guide:

Virtual Server
This term refers to an individual account's authentication server (virtual).

Subscriber
When presented in lower case "subscriber" the term applies to all accounts that you create and manage. When presented in proper case, the term "Subscriber" refers to accounts that are not Service Providers.

Root Service Provider
This refers to the root organization that has installed and "owns" SAS, SAS-SPE or SAS-PCE. Every other organization is either a "Virtual Service Provider" or "Subscriber". A Root Service Provider has its own virtual server Virtual Server, and is able to create and manage Virtual Service Provider and Subscriber accounts it creates on SAS, SAS-SPE or SAS-PCE.

Service Provider
A Service Provider has its own virtual server Virtual Server, and is able to create and manage Virtual Service Provider and Subscriber accounts it creates on SAS, SAS-SPE or SAS-PCE.

Virtual Service Providers
A Virtual Service Provider has its own virtual server Virtual Server, and is able to create and manage Virtual Service Provider and Subscriber accounts it creates on SAS, SAS-SPE or SAS-PCE.

Are service provider accounts which have a service provider as a parent.

Customer Feedback

Help us to improve this documentation, our products and our services by communicating any ideas and suggestions that you feel would improve the usefulness and clarity of the documentation, product feature set or application in practice. Suggestions should be sent to:

sasfeedback@safenet-inc.com

Additional Reading

This guide is supplemented by a range of integration, branding and subscriber guides. These include:

- Service Provider QuickStart Guide.
- Operator Guide for Subscribers.
- LDAP Synchronization Agent Guide.

- Branding and Customization Guide.
- Service Provider Billing and Reporting Reference Guide.
- Using SafeNet Authentication Service to protect:
    - Network Access through VPNs, Citrix, Terminal Server and other similar remote access methods.
    - Logon to Windows and Linux machines and networks.
    - Microsoft Web Application such as OWA, SharePoint and Remote Web Workplace.
- Cloud applications such as Salesforce.com, Google Apps etc.
- Custom Web applications.
- Best Practices for migration users and companies to your service including transparent, interruption-free migration:
    - From an in-house strong authentication solution.
    - From static passwords.
    - For mixed environments supporting B2B, B2C and other combinations of users and organizations.
    - Using and importing 3rd party authenticators.
    - Extending Services to complex organizations with:
    - Regional cost centres.
    - Distributed management.
    - Complex networks including multiple LDAP directories and user sources.

New in Version 3.2

The following new features and functionality have been added:

- Self-service / Self-enrollment (refer to Self-Service Tab on page 149)

  This has been completely refactored to be highly customizable and very user centric. For example:

  Users can now request a token which in turn can be tied to a very flexibly approval and issuing process. This is ideal for organization that wants to offer strong authentication as an option to consumers in an efficient, low-touch service.

  - The entire user experience can be customized:
  - Logos, backgrounds, colours
  - Multilingual pages and descriptions
  - Optimized experience based on the user's computing platform
    - OS
    - Colour
    - Resolution
    - Browser
  - Detailed audit and activity reports.

- New Tokens
  - The MP-1 software token can now be provisioned to Windows Mobile 7+ and Blackberry (replacing the ST-1 token for Blackberry).
  - The MP-1 developer SDK is included with this release, allowing developers of applications to integrate the MP-1 token. Examples would be developers of iOS applications that want integrated strong authentication without the need to launch a 3rd party authenticator.
  - SafeNet Authentication Service now supports SafeNet eToken Pass, Gold and Platinum tokens. (refer to Import SafeNet Tokens Module on page 132)
  - GrID tokens
    - Can now be used with SAML authentication
    - The PIP length for GrID tokens can now be modified (refer to GrIDsure Method on page 219)

- RADIUS Token Authentication

  This is a new feature that allows 3rd party tokens to be managed through SafeNet Authentication Service, (adding/suspending deleting tokens, automatic replacement, billing, usage etc.). This feature requires the 3rd party authentication server to support RADIUS. (Refer to RADIUS Tokens on page 133)

- Agents
  - An LDAP synchronization agent that installs on Linux is now available
- Management UI Enhancements
  - A “pinning” feature has been added to all modules displayed on tabs. Now, when a new module is activated, the previous module automatically closes, unless it has been “pinned” open. This enhancement helps keep the active module in the display area. (Refer to Management UI Conventions on page 26)
  - The Virtual Servers list now distinguishes between directly managed accounts and delegated management. (Refer to Virtual Servers Tab on page 91)
  - It is now possible to search for users in a virtual server by email address.
- Reporting

  Several enhancements and new reports are added in this version:

  - Suspended Tokens Report
  - It is now possible to schedule reports for periodic delivery to an FTP, SFTP or SCP server.
  - A “stale date” can be set for generated reports, after which the report is automatically removed from the virtual server.
- SAML

  The logon experience has been enhanced for users that have accounts with two or more SAML service providers (e.g. Salesforce, Google Apps…etc.) such that once a user has authenticated for one service provider, they need not reauthenticate for any of their SAML service providers. Likewise, when they log off any one service provider, they are automatically logged off all other service providers.
- SafeNet Authentication Service Cloud Licensing

  The interpretation of Capacity has been changed in v3.2 to mean the maximum number of users that can authenticate against the service. In v3.1 and early Capacity determined the maximum number of tokens that can authenticate against the service. The change in v3.2 makes it easier and

more economical to issue multiple tokens to the same user. A typical use case would be for a user that wants a token on every computing device they use (laptop, mobile phone, tablet, SMS…) without negatively impacting the cost of the service.

The “Service stop date” for accounts created by Service Providers on SafeNet Authentication Service Cloud cannot be extended beyond the Service Stop Date of the Service Provider’s Virtual Server.

- Workflow Automation
  - Promote to Operator / Account Administrator

    It is now possible to automatically promote a user in SafeNet Authentication Service Cloud to Operator level with an assign a role based on the user’s LDAP/Active Directory security group membership. Refer to Account Role Provisioning Rules on page 89.
  - User Aliases

    It is now possible to assign “aliases” to users. This means that if the user “Bob” has an alias of “Bob-Admin”, he can logon as either Bob or Bob-Admin using the same token. This is a useful feature for SysAdmins who can use a less privileged account for general activities and an elevated account for high asset value activities, without needing more than one token.
  - From Address

    The "From Address" in E-mail settings can now be set in each virtual server without overwriting other default or inherited E-mail settings.
  - Global Replace

    It is now possible to globally replace all occurrences of the term “SafeNet Authentication Service ID” in email and SMS notifications.
  - Alerts

    In previous versions, customers often did not know when their service provider fulfilled an order for tokens and/or capacity. As of v3.2 an alert can be generated automatically and delivered by email, SMS to the customer every time their service provider adds or removes capacity from the customer’s inventory.

    It is now possible to configure custom SMS gateways for sending alerts and one-time passcodes. Default configurations for common SMS gateways supported in v3.1 and earlier continue to be supported.

- API's
  - An api that allows Microsoft Azure developers to build authentication against SafeNet Authentication Service Cloud Managed Service is now available.
  - The management API (WSDL) now support the functionality found on the "Reports Tab".

Chapter 1

SafeNet Authentication Service (SAS, SPE, PCE)

SafeNet Authentication Service is an enterprise class authentication server designed to extend authentication services to users in a single organization or across an unlimited number of entities. These entities can be almost anything, from divisions or cost centres within a company, to subsidiaries or completely independent organizations. It's multi-tier, multi-tenant structure accommodates just about any hierarchy, reporting structure, business structure, security segregation or other delineation.

SafeNet Authentication Service – Private Cloud Edition is meant for organizations requiring an "On-premise" solution.

Safenet Inc. has implemented SafeNet Authentication Service – SPE in its high availability Cloud infrastructure, providing organizations a highly economical and effective Cloud-based management authentication service alternative.

In addition, SafeNet Authentication Service can be used to extend authentication services beyond the corporate perimeter. By supporting SAML, many Cloud applications, from Google Apps and Salesforce through Box.net and web SSO services such as Symplified can be protected by SafeNet Authentication Service. Better yet, users will authenticate with the same UserID and token(s) they use for the corporate network, providing a single, consistent and familiar logon experience.

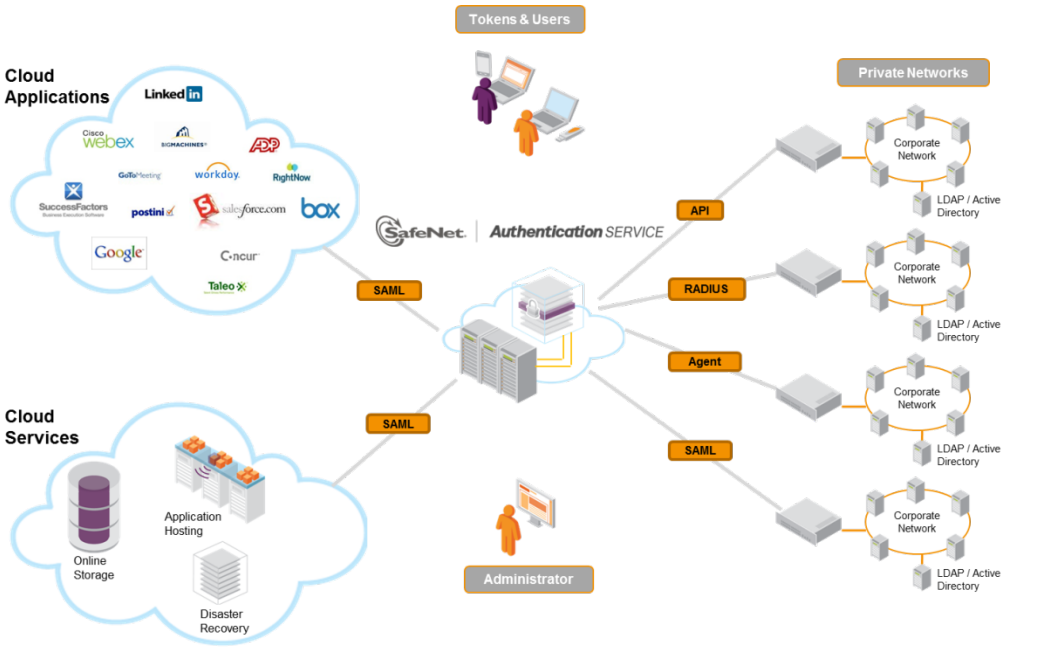


Figure 1: SafeNet Authentication Service Authentication Service Delivery Platform

Throughout this guide we use the term “Service Provider”. This is meant to capture the notion of delivering authentication as a service, whether SafeNet Authentication Service is installed on-premise or consumed as a cloud service. While authentication methods and interoperability remain significant factors you’ll find a significant focus in SafeNet Authentication Service is on using automation to simplify and streamline user and authentication management, driving the cost of service delivery into the ground. Key features include:

Workflow Automation

Accomplished through easy to configure Policy engines that can manage users, provisioning tasks, access control and much more based on changes in LDAP.

Management by Exception
These are alerts delivered through the UI, SMS and email in response to business, security and workflow conditions and other thresholds.

Branding

This goes beyond adding logos to complete customization of all user facing emails, web pages, alerts and URLs.

Billing

A flexible solution that allows inter and intra company billing for services.

Granular Security Roles and Scope

The ability to control right down to the “button” level, who can to what and to whom, all of which is captured in the database for extensive audit control and by alerts for real-time notification of changes to security posture are important.

No matter how many entities you add to your service, each will appear to have a discrete enterprise authentication server, what we throughout this documentation call a “Virtual Server”.

When you as a Service Provider log into the management UI, you’ll be able to view and manage all of your accounts and their Virtual Servers independently. While you will likely standardize on a few service offerings, this independence means that you can customize your service for individual accounts without affecting any other account’s service. This includes pricing, billing, branding and much, much more.

SafeNet Authentication Service does not obligate you to manage all aspects of an account’s service. In fact you can allow some or all of your accounts to manage their own Virtual Server.

SafeNet Authentication Service includes workflow automation and management tools that can reduce your on-boarding and management costs to near zero. For example, by combining LDAP synchronization with provisioning rules, each time your account adds a user in their LDAP server, SafeNet Authentication Service within minutes will automatically create the user account in their Virtual Server and provision the user with a token. All of this without your staff clicking a mouse button.

Finally, you can use SafeNet Authentication Service to create “Virtual Service Providers”. As a Virtual Service Provider, your account can create and manage their own “Subscribers”. You can use Virtual Service Providers to create additional sales channels that resell your service under your banner or under their brand. Of course virtual service providers are not limited to being resellers. They can also be large, complex end-users accounts that need to independently extend and manage the service delivered to many subsidiaries or cost centres, or to accommodate multiple LDAPs and user data sources, or to share access to protected resources across organizational boundaries.

Management UI

Account type determines the view and functionality presented in the management UI.

Service Provider Views

The Service Provider View [Figure 2: Service Provider View - Management UI] includes a row of tabs in the banner area [1] through which Account Managers can manage the service and all of their accounts including On-boarding, Virtual Server Management, Operational Security, Service Metrics and Alerts.

When an Account Manager selects an account's Virtual Server for management, a second row of tabs appears [2] through which they can manage the account's users, tokens, reports, policies etc. The name of the account being managed is displayed above this row of tabs.

The content of Shortcuts and the main work area below the banner is dependent upon which Service Provider tabs or Virtual Server tabs have been selected.

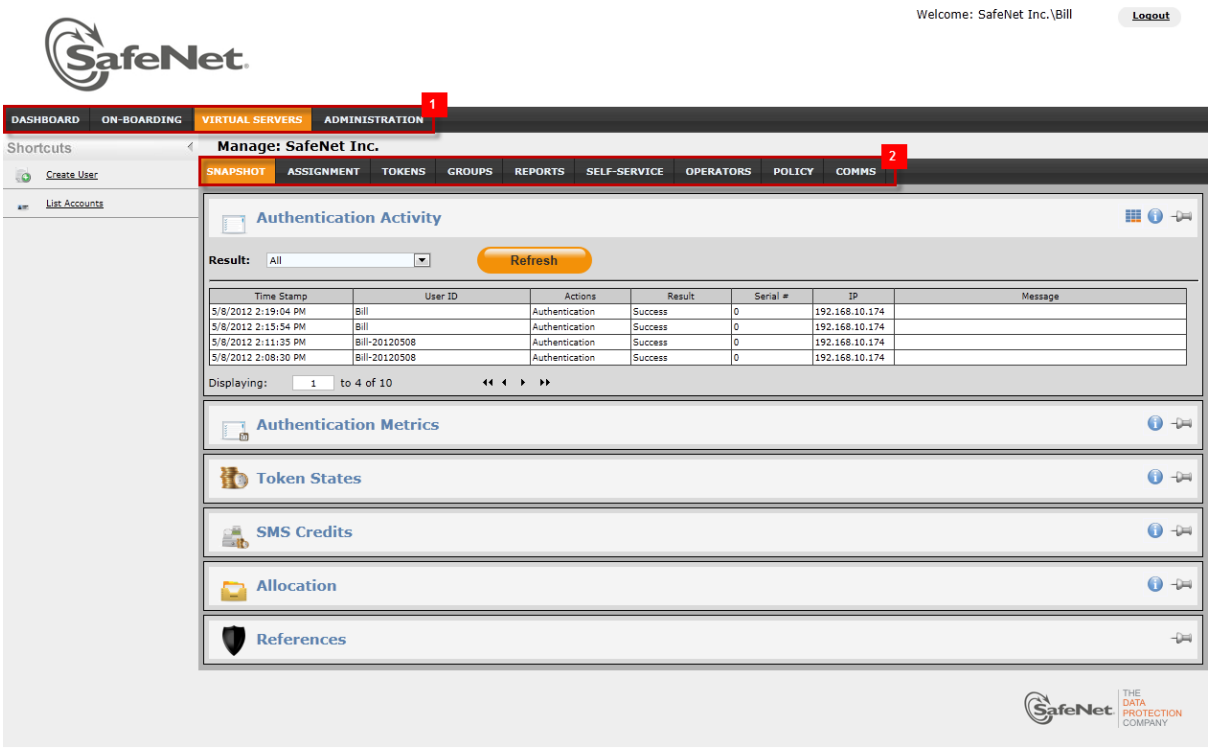


Figure 2: Service Provider View - Management UI

Virtual Service Provider Views

The Virtual Service Provider's (VSP) View is identical to the Service Provider view. Using the Service Provider tabs [1] in the banner area they can manage their own Virtual Server and can create Subscriber and Virtual Service Provider accounts below them which they manage. However, Virtual Service

Providers are restricted to managing their own Virtual Server and those of the accounts they create. They cannot view or manage any other account or Virtual Server.

Subscriber Views

Subscribers that are permitted to manage their Virtual Server are presented with a nearly identical view [Figure 3: Subscriber View - Management UI]. The only differences apart from logos and related branding customizations is that the Service Provider row of tabs is not present and therefore the Subscriber cannot gain access to any other Virtual Server nor create or manage other accounts.

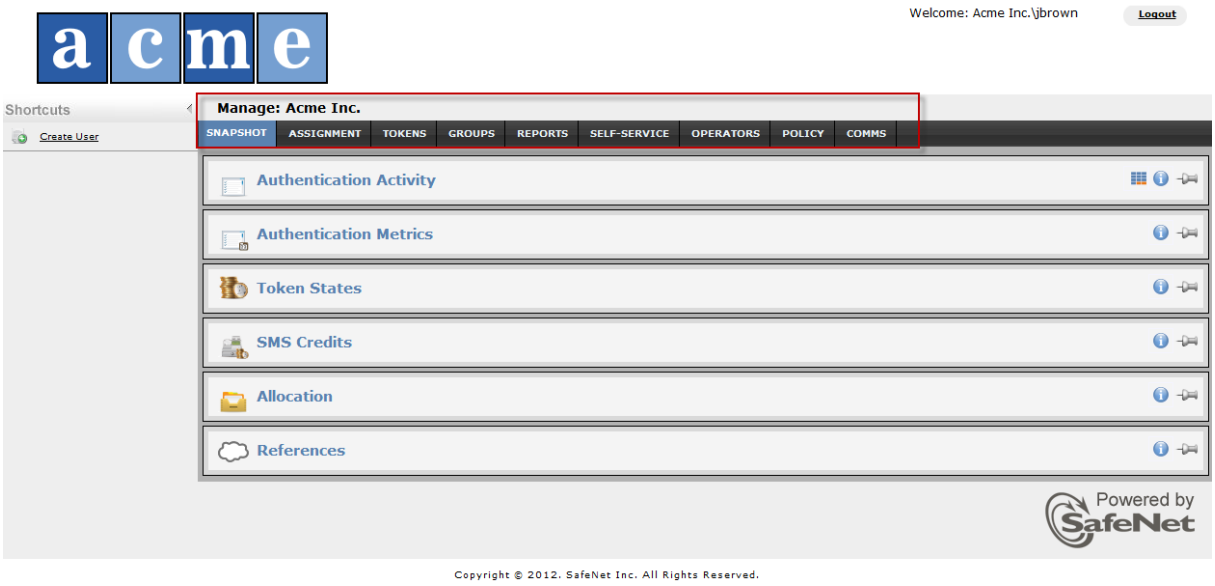


Figure 3: Subscriber View - Management UI

Tabs and Modules

Tabs logically group business, service and management functions. Tasks on each tab are contained within modules. Every module has a specific function such as token management, user management and group management. Within each of the modules are actions such as create, add, edit, delete, save, view, assign, and initialize and so on. [Figure 4: Tabs, Modules and Actions on page 26]

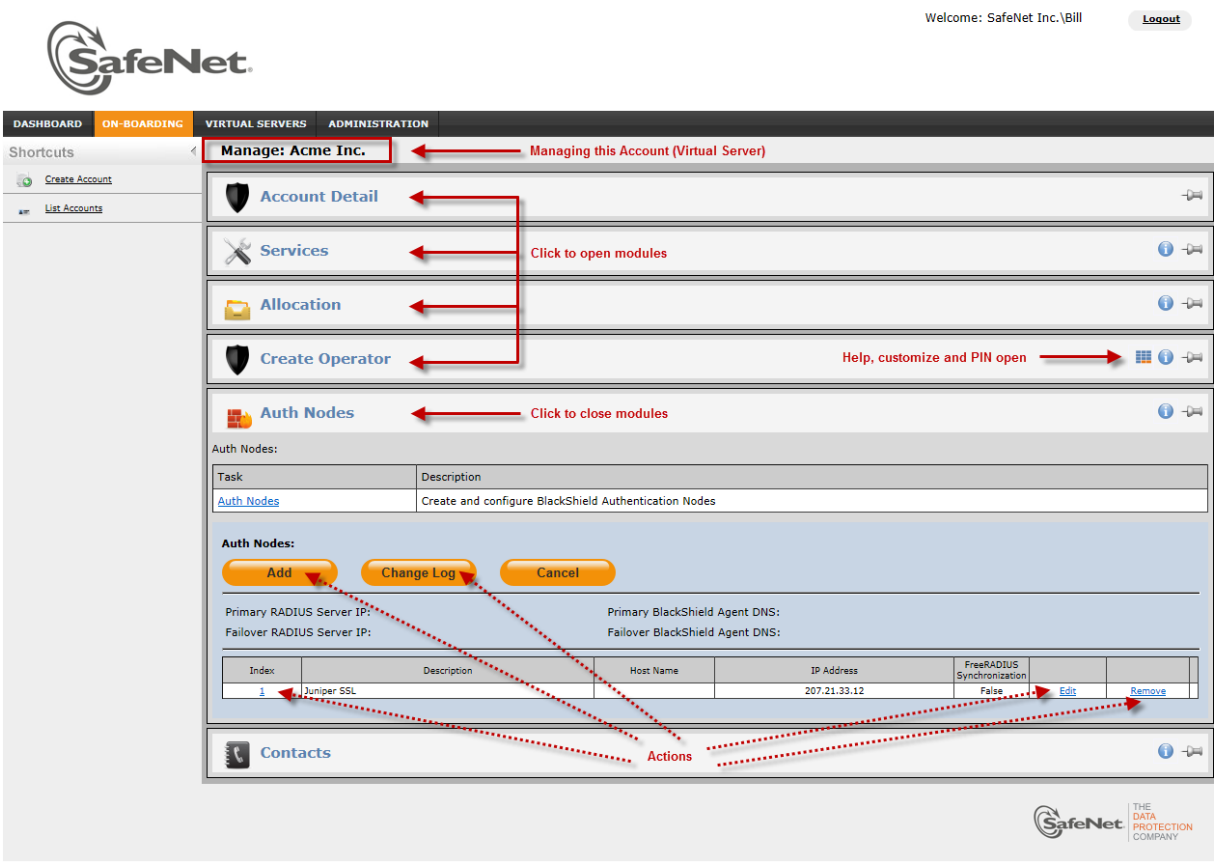


Figure 4: Tabs, Modules and Actions

Administrators can select any combination of tabs, modules and actions within modules and save these as “Roles”. Administrators can create and assign Account Managers to roles, effectively modifying the Account Manager’s view to reflect service objectives, workflow, administrative hierarchy and operational security requirements.

Role management and other Operational Security topics are discussed in detail in the Administration Tab on page 67.

Management UI Conventions

Clicking anywhere in the bar containing the module name toggles the module open or closed. A module that is pinned open will not close when another module is opened. Unpinned modules close whenever another module is opened.

All modules have an information icon towards the right side of the module bar. Clicking on the icon opens context specific help for this module.

All modules that contain lists have a customization icon that is used to change the number of rows displayed in the list. An item count at the bottom of each list shows the number of items displayed of

the total items that meet the search criteria. Navigation arrows beside the item count can be used to page through a long list of items.

The Virtual Server

Every account has a Virtual Server, including your Service Provider account. By selecting your account from the Accounts List on the VIRTUAL SERVERS tab, you can manage your own users, tokens, reporting, etc. A full description of how to manage Virtual Servers is provided in Chapter 3.

Chapter 2

This chapter describes the functionality contained in the Service Provider tabs. It is through this set of tabs that you will:

- On-board accounts and configure their service.
- Create Account Managers and manage their roles and scope.
- Generate security, audit and usage reports.
- Generate billing reports.
- Establish branding and other customizations that reflect your goals.

Dashboard Tab

On this tab:

- **Alerts Module**
  Presents and allows management of alerts generated by the system when an event or threshold condition is detected.
- **Subscriber Metrics Module**
  View account metrics that will help you evaluate the service you are delivering.
- **Inventory Module**
  Displays information about products, capacity, SMS Credits and ICE available for allocation to accounts.

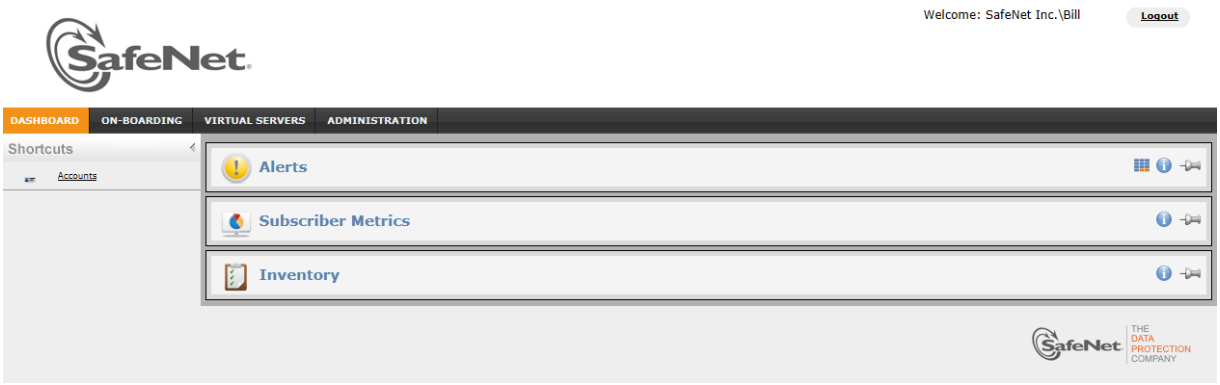


Figure 5: Dashboard Tab

Alerts Module

SafeNet Authentication Service continuously monitors all Virtual Servers for important events that may affect one or more accounts. Alerts are listed in the Alerts Module where they can be viewed, acknowledged and closed. Alerts can also be delivered by email and SMS text message. Which events and thresholds generate alerts and to who alerts should be delivered is configured in the Administration tab. (Refer to Alert Event Thresholds on page 76.)

These include:

- **Account Status Change**
  Detects account service changes to or from Active and Disabled (Refer to Services Module on page 36)

- **Active Evaluation Stop Date**
  This alert is triggered if an account has the Evaluation option checked and the Service Stop date is within X days of the current date.

- **Account Stop Date**
  This alert is triggered if the account Service Stop date is within X days of the current date.

- **Account Capacity**
  This alert is triggered when your Inventory of capacity falls below X. Use this to be alerted to a low capacity condition that may prevent you from On-boarding additional accounts of fulfilling orders from existing accounts.

- **Hardware Assignment Notification**
  This alert is triggered every time a hardware token is assigned to a user.

- **Hardware Provisioning Notification**
  This alert is triggered every time a hardware token is provisioned to a user. The alert contains the user's detail so that the alert recipient is able to arrange for shipment of the hardware device to the user.

- **Account Removal**
  Generates an alert if an Account is removed from the server.

- **AuthNode Changes**
  Generates an alert if an Auth Node is added, removed or modified.

- **Allocation/Deallocation Alert**
  This generates an alert if inventory (capacity, tokens…) are allocated to or deallocated from a virtual server.

- **Account Provisioning Notification**
  Generates an alert when a user is promoted to Account Manager.

- **Remaining Account Capacity**
  This alert is triggered when an Accounts capacity falls below X.

- **Service Notifications**
  Recipients will receive a message whenever a service notification is published by the service provider.

Viewing, Acknowledging and Closing Alerts

To view alerts, begin by opening the Alerts Module.

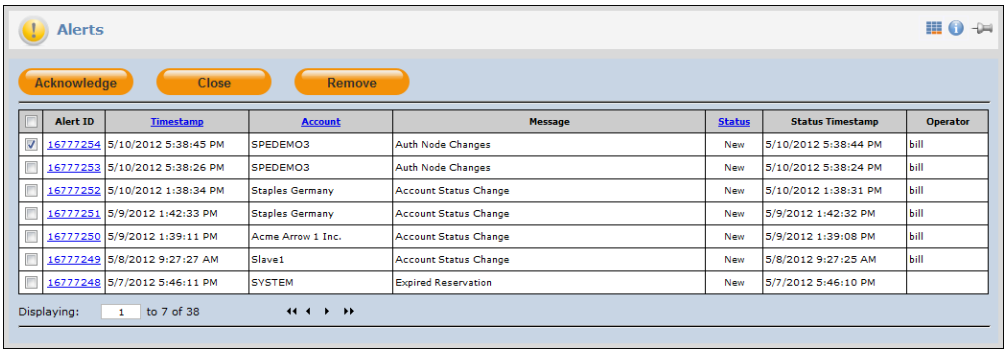


Figure 6: Alerts List

Alert ID

Clicking the hyperlink displays additional detail about the alert.

Acknowledge

The Acknowledge button opens a dialogue that allows the Account Manager to enter a comment and indicates that the Account Manager is aware of the condition. Comments can be used to communicate the status or leave instructions for other Account Managers. When an Alert is acknowledged, the State will change to Acknowledged.

Close

The Close button opens a dialogue that allows the Account Manager to enter a comment that indicates that the condition causing the alert has been rectified. The state of the alert is updated to closed. Closed alerts can be removed by clicking the corresponding remove hyperlink.

Remove

Use remove to delete selected alerts in the list. Note that removing the alert does not remove the permanent record of the event. Event history can be retrieved by running the appropriate reports.

Subscriber Metrics Module

The Subscriber Metrics module displays cumulative data generated by all accounts managed by the Service Provider. Count Metrics (e.g. account count) are continuously updated whereas relative metrics (totals/month) are updated on the first day of each month. Over time the table presenting metrics expands to a full year's worth of data. Thereafter the oldest month is dropped from the table and the data for the current month is added. Metrics older than 1 year can be retrieved by running reports.

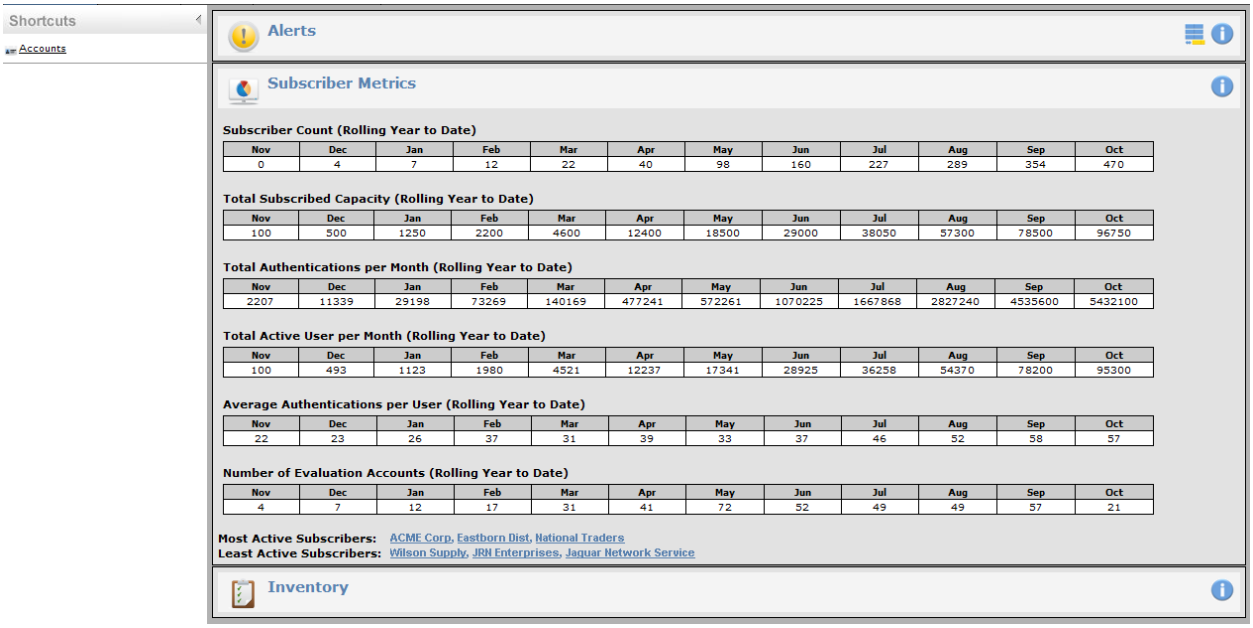


Figure 7: Subscriber Metrics

- **Subscriber Count (Rolling Year to Date)**
  Totals the number of accounts in the current month and in each of the preceding 11 months.

- **Total Subscribed Capacity (Rolling Year to Date)**
  Is the total subscribed capacity in the current month and in each of the preceding 11 months.

- **Total Authentications per Month (Rolling Year to Date)**
  Is the total number of authentications in the current month and in each of the preceding 11 months.

- **Total Users per Month (Rolling Year to Date)**
  Is the total number of users (that can authenticate) in the current month and in each of the previous 11 months. The totals for each of the preceding 11 months reflect the total on the last day of the month.

- **Average Authentications per User (Rolling Year to Date)**
  Is the total authentications/month divided by the total number of Users that can authenticate in the current month and in each of the preceding 11 months. The numbers for the previous 11 months will be based on the number of users on the last day of the month.

- **Number of Evaluation Accounts (rolling Year to Date)**
  Is the number of accounts initially marked as evaluation at the time of account creation in the current month and in each of the preceding 11 months.

- **Most Active Subscribers**
  Lists the 5 accounts with the highest Average Authentications per User in the preceding month, listed in descending order (most to least).

- **Least Active Subscribers**
  Lists the 5 accounts with the fewest Average Authentications per User in the preceding month, listed in ascending order (fewest to most authentications/user).

Inventory Module

As a Service Provider you'll be allocating inventory to your accounts. The Inventory module displays your current inventory available for allocation.

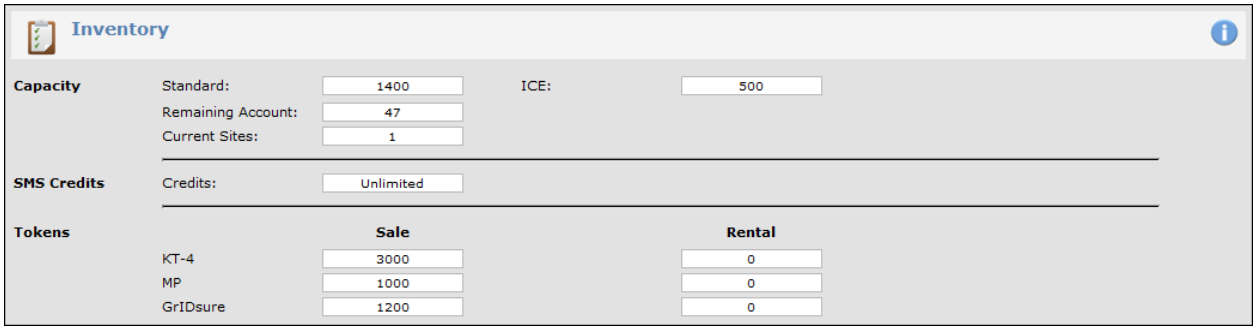


Figure 8: Inventory Module

- **Capacity**
  Capacity determines the maximum number of tokens or authentication methods that can be assigned to users. For example, an account with a capacity of 100 and with 150 tokens could assign 1 token to each of 100 users, assign 100 tokens to 1 user, or any combination in between, but they could not use the remaining 50 tokens without acquiring additional capacity.

- **Tokens**
  There is a separate count for each token / authentication method that you have available for allocation. The Sale count represents tokens that you own and can therefore sell or rent to your accounts. The Rental count represents tokens that you do not own and are therefore available only for rental to your accounts.

- **ICE**
  ICE ("In Case of Emergency") is a special combination of capacity and MP-1 software tokens that can be used to temporarily increase an account's capacity and token inventory. When the temporary period expires the service reverts to pre-ICE conditions. ICE is an effective solution that Service

Providers can use to build business continuity measures into an account's service. This represents the total ICE capacity available for allocation.

- **SMS Credits**
  This is a count of the SMS Credits you have available for allocation. If you have configured an SMS gateway on the Virtual Server, this value will be "unlimited". If not, this value will be the total credits received from your Service Provider and available for reallocation to your accounts.

On-boarding Tab

On-boarding is the business process of creating an account, establishing the type of service to be provided, allocating token inventory and capacity, and adding Auth Nodes. If the account will be self-managed, on-boarding may also encompass adding an Operator.

All on-boarding activities are performed from the "**ON-BOARDING**" tab of the Service Provider management interface.

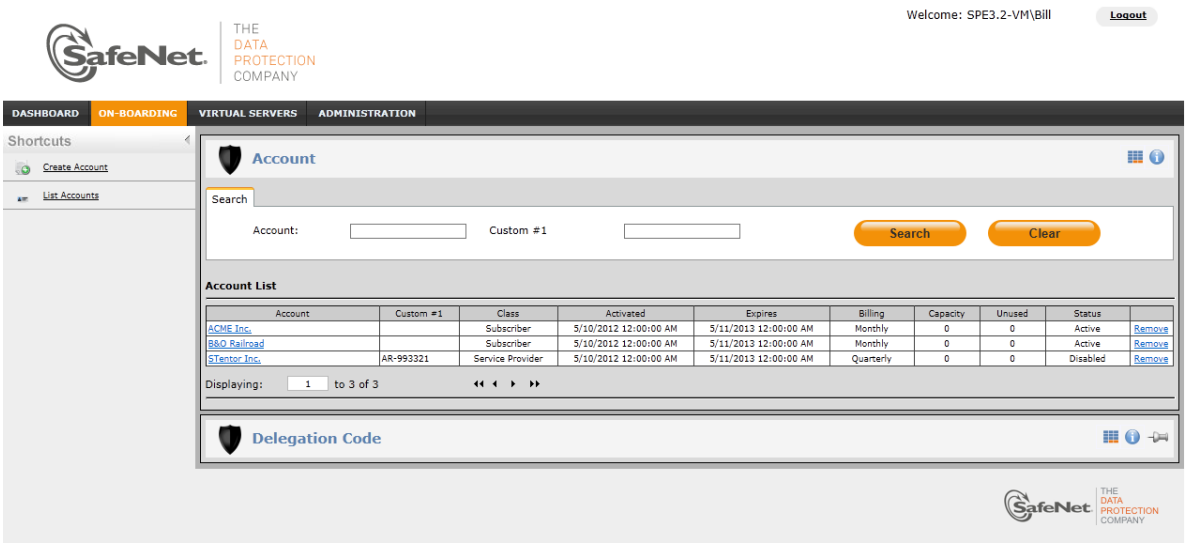


Figure 9: On-Boarding Tab

On this tab:

Account List

Displays a list of on-boarded accounts and provides access to account management functions where:

- Account: Click this account name hyperlink to manage the account's services such as subscription term, token allocation etc.
- Custom #1: This column is populated using data from the Custom #1 field entered during account creation. The field and column label may be renamed to reflect the type of data or use.
- Class: Indicates whether the account is a Virtual Service Provider or Subscriber.
- Activated: This is the date the service was activated for the account.
- Expires: This is the date the service will stop for the account.
- Billing: This is meant to represent the billing period, as set in the services module during account creation.

- Capacity: This is the maximum number of users that may authenticate against the virtual server. Note that for Virtual Service Providers, this value is reduced each time inventory is allocated to an account.
- Status: Set to Active or Disabled as set in the Services Module.
- Remove: Use this hyperlink to remove an account. Note that all inventory must be revoked (i.e. both Capacity and Unused must be 0) before the account can be removed.

Create Account / Account Detail Module
Use this shortcut and module to add new accounts and manage their basic account details.

Services Module
Functions in this module define the type of account, services offered and service period.

Allocation Module
Use this module to allocate or deallocate capacity, tokens, SMS Credits and ICE licenses to accounts.

Create Operator Module
Use this module if you want your accounts to log into the management UI to manage their own Virtual Server, create and manage users, provision tokens and run reports.

Auth Nodes
Use this module to add and activate an account's Auth Nodes such as VPNs, Web applications and Cloud applications, allowing these to authenticate against their Virtual Server.

Contacts Module
This module allows you to add account contacts with whom you may need to correspond.

Create Account Shortcut

The On-boarding process begins by clicking the "Create Account" shortcut and completing the Create Account information form.

- The Account name must be unique.

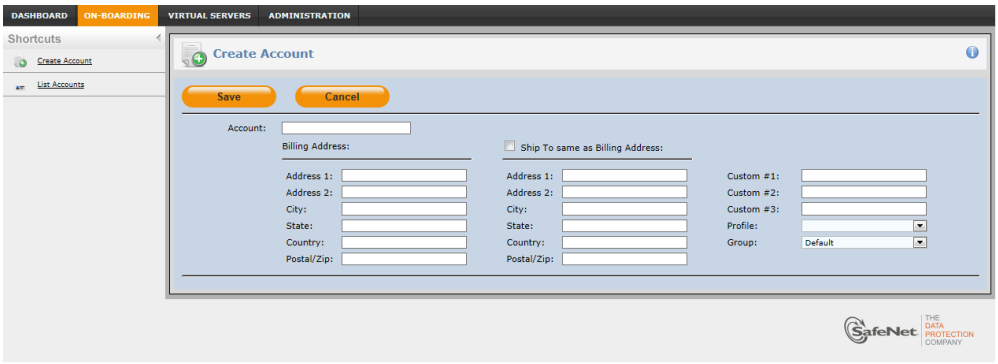


Figure 10: Create account

The Custom #1 field can be used to link the account to an external system. A typical use is to add the account number generated by your billing system for this account in this field. This allows all reports to be linked to the billing number, Account name, or both. Custom fields #2 and #3 can be used for similar purposes.

The Custom # labels can be changed to reflect your requirements. Refer to Custom Branding Module on page 295.

The Group drop down is a list of all configured Account Management Groups. Account Managers are only able to manage accounts that are in groups to which the Account Manager has access. Refer to Operational Security Overview on page 68 and Account Manager Maintenance on page 73.

Services Module

Once an Account has been created, the next step is to configure its type of service, duration and other basic parameters. To configure services, begin by opening the Services Module.

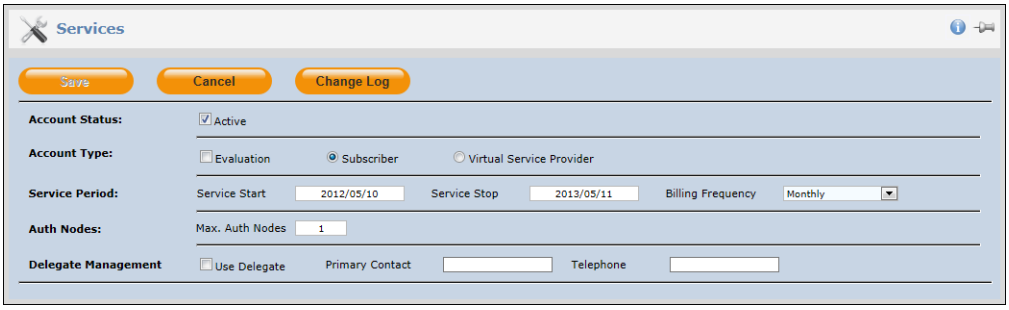


Figure 11: Configuring account Services

Account Status

To activate Services, check the Account Status option and click Save. Services settings can be changed at any time by adjusting the values in any of the fields and options and committing with the Save button. Services can be suspended by clearing the Account Status option and committing the change with the Save button. Suspending Service stops all authentication services for the account's Virtual Server and

prevents any Operators they may have from logging into the management UI. Re-activating Services restores the Service and Operator rights to the state immediately prior to suspension.

Account Type - Subscriber

In most cases the Account Type selection will be “Subscriber”. This type is ideal for accounts that will add users to the service manually, by import or by LDAP synchronization from a single LDAP server. This account type is not permitted to create or manage additional accounts.

Account Type - Virtual Service Provider

To allow an Account to create, manage and share resources with subordinate accounts or to support LDAP synchronization with multiple LDAPs, it must be configured as a Virtual Service Provider. Typically this option will be selected:

- Where the Account is reselling your service to its customer base and therefore will create and possibly manage its own accounts.
- Where the subscribing organization wants to on-board subsidiary companies or segregate management and services between internal groups, or where multiple LDAP servers will be synchronizing users on the service.

Evaluation

The Evaluation check box does not affect the type of account but it does add a flag that can be used in reporting to distinguish “paying” customers from those evaluating the service. In conjunction with Operational Security and Alerts, it can also be used to generate an alert to Account Managers a defined number of days before the service stops, allowing the Account Manager to proactively manage the account while it is still active.

Service Period

The Service Period uses the start/stop dates to limit the period of availability of the service to the account. These dates are modified by the Account Status option which, if set to Active, makes the service available for the period commencing with the start date and ending on the stop date. If the Account Status is set to not active, the service is disabled regardless of the service period.

Billing frequency is simply a flag to Account Managers and reproduced in reports. In conjunction with the other information in this module, this allows Account Managers to ascertain the service and billing commitments with the Account without referring to contracts.

Auth Nodes

The Virtual Server will receive and process authentication requests from VPNs, applications and so on, collectively referred to as “Auth Nodes”, configured for this account. This setting allows the Service Provider to limit the number of devices or applications that can authenticate against the service for this Account. The minimum value is 1. In general, setting this value to reflect the minimum Account requirements is recommended. Service Providers can use this setting to create up-sell opportunities, attaching a service cost for additional auth nodes.

Delegated Management

Though in most cases a Virtual Service Provider will manage the accounts they create, there are situations where they may wish to delegate management responsibility to their Service Provider or "Parent" organization. For example, (referring to Figure 12: Delegated Management on page 38.) SP2 has created and can manage SUB1, however SP2 has also delegated management of SUB1 to SP1. This allows SP1 to manage the SUB1 account on behalf of SP2. Some useful applications of delegated management include:

- Supporting intermediate sales channels (e.g. SP2 is purely a sales organization with no support capability, whereas SP1 is able to provide a full range of support functions.)
- SP2 is a customer with several subsidiary organizations, LDAP domains, etc. (SUB1, SUB2, SUB(N)) but all user and account management is to be performed by SP1.
- Checking the Delegated Management option immediately delegates management to the Virtual Service Provider's parent, where it will appear on their Virtual Servers tab. The Primary Contact and Telephone fields can be populated to add a point of contact reference at the parent (SP1).

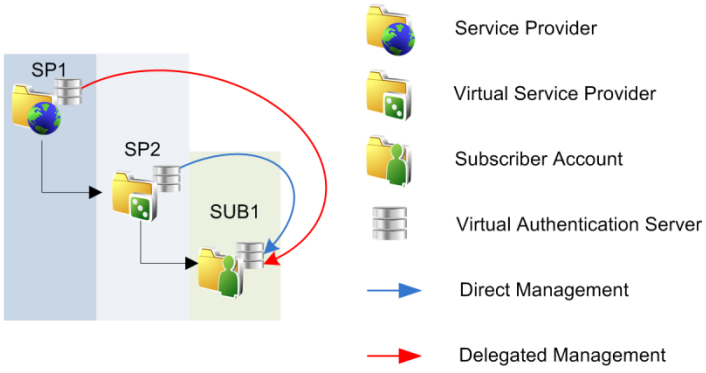


Figure 12: Delegated Management

Change log

Every time the service is modified a record of the change is stored in the database. The 5 most recent changes can be viewed by clicking the Change Log button. A complete list of changes can be retrieved using reports.

Allocation Module

Now that the service has been configured, it's time to allocate tokens and capacity to the Account. This process moves inventory into the account's Virtual Server. A summary of your inventory available for allocation to an account can be found in the Inventory Module on the Dashboard (page 32). Capacity determines the maximum number of tokens that can be in use (assigned to users). The allocation module displays a table showing the capacity and quantity of all token and authentication types allocated to the account's Virtual Server where:

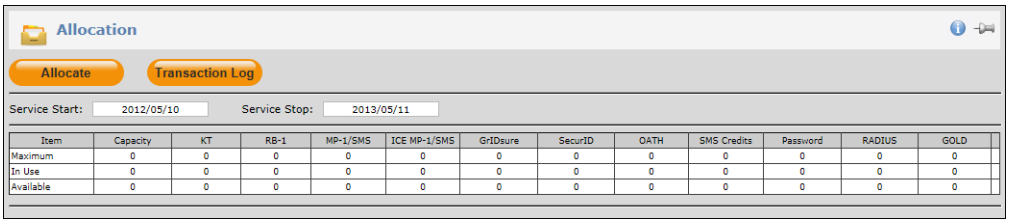


Figure 13: Allocation List

- **Maximum**
  This row shows the total by capacity, token and authentication method allocated to the account's Virtual Server

- **In Use**
  Shows the capacity, tokens and authentication methods consumed by the account for their own use or in the case of Virtual Service Providers for their own use or allocated to accounts they manage.

- **Available**
  Shows unconsumed capacity, tokens and authentication methods.

- **Deallocate**
  Shows the quantity by type that can be deallocated from the account's Virtual Server and returned to your Inventory.

The following paragraphs describe a few of the many options available in allocation.

- **Rental**
  The rental option is applied to accounts that will pay a recurring fee per user for capacity or some combination of capacity and tokens. Rental ensures that the ownership of tokens does not transfer to the account.

- Choose **Capacity** if you are migrating an Account from an in-house system with tokens that are compatible on the SafeNet Authentication Service. Essentially this option allows you to bill for the service without billing for tokens.

- Choose **Tokens, Transaction Type Rental** and **Automatically add Capacity with this allocation** and if the Account will be paying a fee per user for the service including a token per user.

- **Sale**
  The sale option transfers ownership of tokens to the account. This option is ideal where the account wishes to own the tokens rather than have that cost bundled into their recurring cost per user.

  Choose **Tokens, Transaction Type Sale** if the Account is purchasing tokens and does not require additional capacity. Example uses include an Account replacing owned tokens that have been lost or replacing one token type with another.

Choose **Tokens, Transaction Type Sale and Automatically add Capacity with this allocation** where the Account requires an equal amount of additional capacity to support the purchased tokens. Note that this option is the equivalent of two separate allocation transactions: **Tokens, Transaction Type Sale** and **Capacity Only**.

ICE (In Case of Emergency)

ICE is a service you can offer your Accounts allowing them to increase capacity and issue tokens for a limited period of time after which capacity returns to pre-ICE levels. ICE includes MP-1 software tokens equal to the ICE capacity. These tokens can be deployed to any MP-1 target such as pc's, iPhones™ and BlackBerrys. Expiration of ICE stops the authentication service only for users with ICE tokens.

Though only 1 ICE license can be activated at a time, additional ICE licenses can be allocated at any time to replace a consumed license or replace an in-use license prior to expiration.

- Note that only 1 ICE license can be in use at a time. Activation of an ICE license replaces an in-use license. It does not extend an in-use license.

SMS Credits

This option is used to charge Accounts in advance for use of SMS services. Each SMS message sent by the Account uses 1 credit (assuming customized message lengths do not exceed the SMS character limit resulting in 2 or more SMS transmissions per message). SafeNet Authentication Service decrements the Account's SMS credits inventory every time a message is sent.

Use this option if the Account will be using SMS/OTP or if it will be configured to send alerts via SMS.

- This option is available only if the Virtual Server has a configured SMS gateway or SMS modem, or if you are a Service Provider and have SMS credits in your inventory.

SafeNet Authentication Service can send an alert to an Account Manager if an account's remaining SMS credits fall below a specified threshold.

Using the Allocation Wizard

Each type of token and/or capacity is allocated to an account in separate transactions. Begin allocation by clicking the Allocate Button. This starts the Allocation Wizard. The number of steps in the wizard depends on the type of allocation. In general allocation includes:

- Selecting the type of allocation – Rental, Sales, ICE or SMS Credits.
- Indicating the quantity of inventory to be allocated.

Creating a billing reference – the amount to be charged for the transaction or unit of transaction, billing triggers, customer reference and comments.

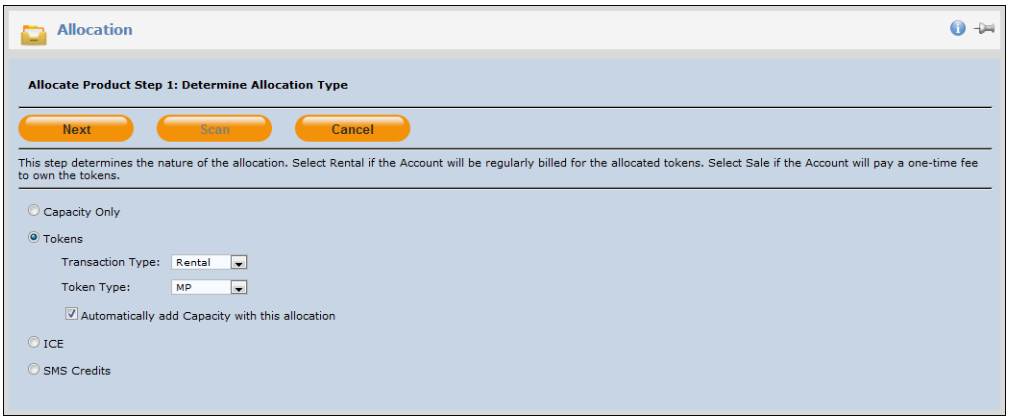


Figure 14: Select Allocation Type

Allocation Wizard Step 1 – Determine Allocation Type

Select the transaction type and sub options. For example if your service bundles capacity and tokens into a single cost/user/month, select Tokens, then select the Transaction Type Rental and check the **Automatically add Capacity with this allocation** option.

- **Rental**
  Indicates that ownership will not transfer. This transaction type can allocate from token inventory containing sale and rental tokens.

- **Capacity Only**
  Indicates that tokens are not included in this allocation. A typical use of this option would be to allow an account to use tokens they already own and will import or initialize into their Virtual Server.

- **Tokens and Capacity**
  Allocates a specific quantity and type of token and a corresponding quantity of capacity.

- **Sale**
  Indicates that token ownership is transferred. Inventory that is not owned cannot be allocated in a sale transaction.

- **Token Type**
  Indicates the type of token to be allocated.

- **Automatically add Capacity with this allocation**
  Allocates corresponding rental capacity with the sale tokens.

- **ICE**
  Indicates the quantity of ICE to be allocated to the account.

- **SMS Credits**
  Transfers a quantity of SMS credits to the account.

Click Next to continue.

Allocation Wizard Step 2 – Select Inventory for Allocation

The next step is to select the inventory to be allocated. The dropdown lists will vary depending on how your inventory is managed:

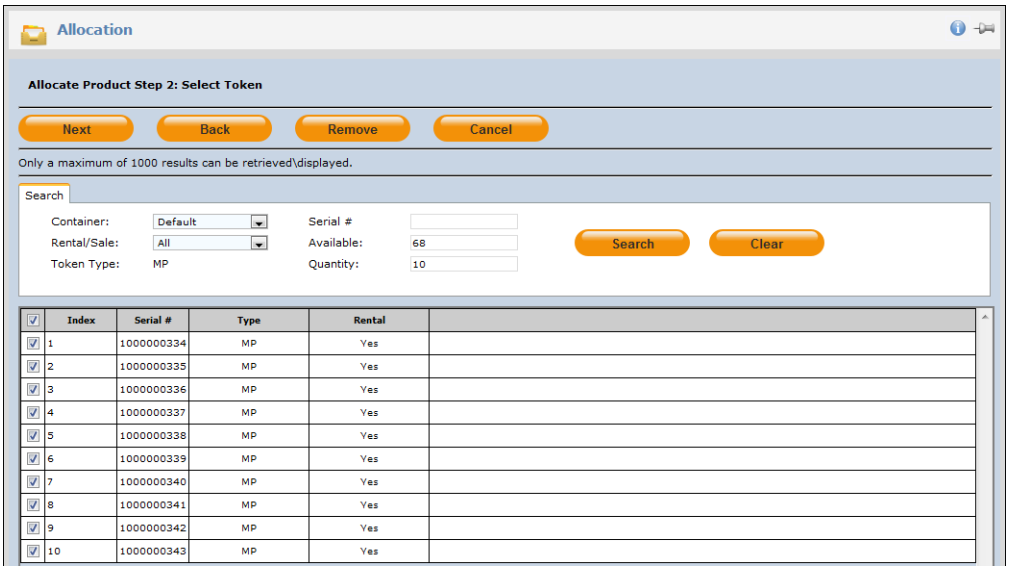


Figure 15: Select Inventory to Allocate

- **Container**
  Indicates the container from which token inventory should be allocated. Default holds all tokens unless additional containers have been created and inventory added to them. For more information on containers refer to the Containers section on page 141.

- **Rental/Sale**
  Is used to limit the tokens displayed in the list to Rental or Sale. Note that Sale tokens can be allocated as sale or rental while Rental tokens can only be allocated as rental.

- **Serial #**
  Is used to select a specific token from inventory by serial number.

- **Available:**
  Indicates the quantity available for allocation.

- **Quantity**
  Indicates the quantity to be selected.

At a minimum enter the quantity to be allocated, and then click the search button. The list will be populated with inventory that matches the search criteria. Select the inventory in the list by clicking the column check box, and then click Next to proceed to the next step.

You can use the remove button to remove checked inventory from the allocated list.

Allocation Wizard Step 3 – Create Billing References

Billing references are used in reporting to indicate how the transaction should be billed and to link the transaction to customer references such as purchase order numbers.

Figure 16: Create Billing References

- **Billing Basis**
  Is a flag used by the reporting system to indicate the billing method associated with the transaction. Options are:

- **Allocation**
  Indicates that billing occurs on the date the inventory is allocated to the account.

- **Activate**
  Indicates that billing is to occur when the token/method is assigned to a user. This could be a user of this account or any account to which it transfers the token.

- **Authentication**
  Indicates that billing is based on token usage where each authentication incurs a charge.

- **Transfer**
  Indicates that billing should commence when this account (Virtual Service Provider) allocates inventory to an account it creates and manages. Transfer provides a mechanism to bill for the entire transaction or only the quantities transferred.

- **Billing Start**
  This date modifies the Billing Basis to indicate a date other than the transaction date to start billing. This is useful for allowing a grace period before billing commences. For example, on allocation, the Billing Start could allow 30 days after allocation before billing commences whereas on Transfer, the

Billing Start date could mean commence billing on this date whether or not the inventory has been transferred.

- **Rate/Month**
  Is a value which indicates the charge to be applied per unit being transferred. Note that a character that is not easily used within the external billing system (e.g. $, £) should not be included in this field.

- **Reference**
  Can be used to reference external information related to this allocation such as the customer purchase order number or a sales order number. This allows the transaction to be linked to external processes such as order fulfillment.

- **Warranty Replacement**
  Is a flag attached to the transaction indicating that the allocation is to replace product under warranty. This is helpful for distinguishing between new orders, billable product and no-charge warranty replacements when producing billing reports.

  - Use the Reference field to record the RMA (Return Material Authorization) number with the warranty replacement.

- **Evaluation**
  Is a flag attached to the transaction indicating that the allocation is provided for evaluation purposes.

- **Comment**
  Is a freeform text area in which to include comments related to the transaction. Comments form a permanent part of the transaction record.

Allocation Wizard Step 4 – Confirm Allocation

This is the last step which provides the opportunity to verify before committing the entire transaction.

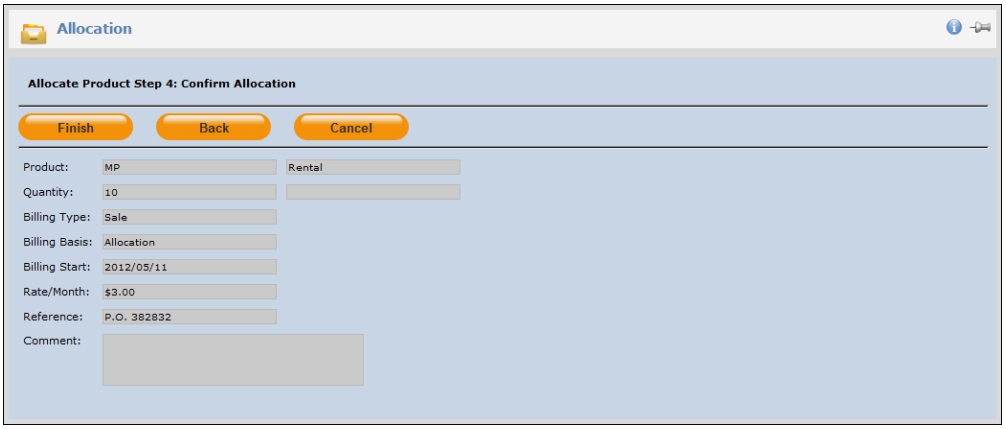
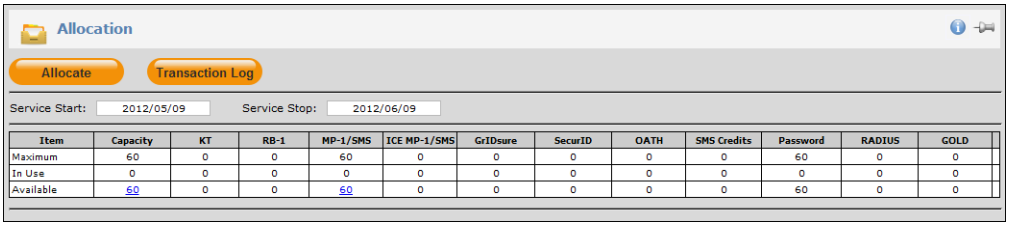


Figure 17: Confirm Allocation Transaction

The Allocation table is updated when the wizard finishes.



Item	Capacity	KT	RB-1	MP-1/SMS	ICE MP-1/SMS	GrIDsure	SecurID	OATH	SMS Credits	Password	RADIUS	GOLD
Maximum	60	0	0	60	0	0	0	0	0	60	0	0
In Use	0	0	0	0	0	0	0	0	0	0	0	0
Available	60	0	0	60	0	0	0	0	0	60	0	0

Figure 18: Updated Allocation Table

Allocation Wizard for Sale, ICE and SMS transactions

Sale Transactions

The process for Sale transactions is identical to the Rental example in the preceding pages except as follows:

- Only inventory available for sale can be used in a Sale transaction.
- Tokens can be allocated without capacity. Choose this option if replacing lost or damaged tokens owned or rented by the account.
- Tokens can be allocated with a corresponding quantity of rental capacity. This option is the equivalent of two separate transactions: Rental | Capacity Only and Sale | Token (without capacity).

ICE Transactions

To allocate ICE, select the ICE option, enter a quantity in the Allocate field to reflect the required ICE capacity, and then follow the wizard steps described in Using the Allocation Wizard on page 40.

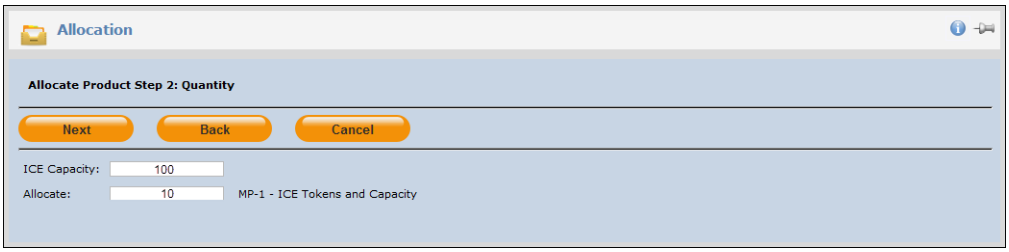


Figure 19: Allocating ICE

All ICE licenses have duration of 30 days from activation on the account's Virtual Server.

SMS Credits Transactions

To allocate SMS Credits, select the SMS Credits option, then enter the quantity of SMS credits to allocate to the account, then follow the steps described in Using the Allocation Wizard on page 40.

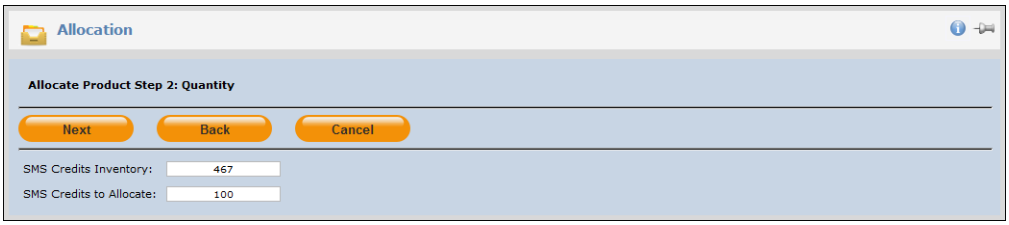


Figure 20: Allocating SMS Credits

- The SMS Credits Inventory will be "Unlimited" if, as a Service Provider you have configured an SMS Gateway in the Virtual Server. Refer to **SMS Settings** on page 238.
- An SMS Credits Inventory of "0" indicates that as a Virtual Service Provider you have not configured an SMS Gateway and have either not purchased, or have consumed all SMS credits allocated to your account by your Service Provider.

Transaction Log

A transaction record is created for each allocation. Transaction details can be viewed by clicking the Transaction Log button.

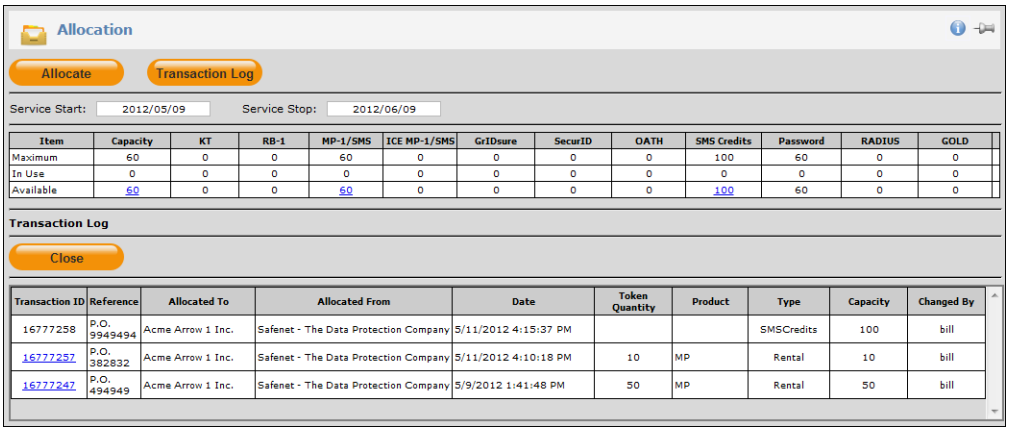


Figure 21: Allocation Transaction Log

Every allocation has a unique Transaction ID. The Transaction ID will be a hyperlink if the allocation included tokens. Clicking the hyperlink displays a list of all tokens by serial number included in the transaction.

A duplicate of the allocation table and transaction log is presented on the Snapshot tab of the account's Virtual Server.

De-Allocating an Account's Inventory

From time to time it may be necessary to deallocate some or all of the inventory allocated to an account to accommodate:

- An account not renewing the service.
- Warranty claims.
- Correcting fulfillment errors.

To deallocate inventory, begin by clicking the hyperlink in the Deallocate row corresponding to the appropriate product. This will start the Deallocation wizard.

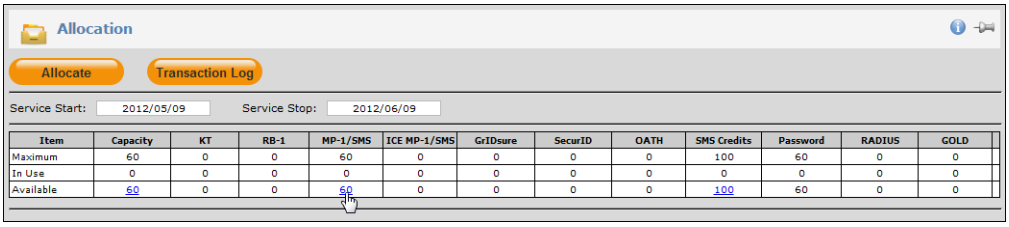


Figure 22: Deallocation Wizard

Deallocating MP-1/SMS Software Tokens and/or Capacity

The wizard displays the type and quantity of tokens that may be deallocated where:

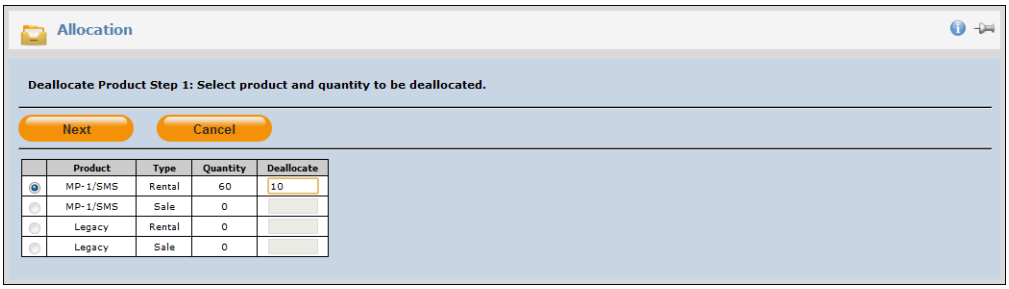


Figure 23: Deallocate MP Tokens

- **Rental**
  This indicates the tokens were allocated to the account as a rental, bundling the cost of each token with a unit of capacity. Therefore a unit of capacity will also be deallocated for each MP token deallocated.
- **Sales**
  This indicates that the tokens were sold to the account. A unit of capacity will not be deallocated with each token.
- **Legacy**
  This type provides support for ST-1 software tokens imported into the system from legacy systems.

- **Quantity**
  This indicates the maximum quantity that is not in use in the account's Virtual Server and is therefore available for deallocation.

- **Deallocate**
  Enter the quantity to be deallocated in this field. The field is activated by the radio button in the left-hand column.

Click Next after entering a quantity to deallocate.

Each deallocation transaction offers the opportunity to add reference information where:

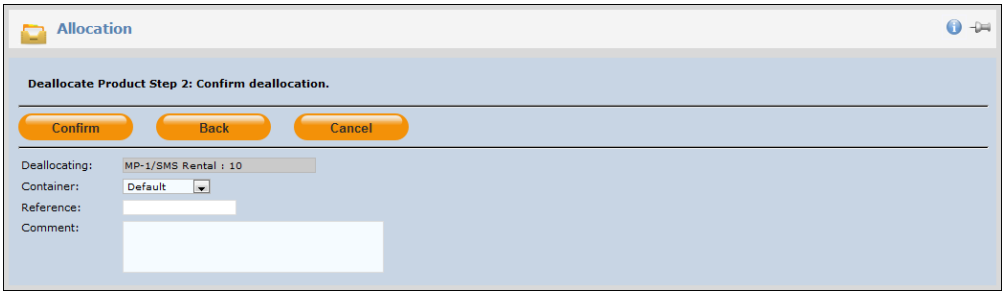


Figure 24: Deallocation References and Confirmation

- **Deallocating**
  Summarizes the product and quantity being deallocated.

- **Container**
  This dropdown list displays a list of containers in the Virtual Server into which deallocated tokens can be placed. Refer to the Containers on page 141 for more information on using Containers.

- **Reference**
  Use this field to enter a transaction reference such as an RMA number that will allow this transaction to be linked to billing, inventory management or other procedures you may have.

- **Comment**
  Use this field to enter additional information about this transaction. This information will appear in reports.

As a general rule you should not deallocate hardware tokens until you have received the product from your account. This is because deallocation will add the hardware tokens to your inventory, causing confusion if there is a discrepancy between the deallocation and what is actually returned by the account. Software tokens and capacity can be deallocated at any time as they are immediately returned to your inventory and are available for re-allocation to other accounts.

Deallocating Hardware Tokens

Hardware token deallocation begins by generating a list of serial numbers for tokens available for deallocation. Enter the maximum value in the quantity field, then click Search. This will generate a list of serial numbers. Select one or more serial numbers from the list corresponding to the physical devices returned by the account, then use the arrows to move to the Deallocate field.

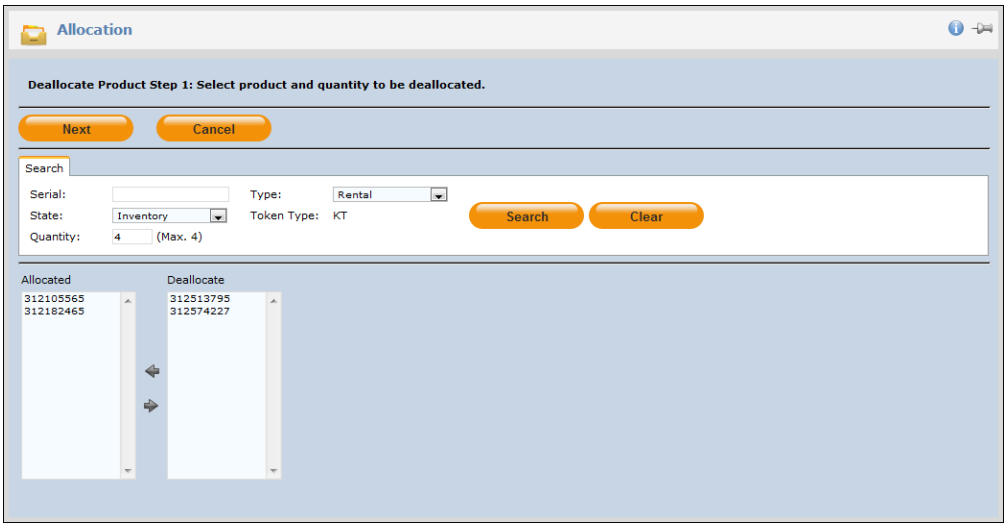


Figure 25: Deallocating Hardware Tokens

When all tokens to be deallocated have been moved, click the Next button.

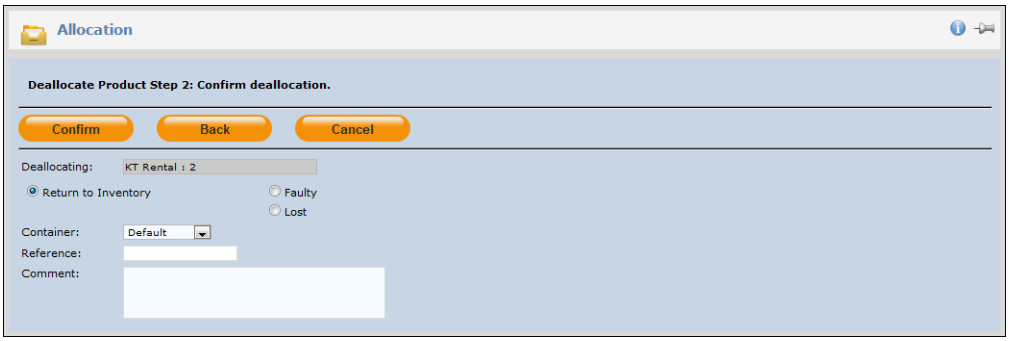


Figure 26: Deallocation References and Confirmation

The final step in de-allocation is to determine where the returned product should be placed in the Virtual Server's Inventory. The options are:

- **Return to Inventory**
  Choose this option for all Inventory items including hardware tokens that do not require re-initialization. Tokens returned with this option are immediately available for allocation to accounts.

- **Initialize and return to Inventory**
  Use this option for tokens that must be re-initialized before they can be allocated to accounts. This

option is rarely required and typically applies only to RB-1 tokens issued with token-side PINs. Token PIN requirements can be viewed in the account's Virtual Server prior to de-allocation. Refer to the

- **Tokens List** section on page 131.

- **Faulty**
  Use this option for hardware tokens that do not appear to work. This option returns the tokens to Inventory in the "Faulty" state preventing their use. If testing determines that the token is functional it can be made available for allocation by re-initialization.

- **Lost**
  Use this option to indicate the token is lost.

- **Container**
  This dropdown list displays a list of containers in the Virtual Server into which deallocated tokens can be placed. Refer to the Containers on page 141 for more information on using Containers.

- **Reference**
  This can be any alphanumeric string up to 64 characters in length. Best practice is to enter a reference number such as the RMA, work order or similar document that authorized the de-allocation.

- **Comment**
  This allows the Account Manager to enter a comment of up to 128 characters describing the reason for the de-allocation.

To commit the de-allocation, click the Confirm button. This Allocation table will be updated as will the transaction log. Clicking the Transaction ID hyperlink for the de-allocation will display the list of tokens returned to your Inventory.

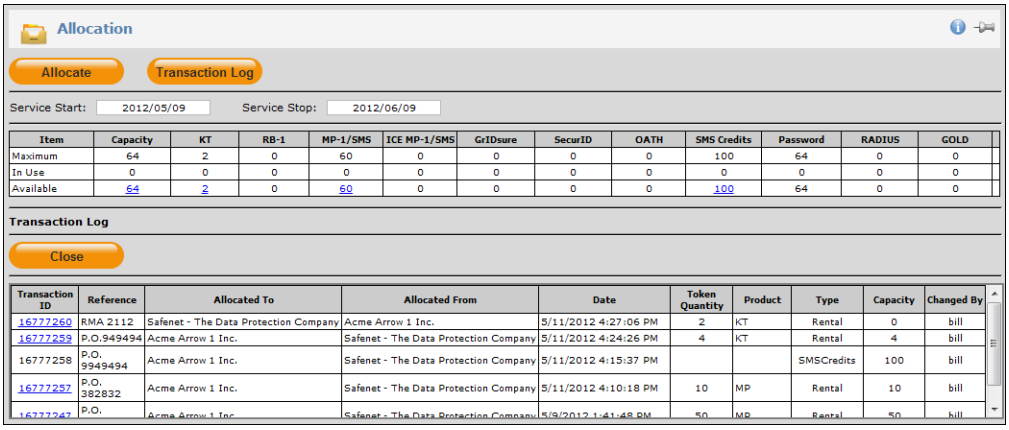


Figure 27: De-Allocation Updates and Transaction Logs

Create Operator Module

By default, a Service Provider can manage every account's Virtual Server. If the account is to manage their own Virtual Server rather than, or in addition to, their Service Provider, they must have an Operator created for them within their Virtual Server. Conversely, if the account is fully managed by the Service Provider there is no requirement to create an Operator.

Use the Create Operator module if you want the account to manage their Virtual Server.

If you will be managing all aspects of your account's Virtual Server you may skip this module.

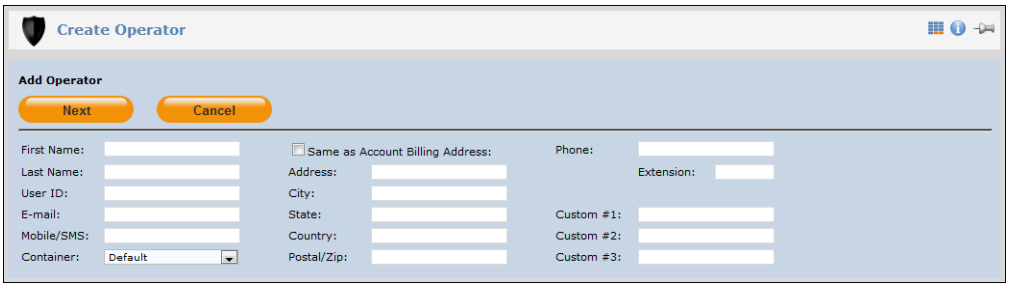


Figure 28: Create Administrator

The Create Operator process is a shortcut that creates a user in the accounts Virtual Server, assigns an authentication method to the user, prepares for enrollment, promotes the user to Operator status and prepares the Operator e-mail validation process.

If the account is created as a Subscriber account, this process creates an Operator within the account's Virtual Server. On login the Operator will have the Subscriber view and have full control of all aspects of their Virtual Server. (Refer to Subscriber Views on page 25.)

If the account is created as a Virtual Service Provider account, the user is also promoted to Account Manager at the Service Provider level. On login the user will have the Service Provider view and have full control of all aspects of their Virtual Server as well as the ability to create and manage accounts. (Refer to Service Provider Views on page 24)

In both cases, an e-mail containing enrollment instructions is sent to the user. When enrollment is complete, the user will receive a second e-mail with instructions for validating their e-mail address which results in login to the management UI.

The Create Operator wizard is self-explanatory with a couple of exceptions:

Mobile/SMS
The number in this field is used to send SMS/OTP and other SMS messages to the Operator if SMS is enabled for the account's service. This field must contain only digits and the first digit(s) must be the country code, followed by the city code.

In North America this would result in an entry in the format: 16131112222 where 1 is the country code, 613 is the area code and the remaining 7 digits the phone number.

In the UK this would result in an entry in the format: 448701112222 where 44 is the country code, 870 the city code and the remaining digits the phone number.

Container

Corresponds to the containers configured in the account's Virtual Server. (Refer to Containers on page 141.)

Custom #1, #2, #3

Corresponds to 3 custom fields allowed for each user account and should not be confused with the similarly labeled fields in Account Detail. As with all other custom fields, these can be used to store information relevant to the record and to distinguish similar users.

The wizard prompts for an authentication method to be associated with the user. The available methods reflect the inventory allocated to this account and present in its Virtual Server inventory.

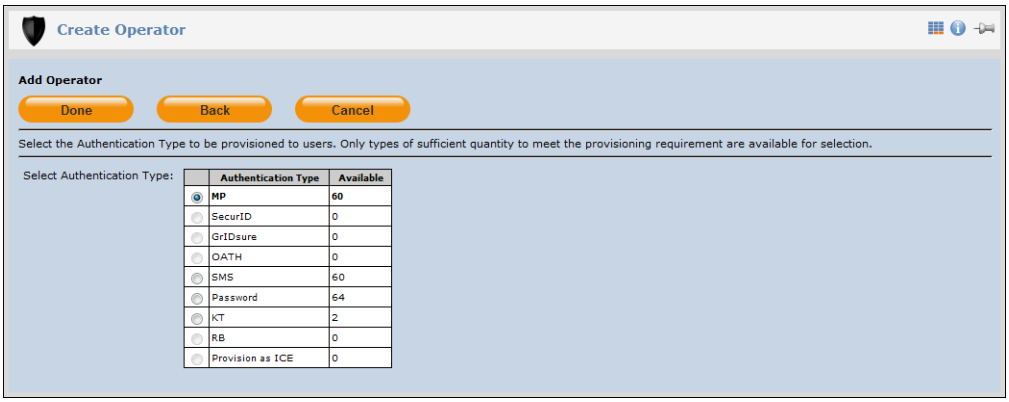


Figure 29: Authentication Method Assignment

- The "Available" quantity for an Authentication Type (Figure 29: Authentication Method Assignment) may differ from the corresponding value in the Available row of the Allocation List (Refer to Figure 13: Allocation List on page 39). This occurs if tokens in this Virtual Server have been moved to containers other than "Default". Only tokens that reside in the Default Container on the account's Virtual Server are available through this wizard.

The wizard finishes and the Operator List is updated.

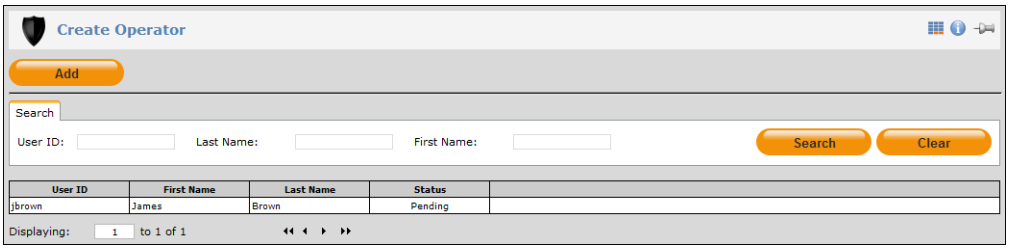


Figure 30: Updated Operator List

The status of the Operator is set to pending until enrollment and e-mail validation has been completed. The enrollment process will vary depending upon the assigned authentication method.

Once enrolled, the user will receive an Operator e-mail validation message similar to the following:

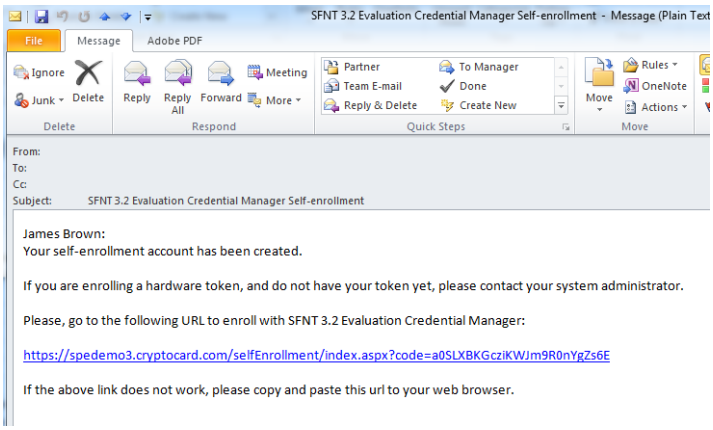


Figure 31: Validation Email

Completing this step logs the Operator into their Virtual Server.

Auth Nodes Module

An Auth Node is any RADIUS client, Agent or application (e.g. VPN and web applications such as Outlook Web Access) that will send authentication requests to the Virtual Server. The Auth Nodes module is a shortcut for adding RADIUS Clients and SafeNet Authentication Service authentication agents to the Account. Only authentication requests received from Auth Nodes in the Auth Nodes list will be processed by the account's Virtual Server.

The Virtual Server can accept and process authentication requests from an Auth Node in the list within approximately 5 minutes of configuration.

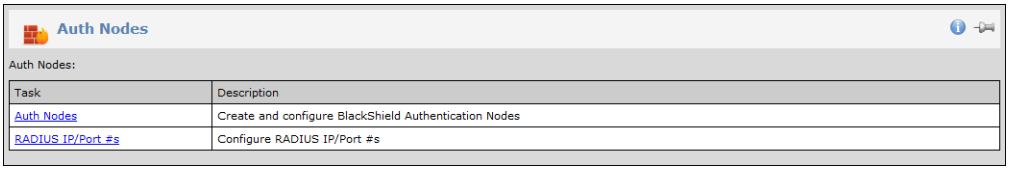


Figure 32: Auth Nodes Module

In this module:

- Auth Nodes: Click this hyperlink to list, add, modify or delete auth node entries.
- RADIUS IP/Port #: Click this hyperlink to modify the default IP address and port number for the RADIUS server. Note that the default values should not be modified unless you are using RADIUS proxy.

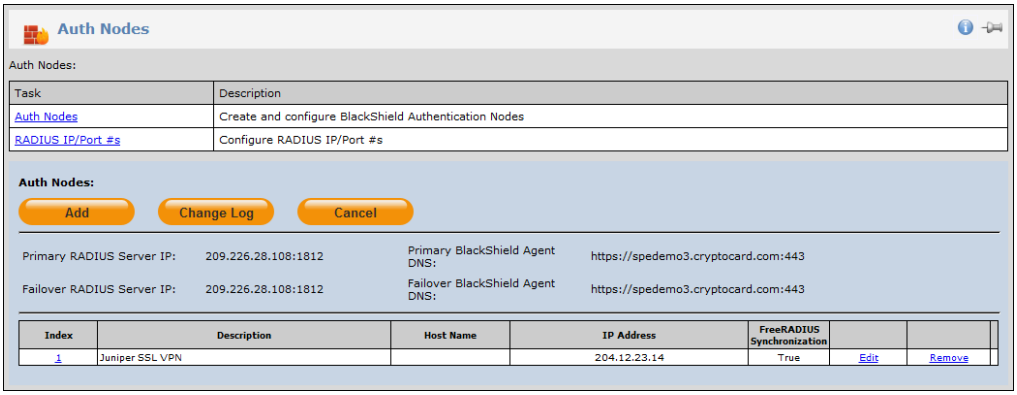


Figure 33: Auth Nodes List

Where:

- Add: click this button to add an auth node
- Change Log: click this button to view the last 5 changes to auth nodes.
- Index: click this hyperlink to view auth node configuration
- Description: the data entered in the description field when the auth node was added.
- Host Name: the data entered in the Host Name field when the auth node was added.
- IP Address: the external IP address of the auth node (i.e. the address from which the Accounts virtual server will receive authentication requests).
- FreeRADIUS Synchronization: if True, changes to auth nodes will be effective in less than 5 minutes on managed services or on instances using the FreeRADIUS plugin. This value must be false if using Microsoft IAS or NPS as the RADIUS server.
- Edit: click this hyperlink to edit the corresponding auth node configuration.
- Remove: click this hyperlink to remove the corresponding auth node configuration.

Adding an Auth Node

Begin by clicking the Add button.

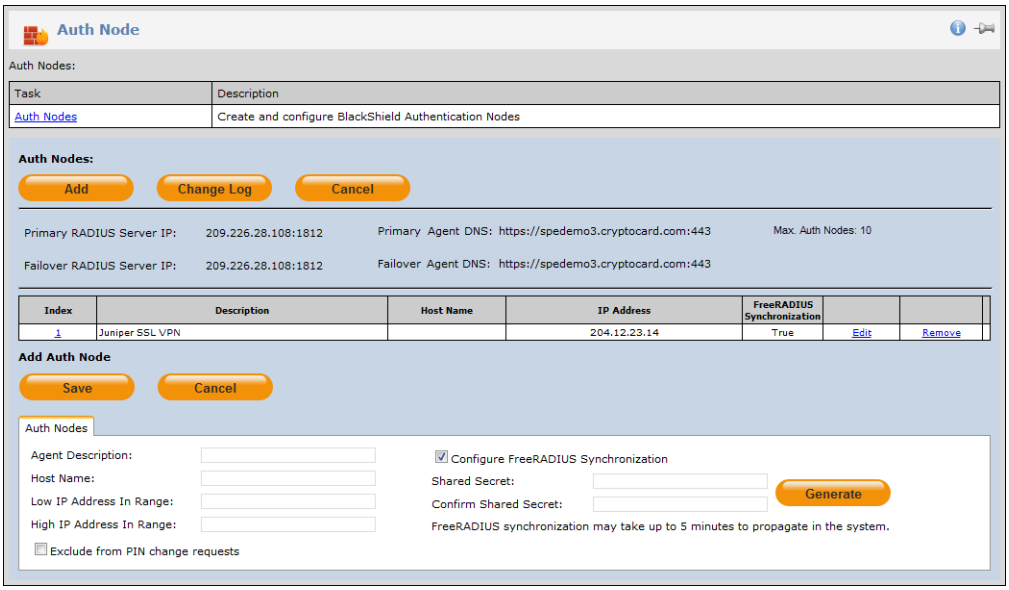


Figure 34: Auth Node Configuration

When adding Auth Nodes:

- **Primary RADIUS Server**
  Configure your RADIUS client (e.g. VPN gateway) to use this address as the primary RADIUS server.

- **Failover RADIUS Server**
  Configure your RADIUS client (e.g. VPN gateway) to use this address as the failover RADIUS server.

- **Primary Agent DNS**
  Configure your Agent (e.g. Logon Agent for Windows) to use this address as the primary authentication server.

- **Failover RADIUS Server**
  Configure your Agent (e.g. Logon Agent for Windows) to use this address as the failover authentication server.

- Configuring the RADIUS client to use the failover RADIUS server as its primary or failing to configure a failover RADIUS server may result in reduced performance or authentication outage.

- **Max. Auth Nodes**
  This is the maximum number of auth nodes allowed by your Service Provider. To increase this value, contact your Service Provider.

- **Agent Description**
  Can be used to indicate the vendor and model of the Auth Node product.

- **Host Name**
  Indicates the FQDN (Fully Qualified Domain Name) of the Auth Node. This entry is optional.

- **IP Address**
  Indicates the external IP address of the RADIUS Client or Agent. This field must conform to IPv4 or IPv6 address standards.

- **Shared Secret**
  Is used with RADIUS clients and must match the shared secret configured in the RADIUS client. It is not required for Agents.

- **Exclude from PIN change requests**
  If checked, the Virtual Server will not enforce server-side PIN changes during authentication through this Auth Node. While most RADIUS clients support challenge-response, some do not, preventing server-side PIN change. If affected by this RADIUS non-compliance in this Auth Node, simply check this box and the Virtual Server will not attempt to enforce a PIN change. If no Auth Nodes support challenge-response, a better option is to disable server-side PIN change or select a different form of PIN management.

The number of Auth Nodes that can be added is limited to the Max. Auth Nodes value entered in the Services module for this account.

Configuring Auth Nodes

To configure an Auth Node, click the Add button and enter at least the following:

For RADIUS clients such as SSL VPNs:

- A descriptive name of the device in the Agent Description field
- The IP Address of the RADIUS client
- The RADIUS Shared secret (this must be identical in both SafeNet Authentication Service and the RADIUS client)

For SafeNet Authentication Service Agents such as Agent for Outlook Web Access:

- A descriptive name of the device in the Agent Description field
- The IP Address of the RADIUS client

Some RADIUS Clients are not fully RADIUS compliant and do not support “Challenge-Response” which is a requirement for Server-side PIN changes. If your RADIUS client does not support Challenge-Response and you have configured your Server-side PIN policy to require the user to periodically change their PIN, check the “Exclude from PIN change requests” to prevent a forced PIN change with the non-compliant RADIUS client.

Auth Nodes become active within minutes of configuration.

Sharing and Realms

Sharing and Realms is an optional service feature that allows an Auth Node to be shared with two or more organizations or Virtual Servers. Essentially a Realm is a group of Virtual Servers. For example, (referring to Figure 35: Sharing and Realms) Org 1 manages a Web Application and its own users for authentication. Org 1 wants users from 3 of its subsidiaries (Org 2, 3, 4), each with their own Virtual Server to be able to log into the Web App. In addition each Org has protected applications to which only its users should have access. Using Sharing and Realms, Org 1 can share the Web App with other orgs while restricting access to other Auth Nodes to its own users.

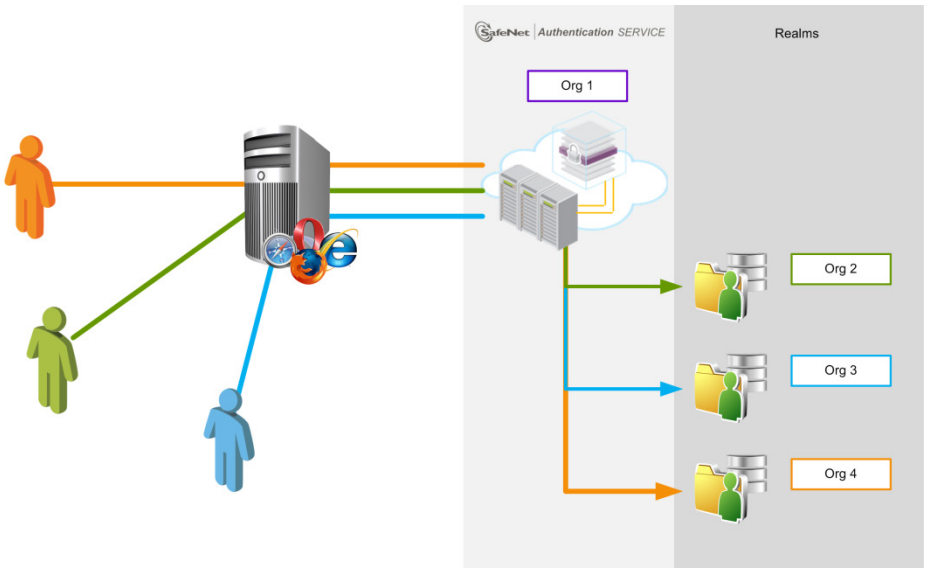


Figure 35: Sharing and Realms

To configure begin by clicking the Sharing and Realms tab, configure as necessary then click Save to commit the configuration where:

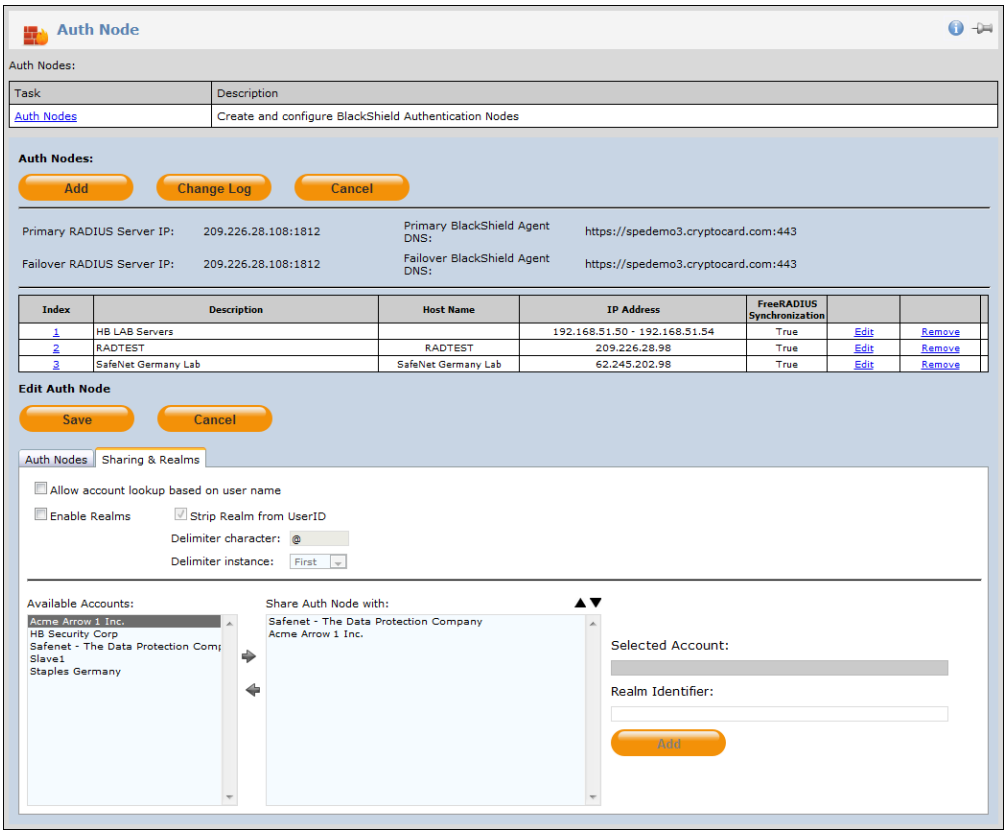


Figure 36: Sharing and Realms

- **Allow account lookup based on user name**
  The submitted UserID will be used to authenticate the user. The Virtual Server will search the "Shared Auth Node" list in descending order. The first matching UserID will be used to authenticate the user. Use the up/down arrows to move a selected realm up or down in the priority list. Effectively this means that all UserIDs must be unique across all Realms.

- **Enable Realms**
  Use this option where UserIDs may not be unique across all realms. If enabled, additional UserID information will be used to determine to which realm the user belongs. Typically the UserID will be an email address. Use this feature in conjunction with the Selected Account and Realm Identifier options.

- **Strip Realm from UserID**
  Strips all data starting with the delimiter character from the UserID. This allows a submitted UserID such as an email address (UserID@myco.com) to be authenticated as UserID.

- **Delimiter Instance**
  Uses the first instance of the delimiter (left to right) or last instance of the delimiter (right to left).

For example, consider two users with the identical UserID of BSmith, one belonging to ACME (acme.com), the other belonging to International Light (IL.com). Configured as follows:

- Realms enabled
- Strip realm from UserID
- Delimiter character is “@”
- Selected Realm= ACME, Realm Identifier= ACME.COM
- Selected Realm=International Light, Realm Identifier= IL.COM
- The UserID of BSmith@acme.com would authenticate against the Acme Virtual Server with an effective UserID of BSmith while BSmith@IL.com would authenticate against the International Light Virtual Server with an effect UserID of BSmith.

Contacts Module

The Contacts module allows contacts and coordinates to be associated with the account. They are simply account contact references.

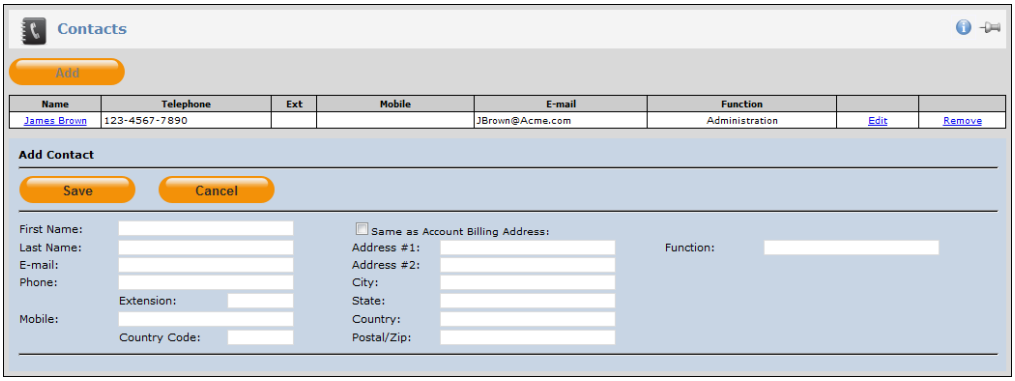


Figure 37: Contacts Module

The Contact list displays the contact detail. Click the Name hyperlink to open the detail view. Select the Receives Service Update and Receives System Alerts checkboxes to send alerts of these types to the contact.

Accounts List

The Accounts list appears on the On-Boarding tab after creation of your first account. It lists relevant information about each account and provides access to all of the account management functions of the On-boarding process.

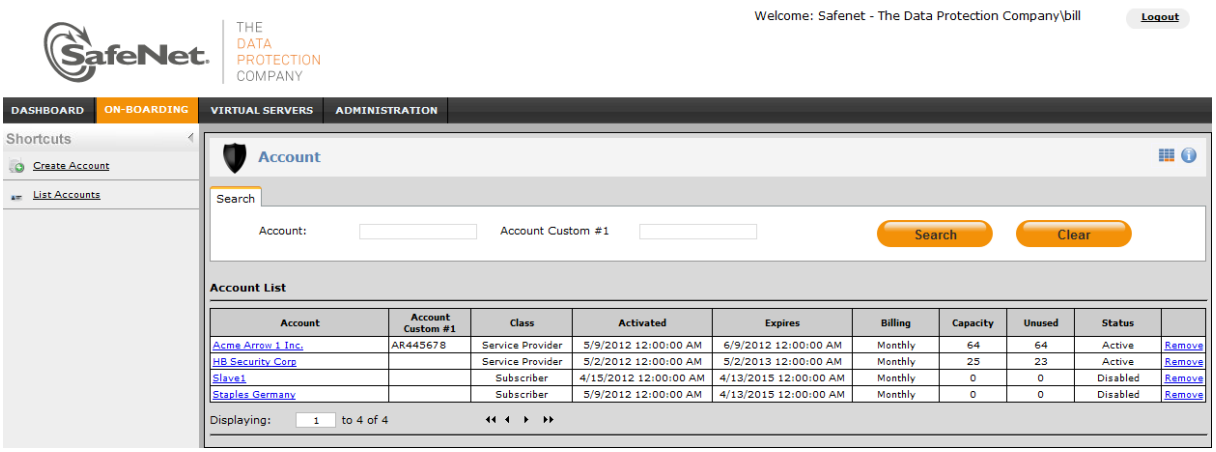


Figure 38: Accounts List

- **Account**
  This is the name of the account. Click the hyperlink to access all of the On-boarding functions for this account.

- **Custom #1**
  This is the data entered in the Custom #1 field in the Accounts module.

- **Class**
  This indicates the type of Account. Possible values are account and Service Provider.

- **Activated**
  This is the date and time the Account Services were set to Active on the Services module.

- **Expires**
  This is the date and time the Services will automatically expire, after which the account will not be able to use the service or log into the management UI.

- **Billing**
  This indicates the value entered for billing in the Services module.

- **Capacity**
  This is the total capacity allocated to this account through the Allocation module.

- **Unused**
  This is the total unused capacity. Note: capacity is consumed when an authentication method is assigned to a user in this accounts Virtual Server, or if this account (Virtual Service Provider) allocates capacity to an account that it has created and manages.

- **Status**
  This field indicates the state of the Service. It will always be set to Active unless the current date is greater than the Expires date or the Services have been deactivated in the Service module.

- **Remove**
  This hyperlink is used to remove the account from the Service. Remove will not function until all capacity and rented tokens have been deallocated.

Delegation Code Module

As mentioned throughout this document, Service Providers are able to view and manage accounts they create but are not able to view or manage any accounts created by any other Service Provider.

There are two exceptions to this rule.

Exception 1:

If Delegated Management is selected in the Services Module, your Service Provider is able to manage your account's Virtual Server (i.e. your parent account is able to manage your child's virtual server). This selection adds this account to your Service Providers Virtual Servers tab. Note: this account is not added to your Service Providers ON-BOARDING tab and therefore they cannot perform any On-Boarding functions for this account.

Exception 2:

Any Service Provider can manage any account, but only if there is mutual agreement. This is accomplished using Delegation Codes.

A Delegation Code is a unique code generated by a Service Provider. The code must be installed in the account's Virtual Server. Installation signals their agreement to have their Virtual Server managed by a new or additional Service Provider. Once the code is installed, the Service Provider that generated the code must activate the code, signaling their agreement to manage the accounts Virtual Server. On completion the account's Virtual Server appears on the Service Provider's VIRTUAL SERVERS tab.

Using Delegation Codes

The sequence for using delegation codes is:

- The Service Provider must generate a delegation code
- The delegation code must be installed in the account's Virtual Server
- The Service Provider must activate the code.

To generate and activate a delegation code

1. Click New to create a new delegation code. Select the Account Group into which the virtual server will be added. This is a list of configured Management Groups (refer to the Account Management Groups Module section on page 68). The account will be added to the selected Management Group on activation of the delegation code where:

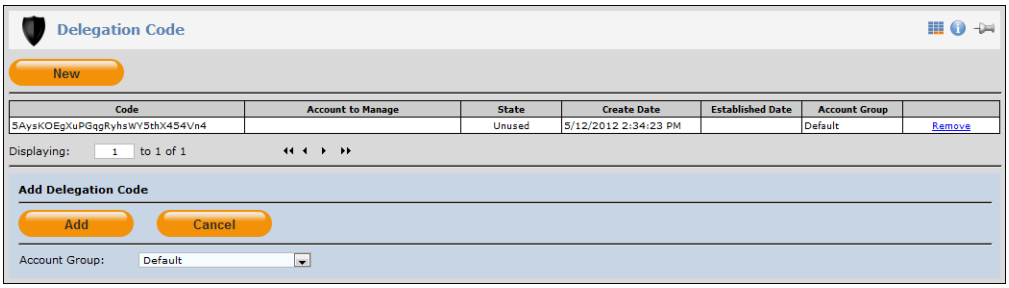


Figure 39: Generate a Delegation Code

- **Code**
  This is the code that must be installed in the account's Virtual Server.

- **Account to Manage**
  This is the name of the account. This field is populated after the code is installed in the account's Virtual Server.

- **State**
  Indicates whether or not the code has been activated. Possible states are pending and active.

- **Created Date**
  This is the date the code was generated.

- **Established Date**
  This is the date the delegation code was activated.

- **Account Group**
  This is the Management Group to which the account's Virtual Server belongs.

- **Remove**
  This hyperlink is used to remove the delegation code and terminate delegated management of the account's Virtual Server.

2. Provide the delegation code to the Account. This code must be added to the "External Operators" module in the accounts virtual server and verified.

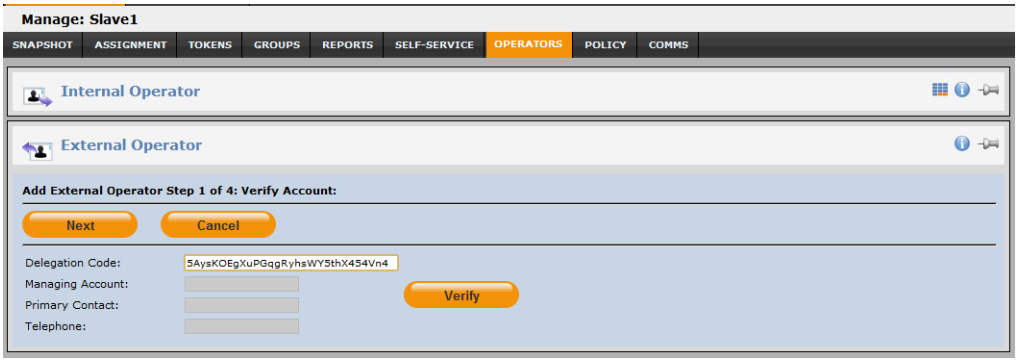


Figure 40: Adding delegation code in Virtual Server

3. Once it's verified, the external operator is assigned a role from one of the roles configured in the virtual server. This role limits the functionality available to the delegated manager.

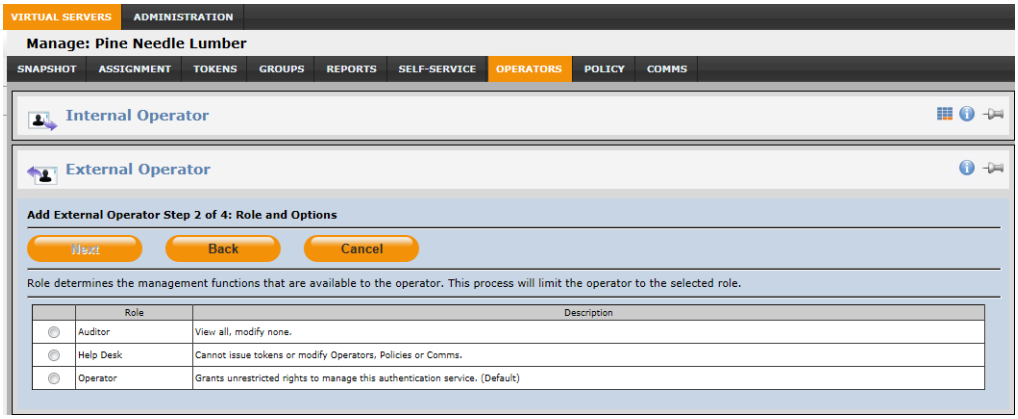


Figure 41: Assigning a role to the delegated manager

4. The delegated manager's scope can be limited to the users and/or tokens in the selected containers of the virtual server.

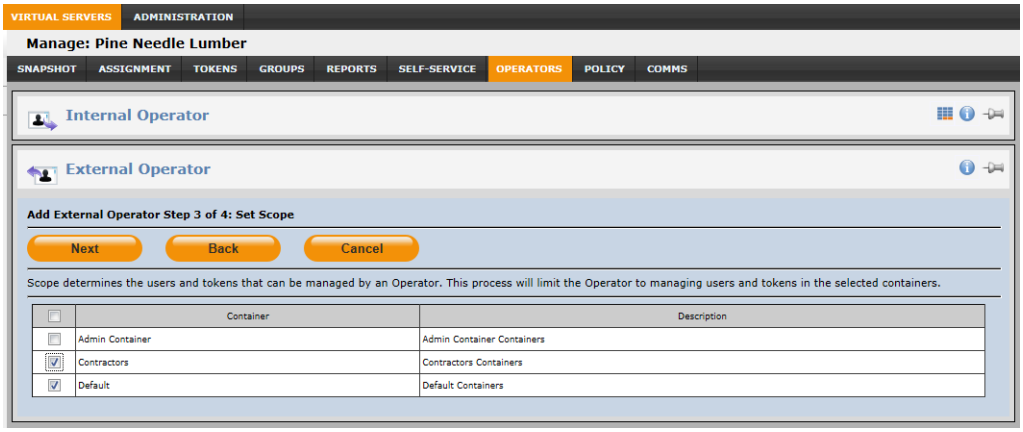


Figure 42: Setting delegated manager scope

5. The activation period for the delegated manager can be limited by setting the day, dates and hours options.

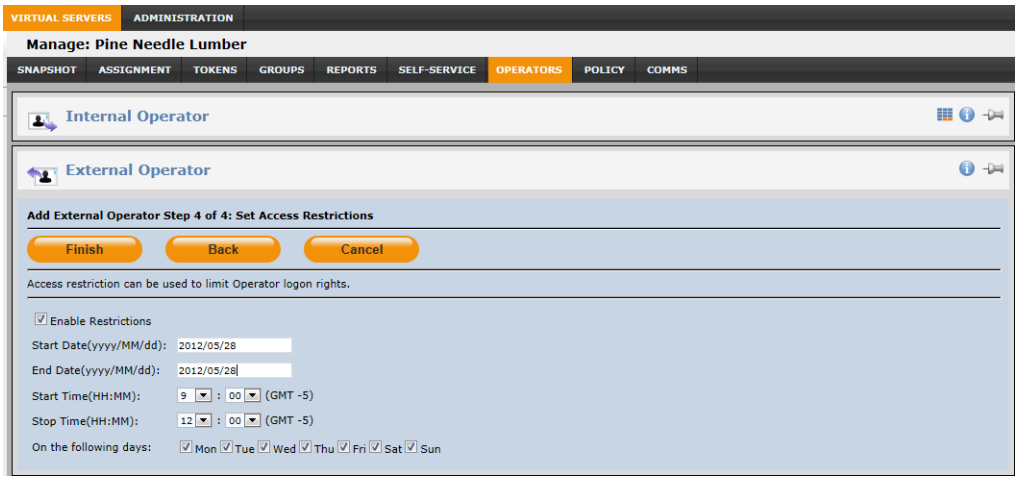


Figure 43: Limiting the delegation period

6. The external operators list is updated with the new external operator.

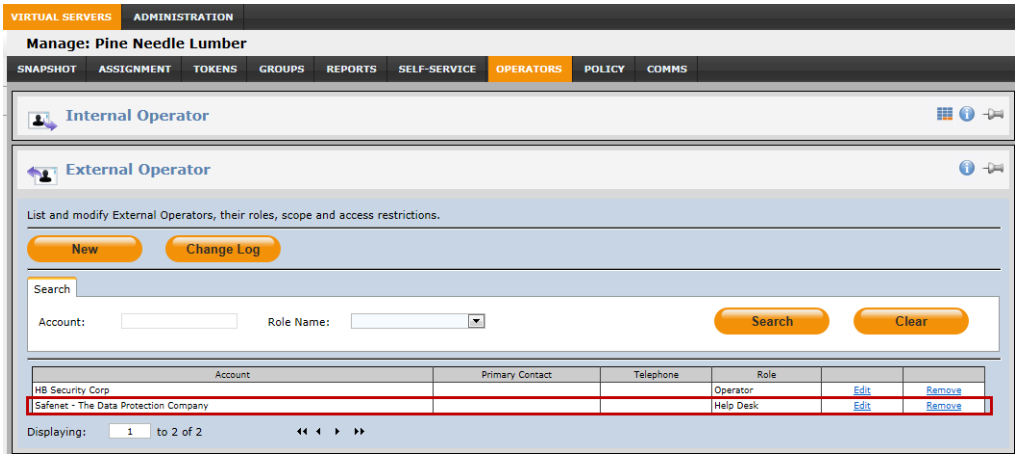


Figure 44: New External "Delegated" manager

7. At the same time, the state of the delegation code provided by the Service Provider is updated to the Pending Acceptance hyperlink. Click the hyperlink, then Apply to confirm the delegation.

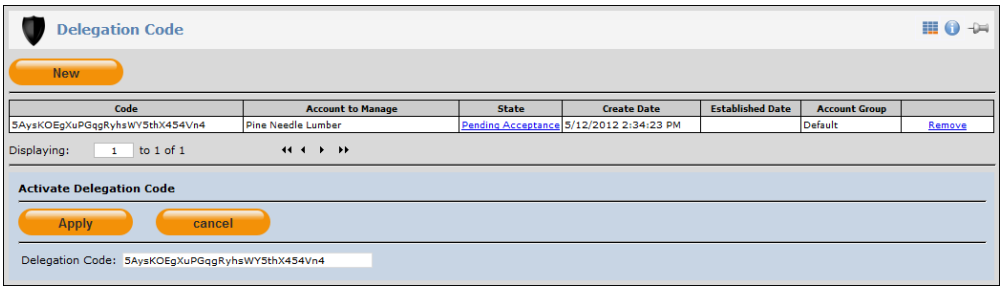


Figure 45: Delegation Code Pending Acceptance

This will change the state of the code to Established.

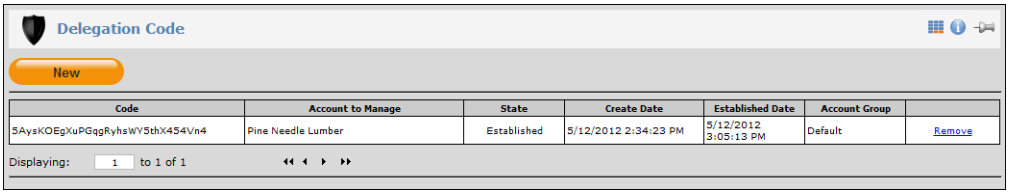


Figure 46: Delegation Established

The virtual server can now be selected from the Virtual Servers tab. A delegation can be removed at any time by clicking the Remove hyperlink for the corresponding delegation. The Role and Scope of the Service Provider is configured in the account's Virtual Server.

Role, Scope and Access Restrictions can be used to limit the management functionality on the

Virtual Server available to the Service Provider's Account Managers. For more information on setting Role, Scope and Access Permission in a Virtual Server refer to the Role Management Module on page 225.

Administration Tab

On this tab:

- **Account Management Groups**
  Use this module to create groups into which you can place accounts. Account Managers will not have access to accounts that exist within Groups that are not within their Scope.

- **Account Manager Roles**
  Use this module to configure the management UI functionality available to an Account Manager. Roles determine which tabs, modules within tabs and actions within modules are available to the Account Manager.

- **Account Manager Maintenance**
  Use this module to add, remove or modify Account Managers, the roles to which they are assigned, their Scope (groups they are allowed to manage) and time/day/date restrictions for management UI logon.

- **Alert Event Thresholds**
  Use this to configure the types of alerts generated and where appropriate, the thresholds that will trigger an alert.

- **Role Alert Management**
  Use this module to attach a list of alerts to a role and configure alternative alert delivery methods such as email and SMS.

- **External Alert Recipients**
  Use this module to send alerts by email and/or SMS to recipients that are not Account Managers.

- **Report and Billing Management**
  Use this module to customize, generate and deliver reports for audit, billing, asset management and operator activity for your entire account base.

- **Customize References**
  Use this to add links to documents, downloads (agents), terms of use agreements; to add help desk coordinates; publish service notifications, all of which are presented in subscriber virtual servers.

- **Account Role Provisioning Rules**
  Use this module to automatically add Account Managers and assign them to a role and scope based on their group membership in the Service Providers virtual server. Typically this is used with Active Directory groups.

- **Auto Remove**
  Use this to set the maximum age of report output and alerts. All reports and alerts older than the

configured number of days are automatically removed. Note that this doesn't delete the data from the system, but only the report itself.

Operational Security Overview

As a Service Provider it is likely that you will add a number of Account Managers to assist with the tasks of on-boarding, managing and supporting accounts. Operational security gives you the tools to tailor Account Manager "Roles" (what they can do) and "Scope" (to whom or what). SafeNet Authentication Service can also generate service alerts and automatically deliver these to specified Account Managers, making them aware of events that require their attention as they occur in real time.

The steps in establishing operational security are:

- Configure Account Management Groups
- Configure Account Manager Roles
- Add Account Managers
- Configure Alert Event Thresholds
- Configure External Alert Recipients

Account Management Groups Module

Management Groups are best thought of as "buckets" that hold some number of accounts. Though accounts can be moved between management groups they cannot exist in more than one group at a time.

Scope determines which groups or buckets (and therefore which accounts) can be managed by an Account Manager.

For example, consider a Service Provider with a global support desk and two sales regions, East and West, each of which is exclusively responsible for On-boarding accounts for their respective regions. The support desk must be able to manage the Virtual Servers for accounts in both regions.

One solution would be to create two groups, East and West. Accounts on-boarded in the East would be placed in the East management group while those in the West would be placed in the West management group. The next step would be to create an on-boarding role and a support desk role. Then as Account Managers are added to the system, they would be assigned one of the following combinations of Role and Scope:

Role	Scope
On-boarding	East Group
On-boarding	West Group
Support Desk	East Group and West Group

Creating Account Management Groups

Begin by clicking the Account Management Group hyperlink on the Administration tab.

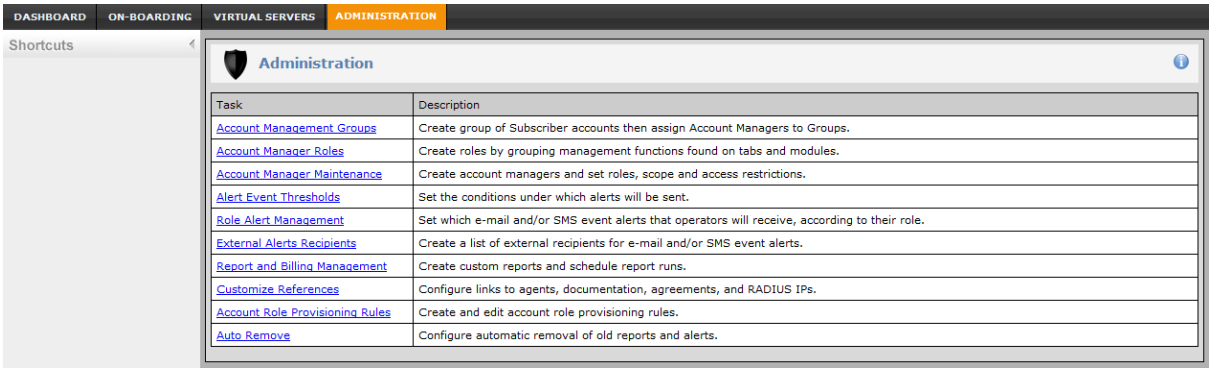


Figure 47: Administration Module

This will display the list of Management Groups with a brief description of each group's purpose.

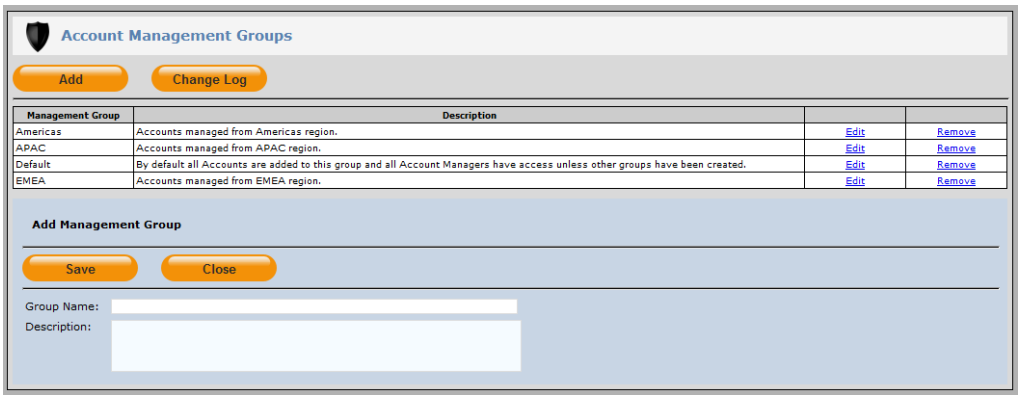


Figure 48: Account Management Groups List

To add or edit a group click the Add button or Edit hyperlink respectively. Click Remove to delete a group that does not contain any accounts.

Note that the Default group cannot be removed. All accounts belong to the Default group and all Account Managers have access to accounts in this group if no other management group is selected or available.

Accounts can be added or moved to a different management group from the Account Detail module on the On-boarding tab. Refer to Create Account Shortcut on page 35.

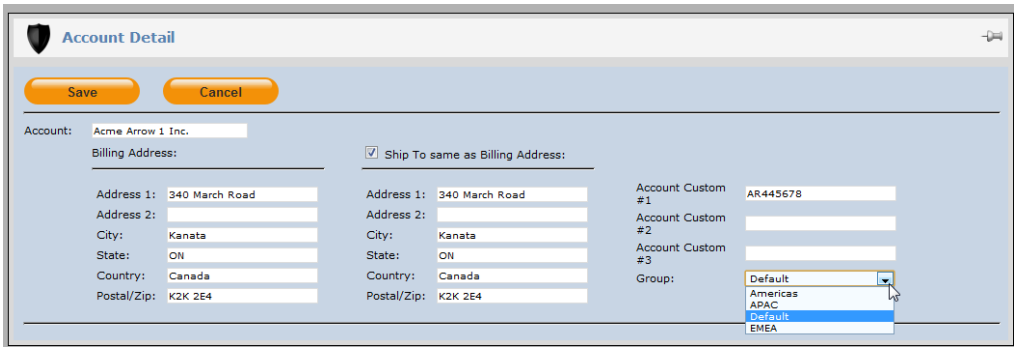


Figure 49: Adding an account to a Management Group

Account Manager Roles Module

A Role is a combination of tabs, modules and actions that are available to an Account Manager. Access to tabs and modules can be disabled. Where access to tabs and modules is allowed, the actions within any module can be restricted. For example:

- Disabling the “Create Accounts” hyperlink under Shortcuts would remove the ability for an Account Manager to create a new account.
- Disabling the “Add, Edit and Remove” actions in the Auth Nodes module would allow an Account Manager to view the Auth Node list and deny the ability to make any changes.

This high degree of granularity means that Operational Security can easily accommodate your operational and security requirements.

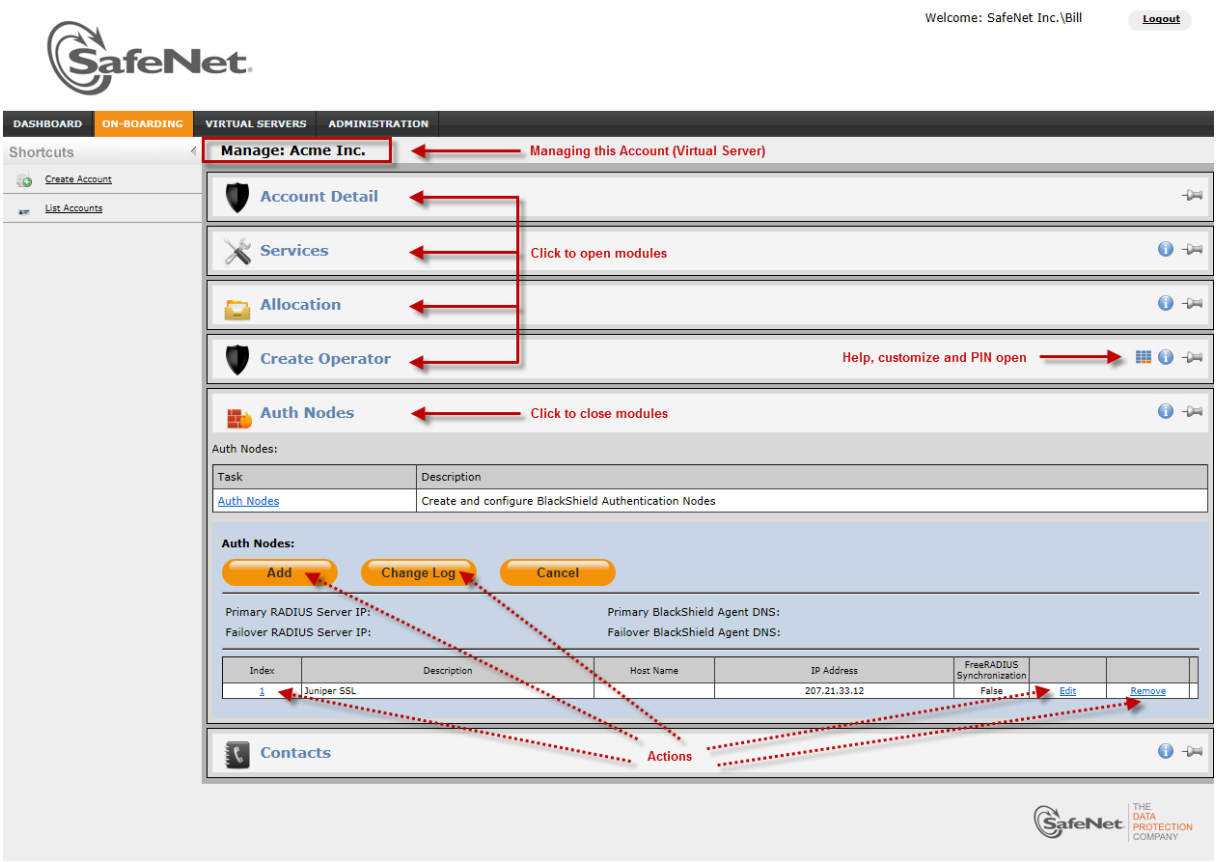


Figure 50: Tabs, Modules and Actions

Creating an Account Management Role

Begin by selecting the Account Management Roles hyperlink on the Administration tab. Refer to Figure 47: Administration Module on page 69.

This will display the Account Manager Roles list. Clicking the Role hyperlink displays the list of tabs, modules and actions available for the selected role. All roles except the default “Account Manager” role can be edited or removed by clicking the Edit and Remove hyperlinks respectively.

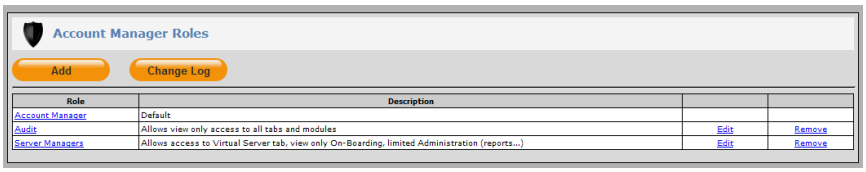


Figure 51: Account Manager Roles List

Adding or Editing a Role

To add a role or edit an existing role, click the Add button or Edit hyperlink respectively. If adding, you will be prompted to create a role name and a role description, after which you’ll be presented with the Role configuration page. (Figure 52: Modify Access to Tabs, Modules and Actions on page 72)

The Role configuration page is split into several horizontal sections, each representing a different tab. Within each section is a table listing all modules available on the tab and a corresponding set of actions available for each module.

Clearing a check box removes the tab, module or action from the role.

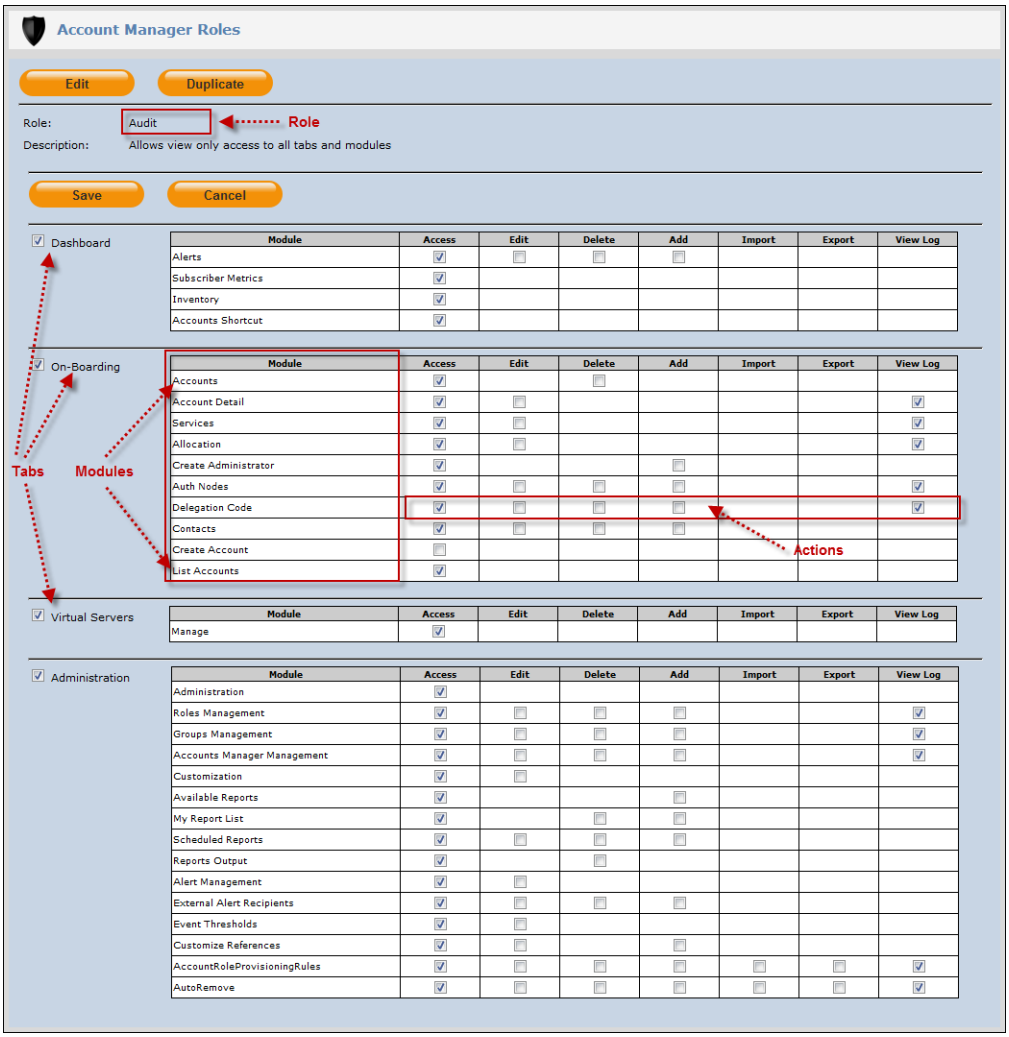


Figure 52: Modify Access to Tabs, Modules and Actions

Module Actions

There are seven possible actions:

- **Access**
  If checked, the module will be displayed.

- **Edit**
  If checked, the Role will have access to all edit functions available in the module.

- **Delete**
  If checked, the Role will have access to all delete or remove functions available in the module.
- **Add**
  If checked, the Role will have access to all Add functions available in the module.
- **Import**
  If checked, the Role will have access to all import functions available in the module.
- **Export**
  If checked, the Role will have access to all export functions available in the module.
- **View Log**
  If checked, the Role will have access to the View Log function available in the module.

Account Manager Maintenance

Account Managers are able to log into the management interface and perform actions corresponding to their Role and Scope. To add an Account Manager begin by clicking the Account Manager Maintenance hyperlink in the Administrator module. Refer to Figure 47: Administration Module on page 69.

This will display a list of all Account Managers with options to View, Add, Edit and Remove Account Managers.

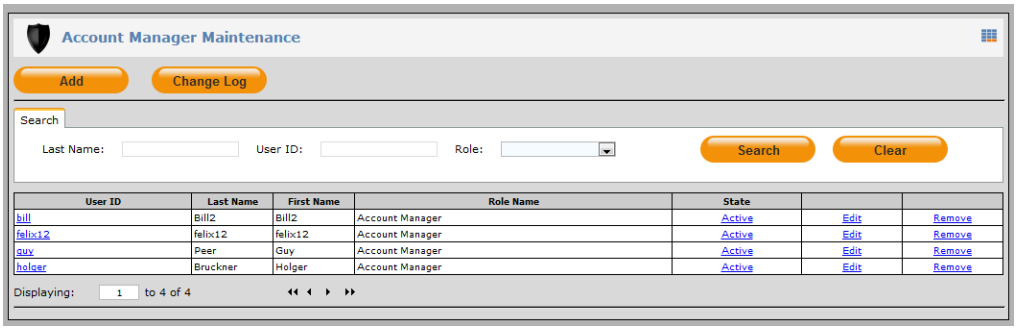


Figure 53: Account Managers List

- Clicking the User ID hyperlink displays the user's detail.
- Clicking the State hyperlink to Suspend or Activate an Account Manager and therefore respectively deny or allow logon to the management UI.
- Click the Edit hyperlink to change the Role, Scope and Access Restrictions for the corresponding Account Manager.
- Click the Remove hyperlink to remove the user as an Account Manager.

Adding an Account Manager

Begin by clicking the Add button to display a list of users eligible for promotion to Account Manager Status.

Only users that have an active authentication method in the Service Providers Virtual Server are eligible for promotion to Account Manager. If the user you wish to promote is not displayed in the list, go to the Virtual Server and assign or provision the user with a token, then return to this step.

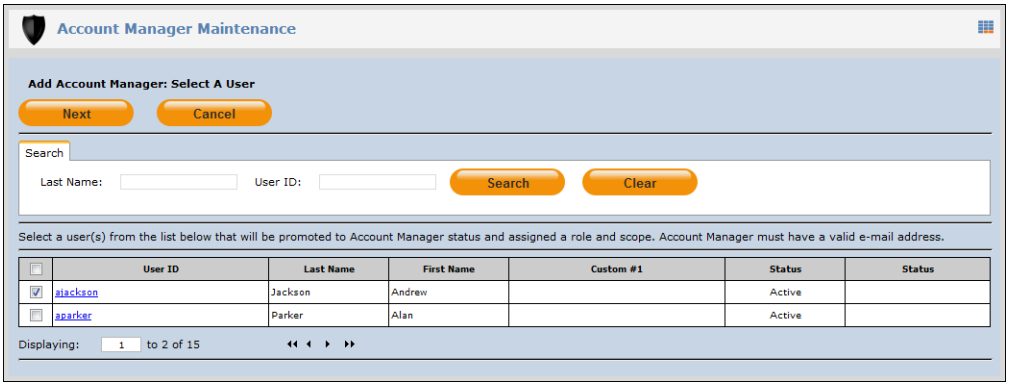


Figure 54: Promoting Users to Account Managers

Next, select one or more users to be promoted to Account Manager status, bearing in mind that the same Role, Scope and Access Restrictions will be applied to all selected users.

Next select the Role to be applied.

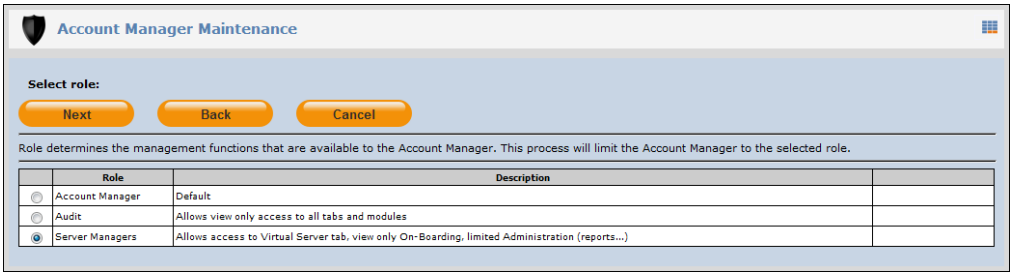


Figure 55: Role Selection

Next set the Account Manager's Scope by selecting the management groups to which they will have access.

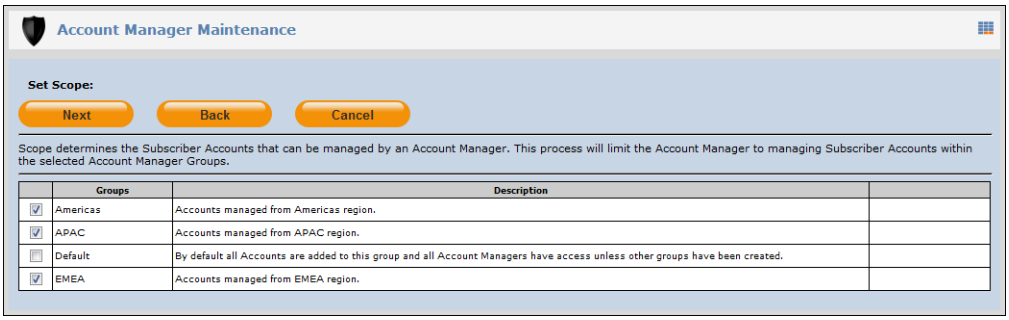


Figure 56: Select Management Groups (Scope)

The final step is to set any desired time and day access restrictions where:

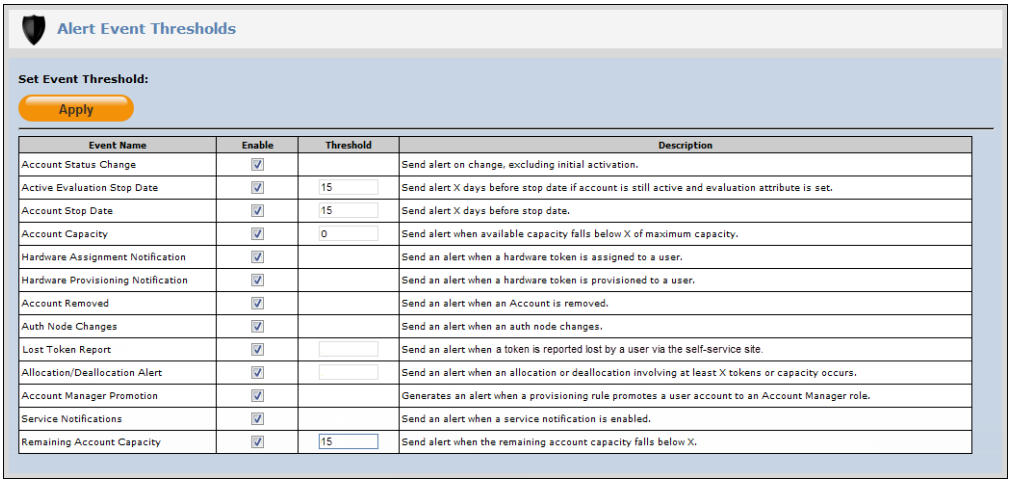
Figure 57: Set Account Manager Access Restrictions

- **Enable Restrictions**
  If checked, restrictions are enabled. If cleared, no time/day/date range restrictions are applied.
- **Start Date**
  Management UI logon is denied before this date.
- **End Date**
  Management UI logon is denied after this date.
- **Start Time**
  Management UI logon is denied before this time.
- **End Time**
  Management UI logon is denied after this time.
- **On the following days**
  Management UI logon is permitted on checked days only.

Note that Account Manager Restrictions apply only Account Manager management UI logons. It does not affect any other logon by the user (e.g. VPN).

Alert Event Thresholds

Alerts can be generated when an event or a threshold is exceeded that may affect one or more of your accounts. To set event thresholds, begin by clicking the Alert Event Thresholds hyperlink in the Administrator module. Refer to Figure 47: Administration Module on page 69.



Event Name	Enable	Threshold	Description
Account Status Change	☑		Send alert on change, excluding initial activation.
Active Evaluation Stop Date	☑	15	Send alert X days before stop date if account is still active and evaluation attribute is set.
Account Stop Date	☑	15	Send alert X days before stop date.
Account Capacity	☑	0	Send alert when available capacity falls below X of maximum capacity.
Hardware Assignment Notification	☑		Send an alert when a hardware token is assigned to a user.
Hardware Provisioning Notification	☑		Send an alert when a hardware token is provisioned to a user.
Account Removed	☑		Send an alert when an Account is removed.
Auth Node Changes	☑		Send an alert when an auth node changes.
Lost Token Report	☑		Send an alert when a token is reported lost by a user via the self-service site.
Allocation/Deallocation Alert	☑		Send an alert when an allocation or deallocation involving at least X tokens or capacity occurs.
Account Manager Promotion	☑		Generates an alert when a provisioning rule promotes a user account to an Account Manager role.
Service Notifications	☑		Send an alert when a service notification is enabled.
Remaining Account Capacity	☑	15	Send alert when the remaining account capacity falls below X.

Figure 58: Alert Event Thresholds

To enable an alert, place a check in the corresponding option in the Enable column where:

- **Account Status Change**
  Detects service changes to or from Active and Disabled (refer to Services Module on page 36.)

- **Active Evaluation Stop Date**
  This alert is triggered if an Account has the Evaluation option checked and the Service Stop date is within X days of the current date. Adjust the threshold accordingly.

- **Account Stop Date**
  This alert is triggered if the Account Service Stop date is within X days of the current date. Adjust the threshold accordingly.

- **Account Capacity**
  This alert is triggered when your Inventory of capacity falls below X. Use this to be alerted to a low capacity condition that may prevent you from On-boarding additional accounts of fulfilling orders from existing account. Adjust the threshold accordingly.

- **Hardware Assignment Notification**
  This alert is triggered every time a hardware token is assigned to a user.

- **Hardware Provisioning Notification**
  This alert is triggered every time a hardware token is provisioned to a user. The alert contains the User's detail so that the alert recipient is able to arrange for shipment of the hardware device to the user.

- **Account Remove**
  This alert is triggered with an Account is removed (On-Boarding Tab).

- **Auth Node Changes**
  This alert is triggered whenever an Auth Node is added, modified or removed.

- **Allocation/Deallocation**
  This alert is triggered whenever inventory (capacity, tokens, ICE, SMS Credits) are allocated or deallocated from a virtual server. Adjust the threshold accordingly.

- **Account Manager Promotion**
  This alert is triggered whenever a user is promoted to Account Manager, any changes are applied to their Account Manager role or they are removed from Account Managers.

- **Remaining Account Capacity**
  This alert is triggered when an Accounts capacity falls below X.

Alerts are displayed on the Dashboard in the Alerts module where they can be viewed, acknowledged and closed. Alerts can also be delivered by email and SMS text message.

Role Alert Management

Once alert event thresholds have been established, the next step is to determine alert recipients. This begins by clicking the Role Alert Management and/or the External Alerts Recipients hyperlinks in the Administration module. Role Alert Management links alerts to Account Manager roles whereas External Alerts Recipients is used to send alerts to individuals who may or may not be Account Managers.

Every time a role is created it is automatically configured with an Alert list with all alerts disabled.

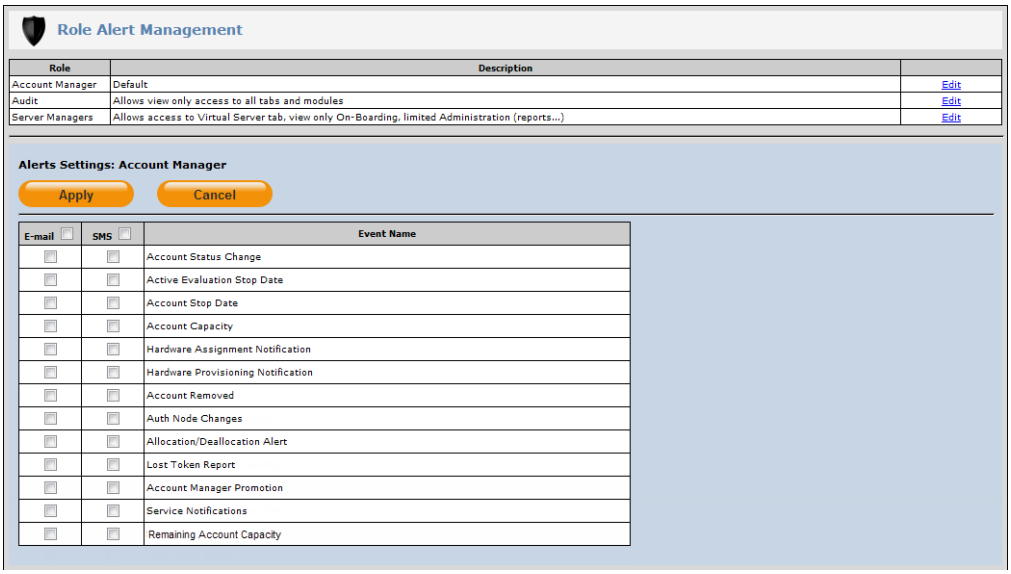


Figure 59: Configuring Alerts by Role

To configure alerts for a role, click the corresponding Edit hyperlink and select the desired delivery method(s) for each alert, and then click Apply to commit the changes.

The process for External Alert Recipients differs only in the requirement to name the Alert configuration and enter the recipient's name, email and SMS number as necessary for the delivery method(s) selected.

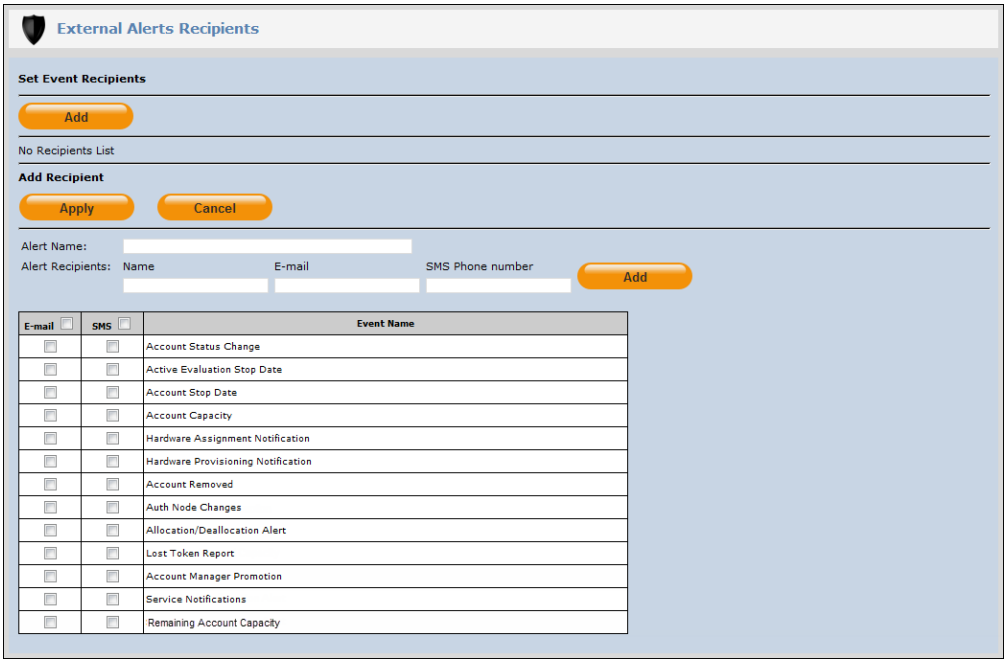


Figure 60: Configure External Alert Recipients

Viewing, Acknowledging and Closing Alerts

Alerts are displayed in a table on the Dashboard tab in the Alerts Module.

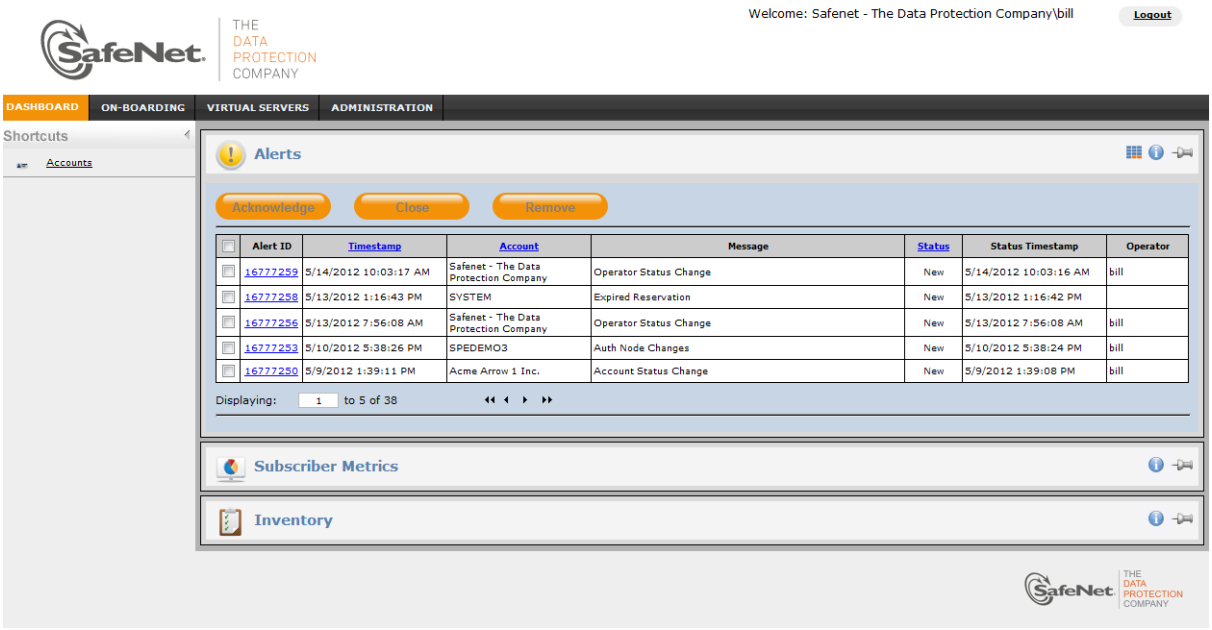


Figure 61: Alerts List

Clicking the Alert ID displays additional detail about the alert.

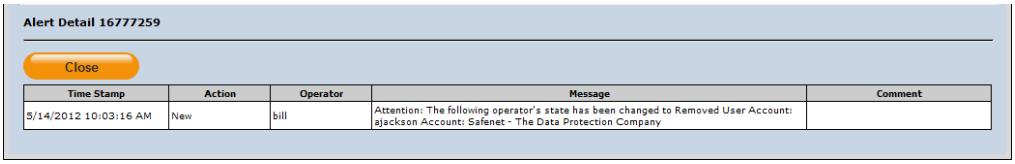


Figure 62: Alert Detail

Selecting an Alert and clicking the Acknowledge or Close button opens a dialogue that allows the Account Manager to enter a comment. The Acknowledge function indicates that the Account Manager is aware of the condition. Comments can be used to communicate the status or leave instructions for other Account Managers. When an Alert is acknowledged, the State will change to Acknowledged. The Close function indicates that the condition causing the alert has been rectified and the condition no longer exists.

One or more alerts can be removed by selecting the alert then clicking the Remove button. This removes the alert from the list however the alert and all related activity are retained and can be retrieved through reports.

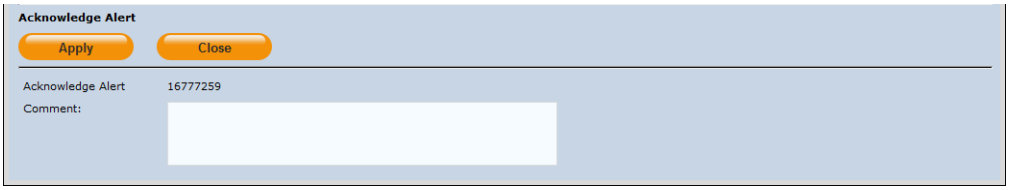


Figure 63: Acknowledge/Close Alert

Remove

Use remove to delete selected alerts in the list. Note that removing the alert does not remove the permanent record of the event. Event history can be retrieved by running the appropriate reports.

Reports and Billing Management

The Service Provider reporting engine provides an extensive range of usage, compliance, inventory management and billing reports. Reports can be customized, scheduled and automatically delivered to recipients or viewed and downloaded through the management UI.

Note that these reports do not include or expose user specific information but rather cumulative information for billing and reporting purposes. For example, a report may include the name of all organizations in the tree below the service provider (i.e. child, grandchild etc.) and include a count of tokens by type and their state, however the reports will not include any user specific information (name, userID, token assignment etc.). Detailed reports including user specific information must be generated at each virtual server. This mechanism provides a way for the subscriber account to protect confidential information from the service provider.

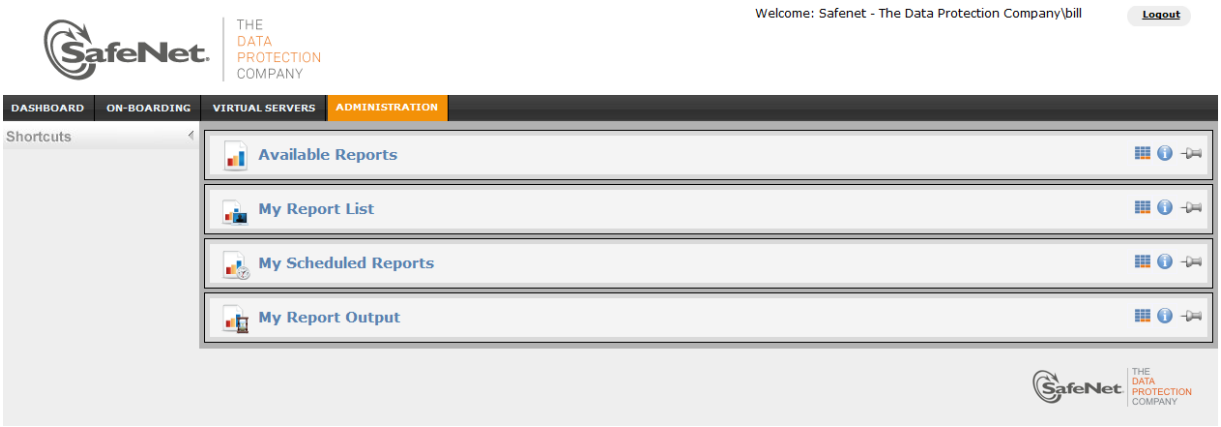


Figure 64: Reports Tab and Modules

Reporting consists of four modules:

- **Available Reports Module**
  This module lists all of the standard reports available in SafeNet Authentication Service for Service

Providers. Reports from this list can be customized and copied to the My Customized Reports module.

- **My Customized Reports Module**
  This module lists all reports that can be run on by the Service Provider. Reports in this module can be scheduled to run once or periodically at regular, predefined intervals. Delivery options and recipients are defined in this module.

- **Schedule Reports**
  All scheduled reports appear in the Scheduled Reports list. Schedules can be modified and reports can be run “Now” without modifying the normal schedule.

- **Report Output**
  This module lists all reports that are currently in the run state or have completed. From this list Account Managers can view or download reports to which they are entitled in a variety of formats.

Account Manager roles determine which modules are available to an Account Manager and whether or not they can modify report parameters. Reports can be customized, scheduled and delivered to the account, the Service Provider and to external parties such as auditors.

Scheduled reports and Report Output will display only those reports to which the Account Manager is entitled.

Available Reports Module

All reports that are available to a Service Provider are listed in the Available Reports module. To view the entire list of available reports, use the navigation controls below the list or expand the number of rows displayed using the customization icon in the module bar. The report class dropdown selects reports corresponding to:

- **Account Management**
  This group of reports deals with account usage, service terms and overall operations.

- **Compliance**
  This group of reports covers Account Manager activities related to managing accounts and operations performed through the management UI.

- **Billing**
  This group of reports provides details of all transactions including capacity, tokens, SMS credits and their related billing terms.

- **Service Metrics**
  This group of reports is similar to the information provided on the Dashboard tab | account Metrics module.

- **Asset Management**
  This group of reports reflects the state and usage of tokens both in Inventory and allocated to accounts.

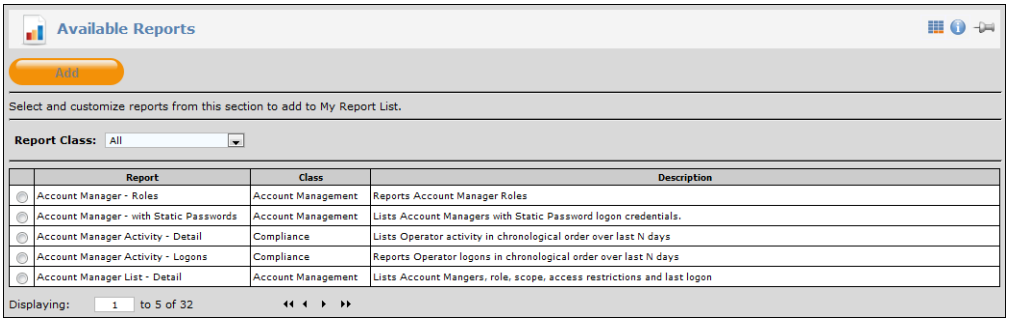


Figure 65: Available Reports Module

To add a report to the My Customized Reports Module list, begin by selecting a report from the list, and then click the Add button.

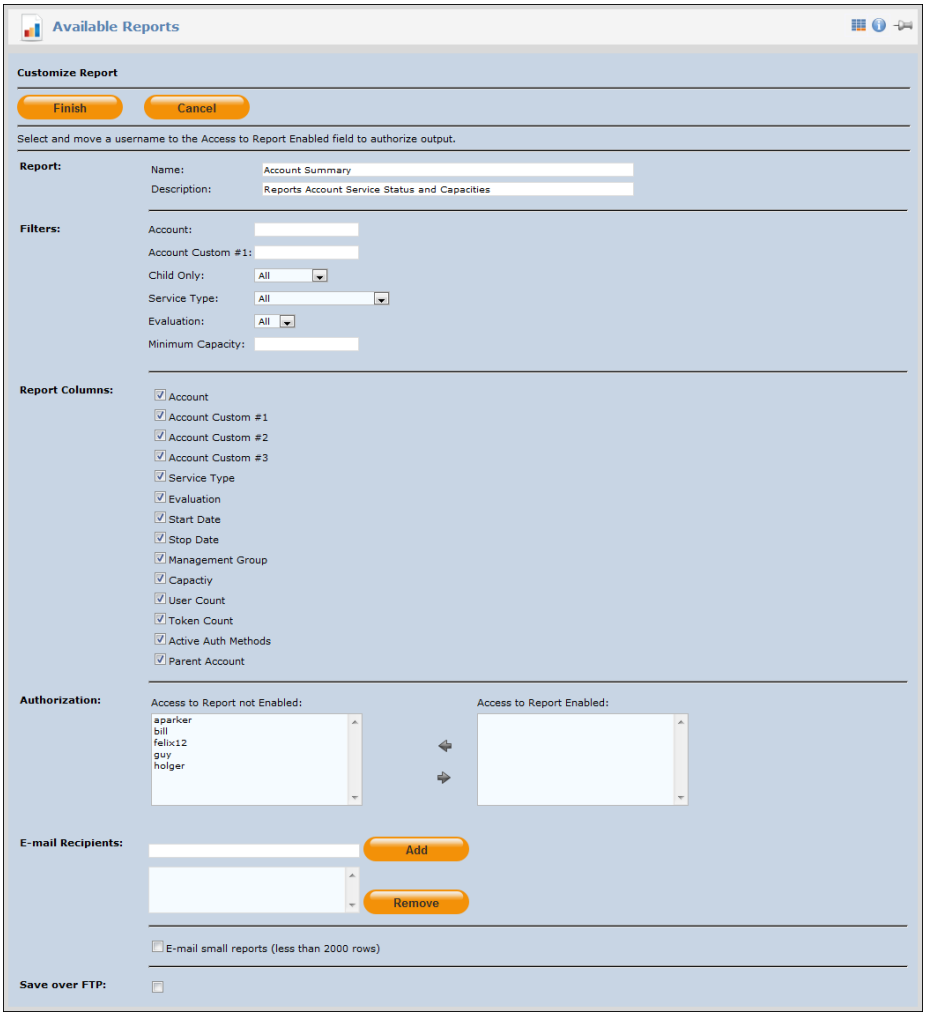


Figure 66: Customize Report

Customize Report

The options for report customization vary depending on the type of report selected. In general:

- **Report Section**
  Customize the name of the report and its description. These changes will appear in the My Reports List module. Note that report names must be unique.

- **Filters**
  If available, filters provide a way to limit the scope of a report, such as the reporting period. Filters will vary depending upon the nature of the report. Common filters include:

- **Child Only or ALL**
  Child only includes data from accounts on-boarded by the Service Provider. All includes data for from all account in the tree below the Service Provider (e.g. child, grandchild etc.).

- **Date Range**
  This can be a specific range, or for regular reports, can be options such as this month, last month, last 3 months etc.

- **Report Columns**
  This shows default fields included in the report. To include/exclude fields, select/deselect fields using the corresponding check boxes.

- **Authorization**
  The Access to Report not Enabled field lists all Account Managers that are potential report recipients. The Access to Reports enabled field lists all Account Managers that will receive the reports. To add or remove from the recipient list, highlight the Account Manager (CTRL Click to select multiple Account Managers), and then click the appropriate arrow to move.

- **E-mail Recipients**
  SafeNet Authentication Service can send the report by email to addresses in the recipients list. Use this option to send reports to people that are not Account Managers and therefore cannot log into the management UI to view and download reports. To add recipients, enter their email address then click the Add button. To remove recipients, highlight their email address then click the Remove button.

- **Save over FTP**
  If checked and configured (Comms Tab), reports can be automatically generated and delivered to an FTP server.

Click the Finish button to commit the customizations and add the report to the My Reports List module.

My Customized Reports Module

This module lists all of your customized reports. It is from this list that you schedule reports to run.

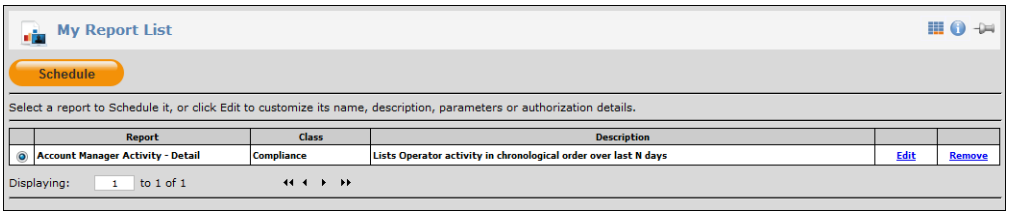


Figure 67: My Reports List Module

To schedule a report, select the report then click the Schedule button.

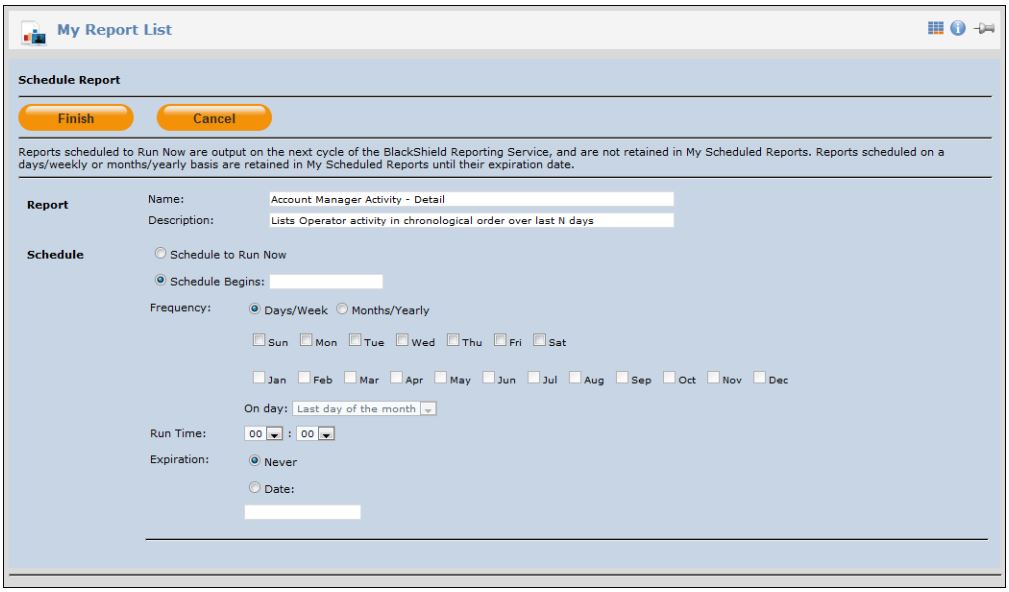


Figure 68: Schedule Report

Schedule Report

The schedule report options are:

- **Run Now**
  The run now option adds the report to the report processing queue. Reports in the queue are run in chronological order.

- **Schedule Begins**
  The report will not run prior to this date.

- **Frequency**
  Reports can be scheduled to run on specific days of the week by selecting the Days/Week option, then selecting the specific days. Alternatively, the report can be scheduled to run on a monthly basis by selecting the Months/Year option, then selecting the specific months. If Months/Year is selected,

the On day option is enabled. Use this option to specify a day in each month that the report should run. Reports will not run after the date specified in Expiration Date. By default report schedules do not expire.

- **Run Time**
  The time at which the report should begin executing.

- **Expiration**
  The date after which the report will be removed from the My Scheduled Reports list.

To commit the report schedule, click the Finish button. This adds the report to the My Scheduled Reports module.

Account Managers with appropriate role permissions can use the Edit hyperlink to modify the report criteria or remove the report from the My Customized Reports list using the Remove hyperlink.

My Scheduled Reports Module

Scheduled reports to which the Account Managers is entitled appear in the My Scheduled Reports module. The list shows the report name, run frequency, run time and expiration date. Clicking the report name hyperlink displays the report criteria. Account Managers can modify a report schedule or run a report “now”. The Run Now option adds the report to the report processing queue. Reports in the queue are run in chronological order. The reporting service checks the queue every 5 minutes and after each report is generated. Run Now reports are processed in order. If no reports are detected, up to 5 minutes may elapse before the service will check the queue for report additions. The Run Now option does not alter the regular report schedule.

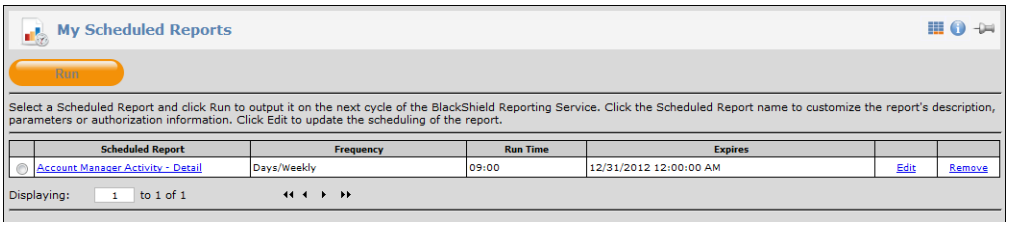


Figure 69: Scheduled Reports List

Account Managers with appropriate role permissions can make changes to the reports schedule by clicking the Edit hyperlink or remove the report from the schedule by clicking the Remove hyperlink.

Reports that are running or have completed are added to the My Report Output module.

My Report Output

All reports that are running or have completed to which the Account Managers is entitled are listed in the Report Output table.

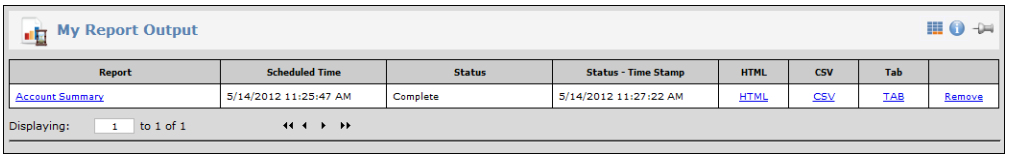


Figure 70: Report Output List

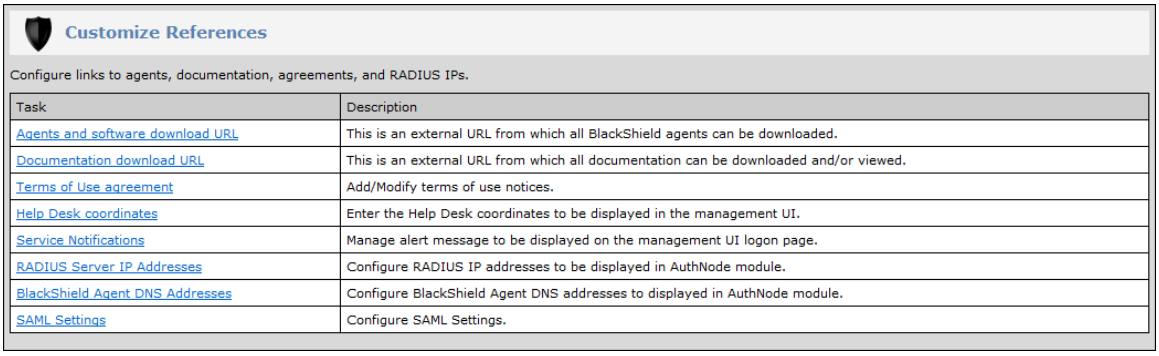
Intended recipients can view their reports in the browser by clicking the report name hyperlink. Alternatively they may be downloaded for local processing by clicking any of the CSV, Tab or HTML hyperlinks. Reports that are no longer required can be deleted from the list by clicking the remove button.

Report hyperlinks are disabled for Account Managers not listed as intended recipients in the report configuration.

Outdated reports will be automatically removed from the My Report Output list after the number of days specified in the Auto Remove Module. Refer to Auto Remove on page 237.

Custom References

This section allows Service Providers to publish information to the References module on the Snapshot tab of each subscriber's virtual server where:



Agents and software download URL

This is the URL to a web page hosted by the Service Provider that contains links to SafeNet Authentication Service Agents and other software that the subscriber may need.

Documentation download URL

This is the URL to a web page hosted by the Service Provider that contains links to administration guides, quick starts and other documentation that the subscriber may need.

Terms of Use Agreement

This is the URL to a web page hosted by the Service Provider that contains links to "terms of use" and related documentation that the subscriber may need.

Help Desk Coordinates

If enabled, a help icon will be displayed in the tab bar of all on-boarded accounts.

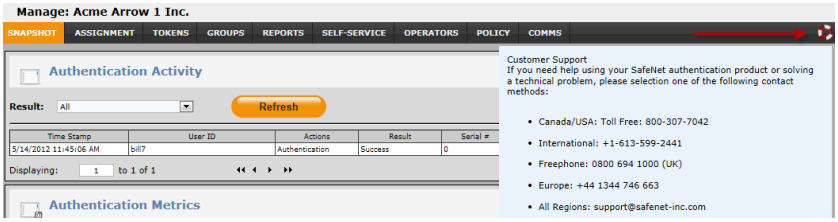


Figure 71: Help Desk Coordinates

Enter your help desk coordinates using HTML tags.

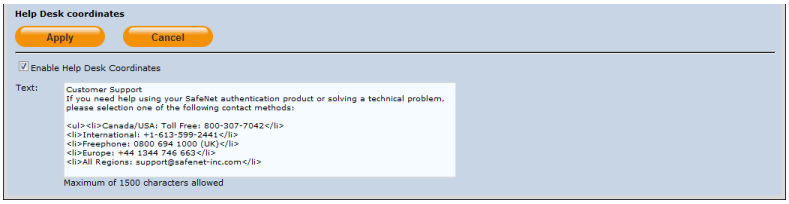


Figure 72: Enabling Help Desk Coordinates

Service Notifications

Use service notifications to alert your subscribers to changes that may affect their service, including upgrade notices. If enabled, an alert icon will be displayed on the logon page. This icon can be customized (refer to Custom Logo Images on page 298). Clicking the icon displays the notification message.

Figure 73: Service Notifications

Notifications can also be sent by email and/or SMS to all Operators. The following is configurable:

- **Default / Custom**
  If default is selected, any service notification published by your service provider will appear on your management UI logon page as well as that of all of your on-boarded accounts. If Custom, then only the service notification you configure will be published to all of your on-boarded accounts.

- **Enable Notification**
  If checked, the notification is published immediately or between the notification start and stop dates if these have been set.

- **Notification Start date**
  Is the first day the notification will be published.

- **Notification Stop date**
  Is the last day the notification will be published.

- **Message Title**
  This is the title of the service notification.

- **Logon page/Email message**
  This is the text presented on clicking the icon on the logon page or delivered by email.

- **SMS Message**
  This is the service notification text sent by SMS. Use the Send Service Event to send notification by Email/SMS.

Enable/disable service notifications by checking/clearing the Enable service notification checkbox respectively.

Click Apply to commit the changes. Click the “Send service event” button to push the notification by email and/or SMS to all Operators in all on-boarded accounts.

RADIUS Server IP Address

This option is only available for on-premise installations. Use this module to publish the IP address and port numbers of the RADIUS server on the AuthNode module in all Subscriber accounts.

SafeNet Authentication Service Agent DNS Address

This option is only available for on-premise installations. Use this module to publish the DNS addresses for all agents configured in Subscriber accounts. This information is published on the AuthNode module in all Subscriber accounts.

SAML Settings

This option is only available for on-premise installations. Use this module to publish the SAML IdP information to the AuthNode Module on all Subscriber accounts.

Account Role Provisioning Rules

Use this function to automatically add an Account Manager and grant access to the management UI based on attributes such as Active Directory group membership. Conversely an Account Manager can be automatically removed if the rule that promoted the user to Account Manager evaluates false.

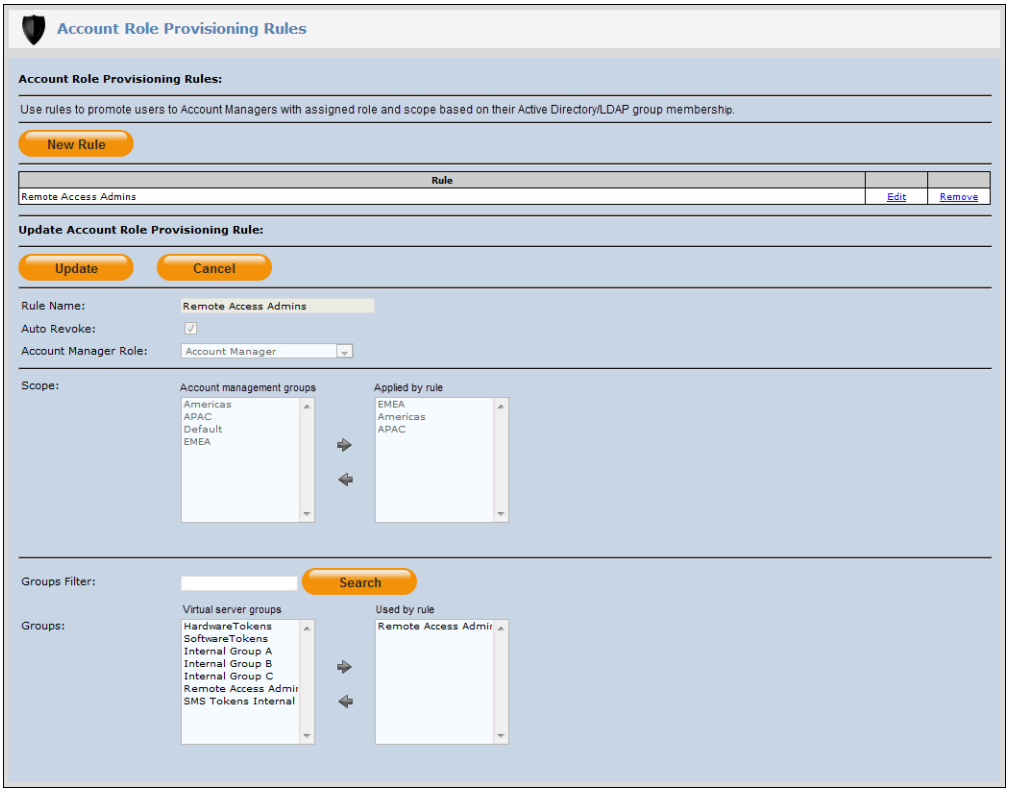


Figure 74: Account Role Provisioning Rules

To add a rule click the New Rule button where:

- **Rule Name**
  This must be a unique name which identifies the rule.

- **Auto Revoke**
  If checked, the Account Manager created by this rule will be automatically removed if the conditions (e.g. group membership) are no longer valid.

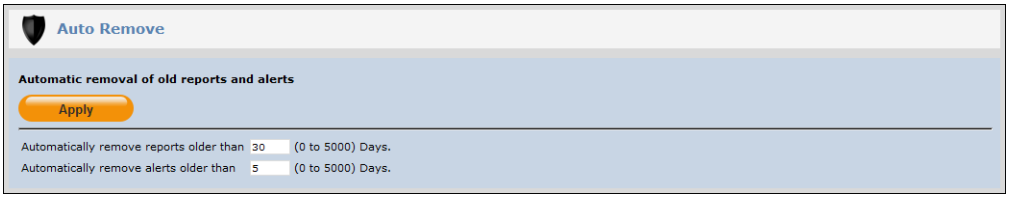
- **Account Manager Role**
  This is the role that will be assigned to the Account Manager. The drop down lists all configured roles.

- **Scope**
  Account management groups list all configured groups. The Account Manager will have access to groups listed in the Applied by Rule window. Use the arrow keys to move highlighted groups between the two windows.

- **Groups Filter**
  The Virtual server groups window lists all groups in the virtual server. Users that are members of one or more of the groups in the Used by rule window will be promoted to Account Manager. Use the arrow keys to move highlighted groups between the two windows.

Auto Remove

Use this module to set the maximum age of competed reports and alerts. Any report or alert older than the configured number of days will be automatically removed from the My Report Output module and Alerts Module. Note that the data itself is not removed and can be accessed through creating or rerunning reports.



To set, enter the number of days in each of the reports and alerts fields, then click Apply.

Virtual Servers Tab

Every On-boarded account has its own Virtual SafeNet Authentication Service Server. It is through the Virtual Servers tab that Account Managers can manage individual Virtual Servers on behalf of, or in cooperation with account Operators.

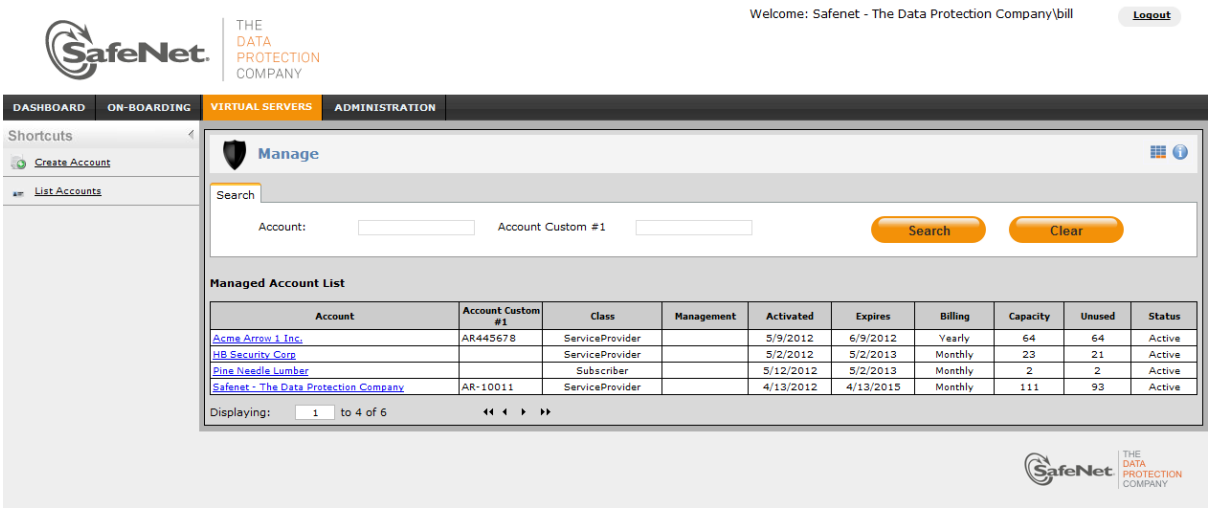


Figure 75: Virtual Servers Tab

This tab lists all of the Virtual Servers that the Account Manager is able to manage, bearing in mind:

- Only accounts within the Account Managers scope will appear on the list.
- Accounts with management delegated to the Service Provider will appear on the Virtual Servers tab but not on the On-boarding tab.
- Where account delegation has occurred, the name of the delegating organization will appear in the Management column.

To begin managing a Virtual Server, click on the Account hyperlink in the managed Virtual Servers list. This will display a second row of tabs which correspond to the functionality available to the Account Manager for the selected Virtual Server.

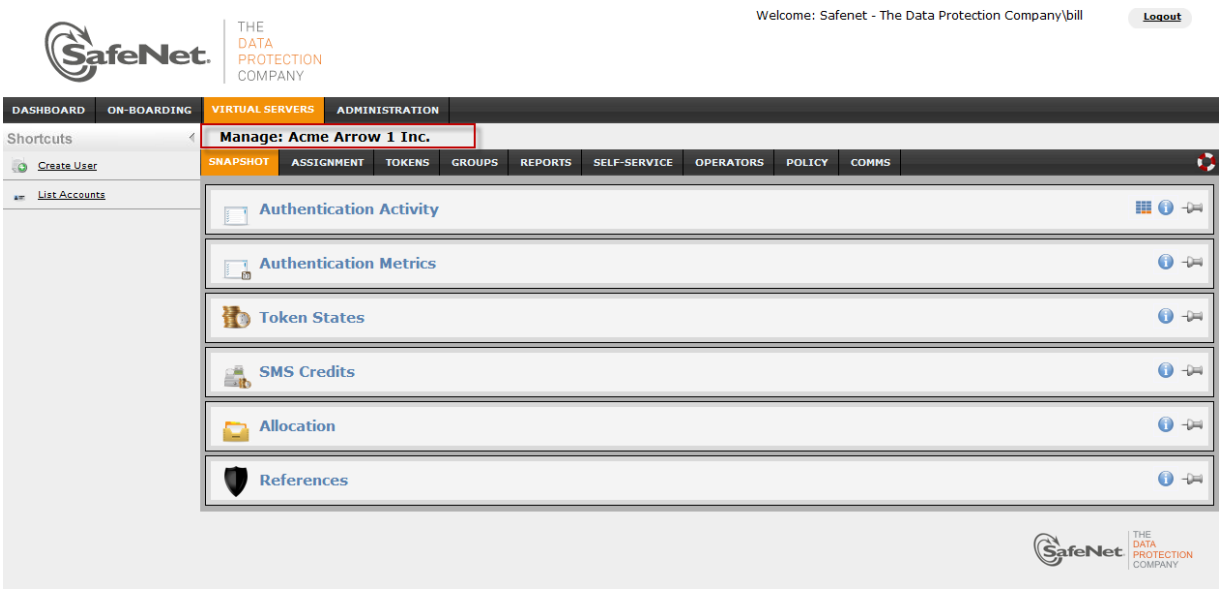


Figure 76: Virtual Server Tabs

Chapter 3

This chapter describes the functionality contained in the Virtual Server tabs. It is through this set of tabs that you will:

- Manage an account's Virtual Server.
- Manage the account's users.
- Provision users with tokens.
- Generate account specific security, compliance, billing and inventory reports.
- Customize provisioning, enrollment, email, SMS and other account specific processes.

Snapshot Tab

This tab provides summary information about the Virtual Server including authentication history, metrics and inventory.

On this tab:

- **Authentication Activity Module**
  Lists up to 100 of the most recent authentications including diagnostic information.
- **Authentication Metrics Module**
  Displays authentication activity metrics over various periods of time.
- **Token States Module**
  Displays all tokens registered in the Virtual Server by state.
- **SMS Credits Module**
  Displays the current SMS credit balance, alert level and SMS sent message count.
- **Allocation Module**
  A complete listing of Virtual Server capacity and token inventory, including detailed transaction records.

Authentication Activity Module

The Authentication Activity module displays a list of the most recent authentications, up to a maximum of 100 records. Opening the module automatically refreshes the list.

Entries in the list can be sorted according to Result:

- **All (default)**
  The list will include all authentication activity.
- **Failure**
  The list will display only failed authentications.
- **Success**
  The list will display only successful authentications.
- **Challenge**
  The list will display authentication events that include a challenge being issued by the server.
- **Server PIN Provided**
  The list will display authentication events where the server has generated a PIN for the user.

- **User PIN Change**
  The list will display authentication events where the user has been prompted to change their PIN.

- **Outer Window Authentication**
  The list will display outer window resynchronization events. (Refer to Synchronization Policy on page 213.)

- **Change Static Password**
  The list will display events where the user was required to change their temporary static password. (Refer to Temporary Password Policy on page 212.)

- **Password Change Failed**
  The list will display events where password change failed.

- **PIN Change Failed**
  The list will display events where user PIN change failed.

Click Refresh to sort the results according to revised criteria, or simply to update the list to include any authentications which occurred since the module was opened.

A count of records shown versus total records found is displayed at the bottom of the list. Click the Customization button on the module bar and enter a new number of Rows in the text field to reset the number of records displayed.

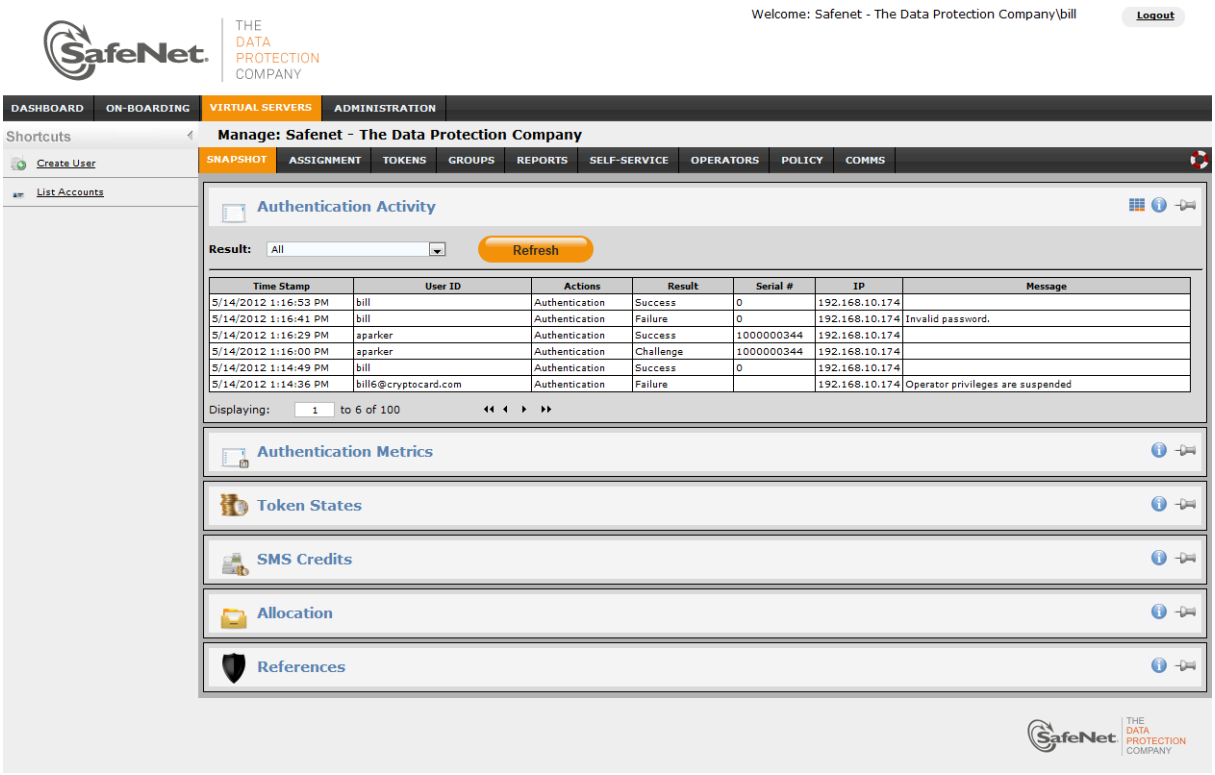


Figure 77: Authentication Activity

In the Authentication Activity Module:

- **Result**
  Use this to filter the authentication activity displayed in the list.
- **Time Stamp**
  This is the time stamp for each authentication event.
- **UserID**
  This is the userID provided by the user attempting to authenticate.
- **Actions**
  This is the action performed during the authentication.
- **Result**
  Possible values are:
  - Challenge: the user was provided with an 8 digit challenge – typically because the user's token is configured for challenge-response operation.

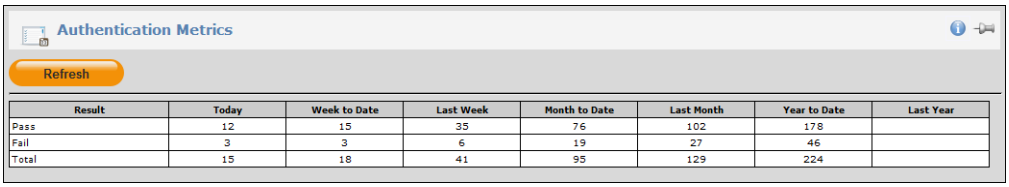
- Outer Window: the user provided a correct OTP value but one that was outside of the “Inner Window”. Outer window success indicates that the user provided the next expected OTP.
- PIN Change: indicates a user PIN change operation.
- Success: the Action was successful.
- Failure: the Action failed.

- **Serial Number**
  This displays the serial number of the token used to successfully authenticate. If the value is 0 and authentication succeeded, this indicates the use of a static password to authenticate.

- **IP**
  This is the IP address of the authentication request. Depending upon configuration, this could be the user’s, access point (e.g. VPN gateway) or agent (e.g. OWA) IP address.

Authentication Metrics Module

This module displays a list of Pass, Fail and Total Authentications over various periods of time:



Result	Today	Week to Date	Last Week	Month to Date	Last Month	Year to Date	Last Year
Pass	12	15	35	76	102	178	
Fail	3	3	6	19	27	46	
Total	15	18	41	95	129	224	

Figure 78: Authentication Metrics

- **Today**
  Lists values for the current day from 00:00:01 , to the time at which the module was opened or most recently refreshed.

- **Week to Date**
  Lists values from 00:00:01 on Monday of the current week, to the time the module was opened or most recently refreshed.

- **Last Week**
  Lists values from 00:00:01 on Monday to 24:00:00 on Sunday of the previous week.

- **Month to Date**
  Lists values from 00:00:01 on the 1st day of the current month, to the time the module was opened or most recently refreshed.

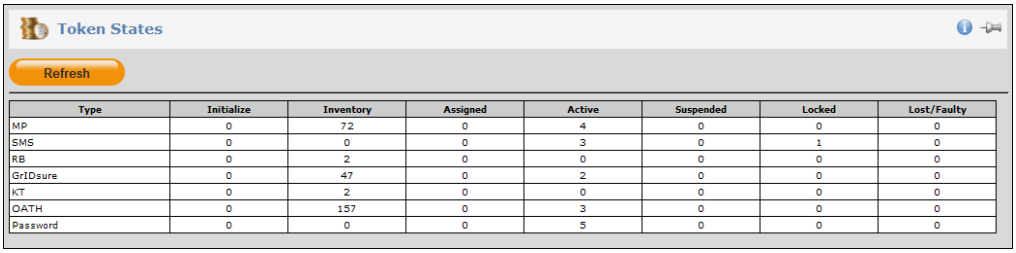
- **Last Month**
  Lists values from 00:00:01 on the 1st day, to 24:00:00 on the last day of the previous month.

- **Year to Date**
  Lists values from 00:00:01 on January 1 of the current year, to the time the module was opened or most recently refreshed.

- **Last Year**
  Lists values from 00:00:01 on January 1 to 24:00:00 on December 31 of the previous year.

Token States Module

The token states module provides a count of all token types in the Accounts inventory by state:



Type	Initialize	Inventory	Assigned	Active	Suspended	Locked	Lost/Faulty
MP	0	72	0	4	0	0	0
SMS	0	0	0	3	0	1	0
RB	0	2	0	0	0	0	0
GrIDsure	0	47	0	2	0	0	0
KT	0	2	0	0	0	0	0
OATH	0	157	0	3	0	0	0
Password	0	0	0	5	0	0	0

Figure 79: Token States

- **Initialize**
  Tokens that must be reinitialized before they can be assigned or provisioned.

- **Inventory**
  Tokens that are available for assignment or provisioning.

- **Assigned**
  Tokens that are assigned to a user but not yet used to authenticate.

- **Active**
  Tokens that are assigned to users and have been used to authenticate.

- **Suspended**
  Tokens that have been suspended by an Operator, preventing their use for authentication by the user to whom they are assigned.

- **Locked**
  Tokens that are in a locked state as a result of excessive consecutive failed authentication attempts.

- **Lost/Faulty**
  Tokens that have been marked as lost or faulty by an Operator.

SMS Credits Module

The SMS Credits module displays the current SMS Credits Balance, the low Balance Alert Level and the total SMS Messages Sent by this Account where:

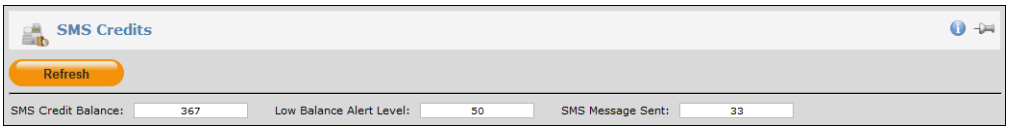


Figure 80: SMS Credits Module

- The SMS Credit Balance is decremented each time an SMS message is sent.
- The SMS Messages Sent value is incremented each time an SMS message is sent.
- The messages sent count resets to zero on the 1 millionth message sent.
- An alert is generated when the SMS Credit Balance equals the Low Balance Alert Level.

Allocation Module

The Allocation module summarizes server inventory. The Transaction Log, displays a detailed list of all allocations and de-allocations related to an account.

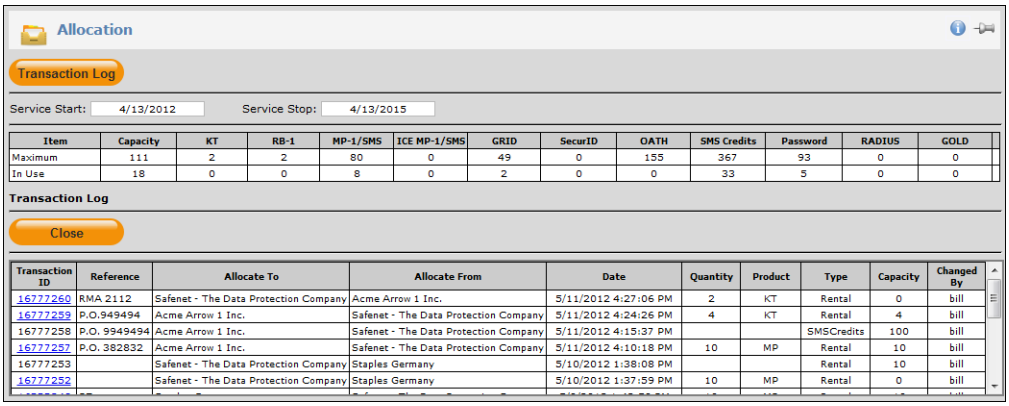


Figure 81: Allocation Transaction Module

In the Allocation table:

- **Maximum**
  This lists the maximum number of users that can authenticate against the server[1]. Users may have multiple tokens and the total number of tokens issued to users may exceed server capacity. In all cases these values are decremented as capacity and tokens/authentication methods are consumed. Note that some authentication methods consume the same resource. For example, all tokens consume a unit of capacity when assigned to a user. Likewise, MP-1/SMS, GrID and Password consume a token license, therefore every time any one of these token/authentication methods is assigned to a user, totals for each token type in this class are decremented.

[1] Note that prior to v3.2, capacity determined the maximum number of tokens and/or authentication methods that could be assigned to users.

- **In Use**
  This lists the capacity consumed as well as totals for all token/authentication methods that are in use.

- **Available**
  List capacity and tokens available for assignment to users.

In the Transaction Log:

- **Transaction ID**
  Is a unique number assigned by the server to each allocation by the Service Provider. The Transaction ID is a hyperlink if the transaction includes tokens. Clicking the hyperlink displays a list of all tokens by serial number included in the transaction.

- **Reference**
  This is a value entered by the Service Provider when allocating the token, generally to aid in identifying the transaction when communicating with the account. This value may have meaning only to the Service Provider.

- **Allocate to**
  This is the account which received the inventory allocation. For example, when a service provider allocates inventory, the value in this field will be the name of the account that received the inventory. Conversely during deallocation inventory is returned to the service provider and therefore the service provider name will appear in this field.

- **Allocated From**
  This is the account that allocated the inventory. The values in this field are the opposite of “Allocate to”.

- **Date**
  This is the date and time of the allocation.

- **Quantity**
  This indicates the item quantity of the transaction, usually tokens or SMS credits.

- **Product**
  This indicates the primary item in the transaction. If the transaction contains tokens, this will display the token family such as KT, RB etc. A transaction cannot contain more than one token type.

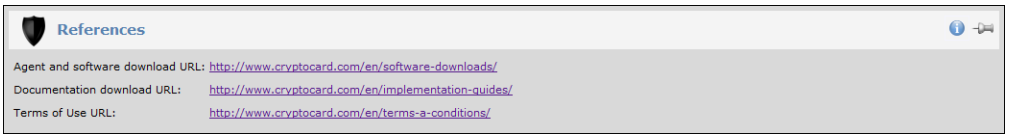
- **Type**
  This indicates Rental or Sale. Rental indicates that the allocation of tokens/authentication methods is part of a subscription, incurring a periodic charge for usage. Sale indicates that tokens/authentication methods have been purchased.

- **Capacity**
  This indicates the quantity of capacity included in the transaction. Note that capacity is always a rental transaction even when included in a transaction with tokens marked as Sale.

- **Changed by**
  This is the name of the Account Manager that performed the allocation.

References Module

The references module lists URLs from which agents, software, documentation and terms of use can be downloaded or viewed. The values in this module are configured by the Service Provider. Refer to Custom References on page 86. These values are automatically inherited by all on-boarded accounts. All virtual service providers can modify these values for their child accounts.



Assignment Tab

It is from this tab that all users, their authentication methods, authentication metrics, access restrictions, group memberships and individual RADIUS attributes are managed.

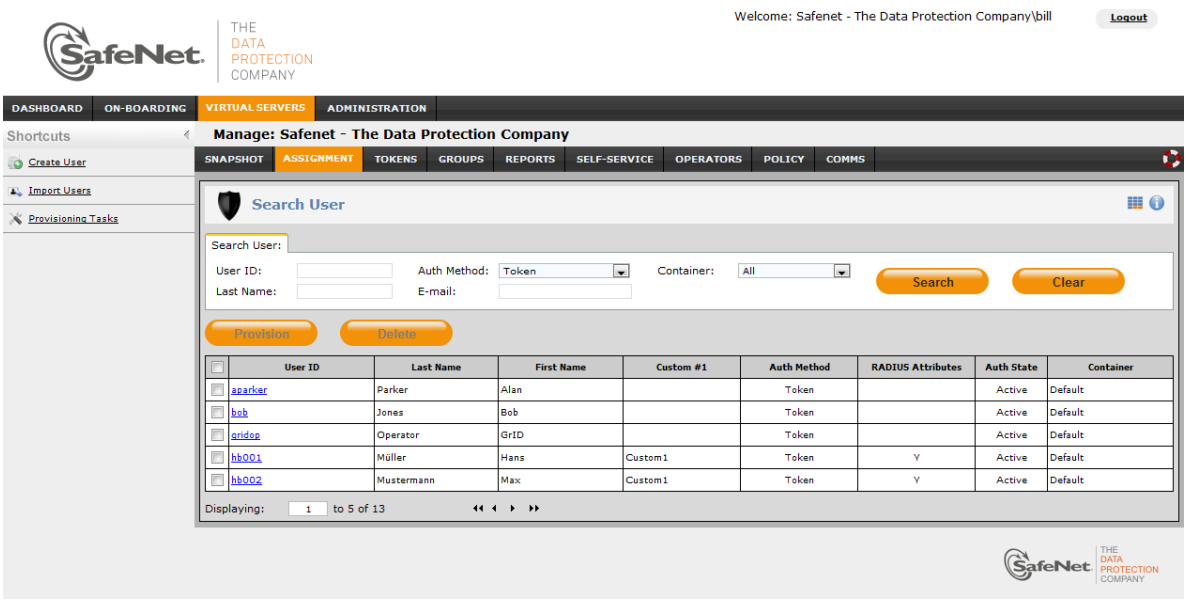


Figure 82: Assignment Tab with User List

On this tab:

- **Create User Shortcut**
  Use this shortcut to manually add users.

- **Import User Shortcut**
  Use this shortcut to import one or more users from .csv or tab delimited flat file.

- **Provisioning Tasks Shortcut**
  Use this to manage active tasks such as removing users from the task or extending the tasks “time-to-live”.

- **Search User Module**
  Provides several ways to find and list users.

- **Users List**
  Use the functions in the list to manage individual users and their tokens, or to perform bulk provisioning of tokens to one or more users in a single operation.

- **Provision Button**
  Use this function to provision all selected users in the list with tokens in one simple operation. (Refer to Provision on page 115)

- **Delete Button**
  Use this function to delete all selected users (excluding LDAP integrated and LDAP synchronized).

- In the list (Figure 83: User List):

- **User ID**
  All user management functions are accessed by clicking the User ID hyperlink.

- **Last Name**
  The user's surname.

- **First Name**
  The user's first name.

- **Custom #1**
  One of three fields that can be populated with custom data to distinguish the user from other similarly named users. Examples include employee number, department etc. Note that the label "Custom #1" can be changed in the Branding Module of the virtual server.

- **Auth Method**
  An indication of the primary authentication method assigned to the user. Options include PwD (Password stored with the user account in the Virtual Server), Token (indicates a two-factor authentication method is assigned).

- **Attributes**
  Indicates whether or not RADIUS attributes have been set for the user. This does not reflect RADIUS attributes applied to a group to which the user may belong.

- **Auth State**
  Set to Active if the user can authenticate against the service. Set to Locked if authentication failures exceed the Account Lockout/Unlock Policy (refer to Account Lockout / Unlock Policy on page 204). Set to Assigned if the user has not authenticated with the assigned token. If multiple tokens are associated with the user, state precedence in the list is Locked, Active, Assigned.

- **Container**
  Indicates the container in which the user account resides. (Refer to Containers on page 141.)

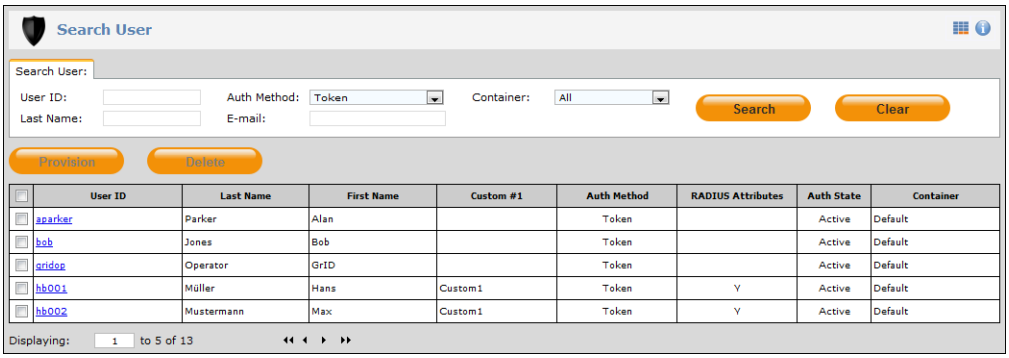


Figure 83: User List

To list user accounts in the Virtual Server, click the Search button in the User Detail module. The list displays a row for each user.

The list of users can be refined by using any combination of:

- **UserID**
  This is normally the value the user will enter to identify themselves when logging into a protected resource such as a VPN. Use * as a wildcard.

- **Last Name**
  The surname of the User. Use * as a wildcard.

- **Auth Method**
  Use this option to select users that have a specific authentication method assigned to them. Options are:

  - **Any**
    Any authentication method.

  - **Token**
    Only users with tokens.

  - **Password**
    Only users with static password set in the authentication server.

  - **External Credentials**
    Only users allowed to authenticate with a credential not validated by the server, such as pass-through to an LDAP server. Note that this option applies only with LDAP integration. It does not apply for LDAP synchronization.

- **Container**
  Find users that are in a specific container.

Clicking the UserID hyperlink in the Users List displays all of the management tasks that can be performed for the selected user, organized in modules where:

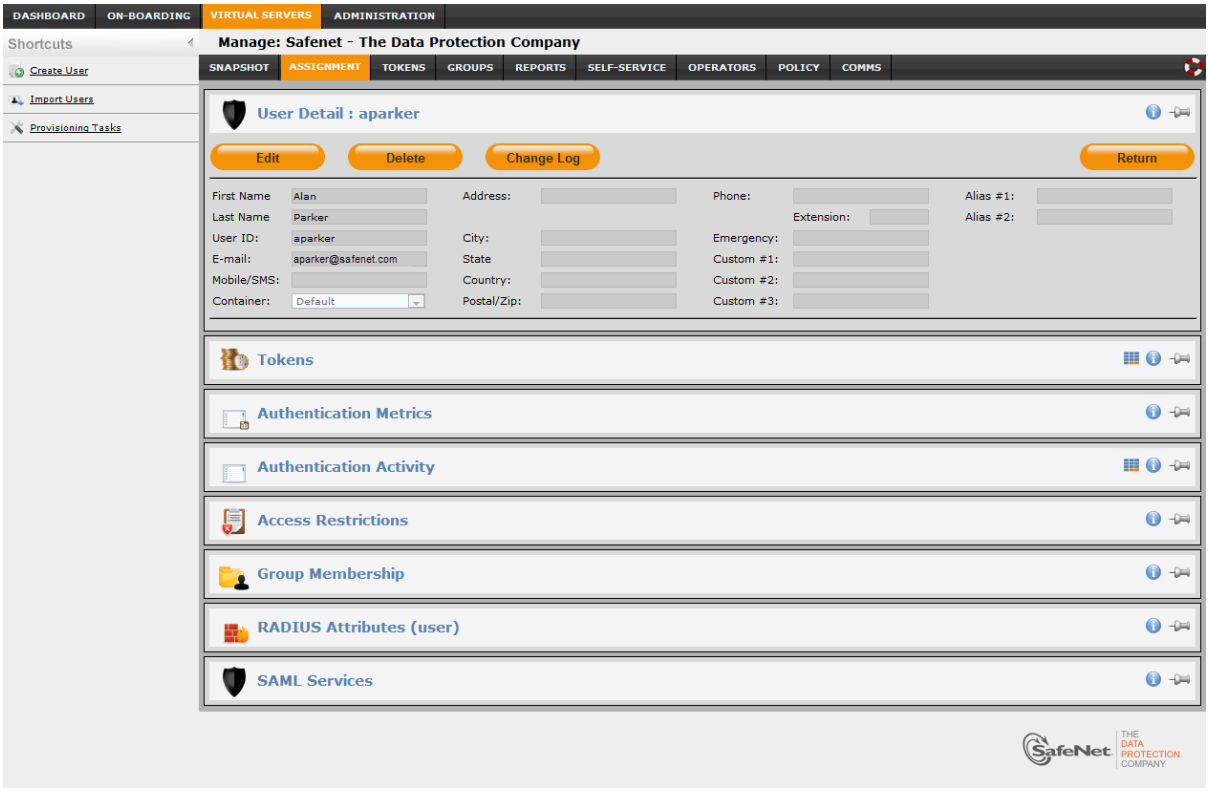


Figure 84: User Management

- **User Detail Module**
  This module displays basic user information. User detail can be modified for all users that were manually created or imported. User accounts created by LDAP integration / synchronization must be modified in the LDAP directory.

- **Tokens Module**
  Use this module to assign, provision and manage all tokens associated with an individual user.

- **Authentication Metrics Module**
  Displays the individual user's authentication metrics over various periods of time.

- **Authentication Activity Module**
  Displays authentication history for up to 100 of the user's most recent authentication.

- **Access Restrictions Module**
  Use this to set specific times/days and periods during which the user is allowed to authenticate or conversely prevent a user from being authenticated.

- **Group Membership Module**
  Use this module to add or remove group memberships for the selected user. Groups can be used to automate provisioning and/or determine the user is allowed to authenticate and/or be granted access to specific resources.

- **RADIUS Attributes Module**
  Use this module to apply RADIUS attributes to the selected user.

- **SAML Services**
  Use this module to manual enable a user to authenticate at one or more configured SAML Service Providers. Service Providers must be configured before this module can be used. Refer to SAML Service Providers Module on page 288.

Creating Users

There are four ways to create users:

1. Manually, one user at a time using the Create User shortcut.
2. Manually, importing one or more user records from a flat file.
3. Automatically by synchronizing with your Active Directory / LDAP server (SAS, SPE Only).
4. Automatically by integrating with your Active Directory / LDAP server (SAS-CPE Only).

You can add users to the Virtual Server using both manual and automated methods, provided that UserIDs are unique. This allows you to extend authenticating to users that exist in your LDAP directory such as employees, as well as users that do not, such as contractors or business partners.

- Consider using Automated Provisioning if you are using automated user creation in conjunction with an external LDAP/AD user source. Automated Provisioning can save administration time by automatically provisioning users with tokens, revoking tokens when users are deleted and applying authorizations based on LDAP groups and much more. (Refer to Provisioning Rules on page 233).

Create User Shortcut

Click the Create User shortcut to manually create a user record. Clicking the shortcut opens the Create User wizard.

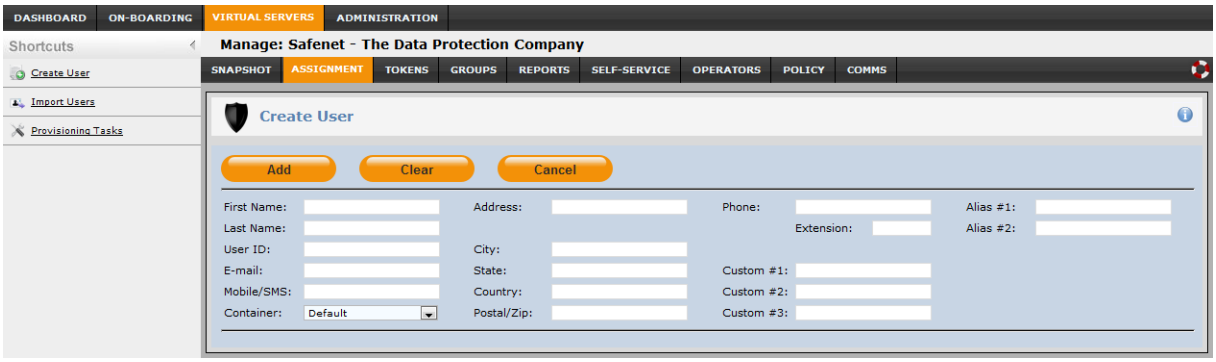


Figure 85: Create User

The minimum requirement for adding a user is First Name, Last Name, User ID and email address. The Add button is disabled until these fields are populated. When the four required fields have been completed, clicking Add creates the record and opens the User Detail page (refer to Figure 84: User Management on page 105).

- **UserID**
  Must be unique. If an identical UserID already exists, an error message is displayed.

- **E-mail**
  Address is required. It is used in provisioning and self-enrollment.

- **Mobile/SMS**
  This field is required to provision the user with the SMS/OTP authentication method and should contain the SMS number of recipient's mobile device. The number must always begin with the country code, bearing in mind that all characters other than digits are automatically stripped.

  For example:
  In North America the entry +1-613-599-2441 after stripping out non-numeric characters would result in a message delivery to: 16135992441 where 1 is the country code, 613 is the area code and the remaining 7 digits the phone number.

  In the UK the entry 44 870 111 2222 would result in an entry in the format: 4408701112222 where 44 is the country code, 870 the city code and the remaining digits the phone number.

- **Container**
  Use this option to place the user in a container.

- **Phone**
  This is an optional field which may contain spaces, periods (.), dashes (-) and plus signs (+) in addition to digits.

- **Custom #1, Custom #2 and Custom #3**
  These are optional fields that can be used to store additional data related to the user. The Custom

#1 field is displayed in the User list. Note that the “Custom #x” labels can be changed from the Branding Module, Custom labels section.

- **Alias #1, #2**
  Aliases can be used to create additional Pseudo-UserIDs for a user, allowing the user to logon using their UserID or aliases and any of the tokens assigned to the user. A common application of aliases would be for a person with 2 domain UserIDs and 2 roles. For example Bob and bob-sysadmin, the former being a standard user account, the latter being an account with elevated privileges. In this example, either ID can use the same token.

Import Users Shortcut

Bulk import of users is a convenient way to add many users in a single operation. To import users, begin by clicking the Import Users shortcut.

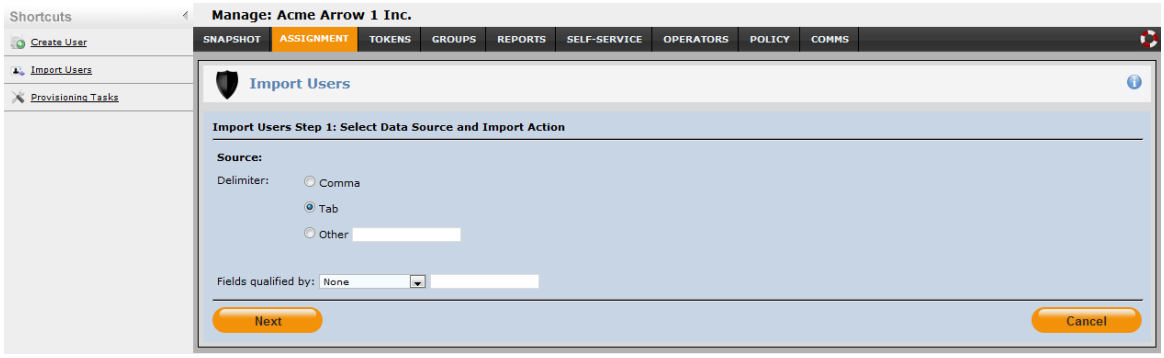


Figure 86: Import Users Wizard - Step 1

Select the import file format and field qualifiers (if any), and then click Next. Browse to and select the user data import file. Clear the “File has a header row” option if the import file does not include a header row, and then click Next.

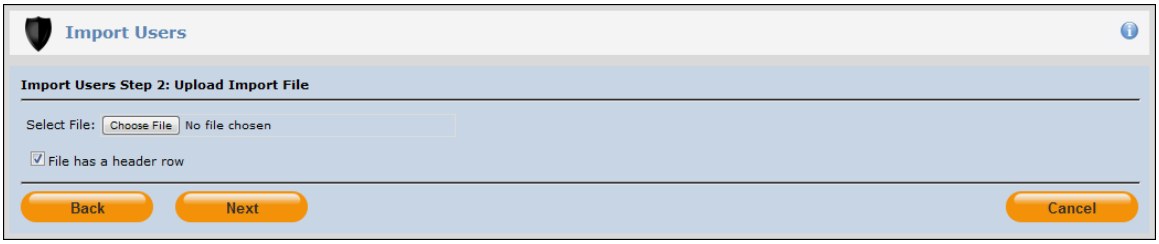


Figure 87: Import Users Wizard - Step 2

In the Confirm Field Mappings and Import pane, select the appropriate Database Field for each Import Data field. There are 4 required Database fields in the Confirm Field Mappings and Import pane (FirstName, LastName, UserID and E-mail), each marked by an asterisk (*). UserID * entries must be unique.

Optionally, use Add Field and select the appropriate unused field name from the dropdown list to add further rows. Add field can be used to force data not contained in the import file into the database. Default values can be created for any added fields.

Data entered into any of the Default Value fields will be used to populate user records that do not have data in the corresponding import file field.

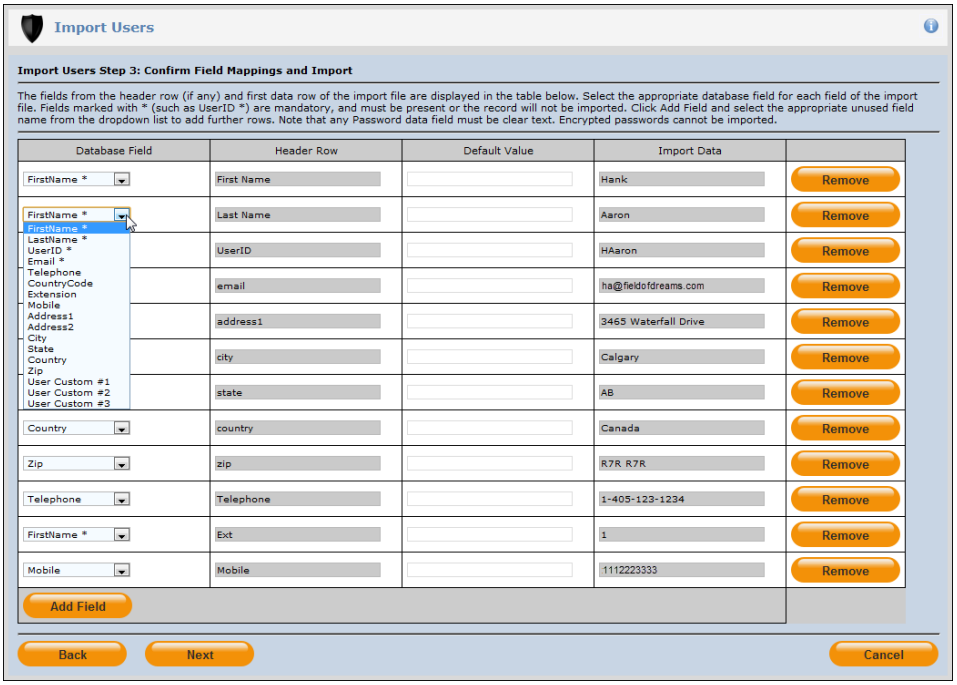


Figure 88: Import Users Wizard - Step 3

Select the container into which users should be imported. The “Do not import if the UserID exists in the database” prevents a user record from being imported if it already exists in the database.

The “Update user record if the UserID exists in the database” will overwrite fields in the database with data from corresponding fields in the import file if a matching UserID is found in the database. Note that populated fields in the database will not be overwritten if a corresponding field is not included in the import file.

Click Import to complete the process. When import is finished the server will display the result of the import, showing users that were imported and/or any errors that occurred.

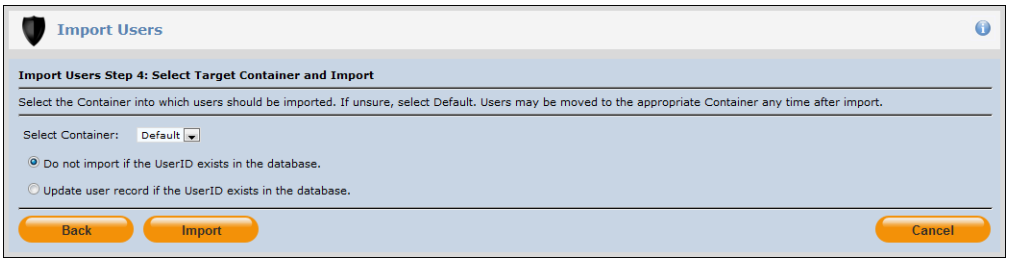


Figure 89: Import Users Wizard – Step 4

LDAP Synchronization

Users can be automatically added, suspended or removed from the account's Virtual Server by utilizing the LDAP Synchronization agent, eliminating the need to manually create and manage users. The agent comes with support for standard Active Directory, eDirectory and SunOne. The agent can be configured to support non-standard schemas.

This method requires the installation of a Synchronization Agent, normally somewhere in the same network as the AD/LDAP directory.

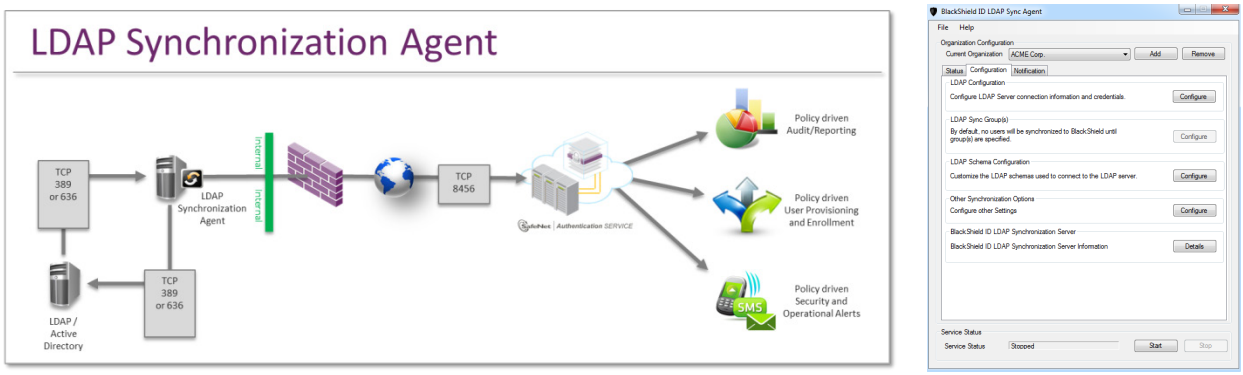


Figure 90: LDAP/AD Synchronization Agent

The Agent is configured to monitor the specified LDAP containers (DNs) and groups for changes such as adding or removing a user, synchronizing and applying these changes at the Virtual Server.

Synchronization can be coupled with other workflow automation policies such as:

- Automatic provisioning of tokens to users (refer to Provisioning Rules on page 233)
- Automatic revocation of tokens from users
- LDAP pre-authentication and authorization

  - Note that SafeNet Authentication Service supports manual creation of users concurrent with LDAP synchronization, bearing in mind that manually created users will not be modified in any way by an LDAP synchronization provided there is no overlap in UserID. If an overlap occurs, any

tokens assigned to the manually created UserID are revoked and marked as lost with a comment, and the UserID is replaced by the overlapping LDAP UserID.

To configure your system for LDAP synchronization, refer to LDAP Module on page 274.

LDAP Integration

Users can be automatically added, suspended or removed from the account's Virtual Server by configuring LDAP integration, eliminating the need to manually create and manage users or use a synchronization agent.

- This option is only available with SafeNet Authentication Service - PCE. SafeNet Authentication Service - SAS subscribers must use the LDAP Synchronization Agent.

With integration, UserIDs, group membership and other LDAP/AD user attributes are validated against the LDAP source for every user lookup and authentication performed in the Virtual Server. Integration supports additional functionality such as chained authentication (LDAP authentication followed by OTP authentication) and static password validation against Active Directory.

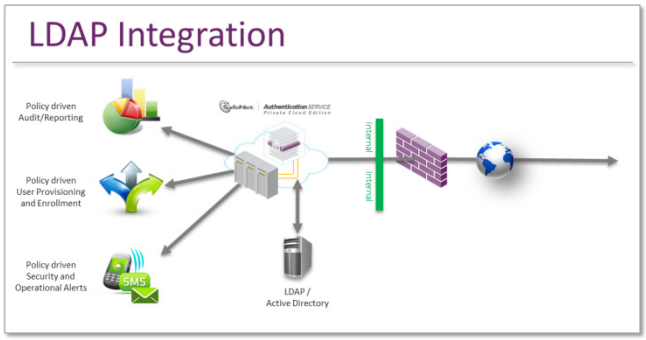


Figure 91: LDAP/AD Integration

In addition to basic user information, synchronization includes the users Active Directory group membership which in turn can be used for:

- Automatic provisioning of tokens to users (refer to Provisioning Rules on page 233)
- Automatic revocation of tokens from users
- LDAP pre-authentication and authorization
- Chained authentication

- Note that for performance reasons LDAP integration is not recommended where the directory server and SafeNet Authentication Service are communicating across the internet. If integration over the internet is required it must be across a high speed, low latency connection with guaranteed availability.

To configure LDAP Integration, refer to LDAP Module on page 274.

User Detail Module

The user detail module displays basic information about a user. If the user account was manually created or imported, the Edit button will be active, allowing the information to be updated. If the user account is synchronized or integrated with LDAP, the edit button will be disabled and required edits to the user account information must be made in LDAP.

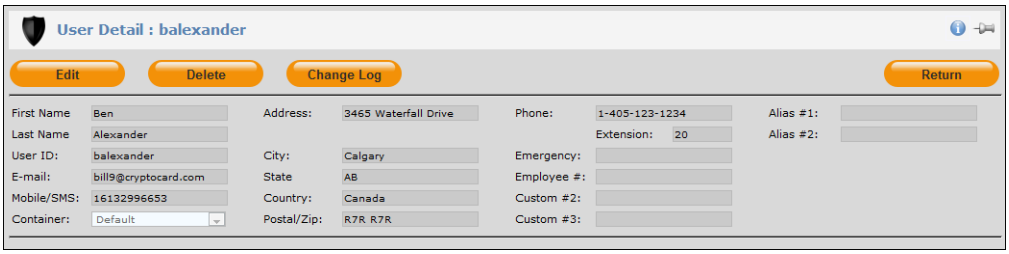


Figure 92: User Detail Module

Container

This is the container in which the user account resides and can be changed by selecting from the dropdown list and applying the change.

Custom #1, 2, 3

These fields are available for holding additional information about the user.

Alias #1, 2

These are alternate logon credentials that can authenticate with the user's tokens.

Tokens Module

The tokens module lists all tokens or authentication methods associated with a user, and provides access to all functions necessary to assign, provision and manage the user's tokens.

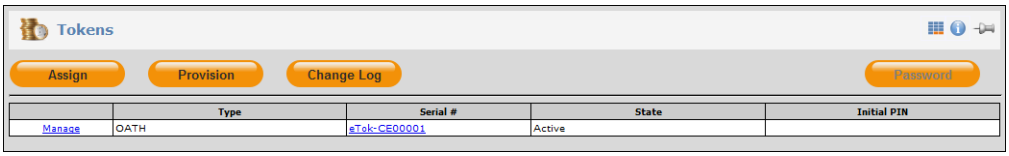


Figure 93: Token Issuing Options

In the tokens module:

- **Assign**
  Use this button to manually assign a token to the user. This is a manual process primarily used when issuing hardware tokens to users, one user at a time and usually where the token can be handed to the user. In most cases Provision should be used instead of Assign.

- **Provision**
  This method is used to issue tokens to 1 or more users in a simple process. Provisioning can be used with any token type (hardware, software, SMS, GrID…), and any number of users. This method works hand-in-hand with Self-enrollment. Provisioning represents major time-savings for administrators and is the recommended method for associating a token with a user.

- **View Log**
  Click the View Log button to view the last 5 token management tasks performed for this user.

- **Password**
  Use this button to assign a temporary static password to a user that does not have an active token.

- There are several ways to issue tokens/authentication methods to users:

- **Auto-Provisioning**
  This method issues tokens to users based on policies such as Group Membership. This method is most often used with LDAP synchronization or LDAP Integration since changes in AD group membership (for example) will cause tokens to be provisioned, revoked or suspended automatically. As with Provisioning, this method works with all token types and Self-enrollment.

- **Assign a Token**
  To assign a token to a user, begin by clicking the Assign button in the Tokens module. Refine the inventory list of tokens available for assignment by selecting from the Token Type dropdown list or entering a partial serial number, and then clicking Search.

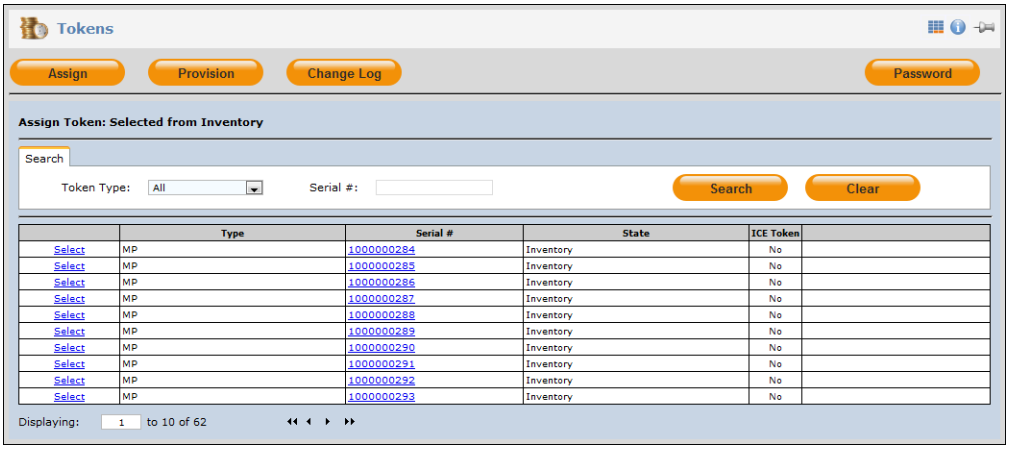


Figure 94: Token Inventory List

Click the Select hyperlink corresponding to the token to be assigned, and then click the Assign button to commit.

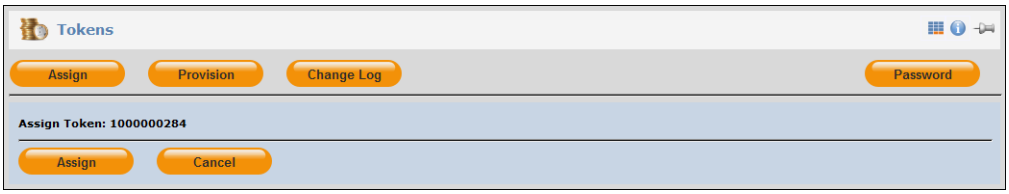


Figure 95: Assign token

The token is now assigned to the user.

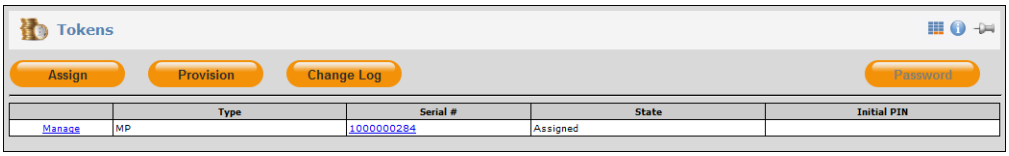


Figure 96: Assigned Token

If this is a hardware token, you should give this to the user now along with the initial PIN shown in the last column of the list. The default policy requires the user to change this PIN on first use of the token to a value known only to them. The value in the Initial PIN field is cleared when the user completes their PIN change.

If this is a software token, you must ensure that the MP-1 application is installed on the user's PC, BlackBerry™, iPhone etc. before proceeding, then:

Click the manage hyperlink, and then click the Issue button.

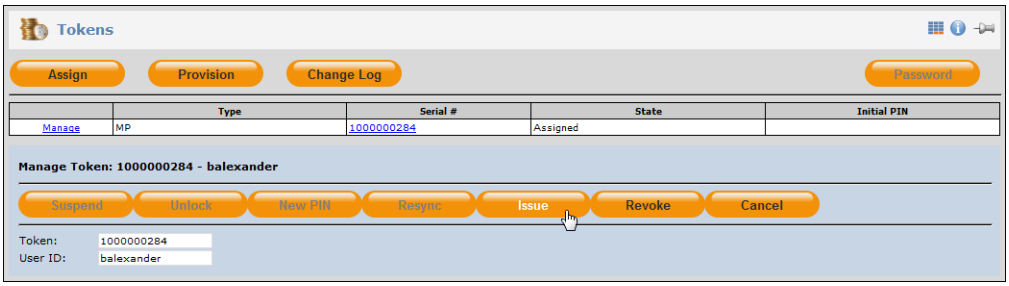


Figure 97: Assigning an MP-1 Software Token

Then choose the delivery method for the token profile.

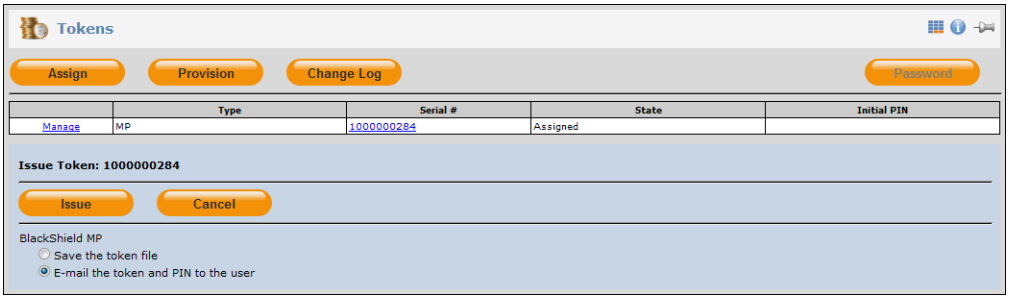


Figure 98: Select Delivery Method

Save the token file

This saves the token profile to a location specified by the Operator. The file must be transferred to the user's device.

E-mail the token and PIN to the user

Choose this option to e-mail the token and initial PIN to the user. Typically this method is used for installation of the MP token on a laptop.

Provision

Provision is used to automate and securely deliver tokens to one or more users regardless of their physical location, in a single bulk operation. This process has significant advantages:

- It saves a tremendous amount of time for Operators.
- It is secure because only the intended recipient can enroll and activate their token.
- It can be used with hardware and software tokens.
- It is not necessary to deliver a specific hardware token to each user.
- It can be time-limited, requiring users to enroll their tokens on or before a specified date.
- It can be used to coordinate migrating users from static passwords to token authentication without interruption of service.

To use the provision function, begin by selecting one or more users from the Users List, and then click the Provision button.

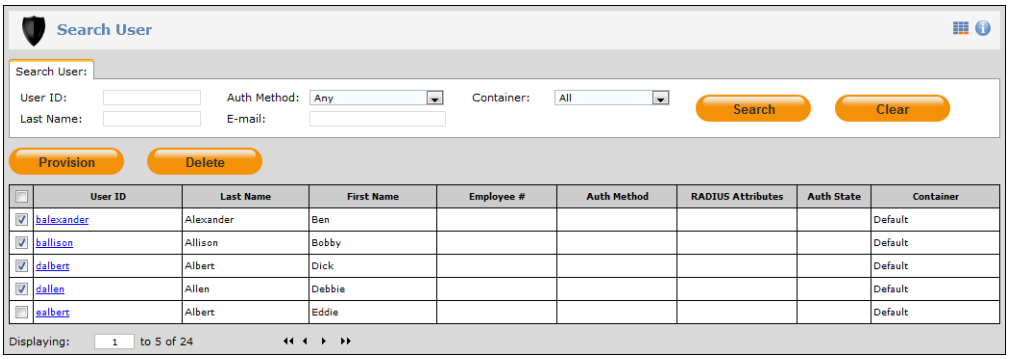


Figure 99: Selecting Users for Provisioning

This will refine the list to include only those users selected for provisioning. Once you've verified the list of selected users, click Provision again. Next, select the type of token to be issued to each of the users in the list. You can add a comment about this provisioning task in the Description field.

- **Available**
  Indicates the quantity tokens by type in inventory and available for provisioning

- **Reserved for Provisioning Tasks**
  Specific tokens (i.e. serial numbers) are not removed from inventory until enrollment is complete. This column represents the amount of inventory that has been committed by other provisioning tasks.

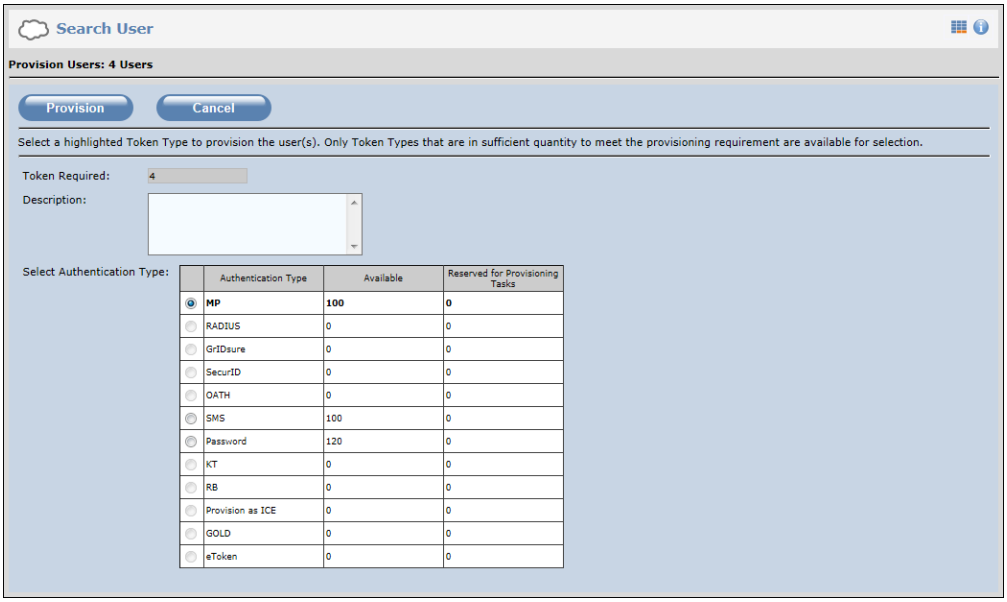


Figure 100: Select Token type to be Provisioned

Click Provision again, and then Confirm to complete the process and create a Provisioning Task.

Self-enrollment

Each user in the provisioning task will receive an email with instructions for enrollment. The content of the email message varies, depending on the token type. Message content can be customized including the use of HTML and images (refer to Custom E-mail Messages on page 244).

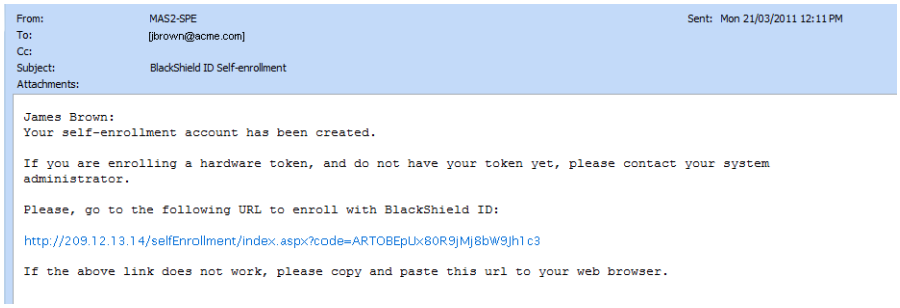


Figure 101: Default MP Token Enrolment Message

Provisioning Tasks

The server creates a Provisioning Task each time the provision function is used. To view or modify a task, click the Provisioning Tasks shortcut.

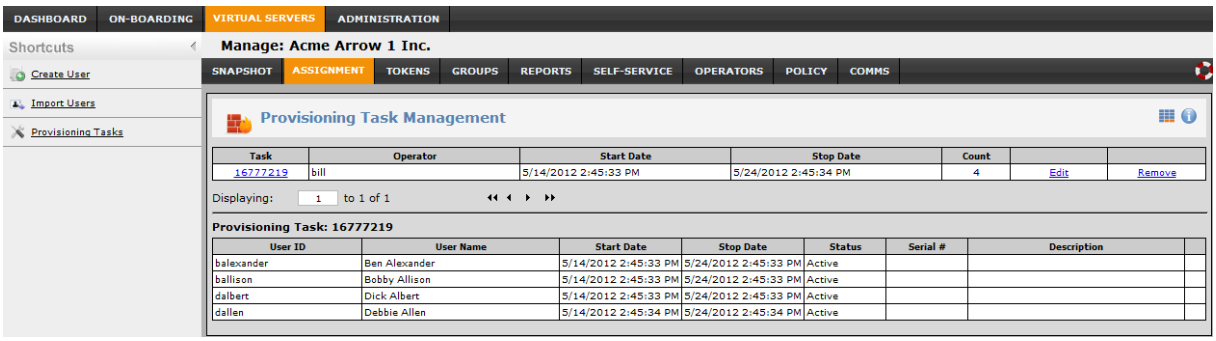


Figure 102: Provisioning Tasks

- **Task #**
  This is a unique number generated by the server for each task. Click this link to view the task details.

- **Operator**
  This is the UserID of the Operator that created the provisioning task.

- **Start Date**
  This is the date the task was created.

- **Stop Date**
  This is the date by which all users must have completed self-enrollment.

- **Count**
  This is the number of users included in the provisioning task.

- **Edit**
  Use this hyperlink to modify the task for one or more users included in the task.

- **Remove**
  Use this to remove a task from the list. Once a task is removed, any users in the task that have not completed enrollment will no longer be able to self-enroll.

- **Status**
  Indicates the status of each user's enrollment:

- **Active**
  User may still enroll the token.

- **Completed**
  User has enrolled their token and used it to authenticate at least one time.

- **Locked**
  User attempted and failed to enroll token within the maximum allowed attempts.

- **Expired**
  User did not enroll token before the stop date.

- **Serial Number**
  The serial number of the enrolled token.

Editing a Provisioning Task

To change a task, begin by clicking the corresponding Edit hyperlink.

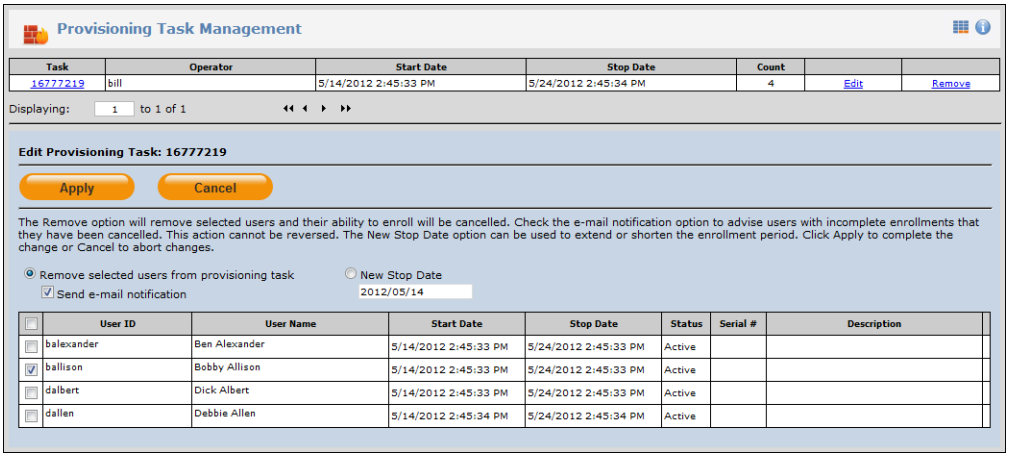


Figure 103: Editing a Provisioning Task

The Remove option will remove selected users from the task, and their ability to enroll will be cancelled. Check the e-mail notification option to advise users that their enrollment has been cancelled. This action cannot be reversed.

The New Stop Date option can be used to extend or shorten the enrollment period. Click Apply to complete the change or Cancel to abort changes.

- **View Log**
  Click the View Log button to view the last 5 token management tasks performed for this user.

- **Password**
  Use this button to assign a temporary static password to a user that does not have an active token.

Managing a User's Tokens

Use the Tokens module to:

- Add a token to a user.

- Provision a token to a user.
- Assign a temporary static password to a user.

Manage all tokens associated with a user.

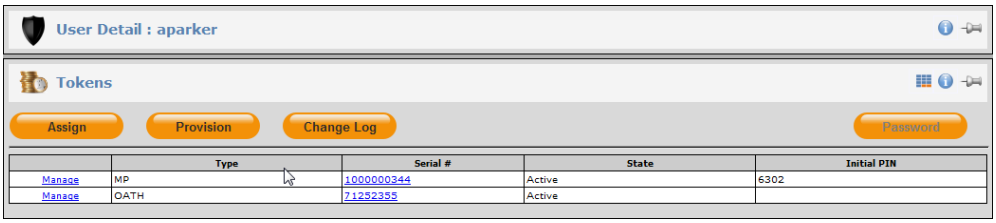


Figure 104: Tokens Module

The tokens module lists all tokens associated with a user where:

- **Manage**
  This hyperlink provides access to all management functions for the corresponding token.
- **Type**
  Displays the authentication method assigned to the user.
- **Serial #**
  Displays the serial number of the token or the word “Password” if a static password is allowed.
- **State**
  This is the state of the token / authentication method where:
- **Active**
  This method can be used to authenticate.
- **Suspended**
  The authentication method is associated with the user but has been suspended by an Operator, preventing it from being used to authenticate until the method is reactivated by an Operator.
- **Locked**
  Indicates that the user has exceeded the maximum number of consecutive failed logon attempts. The token will remain locked until the unlock policy is triggered or an Operator reactivates the token.
- **Assigned**
  Indicates that the token has been assigned to the user but has not yet been used to authenticate.
- **Initial PIN**
  This is the initial PIN value to be given to the user when using “Assign” to issue a token. By default the initial PIN value must be changed by the user during their first authentication. The initial PIN

value displayed in this field is cleared from the display as soon as the user completes the PIN change.

Note that the Password button is disabled if the user has any other assigned authentication methods.

Managing a Token

To manage a user's token, begin by clicking the Manage hyperlink for the corresponding token.

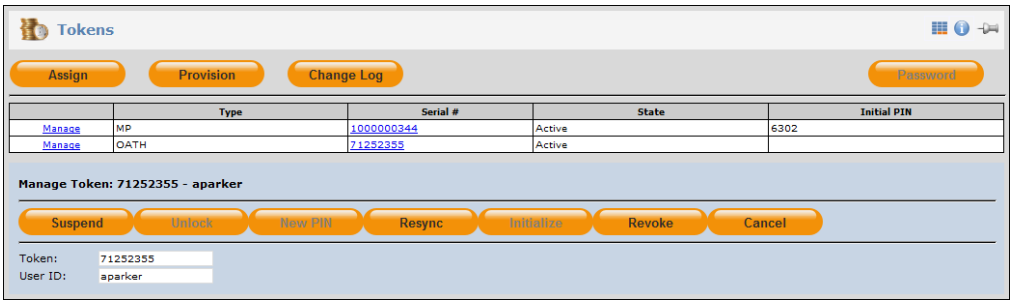


Figure 105: Managing a User's Token

Suspend

Use this option to suspend the token, making it invalid for authentication but leaving it assigned to the user. This button is disabled if the token is not in the Active state.

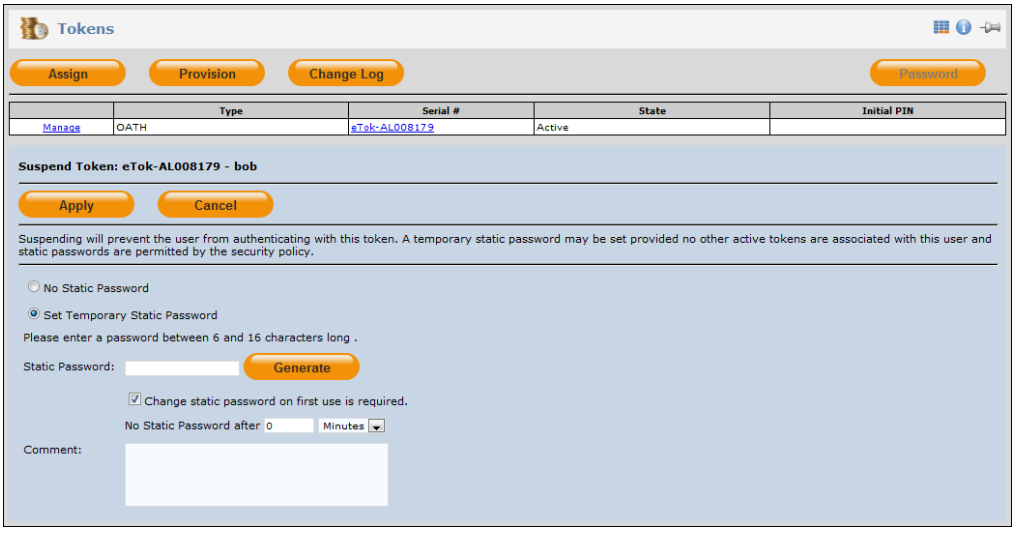


Figure 106: Suspending a Token

If a user has multiple active tokens, the various password options will not be available. If the user has only one active token and the virtual server temporary password policy allows assignment of a password, (refer to Temporary Password Policy on page 212) the following options may be available when suspending a user's token:

No Static Password
The user's token will be suspended and the user will not be given a temporary static password.

Accept LDAP Password
The user's token will be suspended and the user will be allowed to use their LDAP password to authenticate. Note that this option requires LDAP integration.

Set Temporary Static Password
The user's token will be suspended and the user will be given a temporary static password which can be used to authenticate:

Generate button
Use this to generate a static password that complies with the established policy (refer to Temporary Password Policy on page 212)

Change static password on first use option
If checked, the user must change the provided static password to a new value known only to them and which complies with the established policy.

No Static Password after
Use this option to limit the life of the temporary password.

Comment
Use this area to enter a brief explanation for suspending the token. This forms part of the permanent token record and can be viewed by other Operators managing this user's account.

Unlock

Use this option to reactivate a token that is in the locked state, making it valid for authentication. Its use varies depending on the PIN mode:

If the token is locked due to excessive consecutive failed authentication attempts, clicking Unlock will reactivate the token. Check the Set a New PIN option to create a new PIN for the user for this token or use the Random button to generate a PIN that complies with the policy (refer to Server-side PIN Policy on page 210).

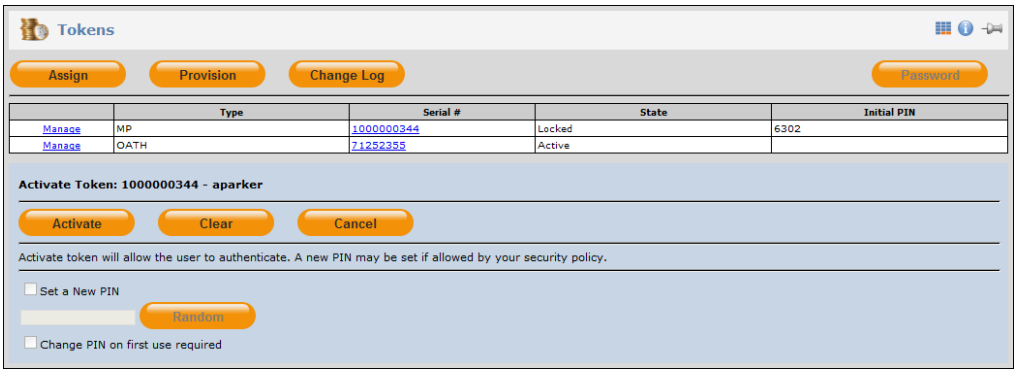


Figure 107: Unlocking a Token

A token initialized with a token-side PIN which has been locked by the user by exceeding the maximum allowed PIN attempts may be unlocked using this function, provided the token was initialized with the unlock token option enabled. (Refer to Token Templates on page 205). This function should only be used if you are certain that the person in possession of the token is the rightful owner.

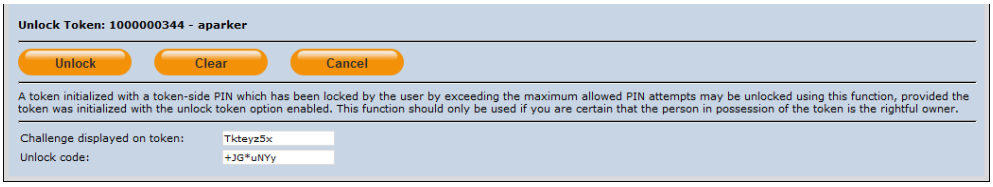


Figure 108: Unlocking with Token-side PIN

To use this function the user must generate an unlock challenge. The method for doing this varies with token type. Refer to SafeNet Authentication Service – Tokens Guide). Enter this value into the Challenge displayed on token field, and then click Unlock to display an unlock code. Give this to the user to enter into their token. If correctly entered, the user will be required to generate a new PIN, after which the token can be used to authenticate.

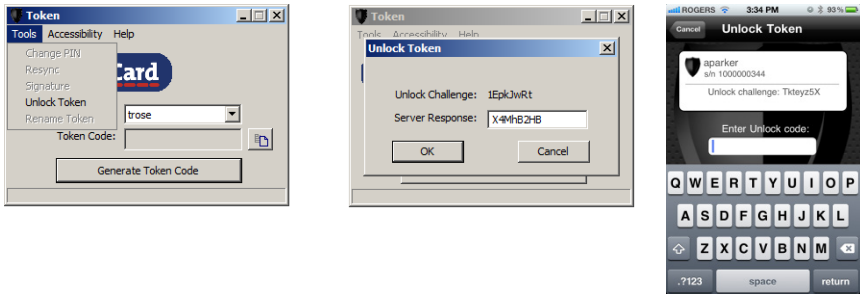


Figure 109: Unlocking Token Example

New PIN

This option is available where the PIN is evaluated by the Server (Server-side PIN). This function sets a new PIN value for this token according to the configured PIN policy (refer to Server-side PIN Policy on

page 210). Use the Generate button to automatically create a new PIN that meets the minimum policy requirements.

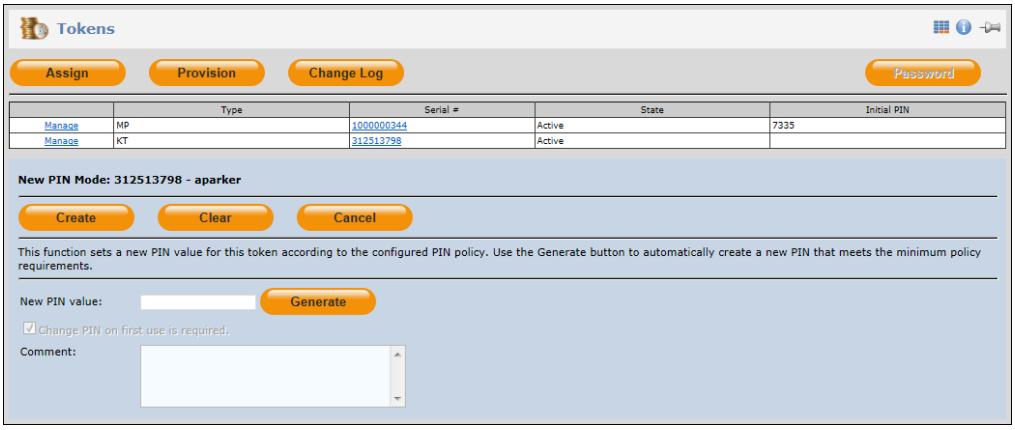


Figure 110: New PIN

The Change PIN on first use option is disabled if the change PIN policy is set to prevent Operator override. If enabled, the Operator can remove the requirement to change PIN on first use. Refer to Server-side PIN Policy on page 210.

Resync

Use this option to resync a token or test the token if there are repeated failed authentication attempts with this token. Generally resync is not required. Resync does not require the user or Operator to reveal the PIN associated with a token.

The resync methods vary depending on the type of token.

- For Challenge/Response resynchronization
  Have the user key the Challenge into their token after enabling resync to generate a Response. Enter the resulting response into the Response field, and then click Resync. The response provided by the user's token for the displayed challenge should result in a successful test. If so, the token is working properly and in sync with the server. (Refer to SafeNet Authentication Service Tokens Guide)

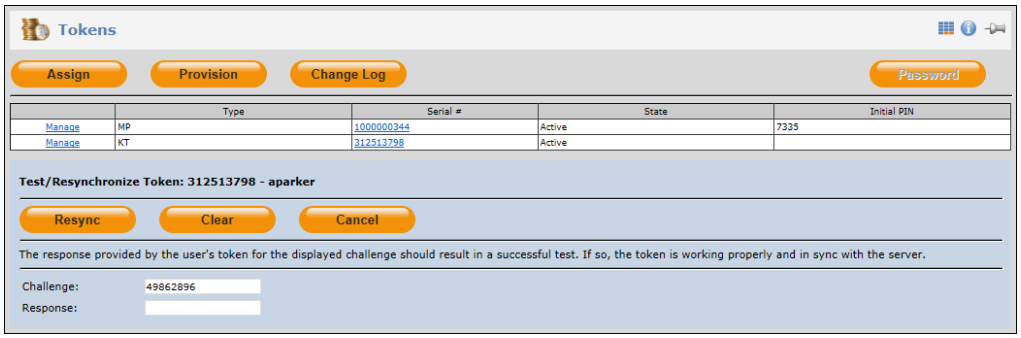


Figure 111: Challenge/Response Token Resync

- For OATH, Safenet Gold/Platinum tokens
  Have the user generate 2 passcodes and enter these in the correct order. A message will be displayed confirming the success or failure of the resync process.

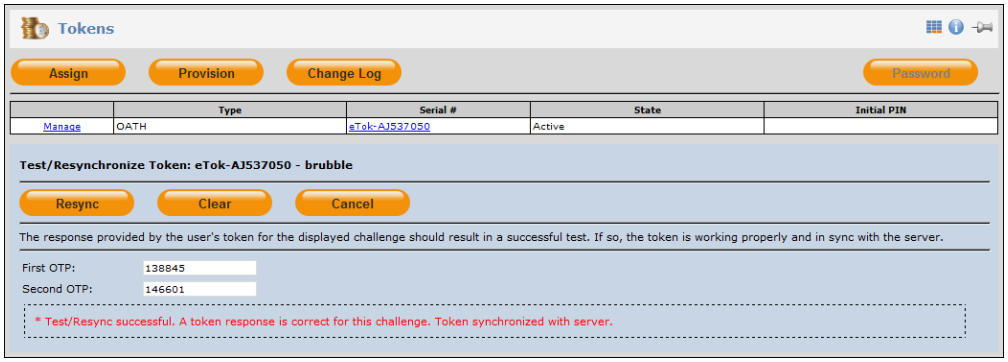


Figure 112: OATH Token Resync

Initialize

Use initialize to generate new token seeds and change the operating parameters of hardware tokens. The current token template (refer to Token Templates on page 205) is applied during initialization. The appropriate token initializer must be connected to the PC. This button is available only if a hardware token is selected.

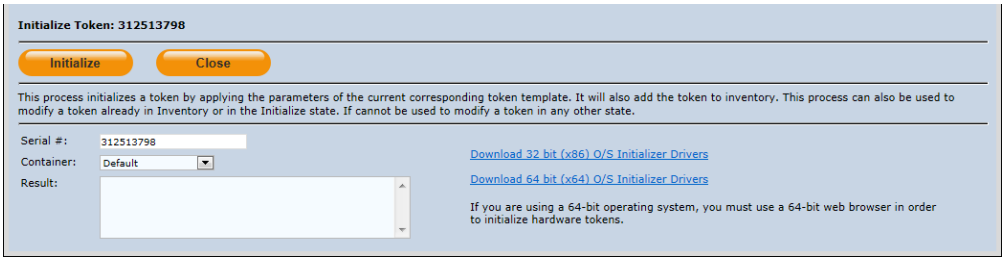


Figure 113: Initialize Token

Issue

Use this button to create an MP-1 token profile (token seed and operating parameters) in conjunction with the “Assign” function.

Revoke

Use this button to revoke a token. A revoked token can no longer be used to authenticate. If the Revoke Password option is not selected, the user can still authenticate using a previously assigned static password. The user can also authenticate with any other active token associated with their account.

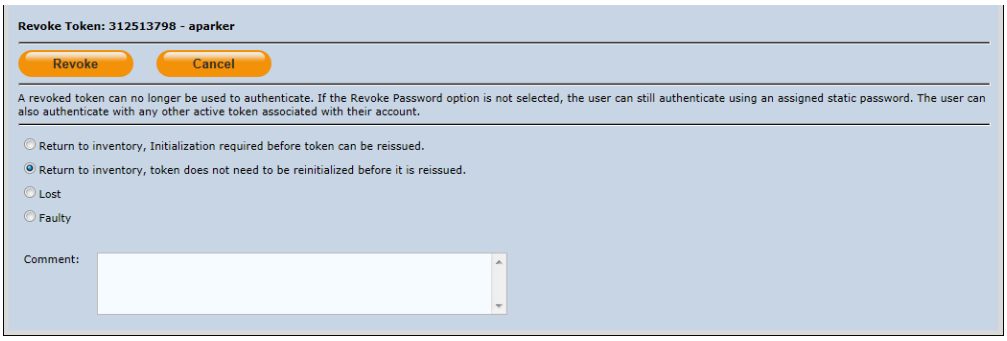


Figure 114: Revoke Token

Return to Inventory, Initialization Required

Choose this option for hardware tokens issued with a token-side PIN or if the token seed and operating parameters must be changed before the token is reissued. Generally this option is used with RB-1 PIN Pad tokens.

Return to Inventory, token does not need to be reinitialized

Choose this option for all other cases where the token is being returned.

Lost

Returns the token to Inventory in the Lost state. Tokens in this state cannot be reissued unless they are recovered and reinitialized.

Faulty

Returns the token to Inventory in the Faulty state. Tokens in this state cannot be reissued unless they are successfully reinitialized.

Authentication Metrics Module

This module displays authentication metrics for the user reflecting pass, fail and total authentication results for the current day, current week, previous week, month to date, previous month, year to date and previous year.

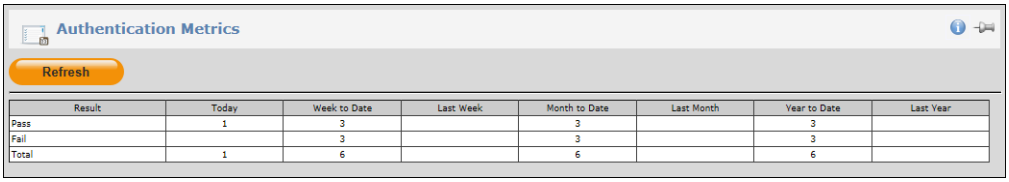


Figure 115: Authentication Metrics Module

Authentication Activity Module

This module is identical to the Authentication Activity Module on the Snapshot tab (refer to Authentication Activity Module on page 94) with the exception that all data is for the selected user.

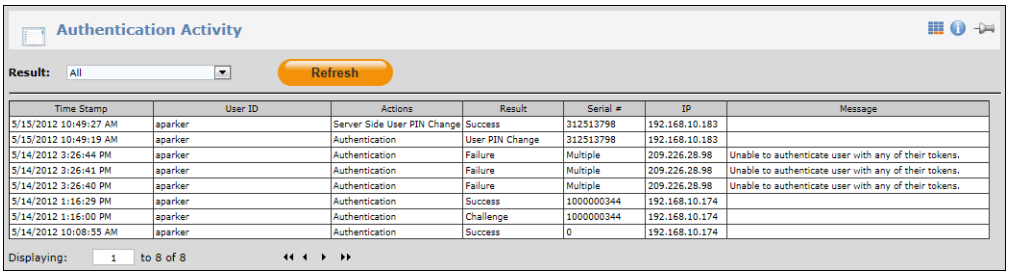


Figure 116: Authentication Activity Module

Access Restrictions Module

Use this module to set time/day/date restrictions on when a user may authenticate. By default restrictions are disabled.

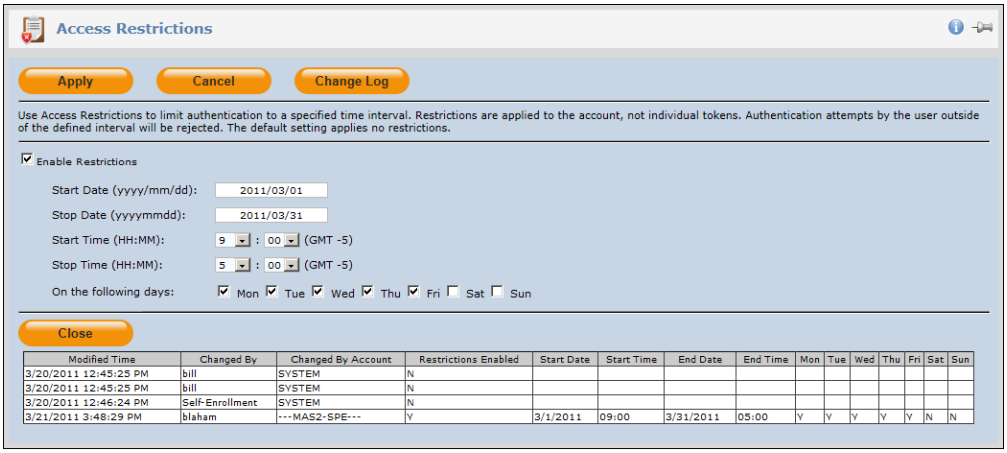


Figure 117: Access Restrictions Module

Options are:

- **Start Date**
  The user cannot authenticate prior to this date.
- **Stop Date**
  The user cannot authenticate after this date.
- **Start Time**
  The user cannot authenticate prior to this time of day.
- **Stop Time**
  The user cannot authenticate after this time of day.
- **On the following days**
  The user can authenticate only on the checked days.

Use the Apply button to commit changes to access restrictions. Use the Change log button to view up to the last 5 changes made to this user's access restrictions where:

- **Modified Time**
  Is the time and date stamp of the applied change.
- **Change By**
  Displays the UserID of the Operator that applied the change.
- **Change by Account**
  Displays the name of the account that applied the change.

Consider using Active Directory time/day/date restrictions if the Virtual Server is configured for LDAP integration. Changes to restrictions in Active Directory will automatically be applied by the authentication server.

Group Membership Module

Use this module to manage the user's group memberships. Groups can be used for auto-provisioning and for authorization (RADIUS attributes and/or Pre-authentication rules). Click the Add button, select the group membership then click apply. To remove a membership, click the corresponding Remove hyperlink and confirm the action.

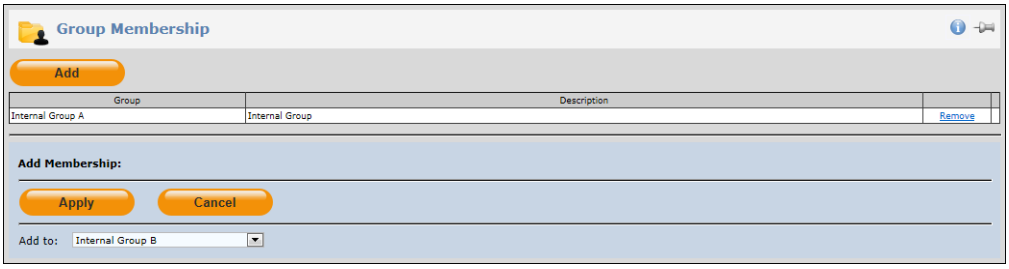


Figure 118: Group Membership

To modify the memberships of many users at a time, use the Group Membership module on the Groups tab instead.

RADIUS Attributes

Use this module to apply RADIUS attributes to the user. Note that user attributes take precedence over attributes applied to groups to which the user belongs. The functionality of this module is identical to the RADIUS Attributes module on the Groups tab except that changes applied here are applied to the user. (Refer to RADIUS Attribute (Group) Module on page 140).

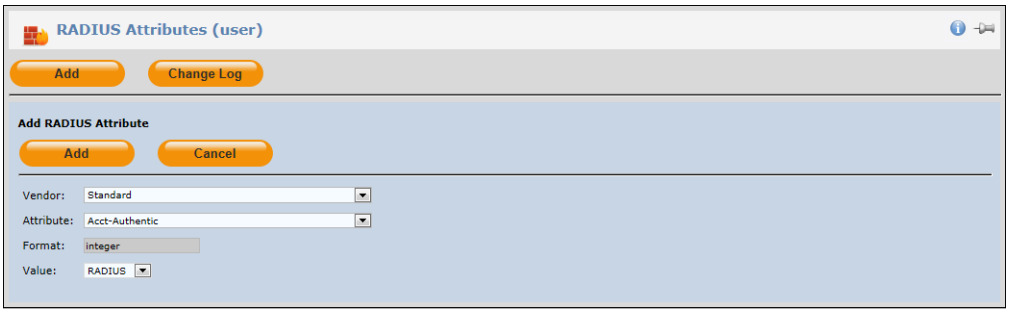
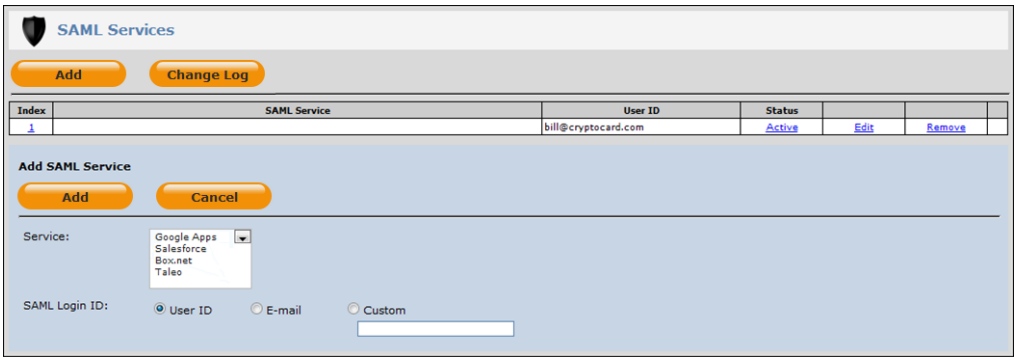


Figure 119: RADIUS Attributes (User)

SAML Services

Use this module to manually enable a user to authenticate against one or more configured SAML Service Providers where:



Service

Lists all of the configured SAML Service Providers (refer to SAML Service Providers Module on page 288)

SAML Login ID

This is the UserID that will be returned to the Service Provider in the SAML assertion on successful authentication. For example, if your service provider (e.g. Salesforce) requires a userID of name@domain.com and this is identical to the user's email address, choose the Email option. Doing so allows the user to consistently use their UserID to authenticate regardless of the Service Providers requirements. In most cases a Service Provider will require either the UserID or Email. For all other cases choose the Custom option and enter the required userID to be returned.

- You can automate the creation/removal of SAML Services for users by creating a SAML provisioning rule. Refer to SAML Provisioning Rules on page 236.

Tokens Tab

On this tab:

- **Tokens Module**
  Use this module to list all tokens registered in the Virtual Server and move tokens between containers.

- **Import SafeNet Tokens**
  Use this module to import token records (.btk files for CRYPTOCard tokens, .dat files for SafeNet tokens). This module is only valid for hardware tokens that have not been allocated and only if they have been purchased and delivered with a .btk / .dat file.

- **Import Third Party Tokens**
  This module is only available to Host Service Providers. Use this module to import RSA/SecurID AES time-based tokens serial number records. This module replaces the Bulk Assign Third Party Tokens module.

- **Bulk Assign Third Party Tokens**
  Use this module to automatically assign a token by serial number to an existing UserID. The tokens must exist in inventory prior to using this module. This module is replaces the Import Third Party Tokens module in Virtual Service Provider and Subscriber accounts.

- **Initialize Token**
  Use this module to initialize one or more hardware tokens into your server or to change the operating parameters of existing hardware tokens, such as OTP length and strength.

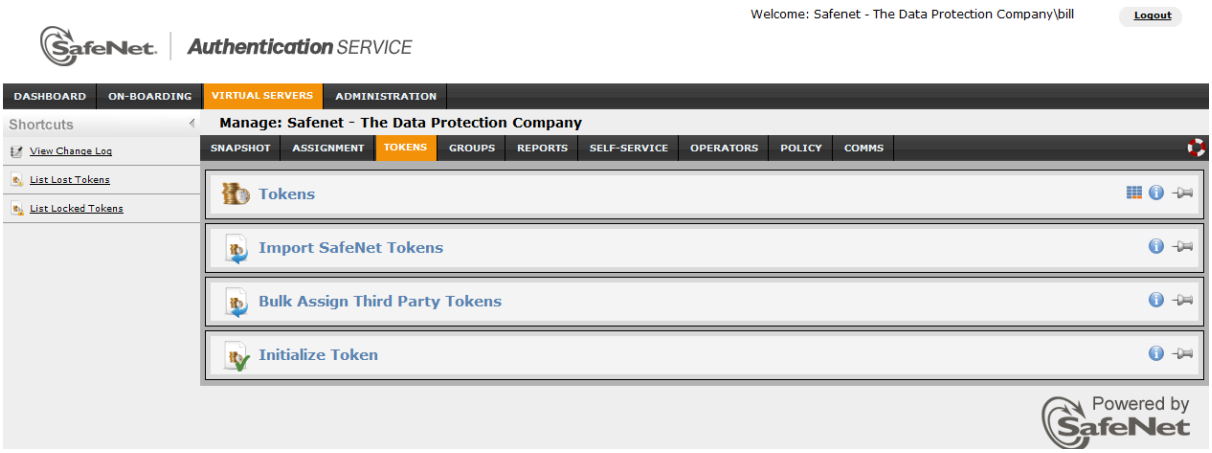


Figure 120: Virtual Server Tokens Tab

Tokens Module

This module is used to list all tokens registered in the Virtual Server.

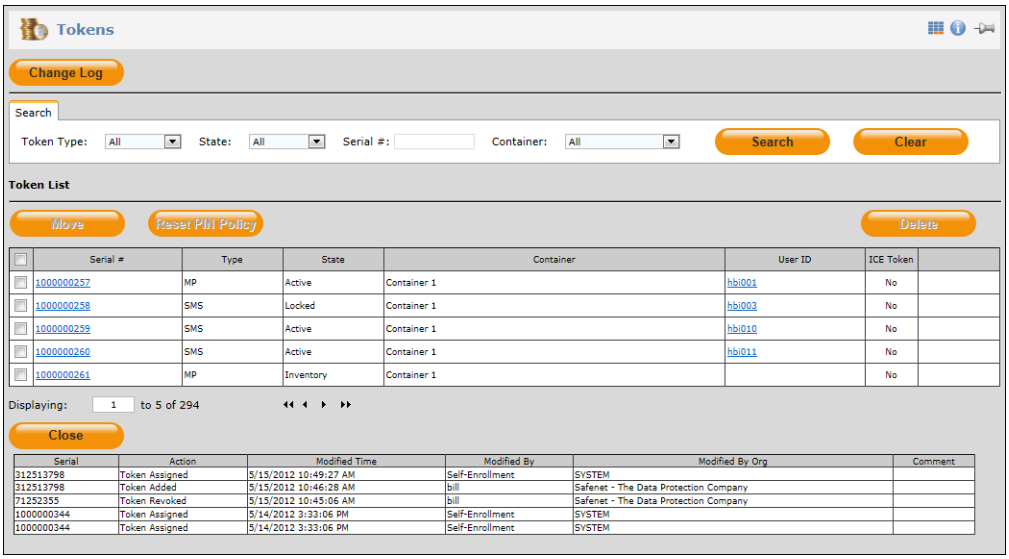


Figure 121: List Tokens

Use the Search button to refresh the list, based on any combination of the following criteria:

- **Token Type**
  This search criterion refines the list to a specific type of token. If All is selected, then all tokens regardless of type are listed.

- **State**
  These criterion refine the list to tokens in a selected state. Options are:

  - **Inventory** – token is available for assignment to users.

  - **Initialize** – a hardware token in inventory that must be initialized before it becomes available for assignment.

  - **Assigned** – the token is no longer in inventory. It has either been manually assigned to a user but not activated or is part of a bulk provisioning operation and has not yet been enrolled by a user.

  - **Active** – the token is assigned to a user and has been enrolled or used to authenticate.

  - **Suspended** – this indicates that an Operator has placed the token in a suspended state, making it invalid for authentication but leaving it assigned to a user. This is usually done if there is a security concern such as a lost or misplaced token. Suspended tokens can be reactivated by an Operator when the security concern has been resolved.

- **Locked** – this state occurs when a user exceeds the maximum consecutive failed logon attempts threshold. A locked token can be reactivated by an Operator. The automatic locking and unlocking of tokens is controlled by the Account Lockout/Unlock Policy.
- **Lost/Failed** – is a state applied by an Operator when revoking a token. Revoked tokens are returned to Inventory in this state where they can be permanently removed or if the token is subsequently found or determined to function properly, it can be reinitialized into the Inventory state.

- **Serial #**
  Search by partial or complete serial number to find a range or specific token.
- **Container**
  Lists only those tokens that are held in the selected container. (refer to Containers on page 141)
- **Change log**
  This displays up to the last five token management operations in the Virtual Server. The log displays a row for each token operation that includes the token serial number, the operation or action, a date/time stamp of the operation, the name of the Operator that performed the action, the organization to which the Operator belongs (i.e. your organization or your Service Provider) and any comment entered by the Operator.

Tokens List

The result of a search is displayed in the tokens list. From this list you can:

- **Move Tokens**
  This option is used to move the selected tokens to a different container.
- **Reset PIN**
  This option is used to apply the current Server-Side PIN policy to the selected range of tokens. Note that this function is not available for tokens initialized with Token-side PINs. Tokens must be in the Inventory state.
- **Delete**
  This function removes the selected token from the Virtual Server Inventory. Note that Delete cannot be used with rented tokens. Rented tokens must be deallocated by the Service Provider.
- **Serial Number** (hyperlink)
  Clicking the serial number hyperlink displays the token operating parameters, in-use statistics and organizational ownership.

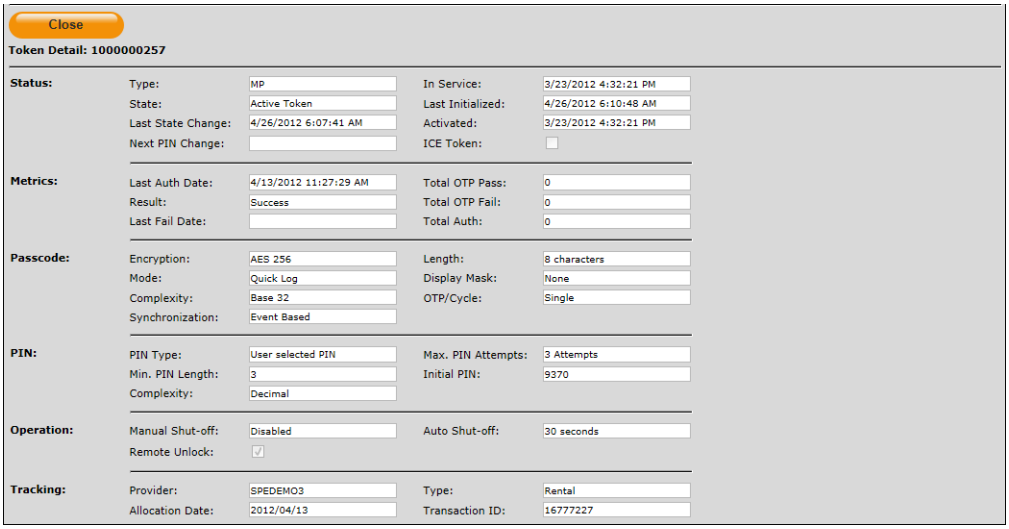


Figure 122: Token Information

- **UserID** (hyperlink)
  Click this hyperlink to access the user's record and management functions. This is the equivalent of selecting the UserID from the Assignment tab.

Import SafeNet Tokens Module

The import tokens module is used to import the seed records for CRYPTOCard and SafeNet tokens. Typically this module is used only if importing CRYPTOCard and SafeNet tokens purchased for use on an in-house SafeNet Authentication Service server that are to be imported and used in the Virtual Server.

To import tokens, browse to the location of the .btk file (CRYPTOCard) or .dat file (SafeNet), select the container into which tokens should be imported, and then click Import.

Note that import will fail for tokens having a serial number that already exists in the Virtual Server. Token seed records can be re-imported after any duplicates are first removed from the Virtual Server inventory.

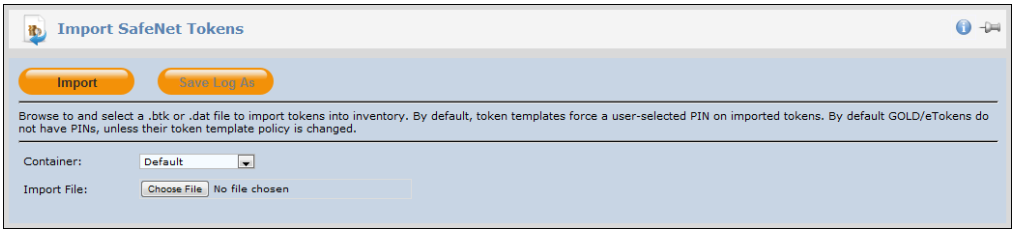


Figure 123: Import CRYPTOCard and SafeNet Tokens

Import Third Party Tokens

This module is available only to the Host Service Provider. This module allows tokens from various manufacturers to be imported and/or managed by SafeNet Authentication Service. Tokens will automatically be bound to an existing UserID in SafeNet Authentication Service if the token import record contains a matching UserID.

If an import record does not contain a UserID, the token will be imported and placed in inventory.

Figure 124: Import 3rd Party Tokens

Options include:

RADIUS Tokens

This import method can be used with any token type provided the 3rd party authentication server will accept authentication requests via RADIUS from SafeNet Authentication Service. To automatically bind a specific token to a user during import:

- Ensure that the UserID already exists in SafeNet Authentication Service.
- Ensure that a record in the import file contains the corresponding UserID and token serial number. Each record in the import file must be in the format:

  UserID,SerialNumber,yyyy/mm/dd

  where Serial Number is 12 characters (pad with leading 0 if necessary)

  If a UserID is omitted in the import record, the token will be imported and placed in inventory. Though the token can be assigned or provisioned to a user in SafeNet Authentication Service, care must be taken to ensure that the same token is assigned to the same user in the 3rd party RADIUS server. Use containers to segregate imported tokens that will be allocated to Subscriber Accounts.

SecurID Tokens

This import method can be used with SecurID tokens, provided the RSA Authentication Manager is configured to accept authentication requests via RADIUS from SafeNet Authentication Service. To automatically bind a specific token to a user during import:

- Ensure that the UserID already exists in SafeNet Authentication Service.
- Ensure that a record in the import file contains the corresponding UserID and token serial number. Each record in the import file must be in the format:

  UserID,SerialNumber,yyyy/mm/dd,#

  where:

  Serial Number is 12 characters (pad with leading 0 if necessary)
  # is the length of the generated passcode. Allowed values are 6 or 8. If omitted, 6 is assumed.

  If a UserID is omitted in the import record, the token will be imported and placed in inventory. Though the token can be assigned or provisioned to a user in SafeNet Authentication Service care must be taken to ensure that the same token is assigned to the same user in the RSA Authentication Manager.

Bulk Assign Third Party Tokens

This module is available to Virtual Service Provider and Subscriber account and allows tokens from various manufacturers to be managed by SafeNet Authentication Service. Tokens will automatically be bound to an existing UserID in SafeNet Authentication Service if the token import record contains a matching UserID.

The token records must be added to your token inventory by your Service Provider. Your Service Provider will require a file containing a record for each token. Refer to RADIUS Tokens on page 134.

If an import record does not contain a UserID, the token will be imported and placed in inventory.

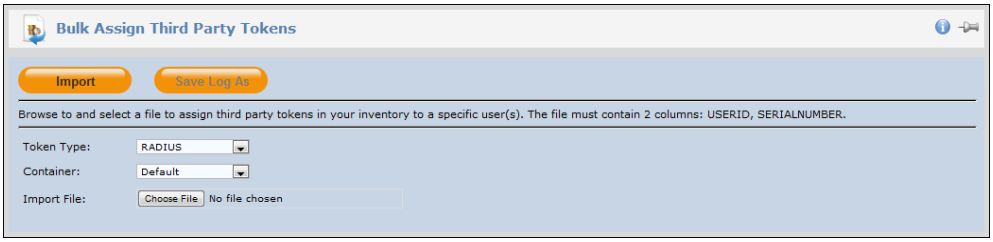


Figure 125: Import Third Party Tokens

Options include:

RADIUS Tokens

This import method can be used with any token type including RSA/SecurID, provided the third party authentication server will accept authentication requests via RADIUS from SafeNet Authentication Service.

Step 1: Provide a Third Party Token Import file to your service provider. This file must be comma delimited file (.csv) and contain a record for each token being imported. Each record must be in the following format:

,SerialNumber,yyyy/mm/dd

Note the leading ","

The Serial Number is 12 characters (pad with leading 0 if necessary)

These tokens will appear in your token inventory when the Service Provider has completed the import process.

Step 2: To automatically bind a specific token to a user during import:

- Ensure that the UserID already exists in SafeNet Authentication Service.
- Ensure that a record in the import file contains the corresponding UserID and token serial number. This file must be comma delimited file (.csv) . Each record in the import file must be in the format:

  UserID,SerialNumber,yyyy/mm/dd

  where Serial Number is 12 characters (pad with leading 0 if necessary)

  If a UserID is omitted in the import record, the token will be imported and placed in inventory. Though the token can be assigned or provisioned to a user in SafeNet Authentication Service, care must be taken to ensure that the same token is assigned to the same user in the 3rd party RADIUS server.

SecurID Tokens

This option is not available to Virtual Service Provider or Subscriber accounts.

OATH Token

3rd party OATH tokens can be imported into SafeNet Authentication Service however these must be converted to a special .btk format prior to import. Contact SafeNet for instructions.

Initialize Token Module

This module can be used with CRYPTOCard/SafeNet RB and KT series hardware tokens. It applies the corresponding series template which determines the operating characteristics of the token such as passcode length, strength, PIN options and so on. (Refer to Token Templates on page 205)

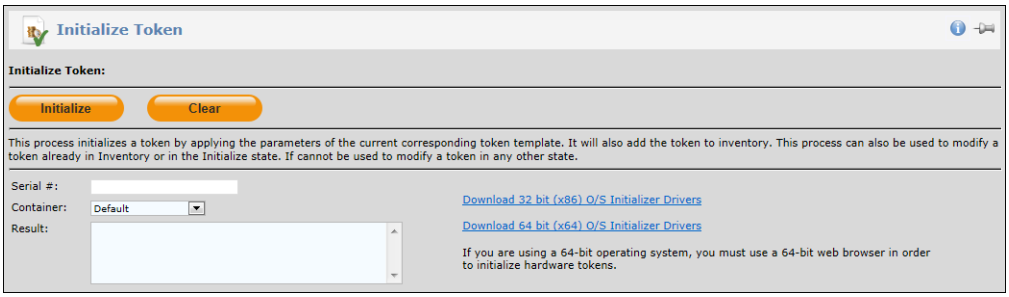


Figure 126: Initialize Token Module

This process requires an RB and/or KT token initializer attached to a USB port on the Operators PC. The necessary drivers can be downloaded and installed using the links displayed in the module.

Preparing the KT series token for Initialization

Starting with the KT-x off, press and hold the button until the display shows “Init” (approximately 3-4 seconds). Release and press the button again. The display will show the prompt: **RDY 4 IR**. Insert the token in the initializer with the LCD display facing the front of the initializer. Click the Initialize button. Note that the KT-x will remain in the RDY 4 IR state for approximately 15 seconds. The token cannot be initialized while in any other state. Initialization will complete in 7-10 seconds.

Preparing the RB series token for Initialization

Place the RB-x token in the initializer with the LCD display down and facing the front of the initializer. The RB-x does not need any other preparation before initialization. Click “Initialize” in the Token Mgt group to complete the process. Initialization will complete in 7-10 seconds.

Figure 127: KT-1, KT-2/3 Series Token Initializer

Figure 128 - RB Series Token Initializer

Figure 129 – KT-4/5 Series Token Initializer

Groups Tab

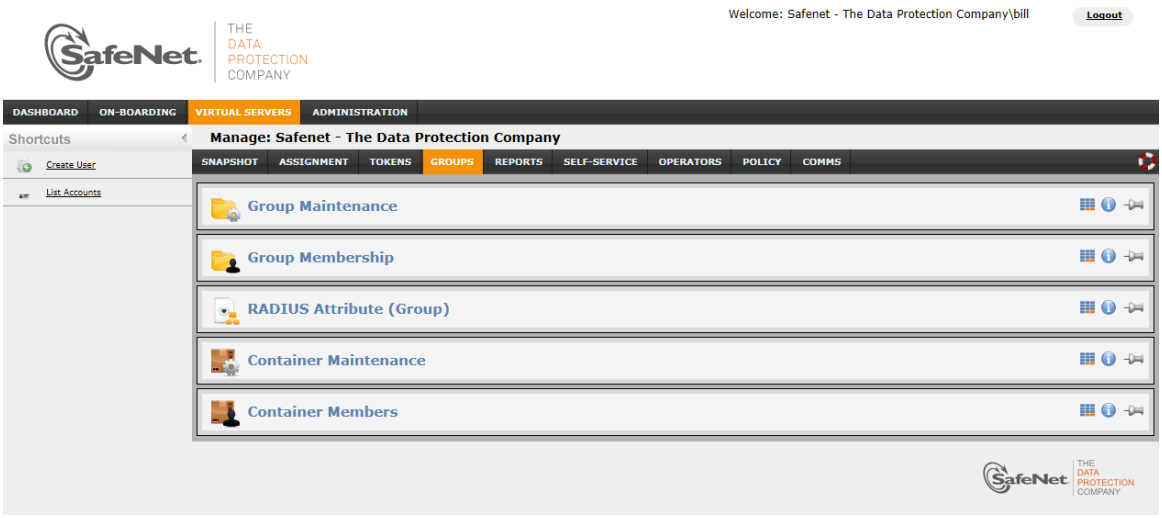


Figure 130: Groups Tab

The groups tab provides access to all functions necessary to:

- Create and Manage Groups (Group Maintenance Module)
- Manage User Group Memberships (Group Membership Module)
- Apply RADIUS Attributes to Groups (RADIUS Attribute (Group) Module)
- Create and Manage Containers (Container Maintenance Module)
- Manage Container Objects (Container Members)

Group Maintenance

Groups are attributes that can be attached to a UserID and used for authorization during the authentication process. Group attributes provide a way to distinguish between valid users (all users that can authenticate) and those that should be allowed to authenticate to gain access to a particular resource.

For example, assume you have 2 valid users User1 and User2 both of which can authenticate. However, one of your protected resources is the HR network which should only be available to User1. By creating and adding User1 to the “HR” group, then creating a firewall rule or a Pre-Authentication rule (refer to Pre-authentication Rules on page 278) in the Virtual Server, only User1 will be able to authenticate to the HR network. This of course is a simple example. Complex requirements are also accommodated using a combination of Group Membership and Pre-Authentication rules.

Internal and Synchronized Groups

You can have 2 types of groups on the Virtual Server:

Internal Groups

These are groups which you create and to which you add members.

Synchronized Groups

These are groups that exist on an external user source such as Active Directory. The Synchronization Agent can be used to "synchronize" Active Directory group(s) in the Virtual Server. Synchronization not only synchronizes AD groups, it also retains each synchronized user's group membership.

- AD groups can be used for authorization. Simply by adding or removing a user from an AD group, the Virtual Server using Pre-authentication rules can allow or deny access to resources based on user group membership attributes.
- Auto-provision users with tokens based on their AD group membership. For example, if in AD there were 3 groups: remote access, KT and MP, the Virtual Server could automatically provision users that belong to the remote access and KT groups with a KT hardware token, and those that belong to the remote access and MP groups with a software token.
- By utilizing a combination of Groups, Pre-authentication and auto-provisioning the Virtual Server can accomplish most authentication management functions (creating users, authorization, assigning tokens, revoking tokens) without any administration.

Synchronized Users can belong to both synchronized and internal groups.

Group Maintenance

To create an internal group, select the Internal option, and then click New.

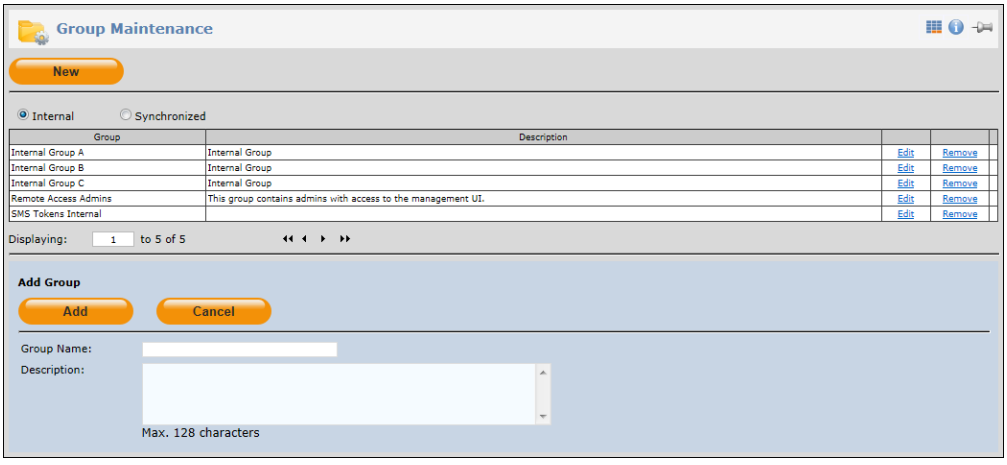


Figure 131: Create an Internal Group

Enter a group name and a brief description of its purpose, and then click the Add button. This will add the group and update the Internal Groups List.

Group names and descriptions can be edited by clicking the edit hyperlink, or removed by clicking the remove hyperlink.

Group Membership Module

This module is used to display all members of a group or to modify the memberships of one or more users. Note that the memberships for an individual user can also be managed from the Group Membership module on the Assignment tab.

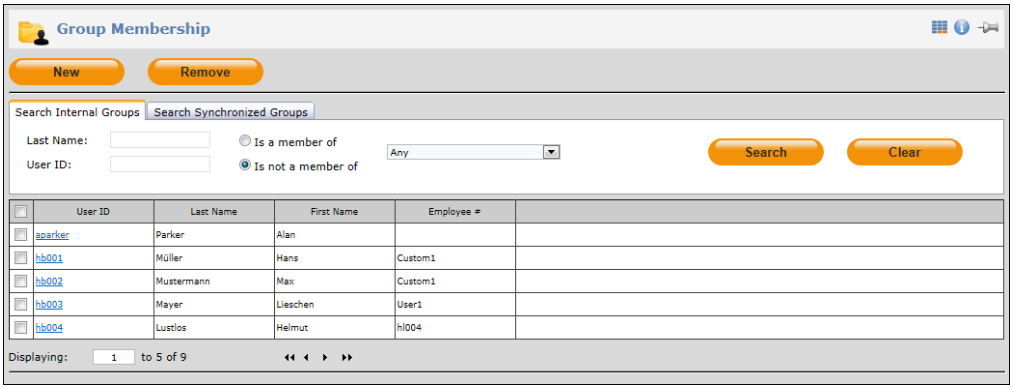


Figure 132: Group Membership and List

To view group membership, use the search function in conjunction with:

- **Is a member of option**
  This refines the list to users that are members of any group or a specific group.

- **Is not a member of option**
  This returns a list of users that do not belong to any group, or do not belong to the specified group.

You can further refine the list by adding the User's last name or UserID to the search criteria.

The UserID hyperlink can be used to display the corresponding User Detail.

- Add Users to a Group (Internal)
  To add users to a group, use the check box options to select one or more users, and then click the "New" button. This will open the Add Membership dialogue.

  Use the dropdown to select the group membership to add to the user, and then click the Add button.

- Synchronized Group Membership

Synchronized Group membership cannot be added or removed from users in the management UI. This is because synchronized group membership is obtained from the AD/LDAP or other external user source. However, you can use the Search Synchronized Tab in Group Membership to view groups and group memberships.

RADIUS Attribute (Group) Module

This module allows RADIUS Attributes to be attached to a group. The attribute will be returned for each member of the group when they authenticate. Note that attributes assigned to users have precedence over attributes assigned to a group to which the user belongs.

Set RADIUS Attribute

To set RADIUS attributes, select the appropriate Internal or Synchronized Group, and then click the New button.

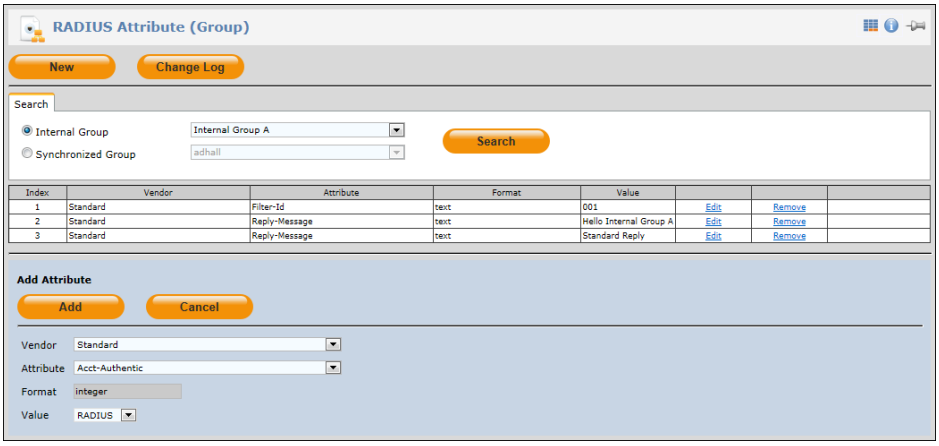


Figure 133: Set RADIUS Attributes (Group)

The options and input values will vary depending upon your selection from the various dropdowns. Consult your network equipment vendor's documentation for guidance on which attributes to use.

Once the attribute is set, click the Add button. This will add the attribute to the Group. Repeat as necessary to add more attributes.

Viewing RADIUS Attributes (Group)

Select the group to view using the internal or synchronized group option, and then click Search. A list of attributes assigned to the group will be displayed in a list. The Edit hyperlink for each attribute can be used to modify the corresponding attribute. Likewise, the Remove hyperlink is used to remove the group attribute.

Containers

Containers are used to separate objects (users, tokens or both) for the purposes of management. Objects can only reside in one container at a time. When a user is moved between containers, all of the user's assigned tokens are moved at the same time.

Containers define an Operator's Scope – what it is they can manage. If a container is not in an Operator's Scope, then all of the objects in the container are also not in Scope and consequently cannot be viewed or managed by the Operator.

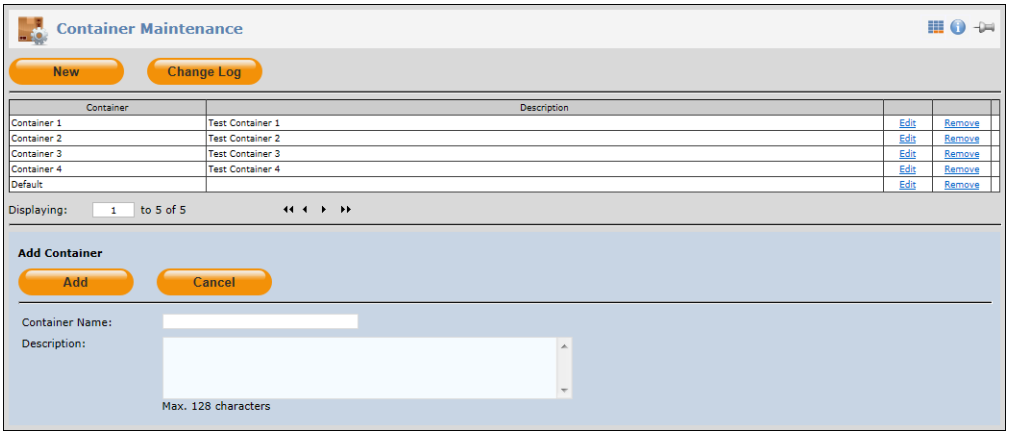


Figure 134: Container Maintenance

There are several applications of containers. Some examples are:

- Use containers to segregate management
  Operator A can see/manage objects in Container A; Operator B can see/manage objects in Container B; Operator C can see/manage objects in Containers A and B.

- Use containers to segregate inventory
  Cost center A purchases tokens which are placed in Container A
  Cost center B purchases tokens which are placed in Container B
  Operator A can only view/manage tokens in Container A
  Operator B can only view/manage tokens in Container B
  Operator C can view/manage tokens in Containers A and B

The Virtual Server has a "Default" container into which users and tokens are automatically placed unless a different selection is made at the time the users and/or tokens were added.

Creating Containers

To create a new container, click the New button, then enter a unique container name and brief description of its purpose, and then click Add. The new container will appear in the Containers List.

Click the Edit hyperlink or the Remove hyperlink respectively to edit the container information or remove it. Note that all objects must be removed from a container before it can be removed.

Container Members Module

Containers and their members can be viewed and members moved between containers using this module.

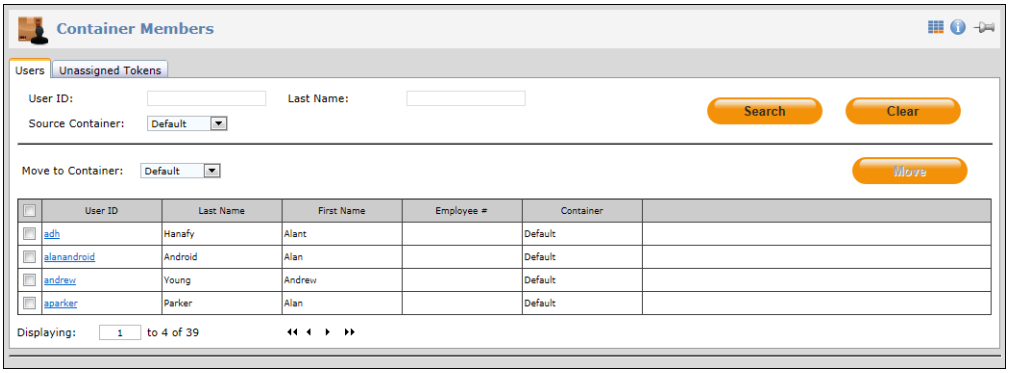


Figure 135: Managing Container Members

The Containers view includes two tabs: Users and Unassigned tokens. To view objects by type, select the appropriate tab. Recall that tokens assigned to Users always reside in the container with the User.

To view the members of a container, select the appropriate Source Container, the click Search. This resulting list displays all objects in the container. Clicking the UserID or Serial Number hyperlink displays the object's details.

Moving Objects

To move objects to a different container, select the objects in the list using the check box option, then select the target container from the "Move to Container" dropdown, and then click the "Move" button.

Reports Tab

Every Virtual Server has a reporting engine that provides an extensive range of usage, compliance, inventory management and billing reports. Reports can be customized, scheduled and automatically delivered to recipients or viewed and downloaded through the management UI.

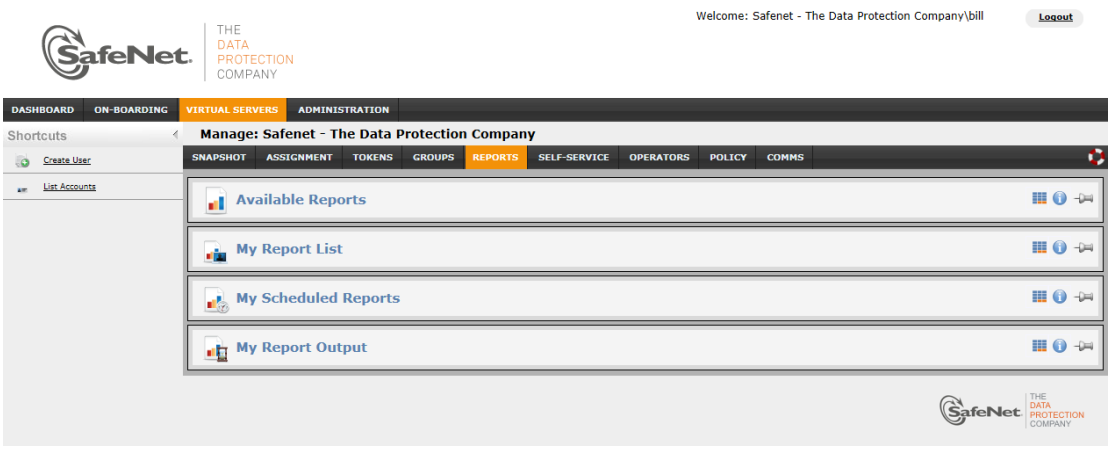


Figure 136: Reports Tab and Modules

Reporting consists of four modules:

- **Available Reports Module**
  This module lists all of the standard reports available in the Virtual Server. Reports from this list can be customized and copied to the My Customized Reports module.

- **My Customized Reports Module**
  This module lists all reports that can be run on the Virtual Server. Reports in this module can be scheduled to run once or periodically at regular, predefined intervals. Delivery options and recipients are defined in this module.

- **My Scheduled Reports**
  All scheduled reports appear in the My Scheduled Reports list. Schedules can be modified and reports can be run “Now” without modifying the normal schedule.

- **My Report Output**
  This module lists all reports that are currently in the run state or have completed. From this list Operators can view or download reports in a variety of formats.

Operator Roles determine which modules are available to an Operator and whether or not they can modify report parameters.

Scheduled reports and Report Output will display only those reports to which the Operator is entitled. Reports can be customized, scheduled and delivered to the account, the Service Provider and to external parties such as auditors.

Available Reports Module

All reports that are available in a Virtual Server are listed in the Available Reports module. To view the entire list of available reports, use the navigation controls below the list or expand the number of rows displayed using the customization icon in the module bar. The report class dropdown selects reports corresponding to:

- **Security Policy**
  This group of reports deals with alert history, container management, Operator Roles and Scope, Auth Nodes and RADIUS attributes.

- **Compliance**
  This group of reports covers user authentication activity, Operator activity and other factors important to internal and external security auditors.

- **Billing**
  This group of reports provides details of all transactions including capacity, tokens, SMS credits and their related billing terms.

- **Inventory**
  This group of reports provides detailed information on tokens, token ownership, states and other general inventory information.

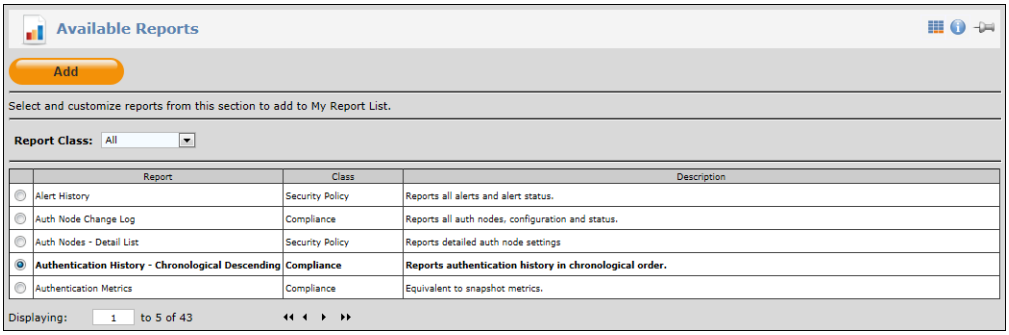


Figure 137: Available Reports Selection

To add a report to the My Reports Module list, begin by selecting a report from the list, and then click the Add button.

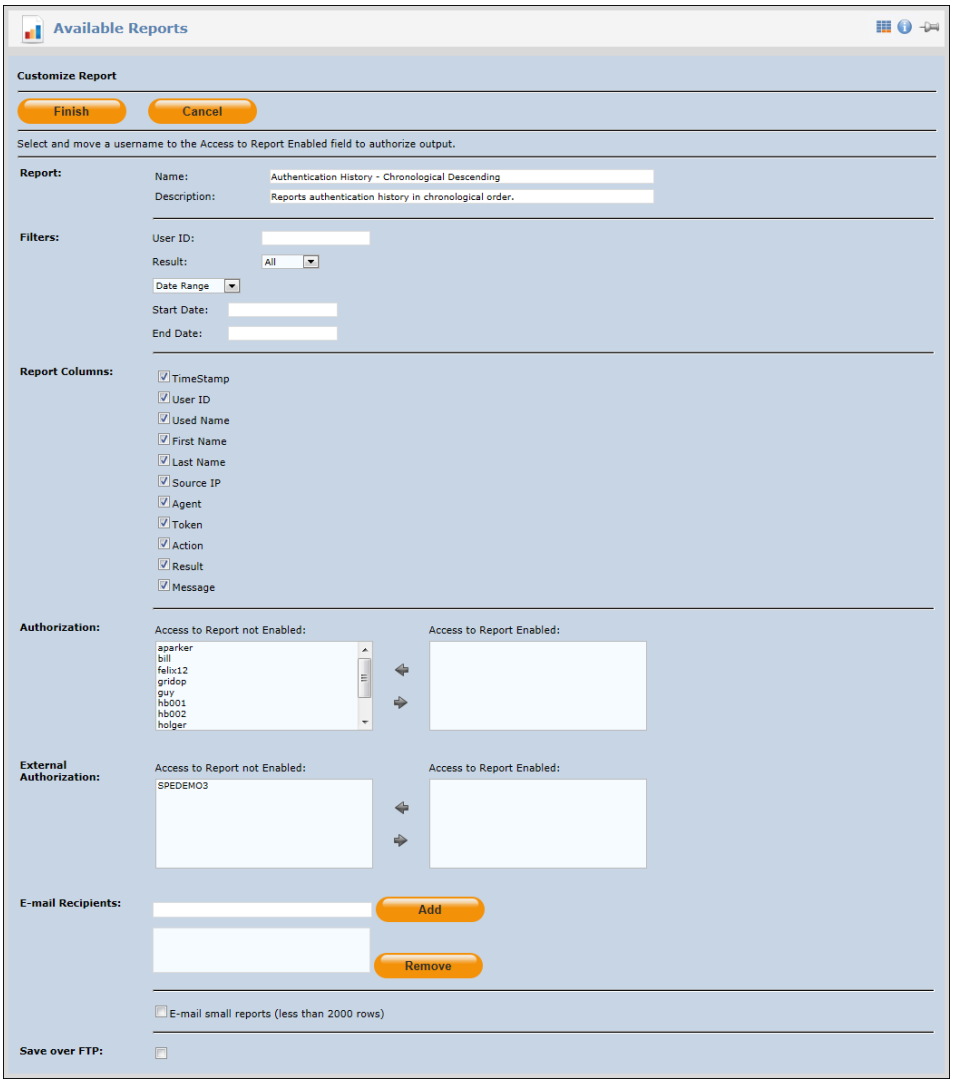


Figure 138: Customize Report

Customize Report

The options for report customization vary depending on the type of report selected. In general:

- **Report Section**
  Customize the name of the report and its description. These changes will appear in the My Reports List module. Note that report names must be unique.

- **Filters**
  If available, filters provide a way to limit the scope of a report, such as the reporting period.

- **Report Columns**
  This shows default fields included in the report. To include/exclude fields, select/deselect fields using the corresponding check boxes.

- **Authorization**
  The “Access to Report not Enabled” field lists all Operators that are potential report recipients. The “Access to Reports Enabled” field lists all Operators that will receive the reports. To add or remove from the recipient list, highlight the Operators (CTRL Click to select multiple Operators), and then click the appropriate arrow to move.

- **External Authorization**
  The “Access to Report not Enabled” field lists all Service Providers that are potential report recipients. The “Access to Reports Enabled” field lists all Service Providers that will receive the reports. To add or remove from the recipient list, highlight the Service Providers (CTRL Click to select multiple Service Providers), and then click the appropriate arrow to move.

- **E-mail Recipients**
  The server can send the report by email to addresses in the recipients list. Use this option to send reports to people that are not Operators or Service Providers and therefore cannot log into the management UI to view and download reports. To add recipients, enter their email address then click the Add button. To remove recipients, highlight their email address then click the Remove button.

- **Save over FTP**
  If checked, the completed report will be transferred by FTP/SFTP or SCP according to the parameters set in the COMMS Tab | Communications Module|FTP/SFTP/SCP Settings. Refer to FTP/SFTP/SCP Settings on page 273.

Click the Finish button to commit the customizations and add the report to the My Report List module.

My Report List Module

This module lists all customized reports. It is from this list that you schedule reports to run.

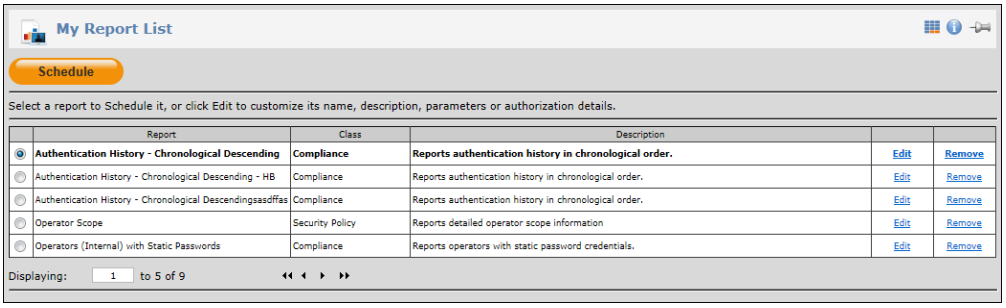


Figure 139: My Report List

To schedule a report, select the report then click the Schedule button.

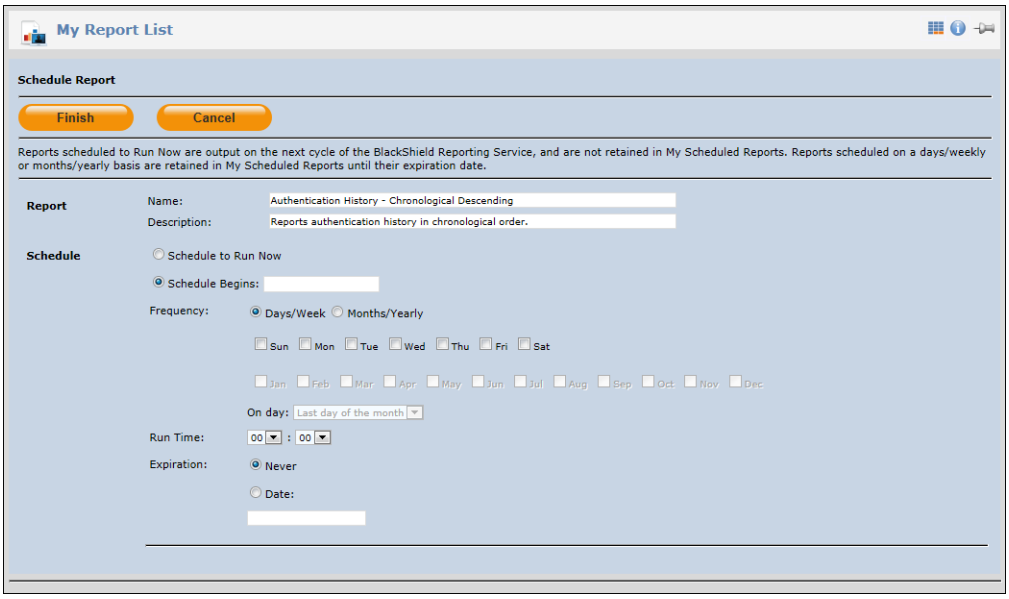


Figure 140: Schedule Report

Schedule Report

The schedule report options are:

- **Run Now**
  The run now option adds the report to the report processing queue. Reports in the queue are run in chronological order.

- **Schedule Begins**
  The report will not run prior to this date.

- **Frequency**
  Reports can be scheduled to run on specific days of the week by selecting the Days/Week option, then selecting the specific days. Alternatively, the report can be scheduled to run on a monthly basis by selecting the Months/Year option, then selecting the specific months. If Months/Year is selected, the On day option is enabled. Use this option to specify a day in each month that the report should run. Reports will not run after the date specified in Expiration Date. By default report schedules do not expire.

- **Run Time**
  The time at which the report should begin executing.

- **Expiration**
  The date after which the report will be removed from the My Scheduled Reports list.

To commit the report schedule, click the Finish button. This adds the report to the My Scheduled Reports module.

Operators with appropriate Role permissions can use the Edit hyperlink to modify the report criteria or remove the report from the My Reports list using the Remove hyperlink.

My Scheduled Reports Module

Scheduled reports to which the Operator is entitled appear in the My Scheduled Reports List. The list shows the report name, run frequency, run time and expiration date. Clicking the report name hyperlink displays the report criteria. Operators can modify a report schedule or run a report “now”. The run now option adds the report to the report processing queue. Reports in the queue are run in chronological order. The reporting service checks the queue every 5 minutes and after each report is generated. This means that all reports will be processed in order however if no reports are detected, up to 5 minutes may elapse before the service will check the queue for new report additions. The Run now option does not alter the report’s regular schedule.

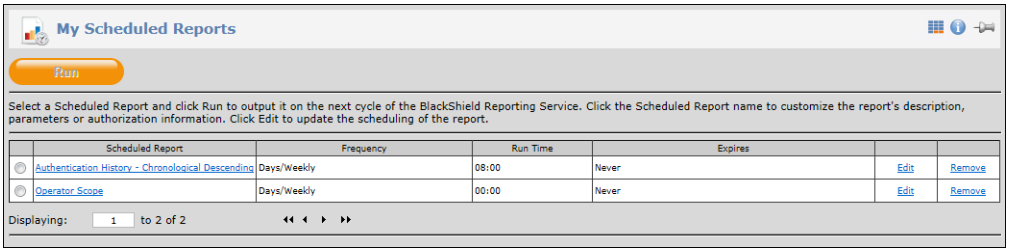


Figure 141: Scheduled Reports List

Operators with appropriate Role permissions can make changes to the reports schedule by clicking the Edit hyperlink, or remove the report from the schedule by clicking the Remove hyperlink.

Reports that are running or have completed running are added to the My Report Output module.

My Report Output

All reports that are running or have completed to which the Operator is entitled are listed in the Report Output table.

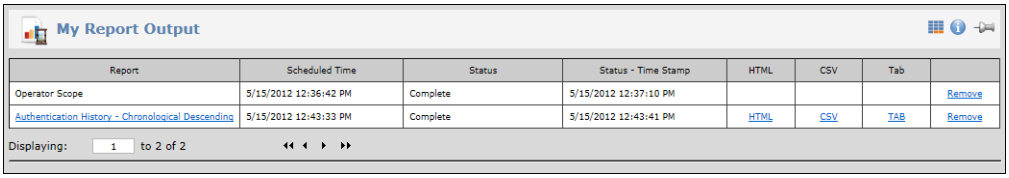


Figure 142: Report Output List

Reports can be viewed in the browser by clicking the report name hyperlink. Alternatively they may be downloaded for local processing by clicking any of the CSV, Tab or HTLM hyperlinks. Reports that are no longer required can be deleted from the list by clicking the remove hyperlink.

Self-Service Tab

SafeNet Authentication Service Self-service has been created for organizations that want to:

- Empower users to perform simple authentication management functions such as resetting PINs, reporting lost tokens or viewing their authentication history, and in the process, reduce the workload and end user reliance on the help desk.
- Invite users to request a token. This is particularly useful for organizations servicing consumers of on-line subscription services. Users can now request a token as part of their subscription for other services.
- Create a customized yet automated workflow for approving token requests, fulfilling and shipping tokens to users.
- Offer a complete user-centric service including Multilanguage support, customized prompts, messages, help and navigation, all optimized for the user based on how they are interacting with self-service (browser type, screen resolution etc.)

Self-Service WSDL API

Self-service functionality can be exposed by SafeNet Authentication Service Platform as a web service. (WSDL), giving developers the necessary tools to build some or all of the self-service functionality into a corporate portal.

Alternatively, organizations can use the stand-alone Self-service installer to create a self-service site on a web server external to SafeNet Authentication Service Platform.

Both options have the advantage to offer self-service from URLs familiar to the users it is intended to server.

For more information about the self-service WSDL, contact SafeNet or your local vendor.

Self-Service Overview

Typically authentication self-service has been limited to extending some token management functionality to “users”; specifically PIN management, OTP resend and token resync. The focus is almost always “token-centric”, assuming that all users are the same, have tokens and that the only issues self-service need resolve are token-related.

In fact, many enterprises want to extend self-service functionality to people that:

- may or may not have tokens. In many organizations the idea that users should be able to request a token (and/or services) makes sense, perhaps as part of some other service to which the user is subscribing. The concept then is “Pull”.

- may or may not be known to the organization. In our common experience, users belong to an organization. But this is not always the case. At a simple level, external parties such as contractors or business partners may require the service. The separation between the enterprise and the possible user community may broader. Think of a user becoming a subscriber to your service for the first time. Until they sign up and are approved, the user is completely unknown. Therefore self-service must accommodate communities which may become legitimate users of the service but are unknown to the service provider prior to “signing-up”.

- may have very diverse requirements, not the least of which is language. It’s difficult to contemplate providing a “global” self-service capability without considering the diversity of the community. It is very unlikely that “users” will all speak the same language or that hardware tokens shipped from Toronto will arrive in Montreal and Shanghai in the same timeframe. In other words, self-service needs to accommodate diversity in such a way as to maximize the simplicity of the user experience, regardless of language, logistics and authentication method.

It is quickly apparent that the “Pull” world demands a new set of tools by which administrators of authentication services can extend self-service functions to current and potential users, determine the validity of requests, how each is to be handled and how, throughout the process the “user” is kept informed.

The key elements to producing an effective and highly marketable Self-service capability depend on:

- Ensuring that the approval process reflects the enterprise’s desired workflow

- Sufficient visibility at all stages of the workflow as to the status of a request

- Effective and simple workflow and communication with the user.

All self-service functionality, from what is presented to the user to back-office workflow is controlled through the configuration and management modules contained in the Self-service tab of the SafeNet Authentication Service platform.

Self-service then is best viewed as three functional areas:

- The self-service web site through which users perform common functions.

- Presentation services through which administrators customize the services, languages and other aspects of self-service presented to users on the self-service site.

- Backend workflow through which administrators manage the services presented to users through the self-service web site.

Self-service Web Site

All configuration and management of Self-service is performed from the Self-service tab of a virtual server. On this tab:

- **Configure Self-service Module**
  The hyperlinks in this module provide access to all of the functions related to customizing the site for appearance, user services and back-office workflow including approving and fulfilling user requests for tokens.

- **Queue Management**
  This module provides lists of outstanding tasks related to user requests for tokens. Operators with appropriate “Authorities” can view and process requests for tokens.

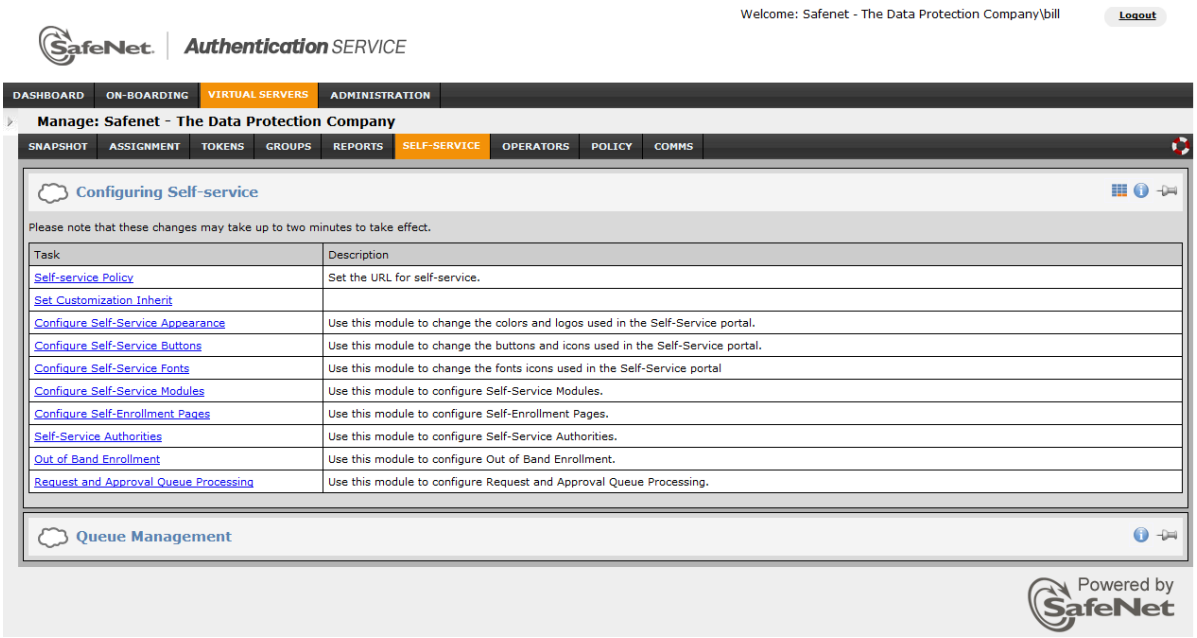


Figure 143: Self-Service Tab

The Self-service site can present users with the following modules:

Service	Default Icon
Request a Token module This service allows users to request a token by type from a list of approved token types and authentication methods. This service accommodates both existing users as well as creation of new user accounts. This module is not published by default.	
Reset PIN module This module allows users to modify their server-side PIN without the assistance of the help desk. PIN changes must comply with the PIN policy. This module is published by default.	

Reset PIN module

This module allows users to modify the PIP (personal image pattern) associated with their GrID authentication method without the assistance of the help desk. The new PIP must comply with the PIP policy. This module is published by default.

Resync Token module

This module allows users to test and resync their token with the server without the assistance of the help desk. This module is published by default.

My Profile module

This module can allow users to modify basic information about their account such as address, telephone number etc. It also presents basic statics about their authentication activity and allows them to manage challenge/response questions valid (if enabled) for sign on to the self-service site. This module is not published by default.

Resend SMS

This module allows a user to request an SMS/OTP resend to their registered mobile device.

Self-service Site Appearance

The Self-service site is highly customizable within each virtual server. This includes:

- Navigation and other buttons
- Logos and icons
- Fonts
- Colors

Inheritance

By default, when a Subscriber Account is On-boarded, (i.e. child account created by the Service Provider) it inherits all customizations applied to the Service Provider's Self-service site. Subscriber Accounts can override these customizations and independently configure their Self-service site.

Figure 144: Self-service Site Inheritance

To override default or Service Provider customizations, select the Set Customizations Inherit hyperlink, clear the User Inherit Customizations option, then click the Apply button. To revert to default site settings which do not inherit from the Service Provider customizations, check the option and click Apply to commit the change.

Module Configuration

Each module is enabled and configured independently for user options and supported languages. Modules may contain more than one web page which will be presented to the user.

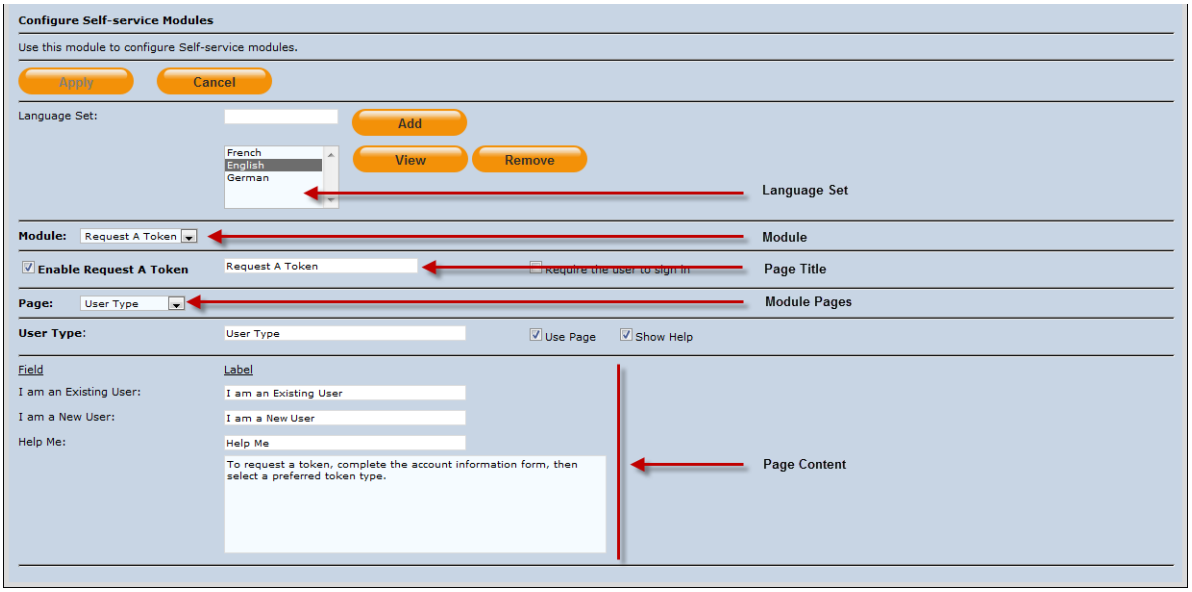


Figure 145: Module Configuration

Languages

The self-service web site can be configured to provide services in any number of languages. The default service is based on an English language set. Administrators can create additional language sets using the English set as a guide.

Authorities

Authorities are special privileges assigned to Operators for the purpose of managing user requests for tokens received from the Self-service site. There are four possible Authorities:

- **Approval Level 1**
  This authority approves or denies user requests for tokens received from the Self-service site. At least one Operator must have this authority if the Request a Token module is enabled on the self-service site.

- **Approval Level 2**
  This authority approves or denies user requests for tokens that have been approved by Approval Level 1 authorities. This is an optional authority.

- **Issuing Authority**
  Requests for tokens that have received the required approvals are fulfilled by the Issuing Authority. This function is the equivalent of using the "Provision" functions available on the Assignment tab unless a Shipping Authority has been created. At least one Operator must have this authority if the Request a Token module is enabled on the self-service site.

- **Shipping Authority**
  The Shipping Authority is a special function that serves two purposes:

  - It can be used to coordinate the delivery of enrollment instructions with receipt of the physical token by the user.

  - It can be used to increase the security of enrollment by requiring the user to provide an additional code during enrollment that is delivered separately and Out-of-Band ("OOB") with respect to all other enrollment instructions.

    Shipping authorities are applied by token type. Token requests for affected token types that have been approved by the Issuing Authority must be completed by the Shipping Authority. This is an optional authority.

Workflow

Requests for tokens include workflow that incorporates appropriate messaging and alerts for the users making requests for tokens and for each Authority involved in the approval and fulfillment process. Alerts and messages can be customized and sent by email and/or SMS. In addition, all requests can be viewed and managed from the Queue Management module.

Provisioning Tasks

A provisioning task is created for each fulfillment. Tasks can be viewed by clicking the Provisioning Tasks hyperlink in the Shortcuts section on the Assignment Tab. A provisioning task shows the date the enrollment reservation was created, the date enrollment must be completed and the status of the enrollment. Tasks may be cancelled or modified prior to user enrollment and an alert can be generated for expired enrollments. For more information on provisioning tasks refer to the Administrator Guide.

Reporting

All self-service requests for tokens and subsequent processing by authorities are available in reports (Reports Tab) including:

- **Provisioning Task Attempts**
  Reports detail of attempts to use provisioning tasks by users.
- **Provisioning Tasks**
  Reports detail of provisioning tasks.
- **Provisioning Tasks – Outstanding**
  Lists all outstanding provisioning tasks

Configuring Self-service

In this module:

- **Self-service Policy**
  Use this module to view or modify the self-service site unique URL.
- **Set Customization Inherit**
  Use this module to override site customizations inherited from the Service Provider or to revert to default settings.
- **Configure Self-Service Appearance**
  Use this module to configure the overall site "look and feel" including colors, logos, and banner images.
- **Configure Self-Service Buttons**
  Use this module to modify navigation items such as buttons, button text and module icons.
- **Configure Self-Service Fonts**
  Use this module to select font types and styles used throughout the site.
- **Configure Self-Service Modules**
  Use this module to customize each of the modules published to the self-service site including language sets, required/optional fields and user help and instructions.
- **Configure Self-Service Enrollment Pages**
  Use this module to customize instructions presented to the user during token enrollment. Instructions and messages can be created independently for each token type.
- **Self-Service Authorities**
  Use this module to add one or more authorities to Operators.
- **Out of Band Enrollment**
  Use this module to require the use of an additional factor during enrollment, delivered to the user "out of band".
- **Request and Approval Queue Processing**
  Use this module to customize message content and delivery method provided to users that have requested a token and to Authorities.

Self-Service Policy Module

This module displays the base URL and unique URL for the Self-Service site. The Self-Service Unique URL must be provided to users. These URLs are automatically created when the virtual server account is activated.

- These URLS should not modified unless a stand-alone Self-Service web site has been installed and configured, in which case these URLs should reflect the location of that web server.

Figure 146: Self-Service Policy

Set Customization Inherit

Use this module to override site customizations inherited from the Service Provider or to revert to default settings. To customize the site, clear the “Use Inherit Customizations” option, the click Apply to commit the change.

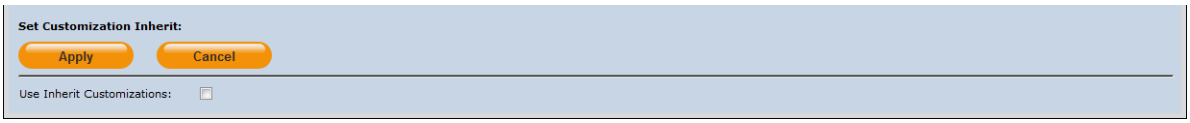


Figure 147: Set Customization Inherit

Configure Self-Service Appearance

Use this module to change the colors and logos used in the Self-Service portal where:

- **Self-Service Logo**
  This is the logo that will appear near the top center of self-service site. Uploaded logos should be in png, jpg or gif format and 387 x 70px.

- **Logo Background Color**
  This is the color behind the logo spanning the width of the page. Dimensions: page width x 70px.

- **Banner Image**
  This is an image in the banner area which includes the navigation buttons. Dimensions: page width x 80px.

- **Banner Color**
  This is the color behind the banner image and spans the width of the page. Dimensions: page width x 80px.

- **Homepage Background**
  This is the image used on the home page background. Dimensions: page width x 80px (max).

- **Homepage Color**
  This is the home page background color displayed behind the Homepage Background image.

- **Page Background**
  This is the background image used on all pages other than the home page.

- **Page Color**
  This is the page background color displayed behind the Page Background image on all pages other than the home page.

- **Language Icon**
  This is an optional icon displayed in the page footer to represent language selection options on the page.

- **Help Text Background**
  This is the background color of all available help text available on the site.

- **Error Text Background**
  This is the background color of behind all error messages.

- **Input Field Border Color**
  This is the color of the border surrounding input fields.

- **Input Field Background Color**
  This is the color of the input fields.

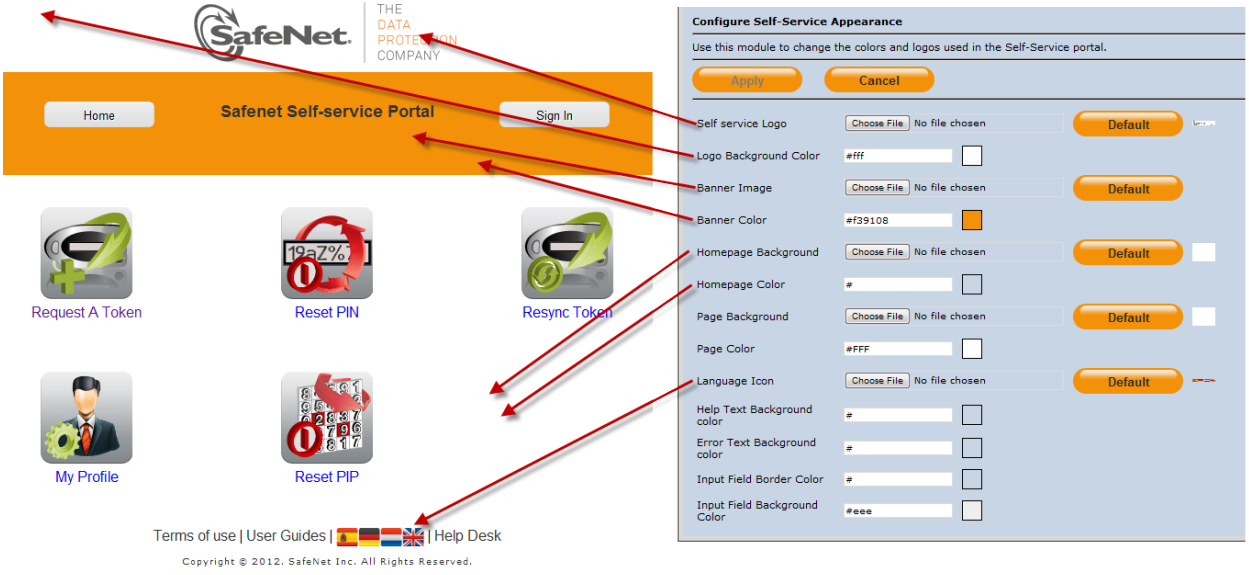


Figure 148: Configure Self-Service Appearance

Configure Self-Service Buttons

Use this module to change the buttons and icons used in the Self-Service portal where:

- **Small Button**
  These are the buttons used for navigation throughout the site. Button images can be uploaded, selected from a list of available buttons or configured as an HTML button. Uploaded buttons should be dimensions 120 x 28px.

- **Button Text**
  This provides options to select the font, font size, color and weight used on small buttons.

- **Button Hover Text**
  This provides options for modifying the appearance of the button text when hovering over the button.

- **Large Button**
  Some selection options such as choosing the type of token use a large button. Button images can be uploaded, selected from a list of available buttons or configured as an HTML button. Uploaded buttons should be dimensions 400 x 28px

- **Icons**
  Module icons can be replaced with uploaded images. Icons should be in png, jpg or gif format and be 100 x 100px.

- **Language Icon**
  The language icon can be replaced with an image or text. Images should be 96 x 20px.

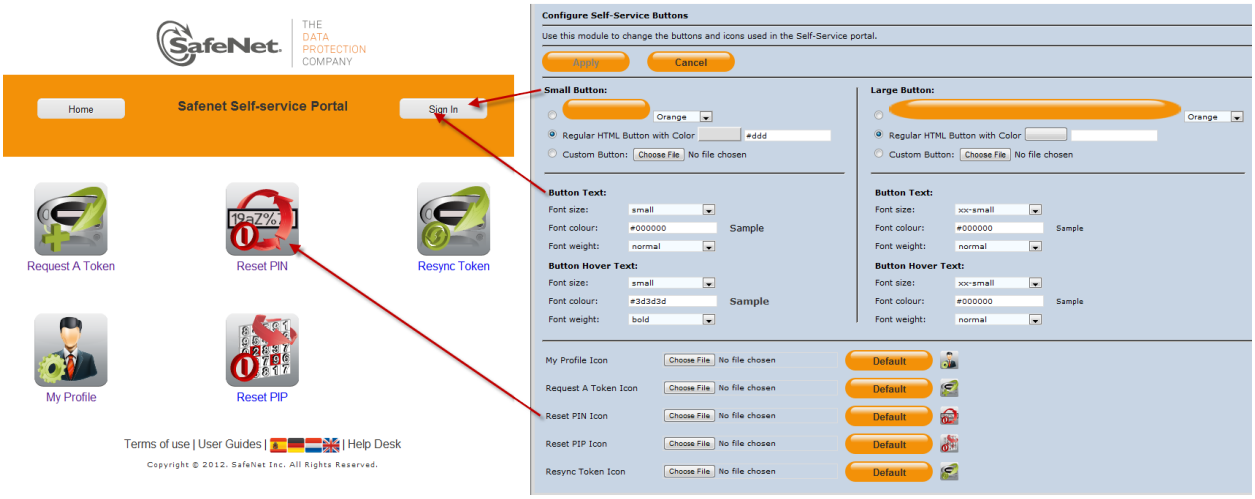


Figure 149: Configure Self-Service Buttons

Configure Self-Service Fonts

Use this module to change the fonts icons used in the Self-Service portal where:

- **Site Title**
  This is the site title displayed in the banner area.
- **Page Title**
  This is the title below the banner area and to the left of the | separator.
- **Page Service**
  This is the title below the banner area to the right of the | separator.
- **Field Label**
  This is the font used throughout the site for all field labels.
- **Help Text**
  This is the font used in all help panels.
- **Error Text**
  This is the font used for all error messages.
- **Footer Text**
  This is the font used in the footer area of the site.

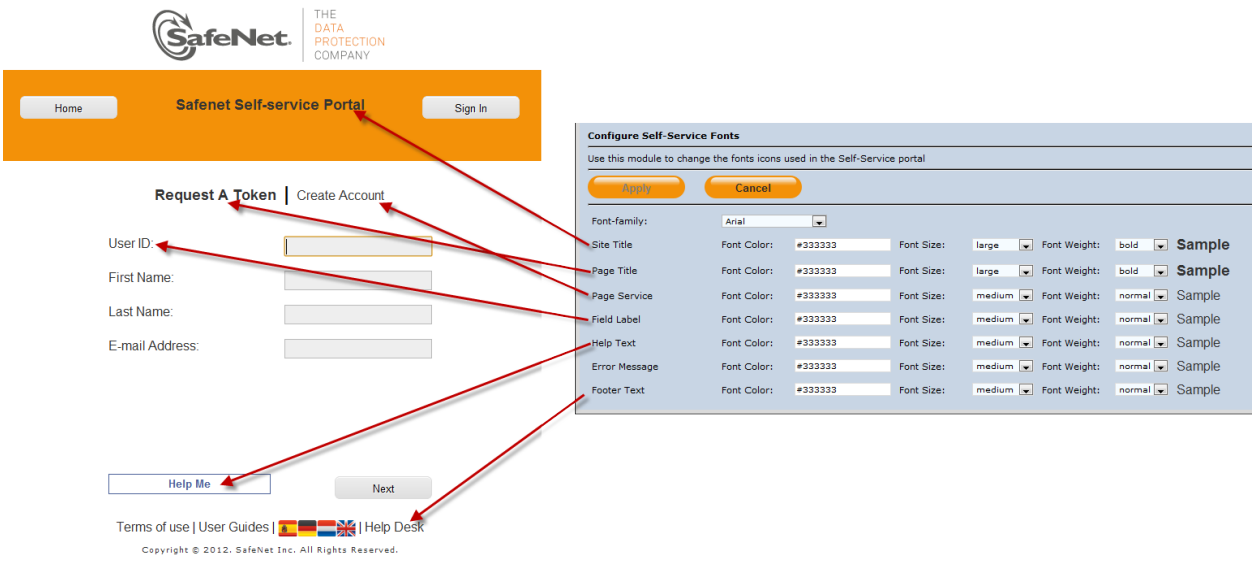


Figure 150: Configure Self-Service Fonts

Configure Self-Service Modules

Use this module to configure Self-service modules.

Language Set

This area supports the viewing and creation of multiple language sets for each of the self-service modules and all of the pages, error messages and help text available in each module.

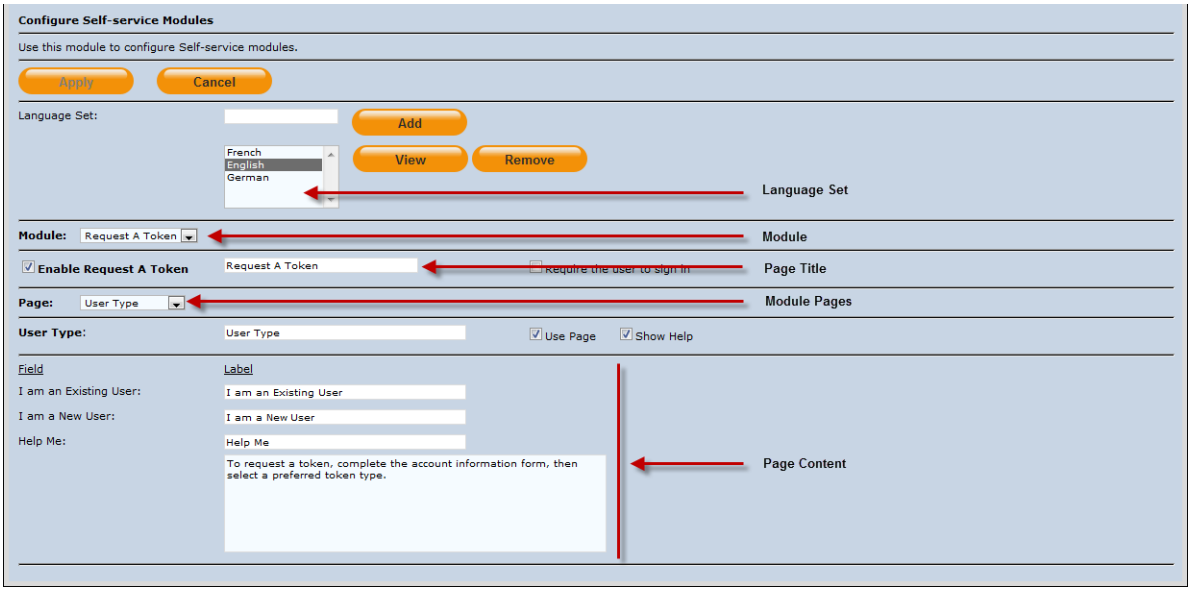
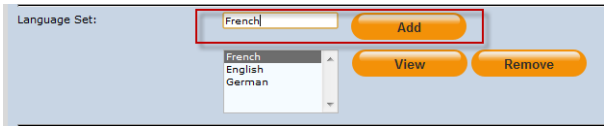


Figure 151: Configure Self-Service Modules

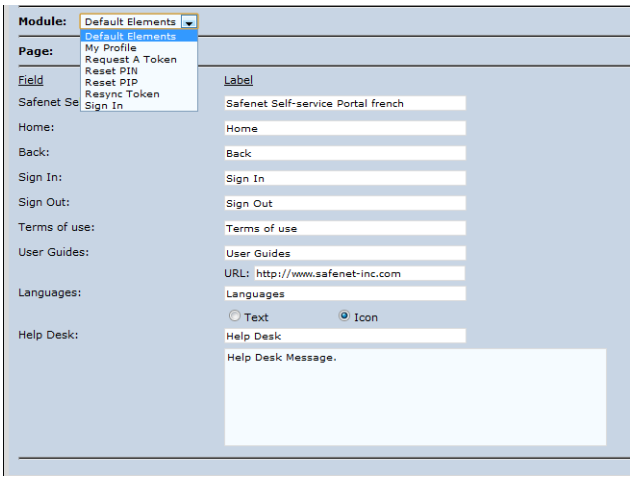
To view a language set, select it from the language list, then click the View button.

To add a language set, type the name for the set in the Language set field, then click the Add button. Next, modify all of the labels, default text, help text and error messages for each of the pages in the selected module. For example, to create French language set:

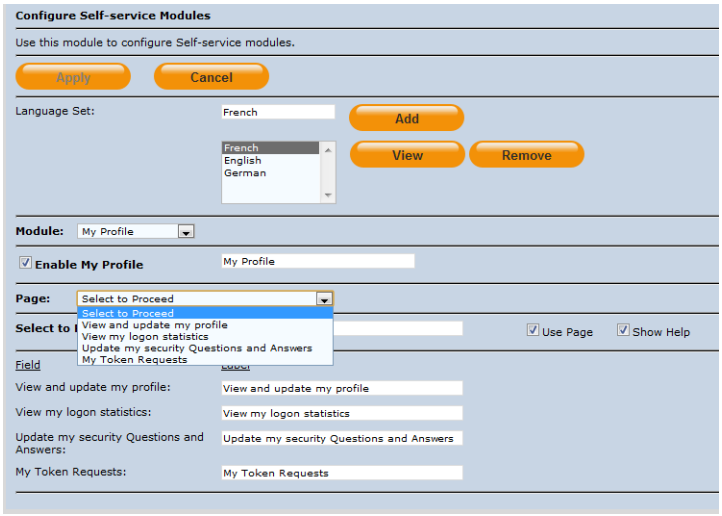
- Add French to the list



- Select a module from the Module dropdown.



- Select a page from the Pages dropdown and modify the text and labels.



- Click Apply to save the set. Repeat steps 3 and 4 until all pages have been modified.

Self-Service Module Options

A module is published to the self-service site if it is enabled. Referring to Figure 152: Self-Service Module Options on page 163:

- **Enable Module Option** – Highlighted Area 1
  To change the publication status of a module, check or clear the Enable option then click Apply to commit the change.

- **Require the User to Sign in** – Highlighted Area 2
  For security reasons some modules such as My Profile or Change PIN should require the user to authenticate before access is granted. To require authentication, check this option, then click Apply to commit the change.

- **Use Page** – Highlighted Area 3
  Most modules contain several pages however depending on your requirements it may not be necessary to publish all pages. For example, the My Profile module includes pages that display token requests made by the user. As this is an information page only, it is not necessary to publish the page.

- **Show Help** – Highlighted Area 4
  Help is available for most pages however it can be removed from the site by clearing this option.

- **Required** – (not shown)
  Some pages such as My Profile allow users to input or update information. The Required option if enabled requires the user to enter data into the field. If unchecked, the field is not displayed.

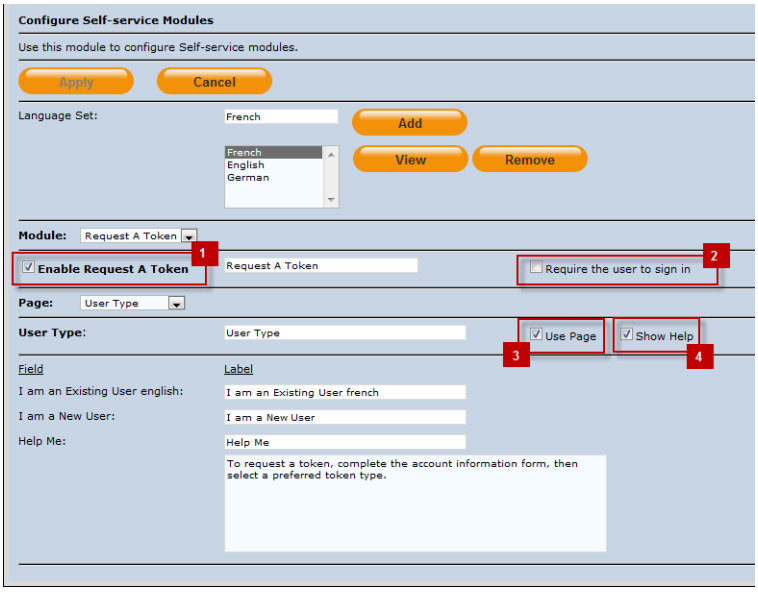


Figure 152: Self-Service Module Options

Default Elements Module

This module has only one page and includes the basic information presented on the self-service site home page. User access to customized Terms of Use policies and documentation can be provided by placing these on a publicly accessible location and updating the corresponding URLs in this module.

The language icon can be replaced with text or a custom image (refer to Configure Self-Service Buttons on page 158)

The Help Desk hyperlink in the footer area should contain information that assists the user in contacting your help desk to obtain assistance.

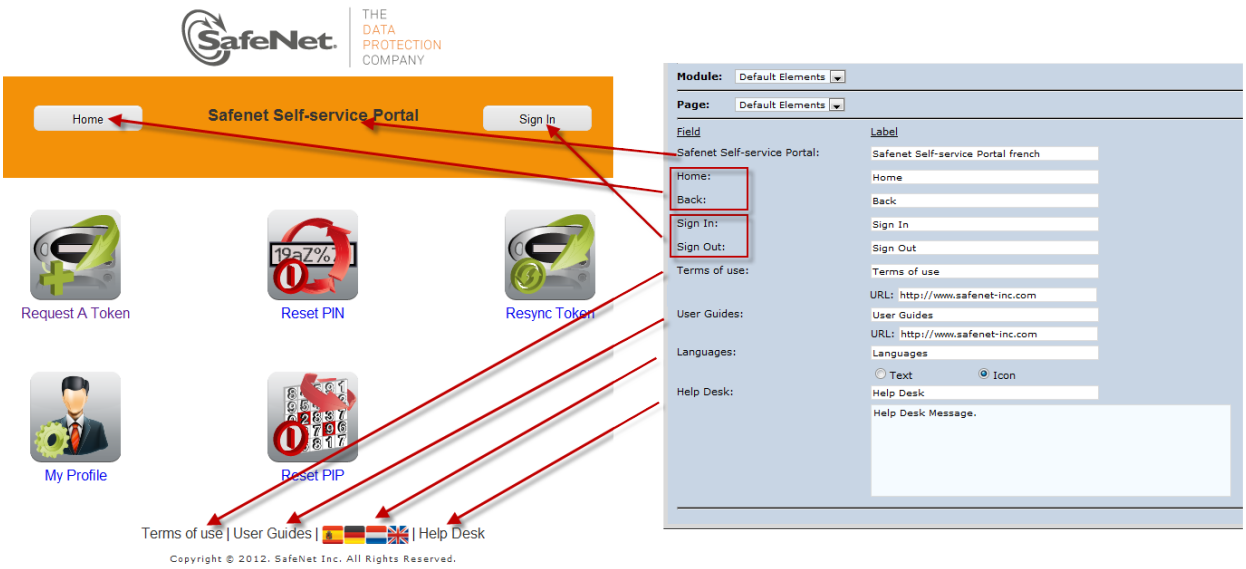


Figure 153: Default Elements Module

Request a Token Module

This module provides the ability for a user to request a token. It is also where outbound messages to users and authorities are configured.

Note: to make this module appear on the self-service site, the virtual server must have at least on Operator and the “Enable Request a Token” option in the Self-service Authorities module must be selected.

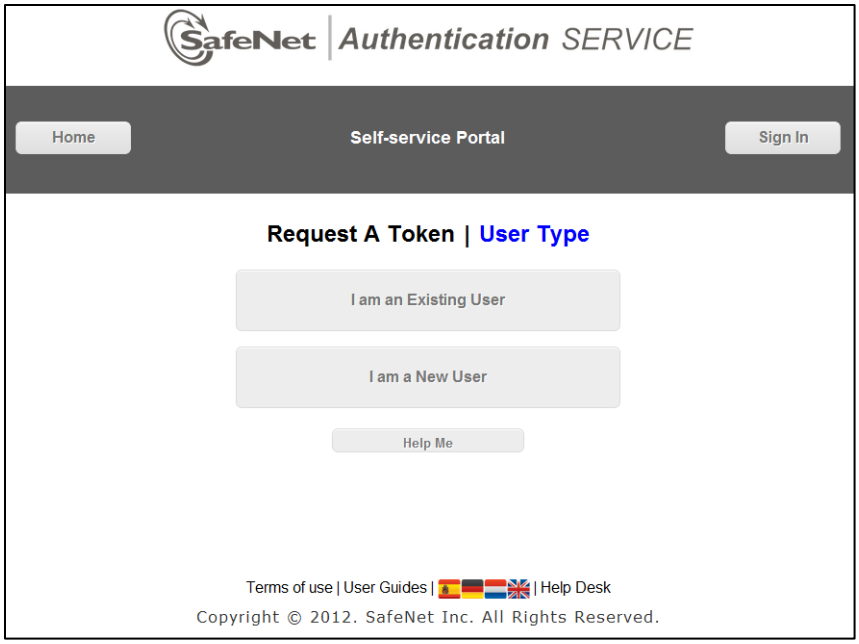


Figure 154: Request a Token Page

There are 6 pages in this module:

User Type Page

This is the first page presented to the user when accessing this module. Users that have an account and an assigned authentication method such as a token can sign into the self-service site and request an additional token.

This page also allows users that do not have an account in the virtual server to create an account (pending approval) as part of the token request process.

Figure 155: Request a Token - User Page

Create Account Page

If enabled, the user will be able to submit a request to create an account in the virtual server during the request a token process. The request must be approved by Approval Level 1 (and Approval Level 2 if enabled) before the account is created.

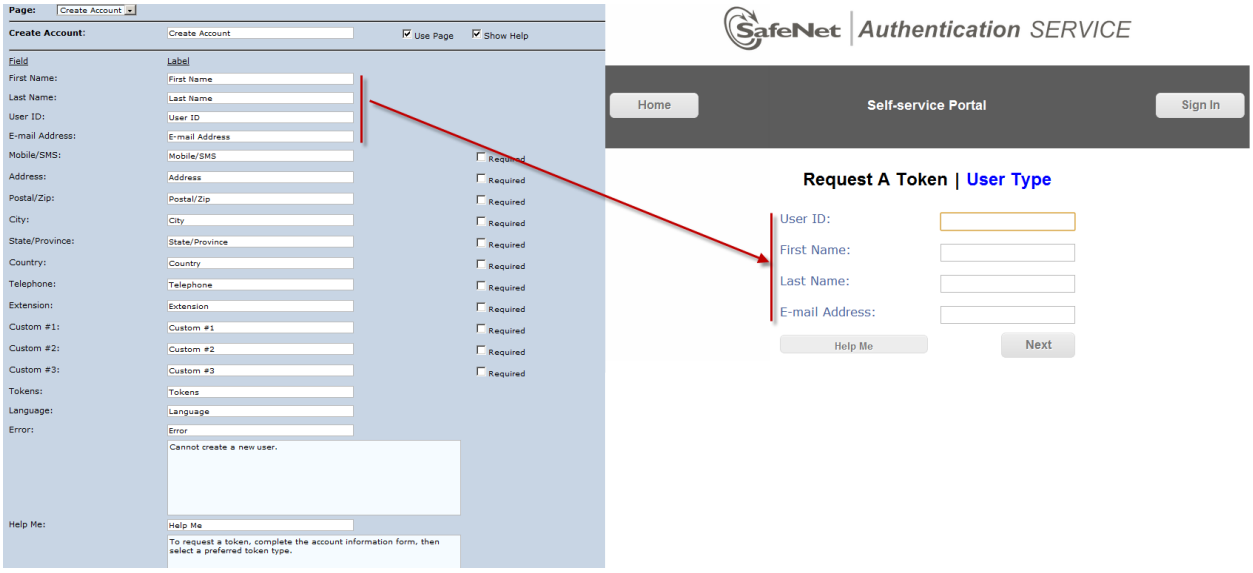


Figure 156: Request a Token - Create Account Page

First Name, Last Name, User ID and E-mail address are mandatory if this page is enabled. Other fields can be displayed by checking the corresponding “Required” option.

To unpublish the create account page, clear the Use Page option.

Token Type Page

This page displays a list of token types that may be requested by the user. Each type in the list has a corresponding enrollment class. For example, the MP for iPhone/iPad would use the “Software” enrollment class. The class selection determines which notification and enrollment instructions the user will receive for the selected token type.

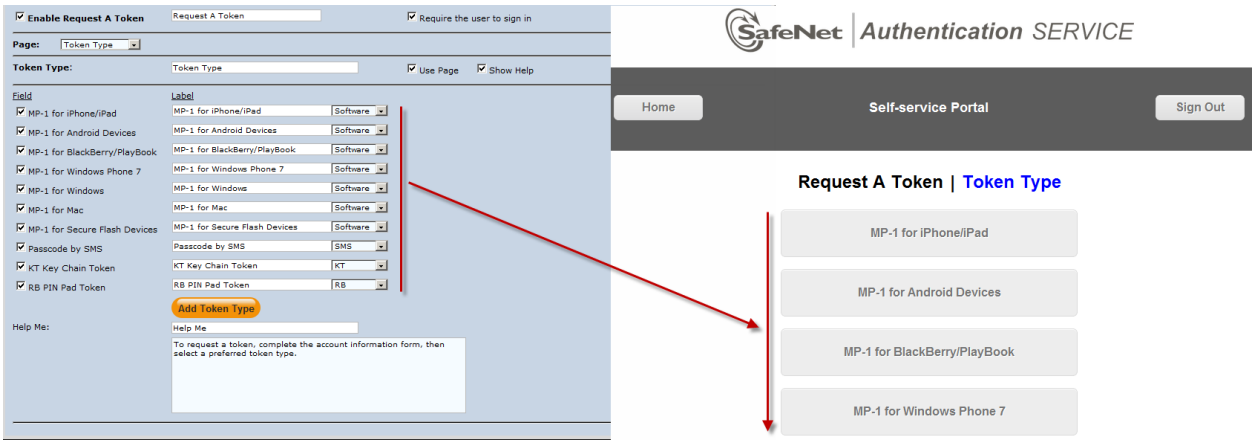


Figure 157: Request a Token - Token Type Page

To publish or unpublish a token type, check or clear the corresponding field option respectively, then click Apply to commit.

To add a type:

- Click the Add Token Type Button
- Enter a description
- Select a class from the dropdown list
- Check the Field option
- Click Apply to commit

Confirmation Page

The confirmation page is used to configure messages that will be displayed to the user immediately following token selection.

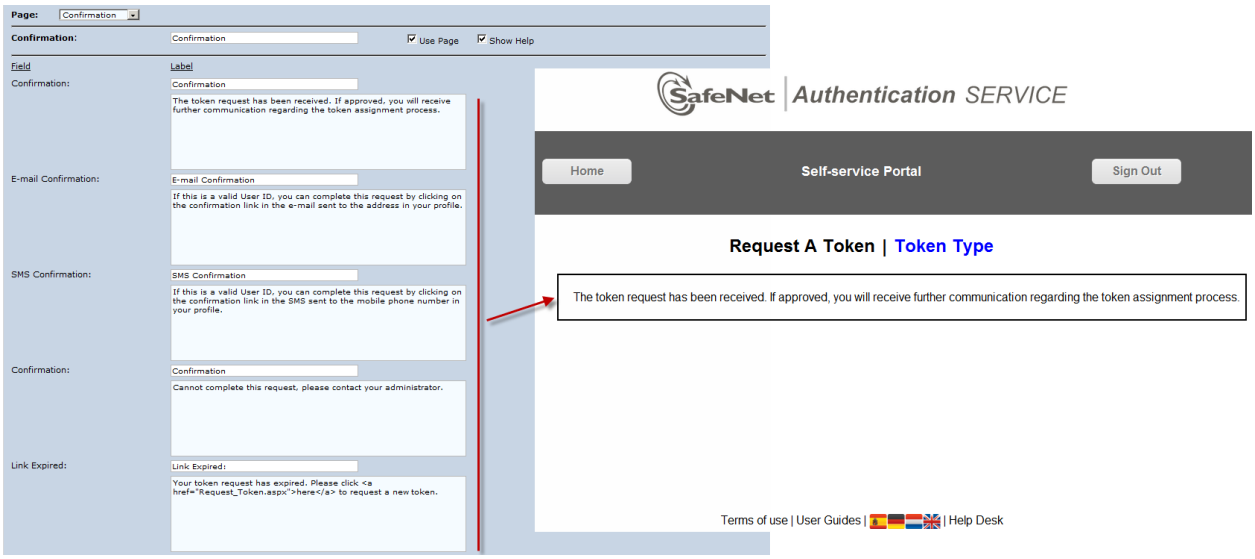


Figure 158: Request a Token - Confirmation Page

Only one of the messages will be displayed, corresponding to the type of validation required/available.

Validation Page

If enabled, the user must confirm their request for a token by replying to a message delivered to them by email and/or SMS. To enable or disable the validation requirement, check or clear the Use Page option, then click the Apply button to commit.

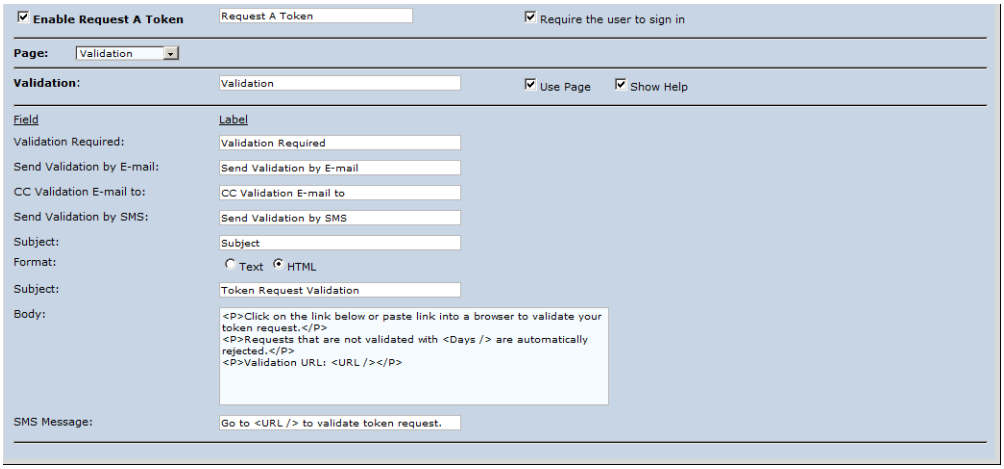


Figure 159: Request a Token - Validation Page

User Page

This page is displayed when the user selections the “I am an Existing User” option. It requires the user to provide their UserID and Sign In to the Self-service portal where:

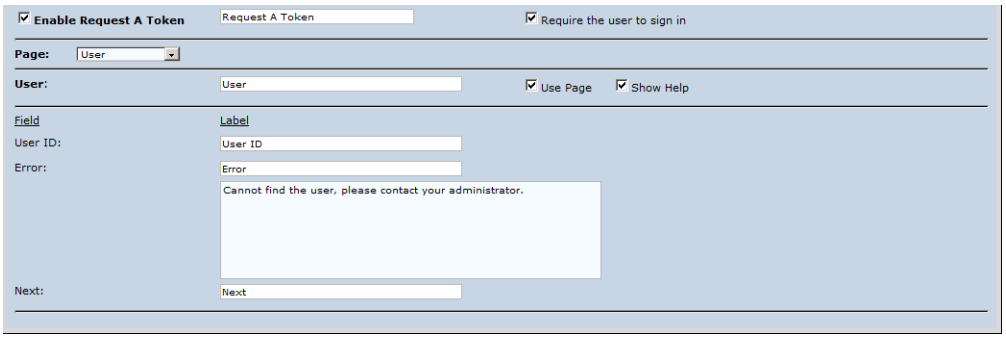


Figure 160: Request a Token - User Page

- **User ID**
  Is the label for the UserID input field
- **Error**
  The error message is displayed if the UserID is not valid.
- **Next**
  Button text

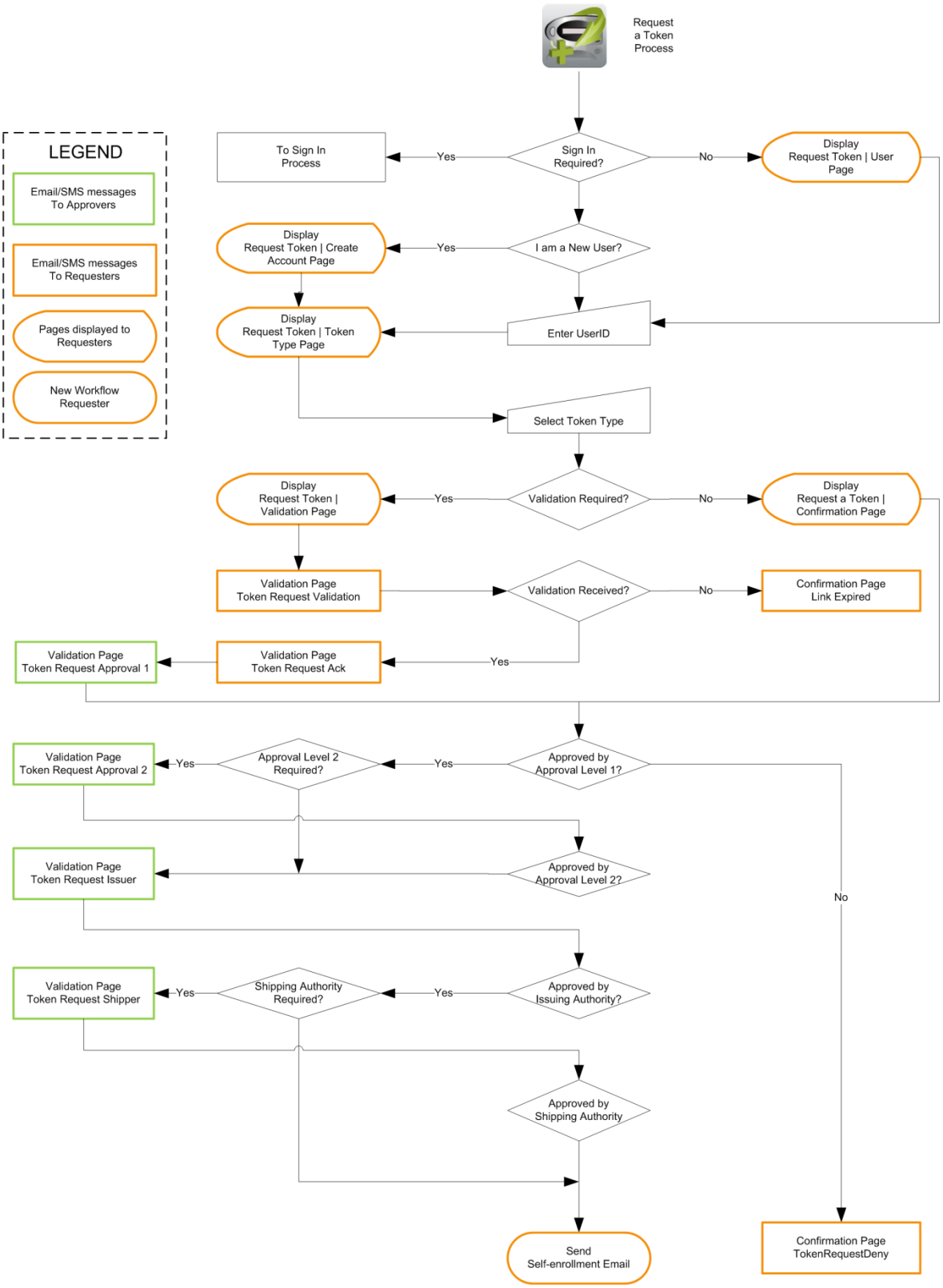


Figure 161: Request a Token Workflow

Reset PIN Module

This module provides the ability for a user to reset the server-side PIN associated with a token assigned to them. There are 5 pages in this module. Each module contains a section for error messages and/or help text.

User Page

This is the content of the first page served to the user when accessing the Reset PIN facilities. If the page is set to require the user to sign in, they will be directed to the Sign In page before being presented with the User Page.

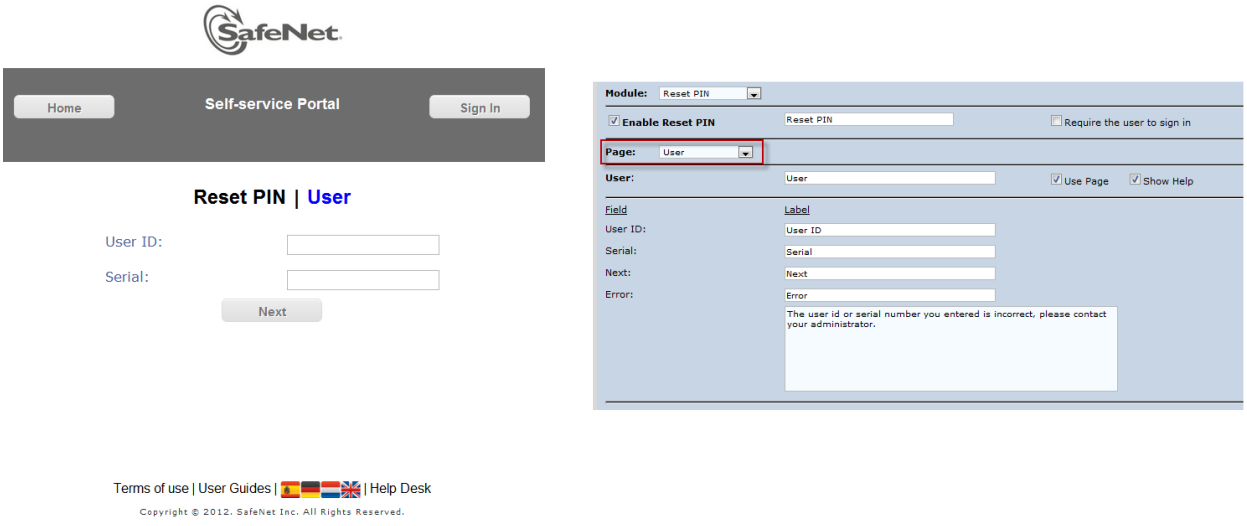


Figure 162: Reset PIN - User Page

Select a Token Page

If a user has more than one token, this page provides a dropdown list from which the user can select the token. PIN reset applies to the selected token.

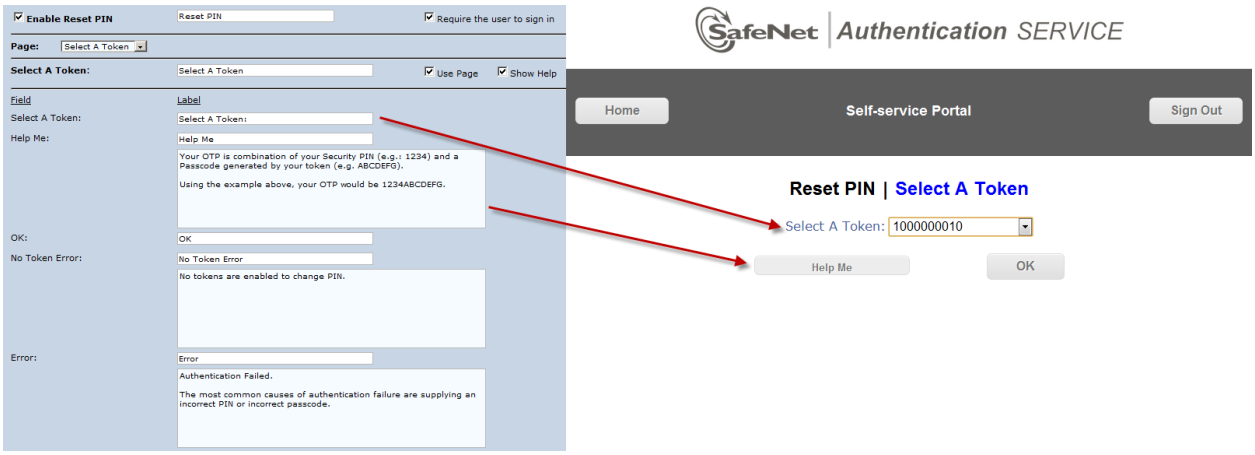


Figure 163: Reset PIN - Select a Token Page

Create New PIN Page

This page is presented when the user has supplied their UserID and the serial number of a token assigned to their account and the PIN associated with the token allows the user to generate a new PIN (i.e. server-side, user select). It requires the user to enter and verify a new PIN.

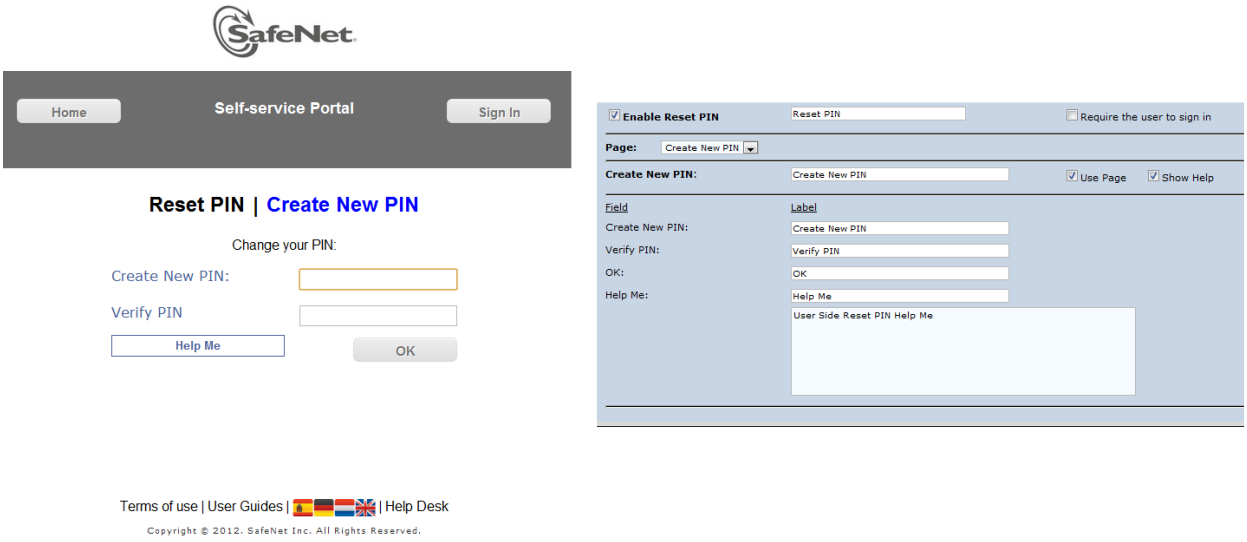


Figure 164: Reset PIN - Create New PIN Page

Server Side PIN Page

This page is displayed if the token issued to a user requires a server-side PIN that is set by the server (i.e. server-side, server select).

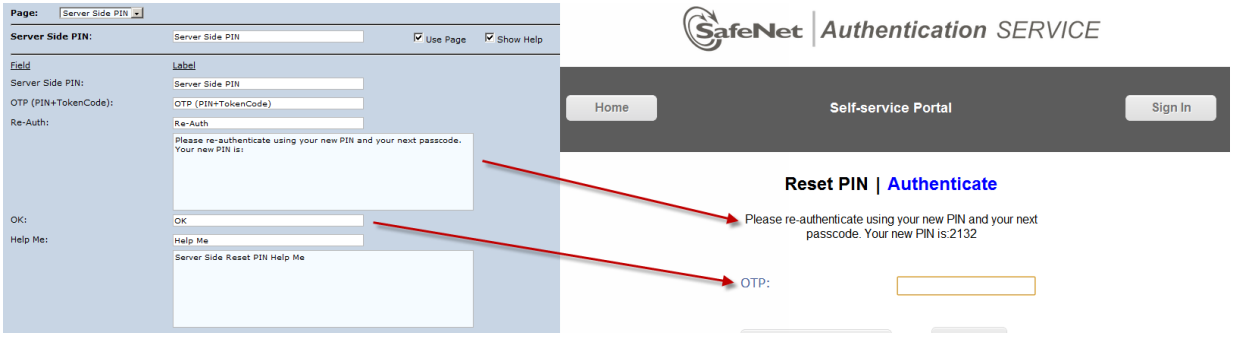


Figure 165: Reset PIN - Server Side PIN Page

Confirmation Page

This page is presented when the user has successfully changed their PIN.

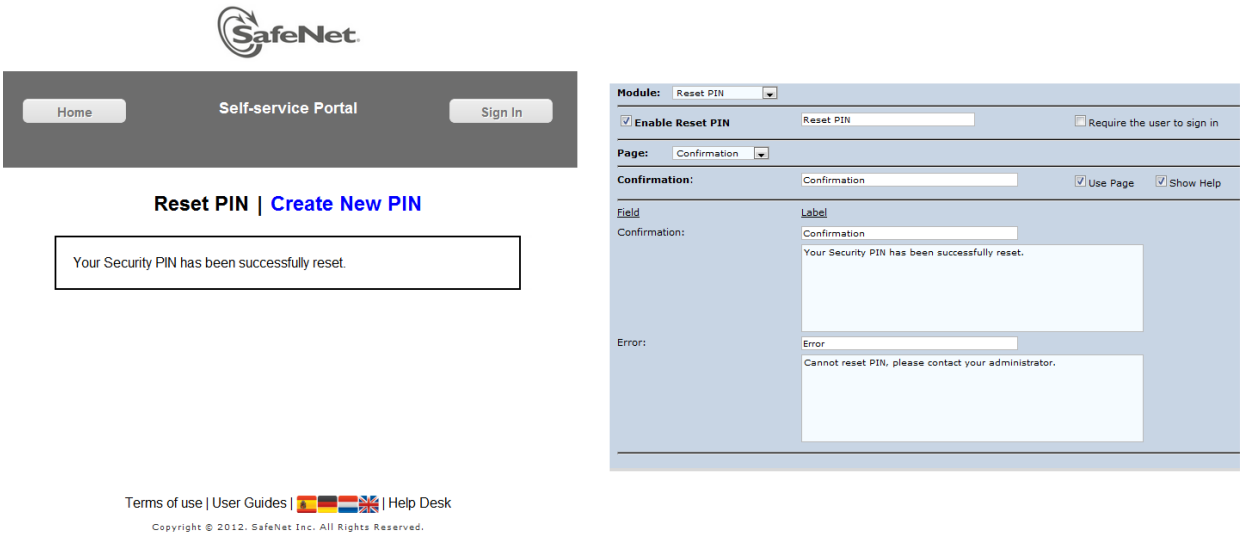


Figure 166: Reset PIN - Confirmation Page

Reset PIP Module

This module provides the ability for a user to reset the PIN associated with their GrID authentication method. There are3 pages in this module. Each module contains a section for error messages and/or help text.

User Page

This is the content of the first page served to the user when accessing the Reset PIP facilities. If the page is set to require the user to sign in, they will be directed to the Sign In page before being presented with the User Page.

If directed to sign in, the user should only provide their UserID. If an OTP field is displayed on the sign in page, it should be left blank. A valid userID and empty OTP field will generate a new page with a GrID and OTP field, allowing the user to authenticate and sign in.

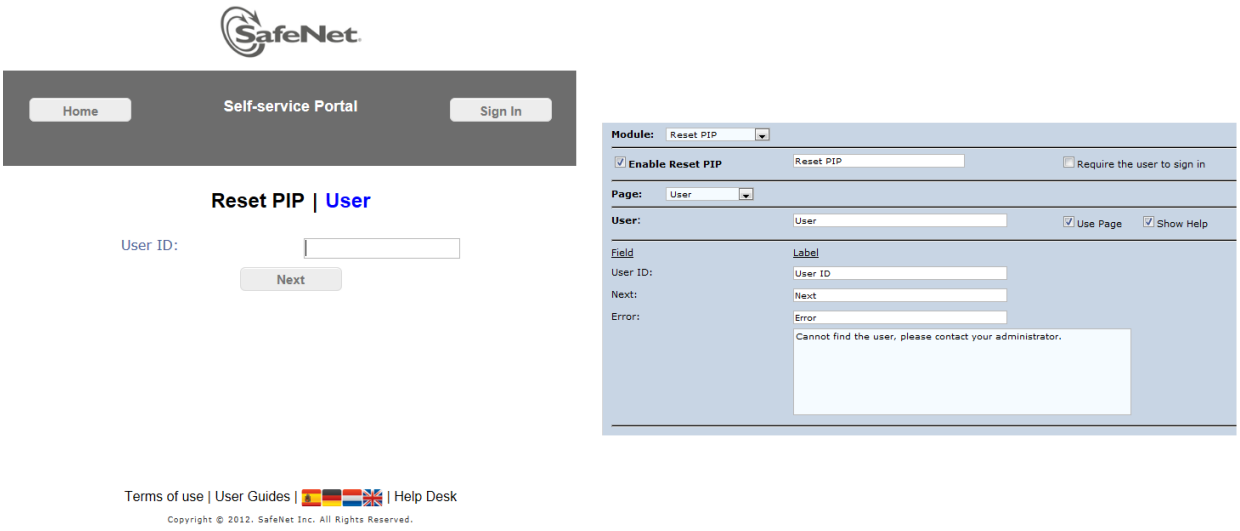


Figure 167: Reset PIP - User Page

Select Pattern Page

This page is presented for a valid UserID provided on the User page and requires the user to authenticate using their current PIP.

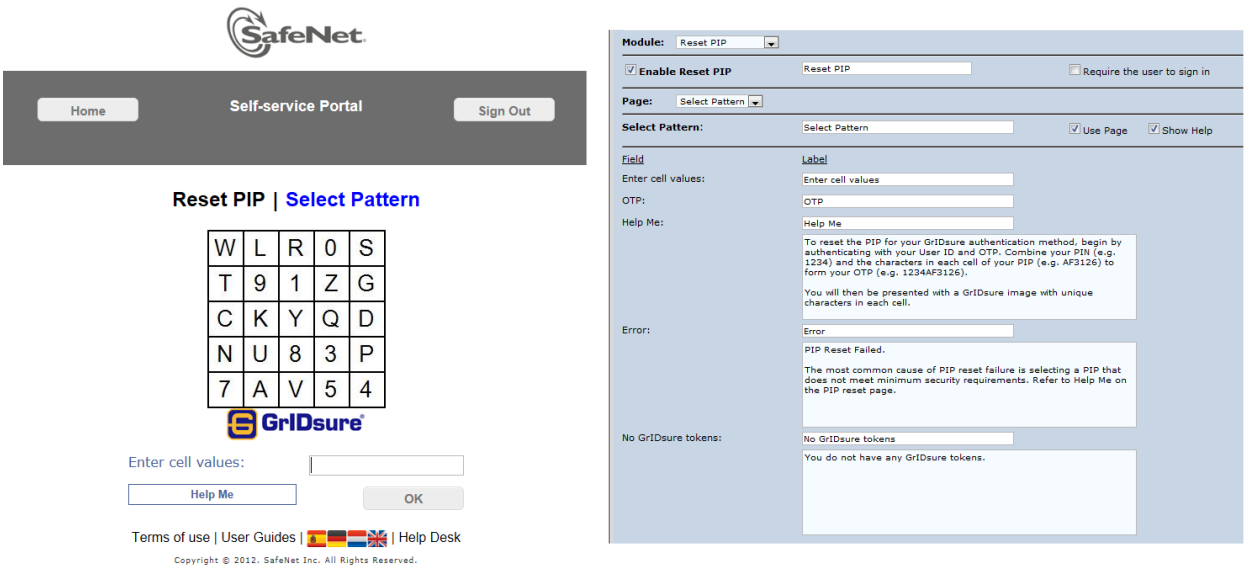


Figure 168: Reset PIP - Select Pattern Page

Confirmation Page

The confirmation page is presented on successfully resetting a PIP.

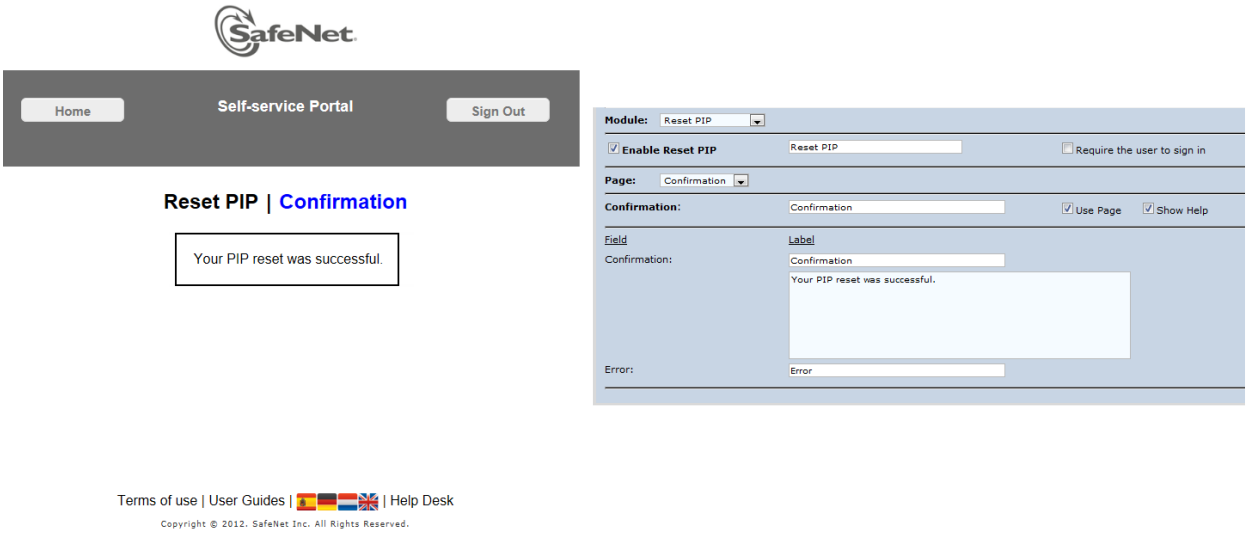


Figure 169: Reset PIN - Confirmation Page

Resync Token Module

This module provides the ability to resync a token with the server and confirm the ability to authenticate with the token. There are 6 pages in this module. Each module contains a section for error messages and/or help text.

User Page

The user page is served up to the user in two parts: the first requires the UserID which if found on the server generates the second part requesting the token serial number.

Figure 170: Resync Token - User Page

Auth Resync Page

This page is presented when the selected token supports resynchronization using 2 consecutive OTPs.

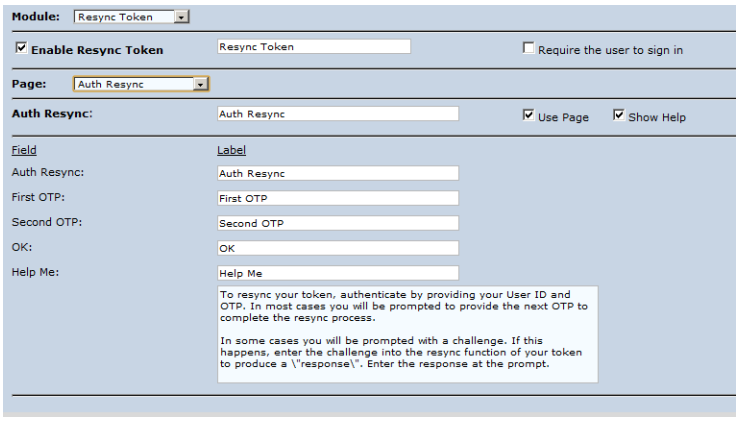


Figure 171: Resync Token - Auth Resync Page

Time-based Resync Page

This page is presented when the selected token is time-synchronous and supports resynchronization using 2 consecutive OTPs.

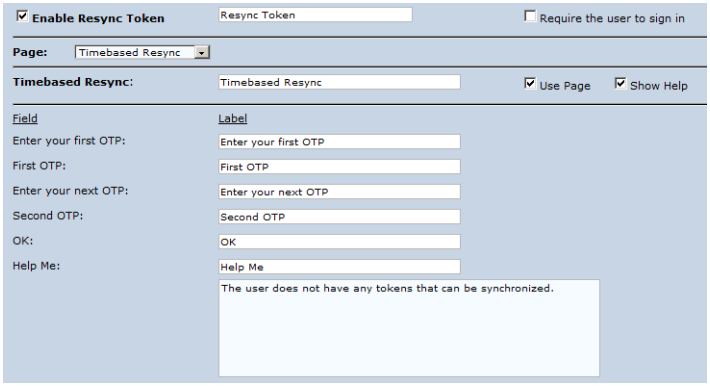


Figure 172: Resync Token – Time-based Resync Page

Challenge Response Page

The challenge/response page is presented when a token fails resynchronization using all other available methods. In this method the user must key the displayed challenge into their token to generate a passcode or “response”, and then enter the response in the indicated field.

Figure 173: Resync Token - Challenge/Response Page

Confirmation Page

The confirmation page displays the outcome of the synchronization attempt whether successful (Confirmation), failed (Error) or not processed (No Token Error).

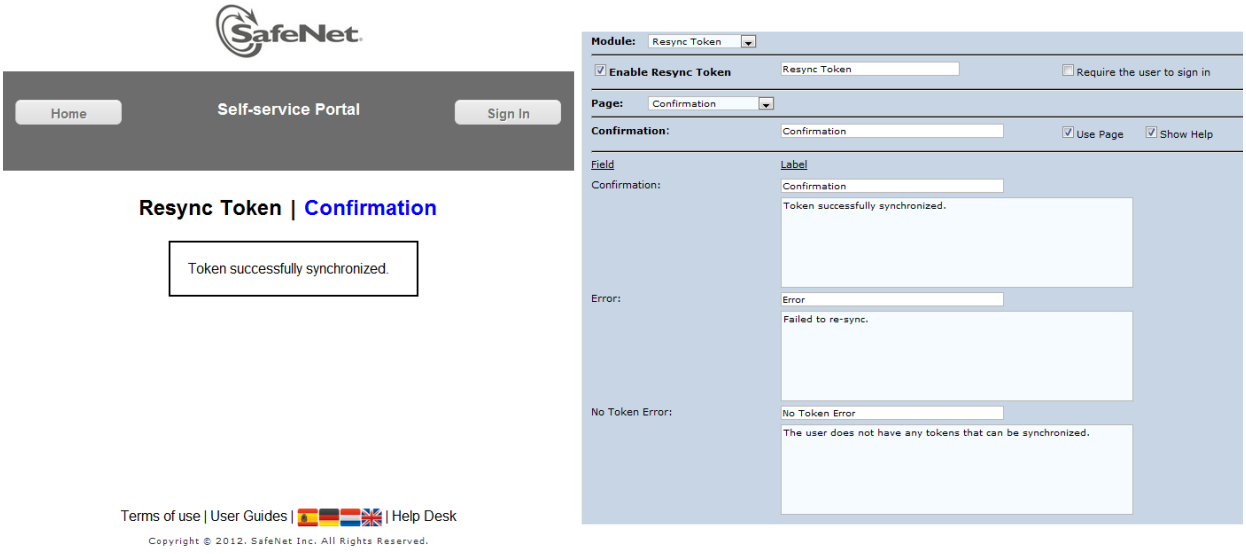


Figure 174: Resync Token - Confirmation Page

Sign In Module

This module provides controls the options for signing into the self-service site. There are 5 pages in this module. Each module contains a section for error messages and/or help text. The Sign In button is replaced with a Sign Out button when a user successfully authenticates to the self-service site.

Authenticate Page

This page presents the allowed methods for authenticating into the self-service site. The remaining pages in this module provide the user experience and process necessary for the method selected by the user.

Figure 175: Sign In - Authenticate Page

Authenticate to Process Page

This page handles authentication using tokens, grids and static passwords. It includes additional prompts to deal with authentication exceptions. In most cases a user authenticating using a token will provide their OTP and gain access to the site. However, it is possible that another policy will be triggered altering this work flow. For example, if there is a server policy that requires the user to change their PIN every 30 days and this happens to coincide with their authenticating to the self-service site, successful authentication will be followed with a requirement to create a new PIN before access to self-service is permitted. This page provides prompts that deal with such situations.

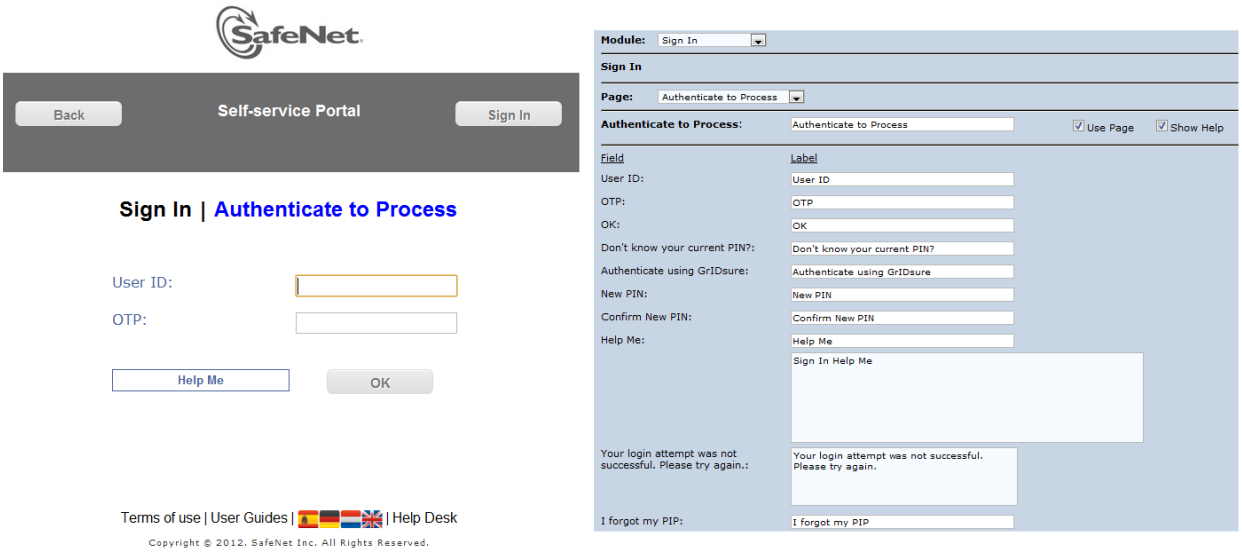


Figure 176: Sign In - Authenticate to Process Page

Send Password by Email Page

This selection sends a one-time password, valid only for the self-service site to the email address associated with the userID. It includes error messages to handle cases where email cannot be sent or the userID cannot be found.

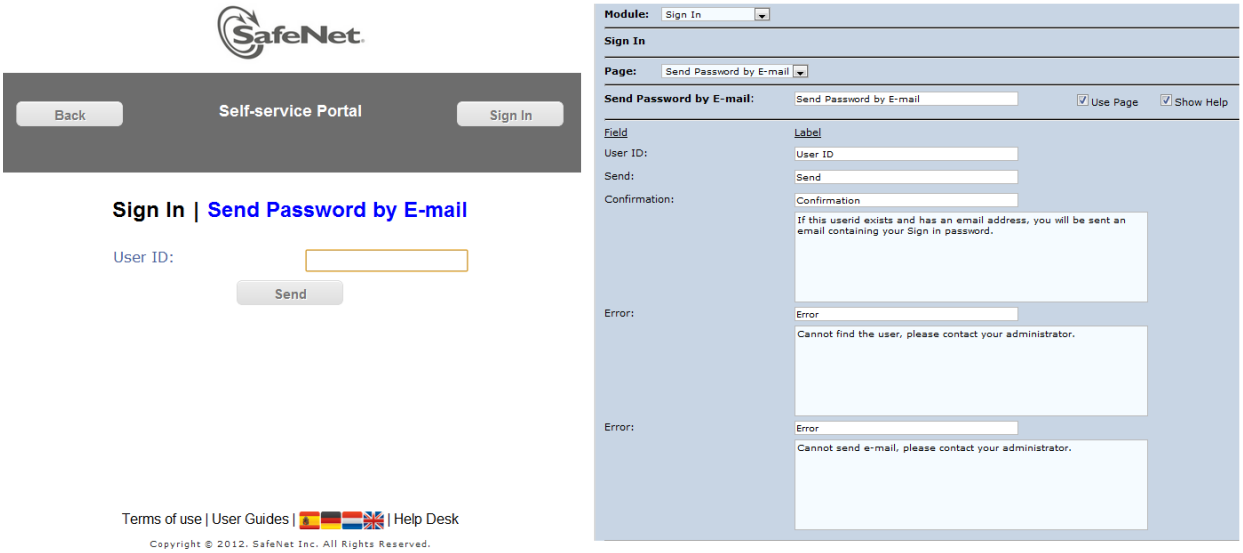


Figure 177: Sign In - Send Password by Email Page

Send Password by SMS Page

This selection sends a one-time password, valid only for the self-service site to the SMS number associated with the userID. It includes error messages to handle cases where SMS cannot be sent or the userID cannot be found.

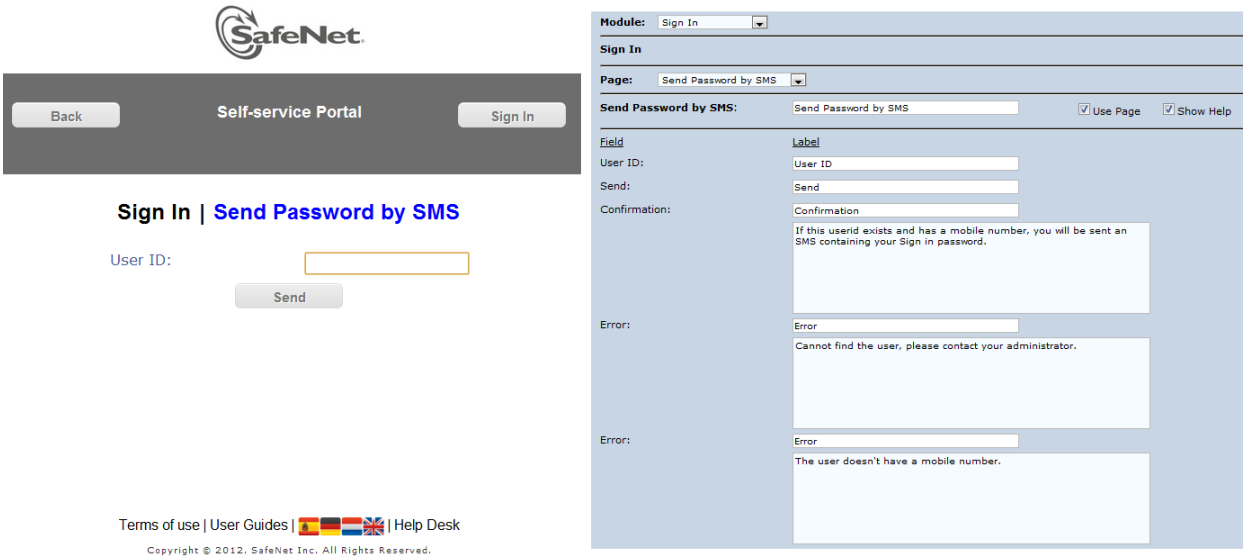


Figure 178: Sign In - Send Password by SMS Page

My Profile Module

This module can allow users to modify basic information about their account such as address, telephone number etc. It also presents basic statics about their authentication activity and allows them to manage challenge/response questions valid (if enabled) for sign on to the self-service site. There are 5 pages in this module. Each module contains a section for error messages and/or help text.

This module requires sign in to the self-service site.

Select to Proceed Page

This is the first page displayed when My Profile is selected by the user.

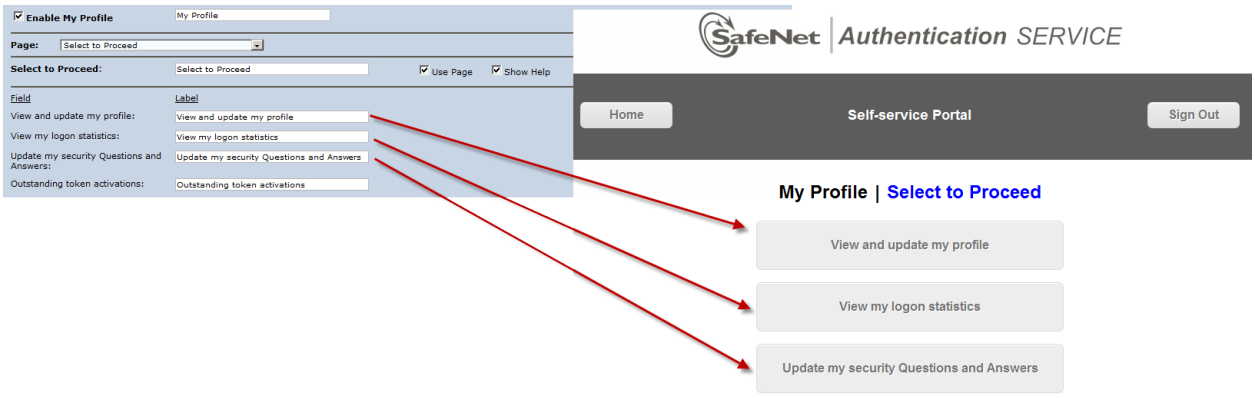


Figure 179: My Profile Module - Select to Proceed Page

View my logon statistics

This displays information about authentication activity by the user including last logon date, number of logons: today, this week this month and this year. This page can be unpublished.

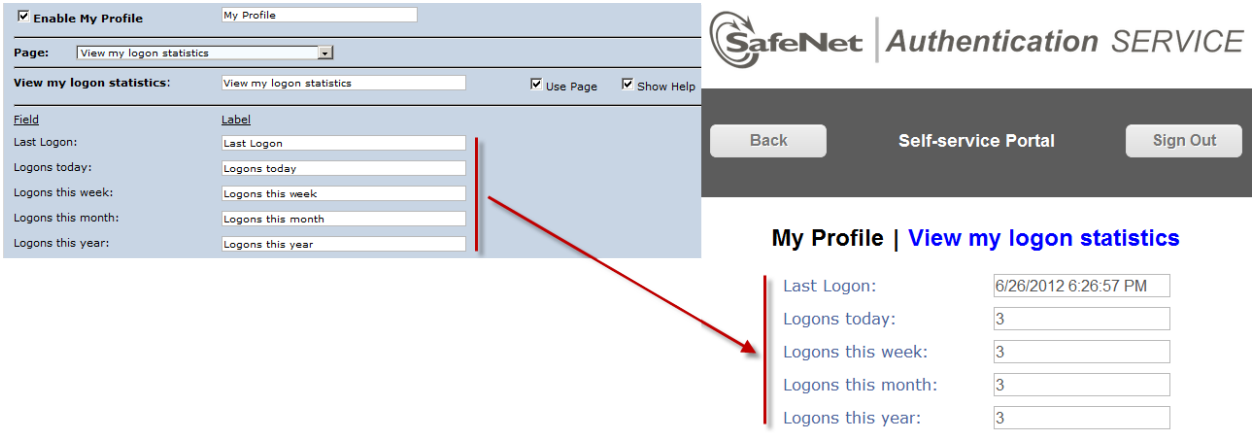


Figure 180: View my logon statistics

View and update my profile

The user can update basic personal information that is stored in the virtual server. Note that this module cannot be used to update information obtained by the virtual server from an external user source such as LDAP. Only users that have been manually created or imported from a flat file can update their information through this module.

This module lists the fields that will accept user input. Some are mandatory (no options), others can be required (made mandatory). It also contains sections for customizing error messages and adding help text relevant to this page.

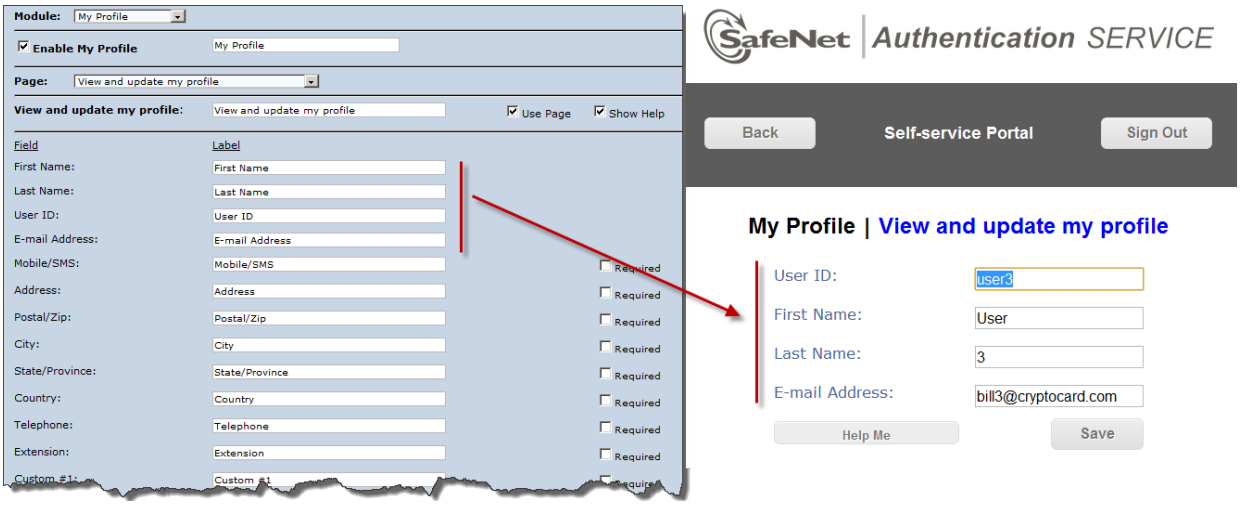


Figure 181: View and update my profile

Update my security Questions and Answers

Security Questions and Answers can be used as an alternative sign-in method for the self-service site. This module allows the administrator to create a series of questions. The user will be required to create a set of answers to these questions. During sign-in the user will have the option of supplying the previously recorded answers to the questions as an alternative sign-in method if this method is enabled. This page can be unpublished.

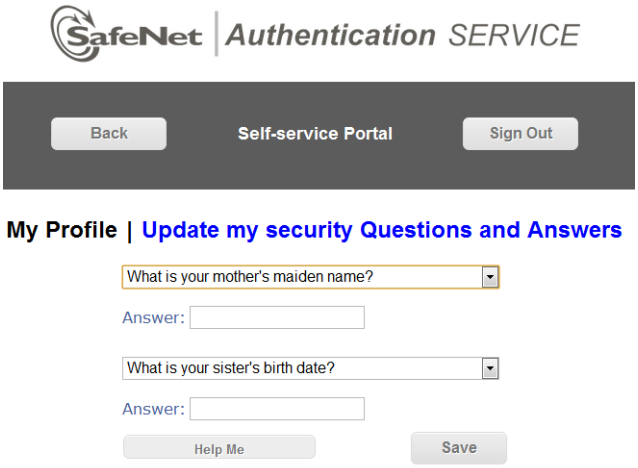


Figure 182: Update my security Questions and Answers.

Question Management Page

Use this page to create questions from which the user will select as an alternate self-service site sign in method.

Figure 183: My Profile Module | Update my security questions and answers | Question Management

In this module:

- **Question Management Dropdown**
  This dropdown provide access to three pages used to configure security question and answers:

- **Question Management**
  Use this page to create questions.

Use the Edit button to modify a highlighted question from the defined question list, including the minimum and maximum answer length, case sensitivity and trivial answer control options.

Use the Add button to add a question created in the “Question” field to the Defined Questions list.

Question Sets Page

Use this page to define the number of question groups that will be displayed to the user. Users must answer one question from the list of questions contained in a Question Set.

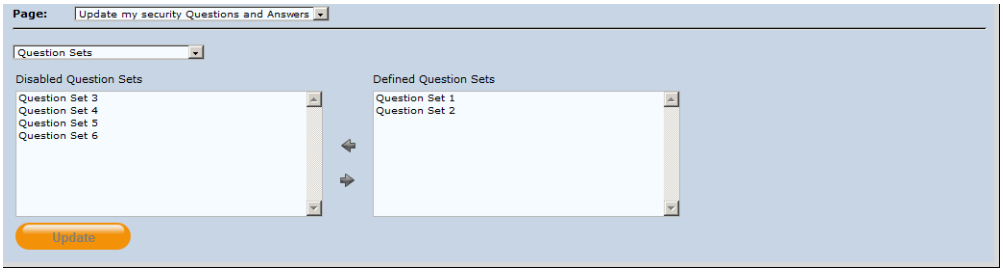


Figure 184: My Profile Module | Update my security questions and answers | Question Sets

Use the arrows to add or remove question sets to or from the Defined Question Sets list. Sets in this list are displayed to the user.

Question Assignment

Use this page to group questions created in Question Management into one or more of the sets enabled in Question Sets.

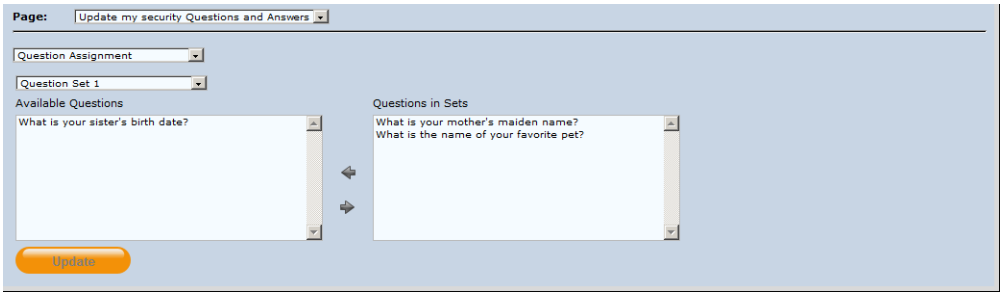


Figure 185: My Profile Module | Update my security questions and answers | Question Assignment

To add one or more questions to a set, select the set from the dropdown list, then using the arrows move the questions to be included in the set to the Questions in Sets list, then click the Update button to commit the change.

- **Minimum answer length**
  Sets the minimum number of characters allowed as an answer.
- **Maximum answer length**
  Sets the maximum number of characters allowed as an answer.
- **Answers are case sensitive**
  If checked, answers are case sensitive.
- **Disallow trivial answers**
  If checked, answers comprised of triplets (e.g. 111, aaa) or 3 character sequential strings (e.g. 123, abc) are disallowed.

Use the Add button to add questions to the list. To edit or remove a question, highlight it in the list then click the Edit or Remove button respectively.

Configure Self-Enrollment Pages

Self-enrollment pages are presented to the user allowing enrollment, binding of the token to the user and activation of the token. Different token types and authentication methods require different enrollment steps. This module contains a page for each enrollment process. There are 5 pages in this module.

My Token Request

This page displays a list of outstanding token requests.

Default/Common Page

This page contains elements that are used in all enrollment processes. The use of these elements varies depending on the token type and enrollment process. For example, UserID and Activation code may be prompts on an enrollment page or may be used as labels in enrollment emails/SMS message

In any case these prompts should be translated for each language set to be supported on the self-service site.

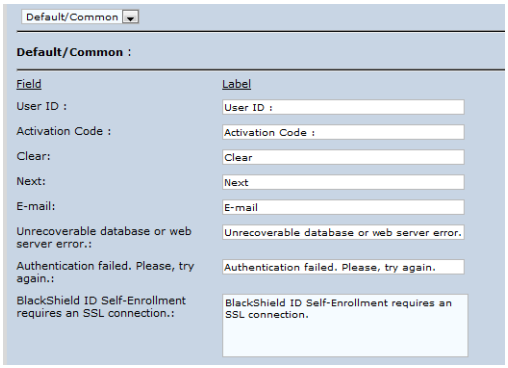


Figure 186: Self-Enrollment - Default/Common Page

Software Token Page

This is a very lengthy page which contains all of the prompts, error messages and instructions for enrolling MP-1 software tokens for each of the possible target devices (iOS, Android, BlackBerry, JAVA, Windows, OS X…)

These prompts and messages should be translated for each language set to be supported on the self-service site.

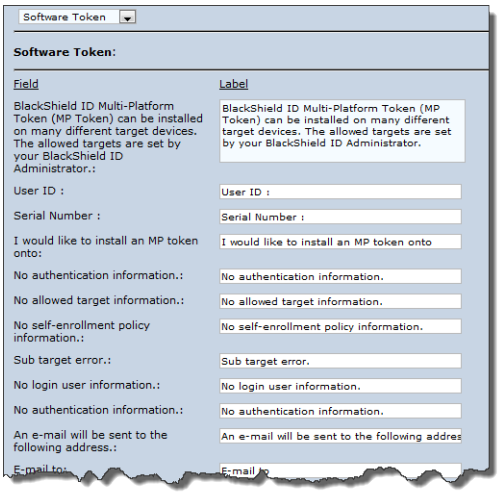


Figure 187: Self-Enrollment - Software Token Page

Custom Token Page

This page contains all of the prompts, error messages and instructions for enrolling custom tokens.

These prompts and messages should be translated for each language set to be supported on the self-service site.

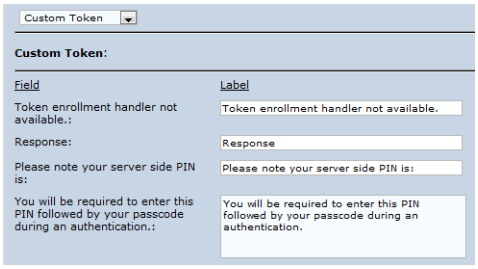


Figure 188: Self-Enrollment - Custom Token Page

Hardware Token Page

This is a very lengthy page which contains all of the prompts, error messages and instructions for enrolling hardware tokens (RB-1, KT-x, eTokenPass, RADIUS Tokens, 3rd party tokens)

These prompts and messages should be translated for each language set to be supported on the self-service site.

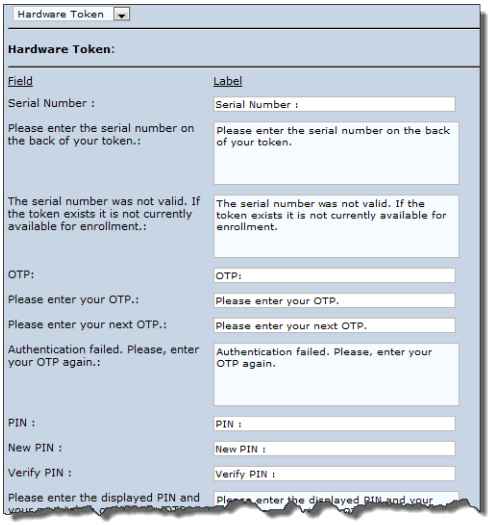


Figure 189: Self-Enrollment - Hardware Tokens Page

Password Page

This page contains all of the prompts, error messages and instructions for enrolling a static password.

These prompts and messages should be translated for each language set to be supported on the self-service site.

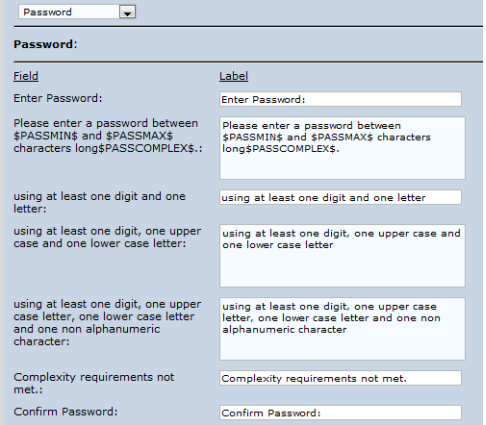


Figure 190: Self-Enrollment - Password Page

Self-Service Authorities Module

Authorities are special privileges assigned to Operators for the purpose of managing user requests for tokens received from the Self-service site. There are four possible Authorities:

- **Approval Level 1**
  This authority approves or denies user requests for tokens received from the Self-service site. At least one Operator must have this authority if the Request a Token module is enabled on the self-service site.

- **Approval Level 2**
  This authority approves or denies user requests for tokens that have been approved by Approval Level 1 authorities. This is an optional authority.

- **Issuing Authority**
  Requests for tokens that have received the required approvals are fulfilled by the Issuing Authority. This function is the equivalent of using the “Provision” functions available on the Assignment tab unless a Shipping Authority has been created. At least one Operator must have this authority if the Request a Token module is enabled on the self-service site.

- **Shipping Authority**
  The Shipping Authority is a special function that serves two purposes:

  - It can be used to coordinate the delivery of enrollment instructions with receipt of the physical token by the user.

  - It can be used to increase the security of enrollment by requiring the user to provide an additional code during enrollment that is delivered separately and Out-of-Band (“OOB”) with respect to all other enrollment instructions.

    Shipping authorities are applied by token type. Token requests for affected token types that

have been approved by the Issuing Authority must be completed by the Shipping Authority. This is an optional authority.

Configuring Authorities

Begin from the Configuring Self-Service module | Self-service Authorities hyperlink. This will display a list of Operators that can be assigned one or more authorities. To enable an authority for an Operator, place a check in the appropriate authority option, then click the Apply button to commit.

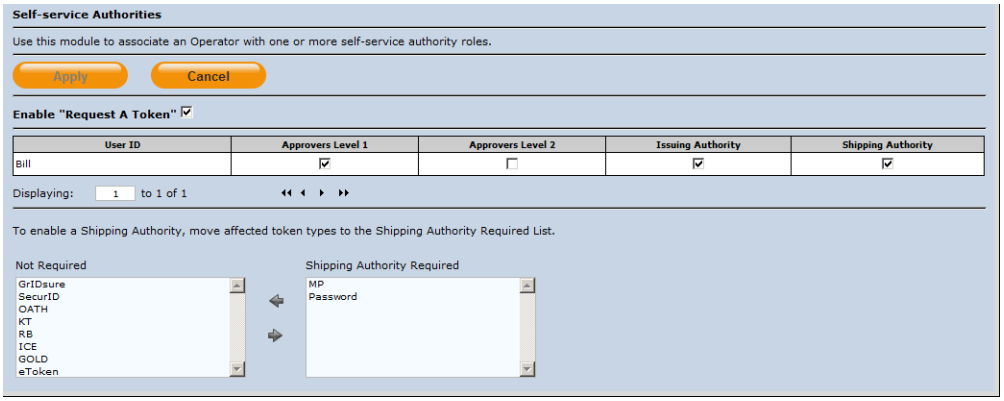


Figure 191: Configure Self-Service Authorities

At least one Approval Level 1 and Issuing Authorities are must be enabled.

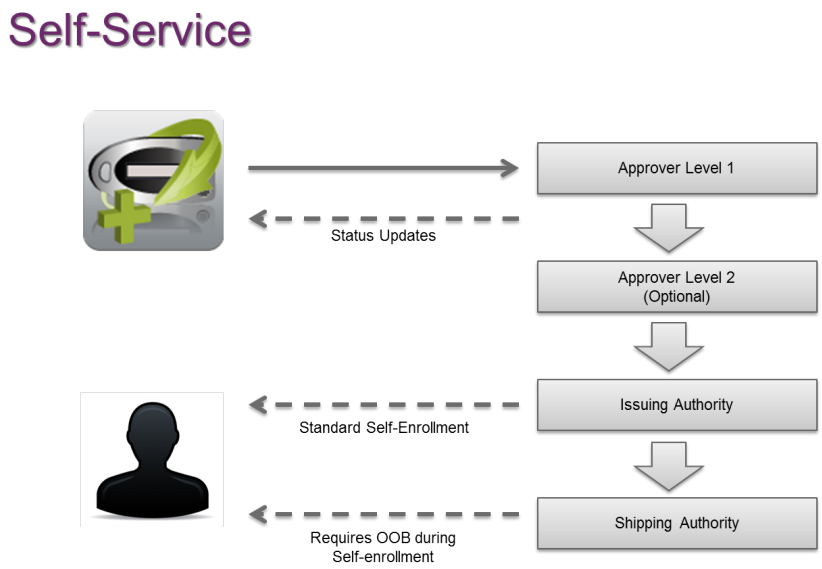


Figure 192: Self-Service Workflow

To add a shipping authority to a token type, first ensure that at least one Operator has been given this authority. (Refer to Configuring Authorities on page 188). Next select the token type from the “Not Required” window and using the arrow, move it to the “Shipping Authority Required” window. Repeat this step for each token type that will require a shipping authority.

Out of Band Notification

Out of Band (OOB) notification requires that the user provide an additional factor during enrollment to further validate their identity. This normally is in the form of an activation code. The code can be delivered by email, SMS or output to a file.

OOB can be used with both hardware and software tokens. To enable OOB, select the tokens to which it will apply and the activation code delivery methods, then click the Apply button to commit.

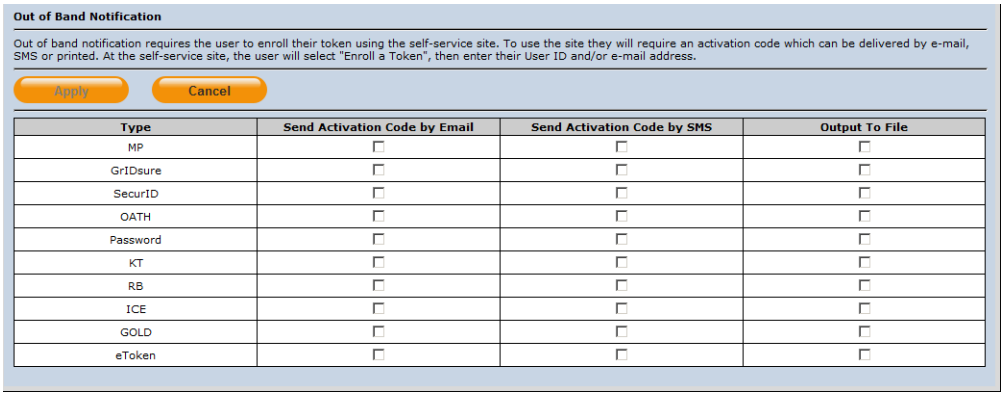


Figure 193: Out of Band Notification

Request and Approval Queue Processing

This module contains a page for each of the messages that will be sent to the user and each of the authorities during the approval and provisioning processes. The intent is that both users should be kept informed of the status of the request and authorities should be notified when action is required of them.

Each message has an enable/disable option. If enabled, the message is sent at the appropriate point in the process. If disabled, the message is not sent.

Configure Request and Approval Queue Processing

The following configuration options are available in this module:

- **Auto-delete unapproved requests after X days**
  If set to 0, unapproved requests will not be automatically removed from the Approval queue. Any other value will automatically remove an unapproved request the indicated number of days after it was received. Note that

- **Allow approval by Email / SMS**
  Check the delivery method(s) the system will use to send status and action alerts to Authorities. If none are checked, status and action alerts will not be sent but the request will be listed in the appropriate Queue (refer toQueue Management Module on page 191)

This module contains several notifications. Use the dropdown in the Configure Queue Processing section to select the message. Each message has 3 sections: 2 for email (Subject, Body) and one for SMS (SMS Content). Most messages contain variables (example: <email />) that must not be removed or modified. Otherwise, modify any other element of each notification according to your needs.

Keep in mind the 160 character limit (including white space) in SMS messages. To prevent a multi-part SMS message avoid exceeding this limit.

Click “Apply” after each message modification to commit the change.

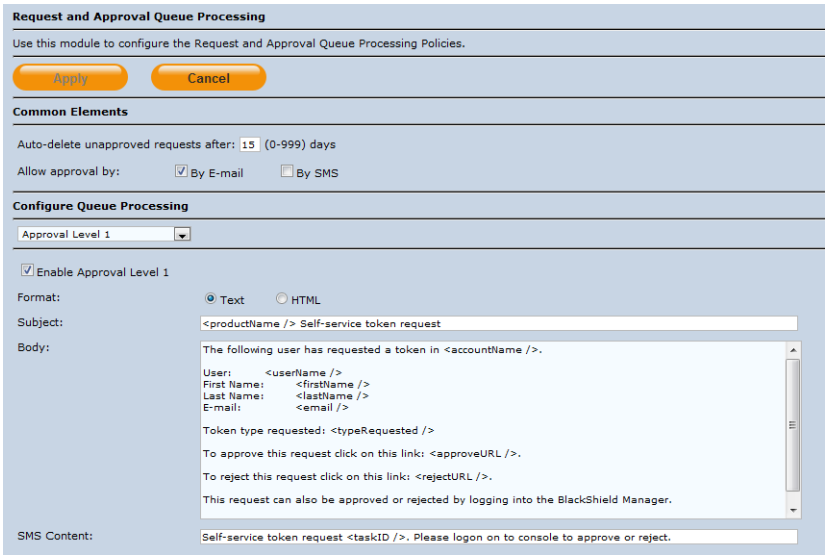


Figure 194: Request and Approval Queue Processing

Queue Management Module

The queue management module provides the interface for each of the Authorities to process requests. Use the State dropdown to select the Authority Queue to be view. Note that an Operator is not able to view a queue for which he does not have the corresponding Authority.

Select a request State from the dropdown then click Search to update the list for the selected state.

All queues have a list containing requests waiting processing. Each row in the list shows:

- **Request ID**
  This is a unique number that identifies this request through all of the queues. As soon as a request has been issued, a provisioning task is created using the same ID number. Provisioning tasks track the user's enrollment activity.
- **Submit Date**
  This is the date/time the user submitted the request.
- User ID
  This is the userID associated with the request. Click the hyperlink to view information about the user. This will correspond with the data for this userID found in the Assignment Tab | User Detail module.
- **First Name**
  This is the user's first name.
- **Last Name**
  This is the user's surname.
- **Email**
  This is the email address associated with this user.
- **Token Type**
  This is the token type requested by the user.
- **Process State**
  This indicates the state of the request. Currently the only option is Pending Approval.

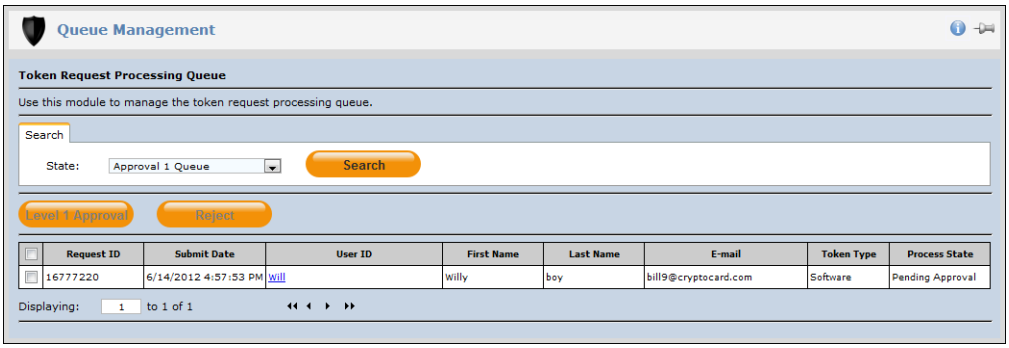


Figure 195: Queue Management

Approval Level 1

Displays a list of all requests awaiting this approval. Select one or more requests then click Level 1 Approve or Reject to approve or reject the request respectively.

- If the request is approved and Approval Level 2 is enabled, the request will be removed from this list and appear in the Approval Level 2 queue, otherwise it will appear in the Issuer queue.
- If enabled, the user will receive a Request Approved or Request Rejected notification corresponding to the Authorities decision. If approved and enabled, the next Authority in the processing sequence will receive a notification.

Approval Level 2

Displays a list of all requests awaiting this approval. Select one or more requests then click Level 2 Approve or Reject to approve or reject the request respectively.

- If the request is approved the request will be removed from this list and appear in the Issue queue.
- If approved and enabled, the next Authority in the processing sequence will receive a notification.

Issue

Displays a list of all requests awaiting this approval. Select one or more requests then click Issue Approve or Reject to approve or reject the request respectively.

- If the request is approved and Shipping Authority is enabled for the requested token type, the request will be removed from this list and appear in the Shipping queue, otherwise the enrollment messages will be sent to the user.
- If approved, a Provisioning Task will be created. The task tracks the status of the enrollment, including enforcement of enrollment policies such as last date to enroll.

Shipping Queue

Displays a list of all requests awaiting this approval. Select one or more requests then click Issue Approve or Reject to approve or reject the request respectively.

- The must receive an out of band activation code/instructions. The method of delivery is determined by the selection by token type.
- If approved, a Provisioning Task will be created. The task tracks the status of the enrollment, including enforcement of enrollment policies such as last date to enroll. Tasks may be view from the Assignment Tab | Provisioning Tasks hyperlink (Shortcuts).

Reporting

Token requests data and related workflow activity is recorded in the database. A number of reports are available to extract this data:

- Token Requests Report
  This report captures all requests and their progress through the workflow including:
  - Request ID
  - User ID
  - First Name (user)
  - Last Name (user)
  - Email (user)
  - Token Type (requested)
  - Request State (Approval 1, Approval 2, Issue, Ship)
  - Request Date
  - Approval Date
  - Approved By
  - Issued Date
  - Issued By
  - Shipped Date
  - Shipped By

Other relevant reports are the Provisioning Task Attempts, Provisioning Tasks and Provisioning Tasks Outstanding reports. Refer to the Administrator Guide for additional information.

Operators Tab

Virtual Servers are managed by “Operators” of which there are two types:

- **Internal Operators**
  These are user accounts in the Virtual Server that have been promoted to Operator status.

- **External Operators**
  This is an Operator account created for the Service Provider allowing Service Provider management access to the Virtual Server.

Both types of Operators are managed from the Operators tab.

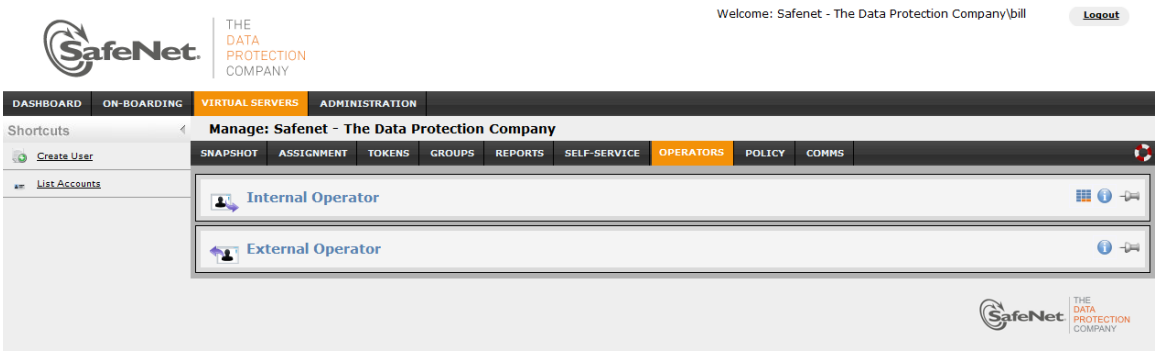


Figure 196: Operators Tab

Internal Operators Module

Any user added to a Virtual Server to which you’ve assigned a token or password can be promoted to Internal Operator, allowing them to log into and perform management functions. Operators appear in the Internal Operator list.

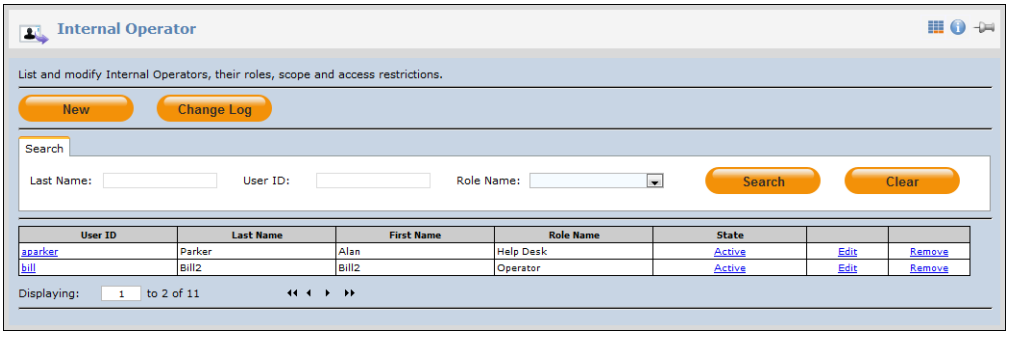


Figure 197: Internal Operators Module

Each row in the list shows:

- **User ID**
  This is the User ID of the Operator. Click the hyperlink to reveal additional user detail.

- **Role Name**
  This is the role assigned to the Operator. Roles determine what an operator is able to do through the management UI.

- **State**
  There are 3 possible states:

- Pending Validation – User has not yet validated their email address.

- Active – Operator is able to logon to the management UI. Click the state hyperlink to Suspend.

- Suspended – Operator account has been suspended. Click the state hyperlink to Re-activate.

- **Edit**
  Click this hyperlink to edit the Operator's role, scope and access restrictions.

- **Remove**
  Click this hyperlink to remove this user as an Operator.

  Operators cannot modify their own role, scope or access restrictions.

Adding an Internal Operator

To add an Internal Operator, begin by clicking the New button in the Internal Operator module. This will produce a list of users that are eligible for promotion to Operator status. Use the Last Name and/or UserID criteria and the Search button to refine the list. Click Next to select a Role.

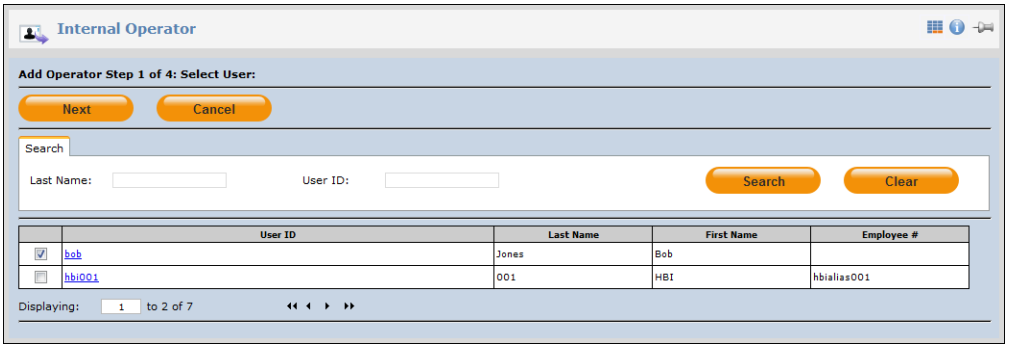


Figure 198: List of Potential Operators

You can select multiple users for promotion, bearing in mind that the same Role, Scope and Access Restrictions will be applied to all selected users.

Assign a Role

Roles determine the task an Operator can perform (refer to Role Management Policy on page 225) Select a Role, and then click Next.

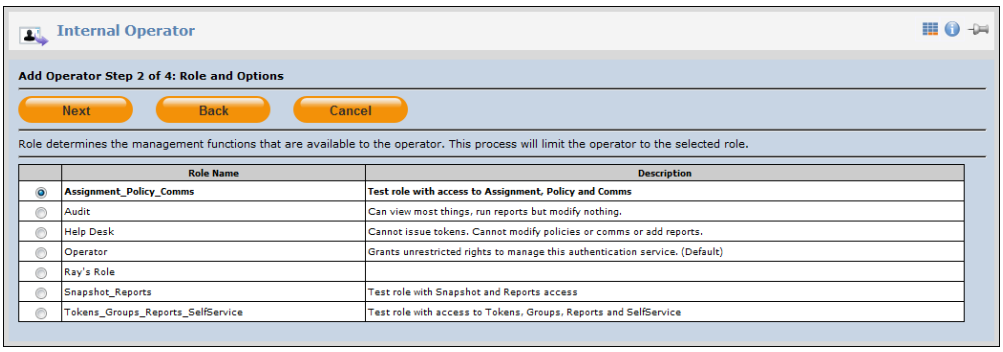


Figure 199: Assign Operator Role

Assign Scope

Containers define an Operator's Scope - what it is they can manage. If a Container is not in an Operator's Scope, then all of the objects in the container are also not in Scope and consequently cannot be viewed or managed by the Operator. Select one or more Containers from the list, and then click Next.

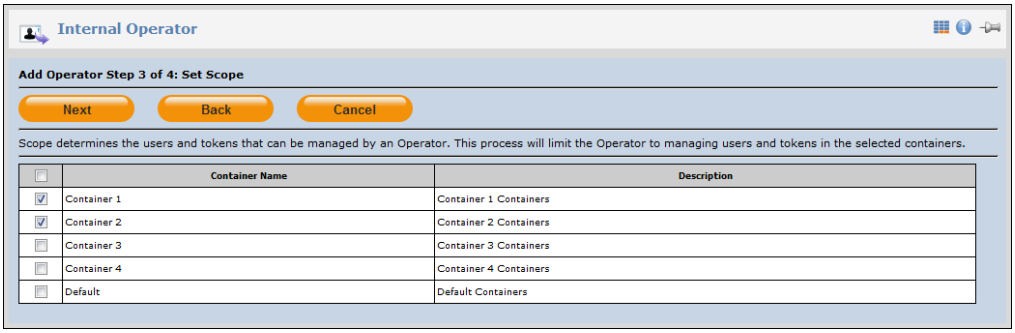


Figure 200: Assign Scope

Access Restrictions

Access Restrictions are used to limit when an Operator is allowed to log into the Virtual Server management UI. If no restrictions are to be applied, click Finish, else enable restrictions then click Finish.

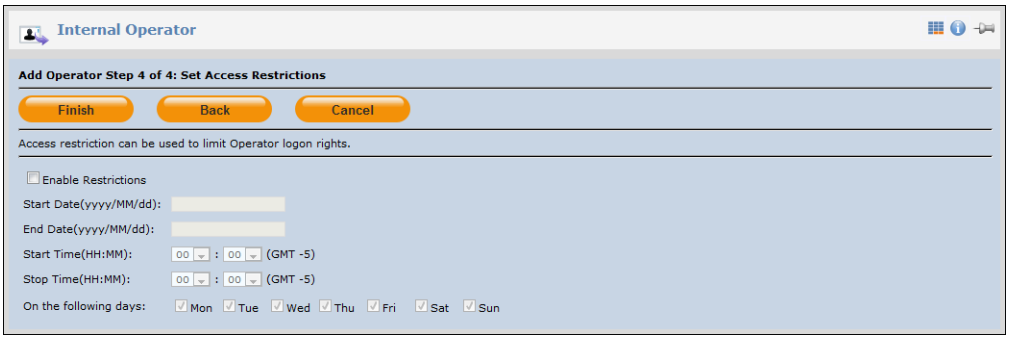


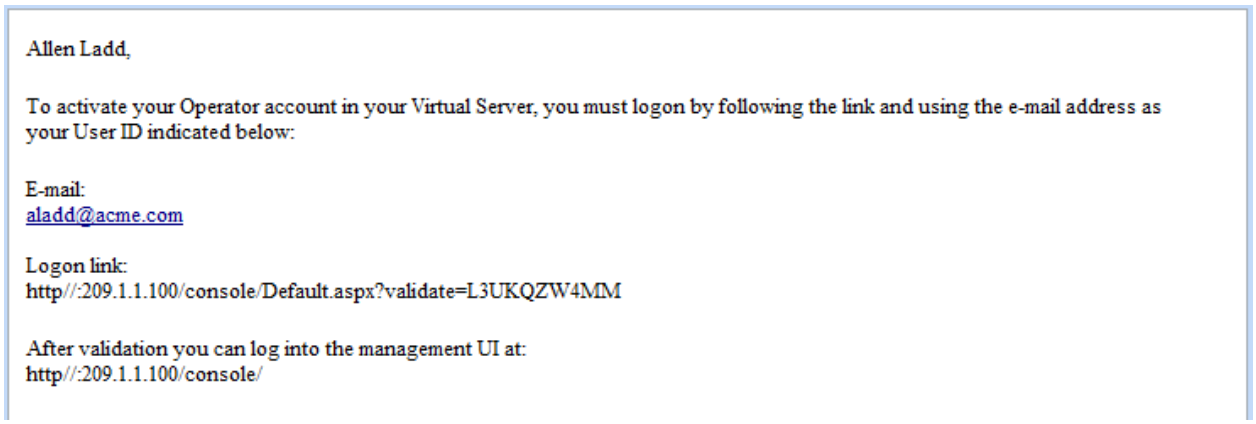
Figure 201: Assign Access Restrictions

If Access Restrictions are required, begin by clicking the Enable Restrictions option, then:

- **Start Date**
  Operator cannot log into the Virtual Server management UI prior to this date.
- **End Date**
  Operator cannot log into the Virtual Server management UI after this date.
- **Start Time**
  Operator cannot log into the Virtual Server management UI prior to this time of day.
- **Stop Time**
  Operator cannot log into the Virtual Server management UI after this time of day.
- **On the following days**
  Operator logon is restricted to the checked days of the week.

Operator E-mail Validation

Operators log into the management UI using the e-mail address associated with their UserID. Before an Operator can logon, they must confirm they own the email account to which the validation message is sent.


Allen Ladd,

To activate your Operator account in your Virtual Server, you must logon by following the link and using the e-mail address as your User ID indicated below:

E-mail:
aladd@acme.com

Logon link:
http//:209.1.1.100/console/Default.aspx?validate=L3UKQZW4MM

After validation you can log into the management UI at:
http//:209.1.1.100/console/

Figure 202: Customizable Operator E-mail Validation

Note that a validation message will be resent if the Operator's e-mail address associated with their UserID changes.

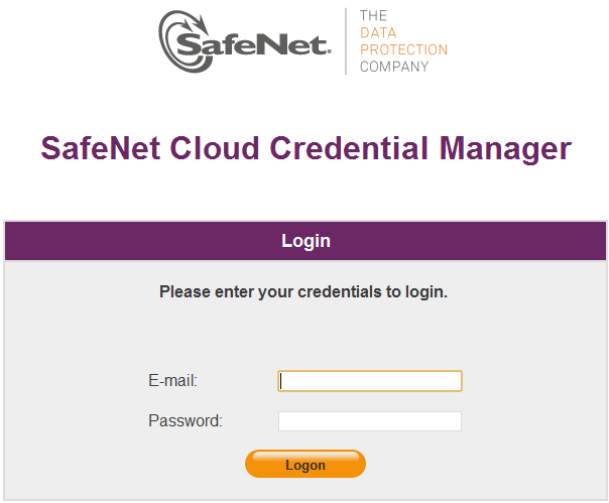


Figure 203: Management UI Remote Logon

External Operator Module

An external Operator is an account that is automatically created for the Service Provider when the Virtual Server is created. It is through this account that Account Managers are able to access the account's Virtual Server (via the Virtual Servers tab).

As with Internal Operators, External Operators have an assigned role, which by default is "Operator", allowing access to all of the Virtual Servers tabs, modules and actions.

A role other than "Operator" can be assigned to an External Operator. By applying a different role, the account can limit the functionality available to the Service Provider through the UI, including denying access to the Virtual Server. To prevent this, the Service Provider must modify all Internal Operator roles to deny access to the External Operator module.

All External Operator activity is recorded in the Virtual Server for audit and reporting purposes.

An additional External Operator account is created for each Service Provider account to which management of the Virtual Server has been delegated. External Operator accounts can have different roles.

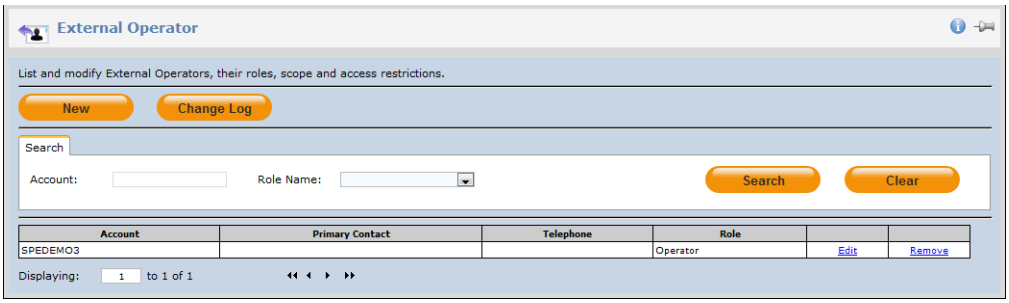


Figure 204: External Operator Module

In the External Operators List:

- **Account**
  This is the name of the Service Provider account.
- **Primary Contact**
  This field is populated using information provided in the Primary Contact field in the Services module on the On-Boarding tab.
- **Telephone**
  This field is populated using information provided in the Primary Contact field in the Services module on the On-Boarding tab.
- **Role**
  This is the role assigned to the External Operator account. refer to Role Management Policy on page 225
- **Edit**
  Allows an Internal or External Operator with sufficient rights to modify the role assigned to this account.
- **Remove**
  Allows an Internal or External Operator with sufficient rights to modify the role assigned to this account.

Note that Operators cannot modify or delete their own role.

Delegation is most commonly used in a multi-tier sales and service model, where the intermediary sales channel On-boards the account but does not have the capacity or business interest to manage the

account's Virtual Server. If the delegation option is selected in the Service Module (On-Boarding Tab), then two External Operator accounts are automatically created, one for the Service Provider and one for the delegated Service Provider.

Adding an External Operator Account (Delegation)

An external operator account can be created for each Service Provider to which management of the Virtual Server should be delegated. Each Service Provider account must provide a delegation code (refer to Delegation Code Module on page 61). This code will be used to create an external Operator account for their exclusive use.

To add an external operator account, begin by clicking the "New" button.

Figure 205: Add External Operator

Enter the delegation code provided by the Service Provider, and then click verify and confirm the Service Provider name in the Managing Account field, and then click Next.

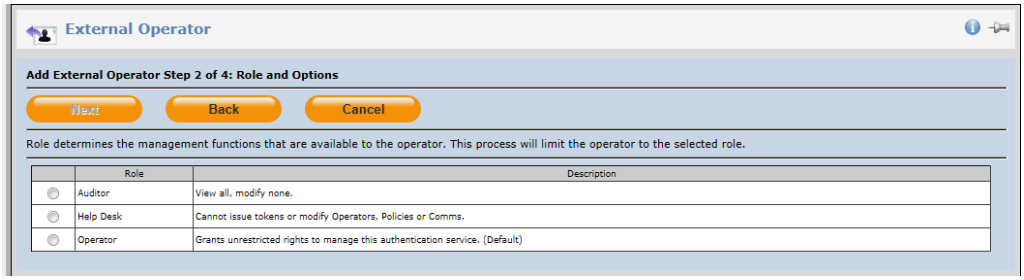


Figure 206: Assign External Operator Role

Select the role (for more detail on roles, refer to Role Management Policy on page 225) to be applied to this account, and then click Next.

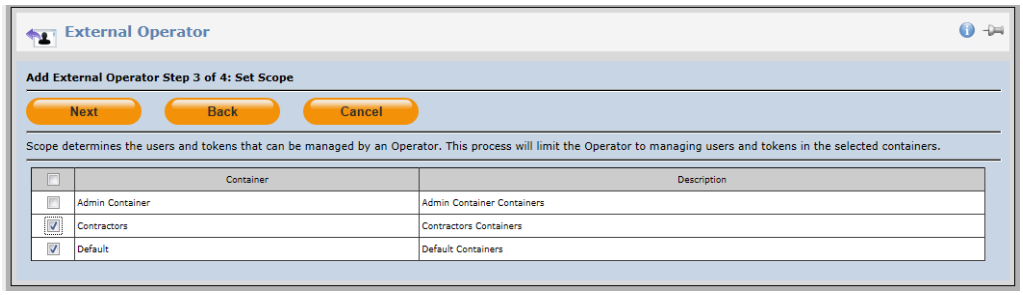


Figure 207: Configure Scope

Select the containers to which this role should have access, and then click “Next”.

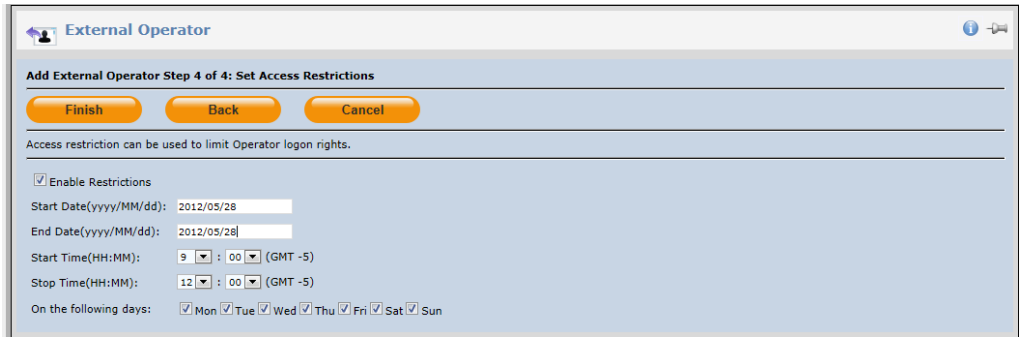


Figure 208: Configure Access Restrictions

To limit when the Service Provider can log in and manage the Virtual Server, turn access restrictions and configure the conditions where:

- **Enable Restrictions**
  If checked, restrictions are enabled. If cleared, no time/day/date range restrictions are applied.
- **Start Date**
  Management UI logon is denied before this date.
- **End Date**
  Management UI logon is denied after this date.
- **Start Time**
  Management UI logon is denied before this time.
- **End Time**
  Management UI logon is denied after this time.
- **On the following days**
  Management UI logon is permitted on checked days only.

Note that Account Manager Restrictions apply only Account Manager management UI logons. It does not affect any logon by the user.

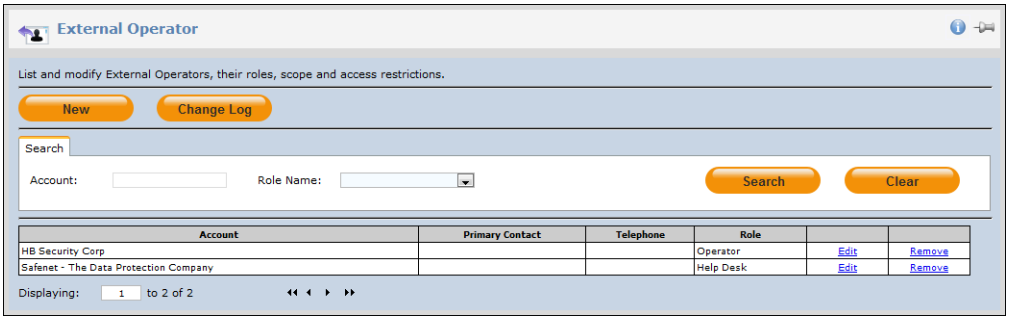


Figure 209: New External Operator

The new external operator account is added to the list. The service provider must now confirm the delegation, after which the accounts Virtual Server will appear in the accounts list on their Virtual Servers tab.

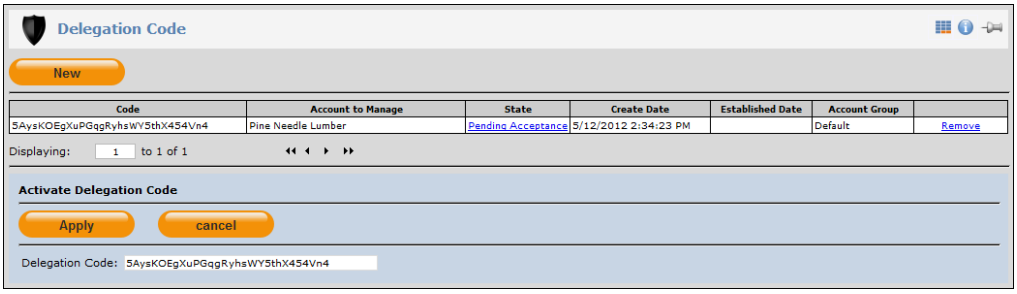


Figure 210: Server Provider Confirmation

Modifying and Removing External Operators

The process to modify or remove External Operators is identical to that for Internal Operators.

Policy Tab

The Policy tab groups all functions related to security policy. Its purpose is to provide a flexible and convenient way to tune the Virtual Server to meet the account's security policy. Through settings on this tab, you can enforce a consistent authentication process and user logon experience and protect against denial of service, brute force and other account credential attacks.

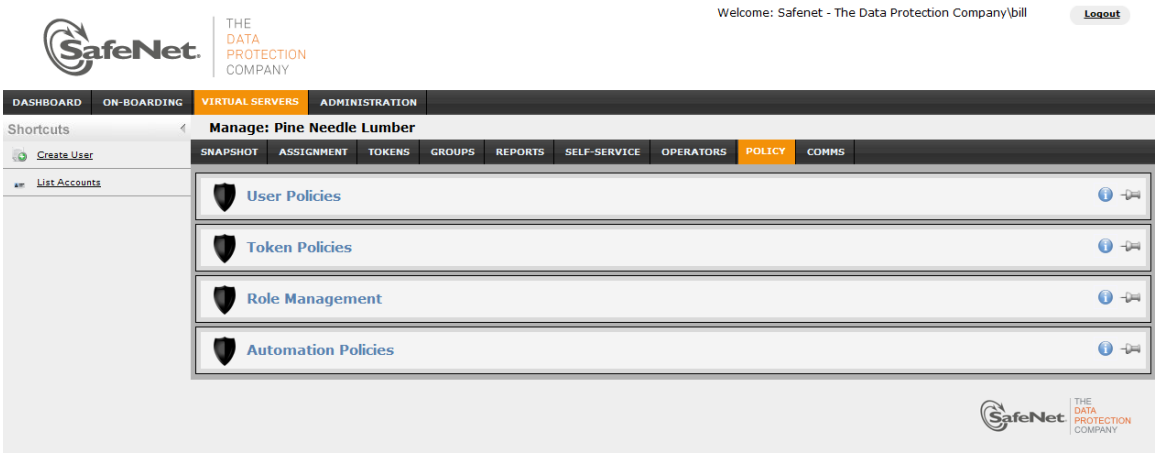


Figure 211: Policy Tab Modules

User Policies Module

This module contains policies that affect user accounts.

Account Lockout / Unlock Policy

The Virtual Server uses this policy to determine how to handle consecutive failed logon attempts.

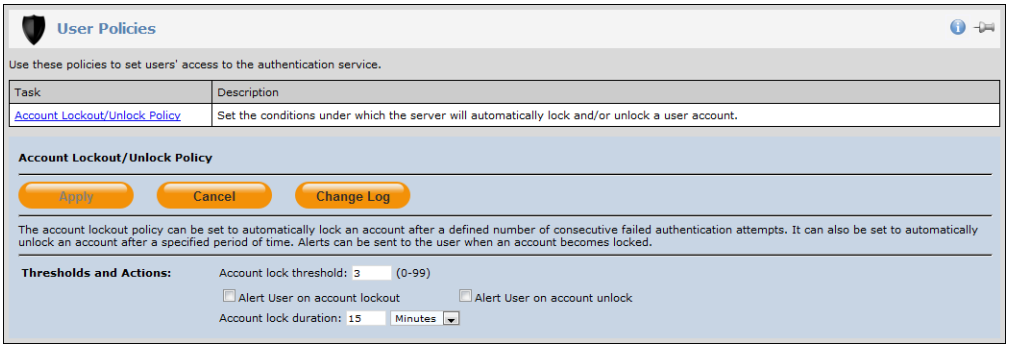


Figure 212: Account Lockout / Unlock Policy

- **Account lock threshold**
  This is the maximum number of consecutive failed logon attempts permitted for a user. If this value is exceeded, the account will lock. Setting this value to 0 is the equivalent of disabling this function. Default value: 3

- **Alert Operator on account lockout**
  If checked, an alert regarding the User's Account being locked will be sent to an Operator.
- **Alert User on account lockout**
  If checked, an alert regarding the User's Account being locked will be sent by email to the User.
- **Alert Operator on account unlock**
  If checked, an alert regarding the User's Account being unlocked will be sent to an Operator.
- **Alert User on account unlock**
  If checked, an alert regarding the User's Account being unlocked will be sent by email to the User.
- **Account lock duration**
  This is the time in seconds, minutes or hours that must elapse after locking the account, after which the User's account will automatically unlock. If set to 0, the account will not automatically unlock. Default value: 15 minutes.

Token Policies Module

This module contains policies that affect token usage and operation.

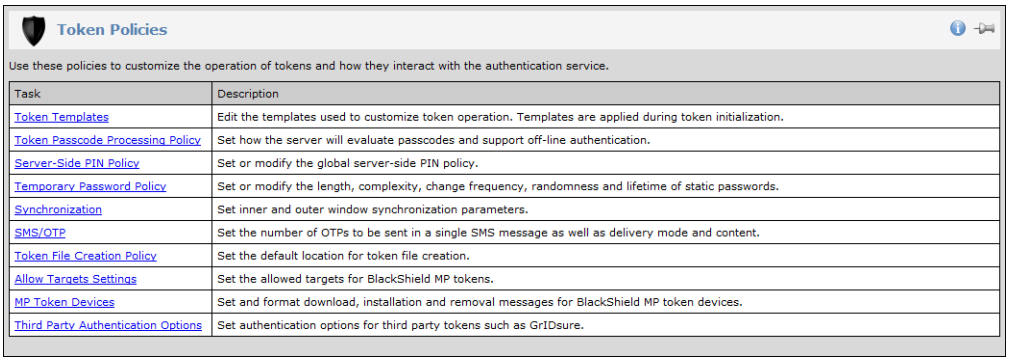


Figure 213: Token Policies Module

Token Templates

Templates are the operating parameters for each type of token. A template is applied every time a hardware token is initialized, or an MP token is assigned/provisioned, or an SMS/OTP or GrID is generated. You can adjust token templates and therefore token operation to optimize usability and adapt to changes in your security policy. To modify a template, begin by clicking the Token Templates hyperlink, then select the token type from the dropdown list, and then click Edit.

Token templates are the operating characteristics such as passcode strength to be applied to all hardware tokens of a given type during initialization, to MP tokens when they are assigned/provisioned to users and to SMS/OTP passcodes. A template modification does not affect tokens that are already initialized and does not affect tokens assigned to users.

Token Templates are provided for KT, RB, MP, SMS, OATH, GrID and Legacy 6.x, Legacy, 5.x and Legacy 4.x software tokens.

The options presented in a template vary depending upon the token type. In addition, the selection of one option may preclude the availability of another option. All possible options are described in the following paragraphs below and apply to all token types unless otherwise noted.

To view or modify an existing template, start by clicking the Token Templates hyperlink, select the token type from the drop down and click 'Edit'. The Edit Token Template dialogue is displayed.

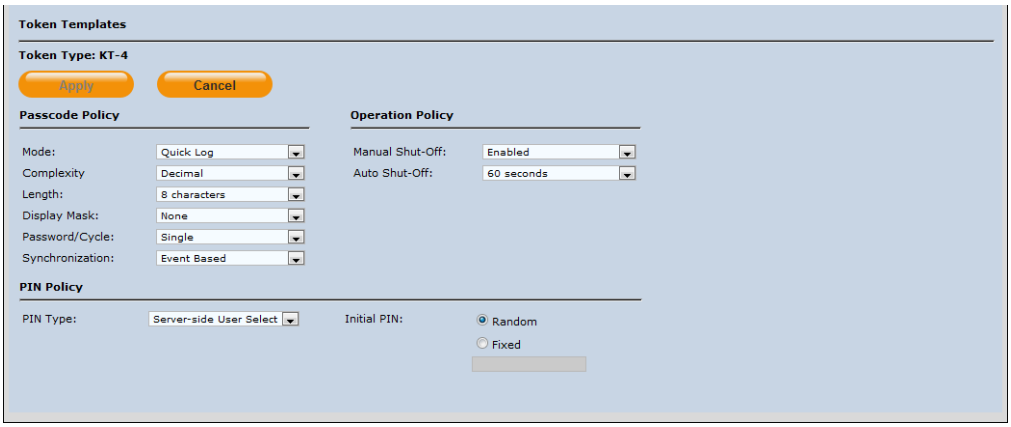


Figure 214: Token Template

By default all tokens use AES 256 bit encryption. Certain 3rd party tokens use 3DES or OATH. SafeNet Authentication Service automatically applies the strongest algorithm supported by the token type.

The options available within each policy vary based on token type.

- **Mode**
  Tokens can operate in either Challenge-Response or Quick Log mode. Quick Log mode is recommended because it greatly simplifies the User logon experience and strengthens security by eliminating the requirement to have the user key a challenge into a token to get an OTP. Default value: Quick Log.

- **Complexity**
  The OTPs generated by the token can be comprised of numbers, letters and additional characters as follows:

- **Decimal**
  Token generates passcodes comprised of digits from 0-9.

- **Hexadecimal**
  Token generates passcodes comprised of digits and letters from 0–9 and A-F.

- **Base32**
  Token generates passcodes comprised of digits and letters from 0-9 and A-Z. (Default value).

- **Base64**
  Token generates passcodes comprised of digits and letters from 0-9 and Aa-Zz, as well as punctuation.

- **Length**
  This option determines the number of characters displayed as the OTP. Options are 5, 6, 7 or 8 characters. Default value: 8.

- **Display Mask**
  If set to 'Telephone Mode', the 4th character of the OTP will always be a dash ("-"). Typically this is used with a decimal OTP, length of 8. Example OTP: 123-5678. If set to 'None', the 4th character is unmodified. Example OTP: 12345678. Telephone mode can be used with any token complexity and length setting. Default value: None.

- **Passwords/Cycle**
  This option is used in conjunction with Operation Policy (Manual Shut-Off, Auto Shut-Off). Tokens can be limited to generating 1 password per cycle or allow multiple passwords to be generated in a cycle. Default value: Single.

  For tokens with a 'No PIN' or 'Server-side' PIN policy, the selection of Single in combination with Manual Shut-Off set to Disabled means that the token will not generate another password until the Auto Shut-Off value has expired. For example, if the value is 60 seconds, the user must wait 60 seconds before another password can be generated.
  For tokens with a 'Fixed' or 'User selected' PIN, selection of Manual Shut-off set to Disabled means that the token will not generate another password until the Auto Shut-Off value has expired and the user enters their PIN into the token.

- **Manual Shut-Off**
  If 'Enabled', the user can clear the OTP from the display and turn the token off at any time by pressing the appropriate button, depending on the token type. If 'Disabled', the OTP will be displayed until the Auto Shut-off value expires. Default Value: Disabled.

- **Auto Shut-Off**
  This value determines the length of time the password will be displayed, 30, 60 or 90 seconds. On expiration of this value, the token automatically clears the display and shuts off. Default Values: 60.

  NOTE: SafeNet recommends using the Operation Policy Group default settings for RB and KT series tokens configured for QUICKLog operation. Doing so ensures that the user must wait at least 60 (default) seconds before the token will generate another passcode.

- **PIN Type**
  This setting determines the type of PIN to be used with the token:

- **No PIN**
  Means that the user will not use a PIN. The token generated password will be sufficient for authentication.

- **Fixed PIN**
  Means that the PIN generated for the token during initialization is permanent and cannot be changed without reinitializing the token. This PIN must always be keyed into the token before a password is generated.

- **User selected PIN**
  Means that the user must change the PIN generated for the token during initialization before a password will be generated. Thereafter the user can change the PIN at any time. Note that the PIN change must conform to the minimum requirements for PIN Length, Complexity and Maximum PIN Attempts.

- **Server-side Fixed**
  Means that the PIN generated for the token at initialization is permanent and cannot be changed without reinitializing the token. This PIN type is evaluated at SafeNet Authentication Service.

- **Server-side User Select**
  Means that the PIN generated for the token can be changed by the User. The new PIN must conform to the minimum requirements set in Server-side PIN Policy on page 210.

- **Server-side Server Select**
  Means that the PIN generated for the token can be changed however the new PIN will be generated by SafeNet Authentication Service and will conform to the minimum requirements set in the Server-side PIN Policy Group on the Policy Admin Tab.

  Note: Server-side PINs require the user to prepend the PIN to the token generated password during login, allowing the PIN to be evaluated by the Virtual Server. For example, if the user PIN is ABCD and the password is 12345678, the user would enter ABCD12345678 at the password prompt. All other PIN types require the user to key the correct PIN into the token before a password is generated. In this case the user provides only the password at the password prompt. For example, if the user PIN is 8432 and the password is 12345678, the user will enter 12345678 at the password prompt. Generally Server-side PINs are used with KT tokens.

- **Initial PIN**
  Determines the nature of the initial PIN created for a token during initialization. If ‘Random’, SafeNet Authentication Service will generate a random PIN that conforms to the minimum PIN Policy options set in the dropdowns for this group for each token during initialization. If ‘Fixed’, all tokens will be initialized with the same PIN. Default value: Random.

- **Min. PIN Length**
  Determines the minimum PIN length that can be used with the token.

- This option is disabled if PIN Type is set to 'No PIN'. The user will not be required to use a PIN at any time.

- This option is disabled if PIN Type is set to Server-side Fixed, Server-side User Select or Server-side Server Select. The user will be required to use a PIN according to the options set in the Server-side PIN Policy Group.

- This option is enabled if PIN Type is set to Fixed PIN or User selected PIN. This requires that any PIN set for the token meets the indicated minimum number of digits. The range is 1 to 8 digits.

- **Allow Trivial PINs**
  If enabled, a PIN may be 3 or more consecutive numbers (i.e. 1234) or 3 or more identical digits (i.e. 2222). Default value: cleared.

- **Max. PIN Attempts**
  Determines the maximum number of consecutive failed PIN attempts permitted by the token. If this number is exceeded, the token will enter the 'Locked' state and cannot be used for authentication until it is reinitialized. This option is available only if PIN Type is set to Fixed PIN or User selected PIN.

  Click the 'Apply' button to apply changes to the template. Changes to the template will be applied to their respective token types during initialization. Previously initialized tokens will be unaffected by changes to a template.

Token Passcode Processing Policy

There are global settings that determine how the server will evaluate OTP's and support off-line authentication.

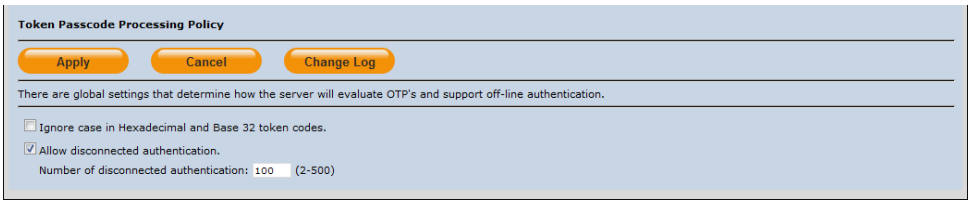


Figure 215: Token Passcode Processing Policy

- **Ignore case in Hexadecimal and Base 32 token codes**
  This is a usability enhancement. If enabled, users will be able to enter OTPs using either upper and/or lower case letters. If unchecked, users must enter Base32 token codes using only upper case letters.

- **Allow disconnected authentication**
  This option is used in conjunction with the SafeNet Authentication Service Authentication Agent for

Windows Logon. If enabled, users will be able to log into their Windows computers using an OTP, even if the computer is not connected to a network. The number of disconnected authentications is the maximum number of times a user can log onto their computer before they must connect to the network and authenticate against the Virtual Server.

Server-side PIN Policy

There are global settings that determine how the server will evaluate PINs that are prepended to the token code.

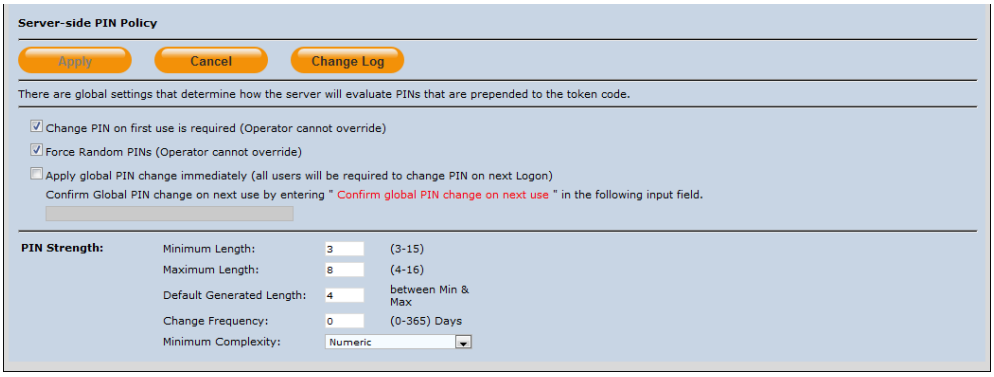


Figure 216: Server-side PIN Policy

- **Change PIN on first use is required (Operator cannot override)**
  This option forces the user to change the initial PIN set for the token during initialization or set by an Operator before they can logon. For example, if the initial PIN is ABCD and the password is 12345678, the user will attempt to logon with ABCD12345678. Assuming this combination successfully authenticates against SafeNet Authentication Service, the user will then be prompted to change their PIN to a new value that meets the minimum requirements of the Server-side PIN. If this option is checked, the Operator cannot override this policy when resetting a User's PIN. If this option is cleared, the Operator can choose whether or not to force a PIN change on first use after resetting the User's PIN. Default value: checked.

- **Force Random PINs**
  If checked the Virtual Server will generate random PINs that meets the Server-side PIN policy requirements for each User. If checked, the Operator cannot choose the PIN to be given to a User. If cleared, the Operator can create a PIN that conforms to the policy or request a PIN be generated by the Server. Default value: checked.

- **Apply global PIN change immediately**
  This forces all users to change their Server-side PINs during their next authentication, regardless of the PIN change frequency setting. A confirmation message must be entered to commit this change.

- **PIN Strength – Minimum Length**
  This setting determines the minimum number of characters in a PIN. Range is 3 – 15 characters.

- **PIN Strength – Maximum Length**
  This setting determines the maximum number of characters in a PIN. Range is 4 – 16 characters.

- **Default Generated Length**
  This is the number of characters in a PIN auto-generated by the Server.

- **Change Frequency**
  This determines how frequently a user will be required to change their Server-side Server Select or Server-side User Select PIN. This period commences with the last PIN change date for a token. Default is 30 days.

- **Minimum Complexity**
  This determines the combination of characters that must be used in a PIN. Default value: Numeric.

- **Numeric**
  The minimum requirement is a PIN comprised of digits 0-9.

- **Alphanumeric**
  The minimum requirement is a PIN that contains at least 1 digit and 1 upper case letter. 0-9, A-Z (excluding the letters “I”, “l” and “O”)

- **Strong Alphanumeric**
  The minimum requirement is a PIN comprised of at least 1 digit, 1 upper case letter and 1 lower case letter. 0-9, Aa-Zz (excluding the letters “I”, “l” and “O”)

- **Complex alphanumeric**
  The minimum requirement is a PIN comprised of at least 1 digit, 1 letter and 1 special character. 0-9, Aa-Zz, and punctuation. (excluding the letters “I”, “l” and “O”)

Temporary Password Policy

This section applies to temporary static passwords assigned to user accounts using the Password button (Tokens module, Assignment tab). As with Server-side PIN Policy, these Options set global temporary password policy. Click 'Apply' in the Actions group to apply changes to these values.

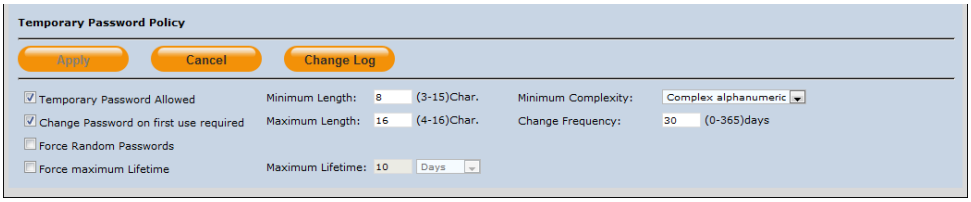


Figure 217: Temporary Password Policy

- **Temporary password Allowed**
  This option determines whether a static password can be assigned. When checked, an Operator can assign a temporary password to a user, provided the user does not currently have an active token. If cleared, Operators may not assign a temporary password to a user. Default value: checked.

- **Change Password on first use required**
  This option forces the user to change the static password assigned by an Operator before they can logon. The user must first provide the assigned password and then is prompted to replace the password. If this box is checked, all users assigned a static password will be required to change it on first use. The Operator cannot override this policy. If cleared, the Operator has the option of requiring a password change on first use. Default value: checked.

- **Minimum Length**
  This is the minimum number of characters required in the temporary password. Range is 3 to 15 characters. Default value: 8.

- **Maximum Length**
  This is the maximum number of characters permitted in the temporary password. Range is 4 to 16 characters. This value must be greater than or equal to the minimum length. Default value is 16 characters.

- **Minimum Complexity**
  This determines the combination of characters that must be used in a password. Default value: Complex alphanumeric.

- **Numeric**
  The minimum requirement is a password comprised of digits 0-9.

- **Alphanumeric**
  The minimum requirement is a password that contains at least 1 digit and 1 upper case letter. 0-9, A-Z.

- **Strong Alphanumeric**
  The minimum requirement is a password comprised of at least 1 digit, 1 upper case letter and 1 lower case letter. 0-9, Aa-Zz.

- **Complex alphanumeric**
  The minimum requirement is a password comprised of at least 1 digit, 1 letter and 1 special character. 0-9, Aa-Zz, and other printable characters.

- **Change Frequency**
  This determines how frequently a user will be required to change their static password. This period commences with the last static password change date for a token. Default value: 30 days.

- **Force Random Passwords**
  This determines whether an Operator can choose the password to be given to a user. If cleared, the Operator can manually create or generate a password that conforms to the policy. If checked, the Virtual Server must generate the temporary password. Default value: cleared.

- **Force Maximum Lifetime**
  This determines how long a temporary password will remain active. Possible values are in minutes, hours, days or weeks. Default value: disabled.

Synchronization Policy

Synchronization is only relevant for QUICKLog (event-synchronous), CRYPTOCard/SafeNet KT series time-based tokens Safenet Gold/Platinum and eTokenPass as well as 3rd party OATH tokens.

Tokens configured for QUICKLog do not rely on time to remain synchronized with the server. Instead, each time the token is activated, a new tokencode is generated. For each logon “event” the server compares the submitted passcode with the expected passcode. Occasionally a user may generate a passcode without using it, causing the token to be “ahead” or out of sync with the server during the next logon.

The Synchronization Window settings provide a secure mechanism through which the server and token can automatically resynchronize during logon.

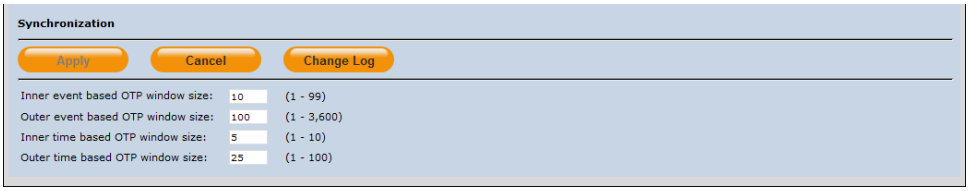


Figure 218: Synchronization Policy

- **Inner Event based OTP window size**
  This represents the number of passwords the server will “look-ahead” from the last successful logon by the user. Using the example above, the server would be expecting passcode number 1 even

though the user provides passcode number 2. Assuming the default inner window value of 3, the server would look from passcode 1 to 3 until a match is found (in this case at passcode 2). If a match is found, the user is authenticated and any unused passcodes are discarded. The next valid passcode on the server would be passcode 3. Default value: 10.

- **Outer Event based OTP window size**
  This handles situations where the user's passcode is not found in the inner window. In this case, the server will look ahead up to the indicated value (by default 100). If a match is found in this window, the user is prompted to provide the next passcode in sequence. For example, if the user provides passcode 4, the user will be prompted for and must provide passcode 5. In essence this window has an effective size of 1. Default value: 100.

- **Inner time based OTP window size**
  This handles time drift for time-based tokens. Similar to inner event based window size, this value determines the number of minutes the token can be out of sync with the server. An OTP found inside this window will be accepted and the server is updated to adjust for this token's time drift.

- **Outer time based OTP window size**
  This handles time drift for time-based tokens. Similar to outer event based window size, this value determines the number of minutes the token can be out of sync with the server if the OTP is not found in the inner window. If the OTP is found in the outer window, the user must provide the next OTP in sequence to successfully authenticate.

SMS/OTP Policy

This policy determines how the server will generate and deliver OTPs by SMS to users.

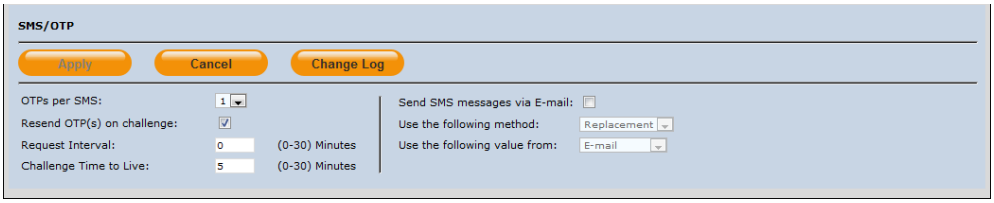


Figure 219: SMS/OTP Policy

- **OTPs per SMS**
  From 1 to 5 OTPs can be sent in an SMS message. This method applies only if the SMS token is issued in QUICKLog mode (refer to Token Templates on page 205). In this mode the user receives an SMS message immediately after each successful authentication. By including more than 1 OTP, users that are temporarily outside of an SMS delivery zone will be able to authenticate until all OTPs in the message have been consumed.

  If the SMS token is issued in Challenge/Response mode, the OTP is not sent until the user attempts to logon. SMS Challenge/Response is usually combined with Single Sign-on, whereby the user must

first successfully authenticate with the Active Directory password, after which the Virtual Server automatically sends the OTP necessary to complete the authentication and logon process.

- **Resend OTP on Challenge**
  If checked, the Virtual Server will send an OTP to the user if an empty or 1 character password is submitted in the OTP/password field during authentication.

- **Request Interval**
  This setting determines the number of minutes that must elapse between Resend OTP on challenge requests. Requests received during this period are ignored by the server.

- **Challenge Time to Live**
  This setting determines the lifespan of an OTP issued in Challenge/Response mode. An OTP that is unused after this period cannot be used to authenticate.

- **Send SMS messages via E-mail**
  If enabled, all SMS token passcodes are sent via SMTP server. Use this option to deliver OTPs to an email address or to send OTPs using email to SMS. If disabled, all OTPs are sent via SMS gateway or modem.

- **Use the following method**
  The options are Replacement and Suffix.

- **Replacement**
  OTPs are sent using the address from the field selected in the “Use the following value” option (described below). Typically this will be a valid email address.

- **Suffix**
  OTPs are sent to an address that is the combination of the data in the Mobile/SMS field (User Detail) and the data contained in field selected in “Use the following value” option. For example, if Mobile/SMS contains 16135992441 and Custom #2 (selected) contains @na.rogers.com, the email will be sent to 16135992441@na.rogers.com.

- **Use the following value**
  This selection determines the field used to provide the data for Replacement and Suffix. Options are Email, Custom #1, #2 or #3.

Token File Creation Policy

This policy determines the default location for saving MP token profiles. This applies to MP tokens issued to users via the “Assign” function with the Save option selected.

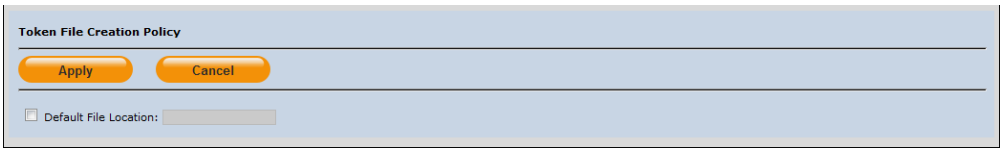


Figure 220: Token Profile creation Policy

Allowed Targets Policy

MP-1 tokens can be installed on a wide range of devices, referred to as “Targets”. The settings in this policy determine which targets are presented to users during Self-enrollment of MP-1 tokens.

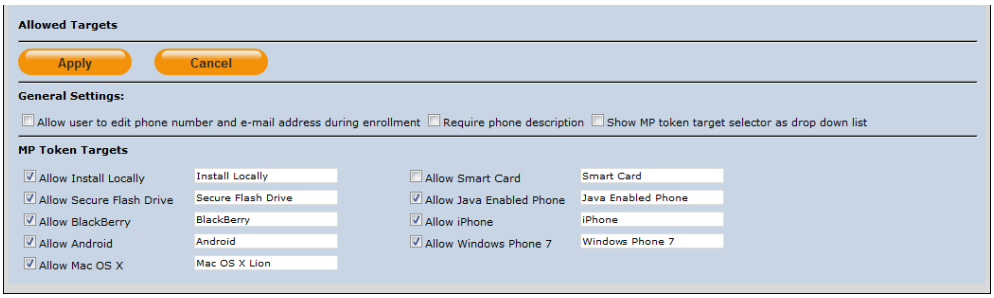


Figure 221: Allowed Targets Policy

- **Allow user to edit phone number and e-mail address during enrollment**
  If enabled, the user will be able to modify the email address and/or mobile phone number to which the token enrollment message is delivered. By default this option is disabled, forcing enrollment to occur through address and number in the users account detail.

- **Require Phone Description**
  If checked, a list of devices configured in the MP Token Devices module (Refer to MP Token Devices Policy on page 218) will be displayed during the self-enrollment process.

- **Show MP target selector as a dropdown list**
  If selected, targets are displayed in a dropdown list. If deselected, targets are displayed as radio button options.

- **Allow Install Locally**
  If enabled, the user will have the option to install the MP on their PC.

- **Allow Java Enabled Phone**
  If enabled, the user will be able to install the token on mobile phones running the Java O/S. Options include USB/desktop and Over-the-Air token installation. The type of method that can be used is determined by the phone manufacturer.

- **Allow Smart Card**
  This option is disabled in this version.

- **Allow BlackBerry**
  If enabled, the token may be installed on BlackBerry devices.

- **Allow Secure Flash Drive**
  If enabled, the token may be installed on supported secure Flash Drives such as IronKey™ Enterprise and SafeStick™. Refer to the SafeNet web site for a list of supported products and versions.

- **Allow iPhone**
  If enabled, the token may be installed on iPhones and iPads running iOS 4.3+.

- **Allow Android**
  If enabled, the token may be installed on devices running Android O/S 2.2+.

- **Allow Mac OS X**
  If enabled, the token may be installed on devices running OS X 10.7 (Lion) or higher.

- **Allow Windows Phone 8**
  If enabled, the token may be installed on devices running Windows Phone 7 or higher.

The device names presented to users during self-enrollment can be modified by changing the corresponding text in the MP Token Targets section.

MP Token Devices Policy

This section allows the messages presented in the browser to the user during self-enrollment to be customized for both content and graphics. The messages will apply to the type of device selected in the "Type" dropdown. Use this module to add instructions and support for target devices such as specific models of mobile phones, USB drives etc.

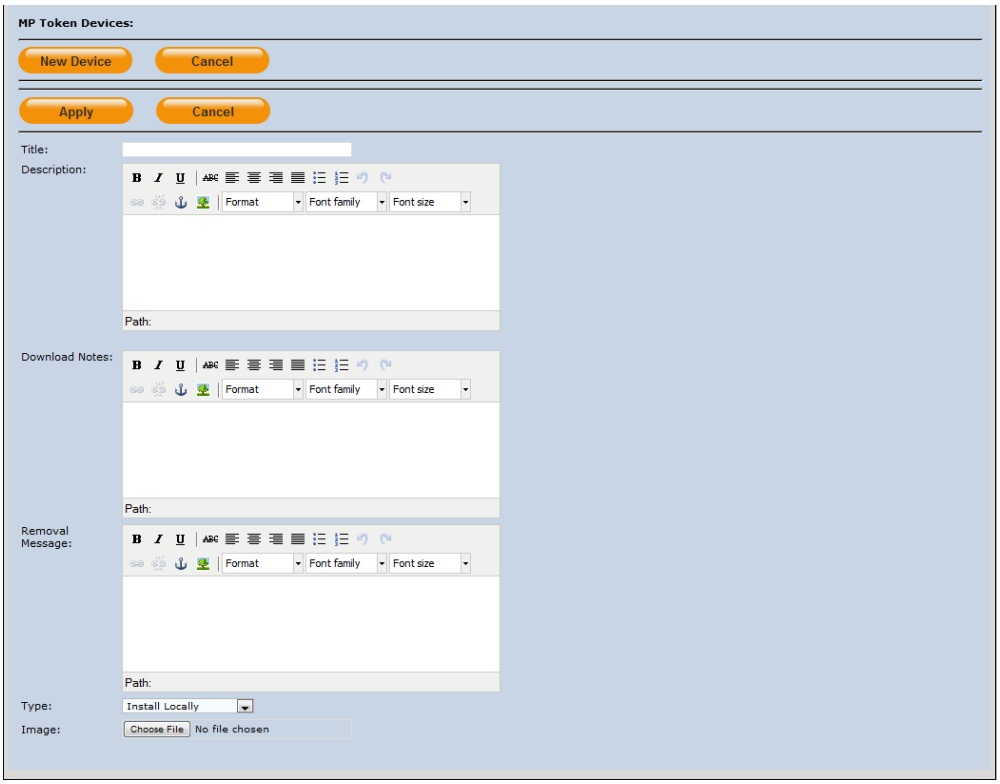


Figure 222: MP Token Devices Policy

An entry is added to the list for each custom device. Use the edit and remove hyperlinks to edit and remove custom messages.

Third Party Authentication Options Policy

This policy determines the operation of the GrIDsure authentication method and "RADIUS" tokens.

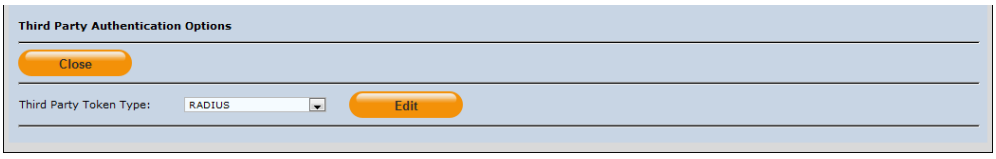


Figure 223: Third Party Authentication Options Policy

GrIDsure Method

This method presents a matrix of characters to the user during authentication. The user's passcode is determined by overlaying their "PIP" (personal identification pattern) on the matrix and using the corresponding characters in the order the PIP was created. The white squares in the following image have been added to demonstrate the concept of a PIP, and a resulting passcode, in this case 87982, bearing in mind that the user might have created the PIP pattern in any order. In other words, had the user created it right to left, the passcode for would have been 28978. There is no restriction on the order in which a pattern is created and indeed some cells in the pattern could have been used more than once. For example, assume left to right, repeating every second cell would mean that the passcode for this PIP would be: 8779882. The PIP can be combined with a PIN for an additional level of security.

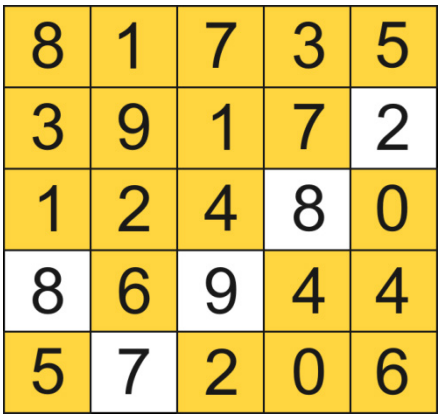


Figure 224: GrID method demonstrating a PIP

To modify begin by selecting the GrIDsure method from the dropdown list, then click Edit.

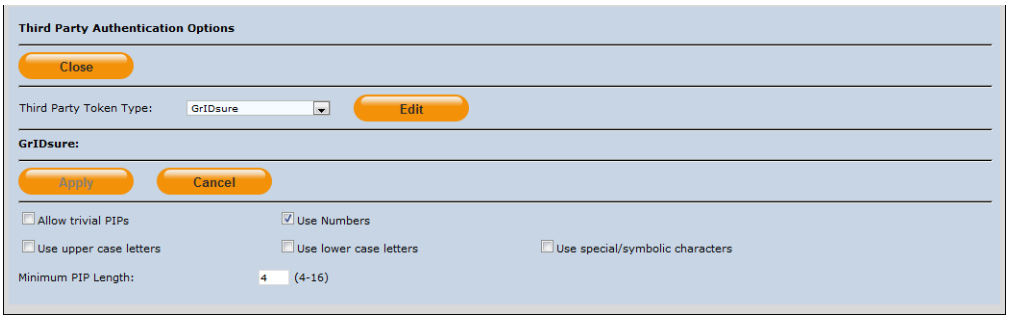


Figure 225: Modify GrIDsure method

- **Allow Trivial PINs**
  If enabled, the user can select a row, column or 4 corners of the grid as their PIP.

- **Use Numbers, lower case letters, upper case letters, symbols**
  Grids will contain characters from the enabled options. Note that grid size is set under Token Templates (refer page 205) as is the requirement for a PIN in addition to the passcode that corresponds to the PIP.

RADIUS Tokens

RADIUS tokens is a configuration that can be used with any 3rd party token. Its purpose is to provide enterprises with a simple and effective migration path from their existing 3rd party vendor's authentication product to SafeNet Authentication Service and in the process, extend most of the SafeNet Authentication Service management UI functionality including PIN management, automated provisioning, authentication history and reporting and pre-authentication rules to users with the 3rd party tokens.

This method bears similarity with RADIUS proxy but there are substantial differences:

Similarities	Differences
SafeNet Authentication Service is configured as a RADIUS Client to the 3rd parties RADIUS server. Configuration is standard RADIUS – IP, port #, shared secret.	In RADIUS proxy, all user, token management, authentication history, reporting etc. must be done at the 3rd party RADIUS server. However, in RADIUS Token mode, all management can be done through SafeNet Authentication Service except for reassignment of 3rd party tokens.

Any tokens imported into SafeNet Authentication Service (refer to Import Third Party Tokens

This module is available only to the Host Service Provider. This module allows tokens from various manufacturers to be imported and/or managed by SafeNet Authentication Service. Tokens will automatically be bound to an existing UserID in SafeNet Authentication Service if the token import record contains a matching UserID.

If an import record does not contain a UserID, the token will be imported and placed in inventory.

Figure 124: Import 3rd Party Tokens

Options include:

RADIUS Tokens

This import method can be used with any token type provided the 3rd party authentication server will accept authentication requests via RADIUS from SafeNet Authentication Service. To automatically bind a specific token to a user during import:

- Ensure that the UserID already exists in SafeNet Authentication Service.
- Ensure that a record in the import file contains the corresponding UserID and token serial number. Each record in the import file must be in the format:

  UserID,SerialNumber,yyyy/mm/dd

  where Serial Number is 12 characters (pad with leading 0 if necessary)

  If a UserID is omitted in the import record, the token will be imported and placed in inventory. Though the token can be assigned or provisioned to a user in SafeNet Authentication Service, care must be taken to ensure that the same token is assigned to the same user in the 3rd party RADIUS server. Use containers to segregate imported tokens that will be allocated to Subscriber Accounts.

SecurID Tokens

This import method can be used with SecurID tokens, provided the RSA Authentication Manager is configured to accept authentication requests via RADIUS from SafeNet Authentication Service. To automatically bind a specific token to a user during import:

- Ensure that the UserID already exists in SafeNet Authentication Service.
- Ensure that a record in the import file contains the corresponding UserID and token serial number. Each record in the import file must be in the format:

  UserID,SerialNumber,yyyy/mm/dd,#

  where:

  Serial Number is 12 characters (pad with leading 0 if necessary)
  # is the length of the generated passcode. Allowed values are 6 or 8. If omitted, 6 is assumed.

  If a UserID is omitted in the import record, the token will be imported and placed in inventory. Though the token can be assigned or provisioned to a user in SafeNet Authentication Service care must be taken to ensure that the same token is assigned to the same user in the RSA Authentication Manager.

Bulk Assign Third Party Tokens

This module is available to Virtual Service Provider and Subscriber account and allows tokens from various manufacturers to be managed by SafeNet Authentication Service. Tokens will automatically be bound to an existing UserID in SafeNet Authentication Service if the token import record contains a matching UserID.

The token records must be added to your token inventory by your Service Provider. Your Service Provider will require a file containing a record for each token. Refer to RADIUS Tokens on page 134.

If an import record does not contain a UserID, the token will be imported and placed in inventory.

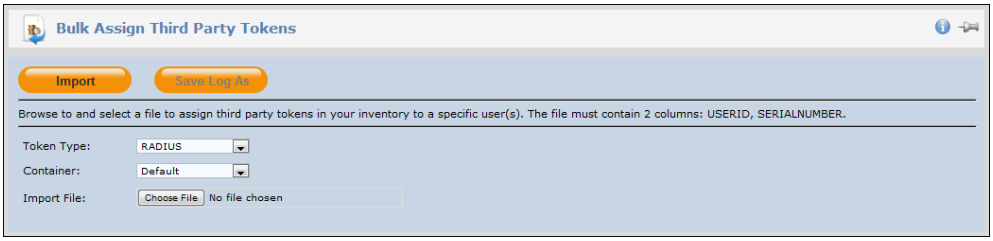


Figure 125: Import Third Party Tokens

Options include:

RADIUS Tokens

This import method can be used with any token type including RSA/SecurID, provided the third party authentication server will accept authentication requests via RADIUS from SafeNet Authentication Service.

Step 1: Provide a Third Party Token Import file to your service provider. This file must be comma delimited file (.csv) and contain a record for each token being imported. Each record must be in the following format:

,SerialNumber,yyyy/mm/dd

Note the leading ","

The Serial Number is 12 characters (pad with leading 0 if necessary)

These tokens will appear in your token inventory when the Service Provider has completed the import process.

Step 2: To automatically bind a specific token to a user during import:

Ensure that the UserID already exists in SafeNet Authentication Service.

Ensure that a record in the import file contains the corresponding UserID and token serial number. This file must be comma delimited file (.csv) . Each record in the import file must be in the format:

UserID,SerialNumber,yyyy/mm/dd

where Serial Number is 12 characters (pad with leading 0 if necessary)

If a UserID is omitted in the import record, the token will be imported and placed in inventory. Though

the token can be assigned or provisioned to a user in SafeNet Authentication Service, care must be taken to ensure that the same token is assigned to the same user in the 3rd party RADIUS server.

- SecurID Tokens
- This option is not available to Virtual Service Provider or Subscriber accounts.
- OATH Token
- 3rd party OATH tokens can be imported into SafeNet Authentication Service however these must be converted to a special .btk format prior to import. Contact SafeNet for instructions.

on page 133) using the RADIUS option automatically use the method as configured in this module.

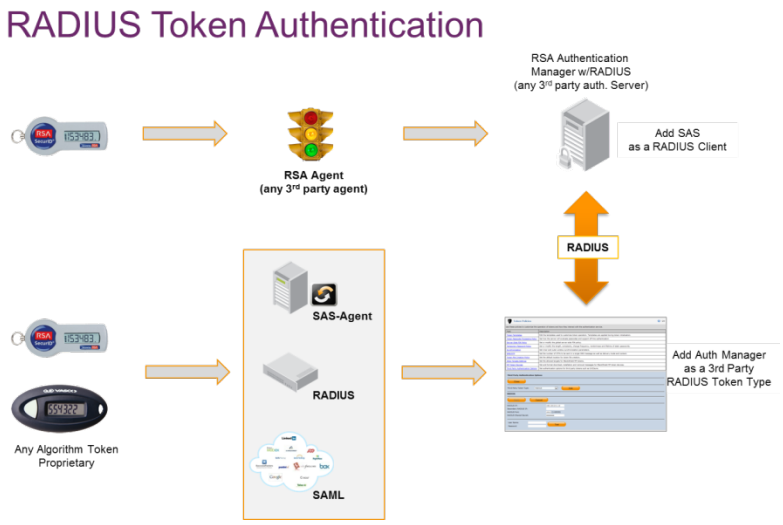


Figure 226: Migration using "RADIUS" Token

To modify begin by selecting the RADIUS from the dropdown list, then click Edit.

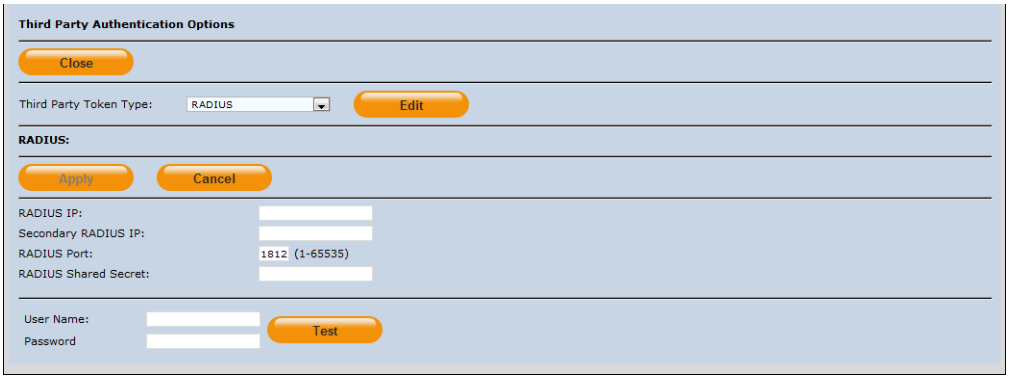


Figure 227: Configure "RADIUS" 3rd Party Token Support

- **RADIUS IP**
  This is the IP address of the 3rd party authentication server's RADIUS server. During authentication, SafeNet Authentication Service will pass the OTP via this connection to the 3rd party server for passcode verification.

- **Secondary RADIUS IP**
  Provides redundancy for the RADIUS IP setting above. This setting is optional but recommended.

- **RADIUS Port**
  The port number on to be used for RADIUS requests. Default is 1812. This value must match the settings at the 3rd party authentication server.

- **RADIUS Shared Secret**
  This is the shared secret used to encrypt RADIUS traffic. It must be identical in both SafeNet Authentication Service and the 3rd party RADIUS server.

- **User Name / Password**
  This provides a way to test the configuration before going into production. The username (userID) must exist in both SafeNet Authentication Service and the 3rd party radius server and the token assigned to the user must have been imported as a "RADIUS" token and must be the same token assigned to the user in the 3rd party server. Results of the authentication test are displayed in this pane.

Role Management Module

Use this module to manage Operator roles, alerts and alert thresholds and select the UI language.

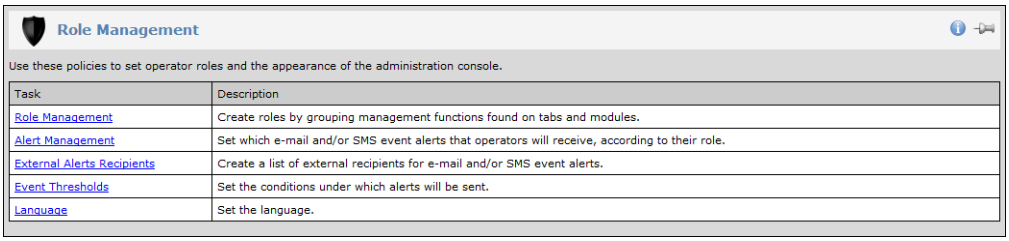


Figure 228: Role Management Module

Role Management Policy

A Role is a combination of Tabs, Modules and Actions within modules that are available to an Operator. Access to tabs and modules can be disabled. Where access to tabs and modules is allowed, the actions within any module can be restricted.

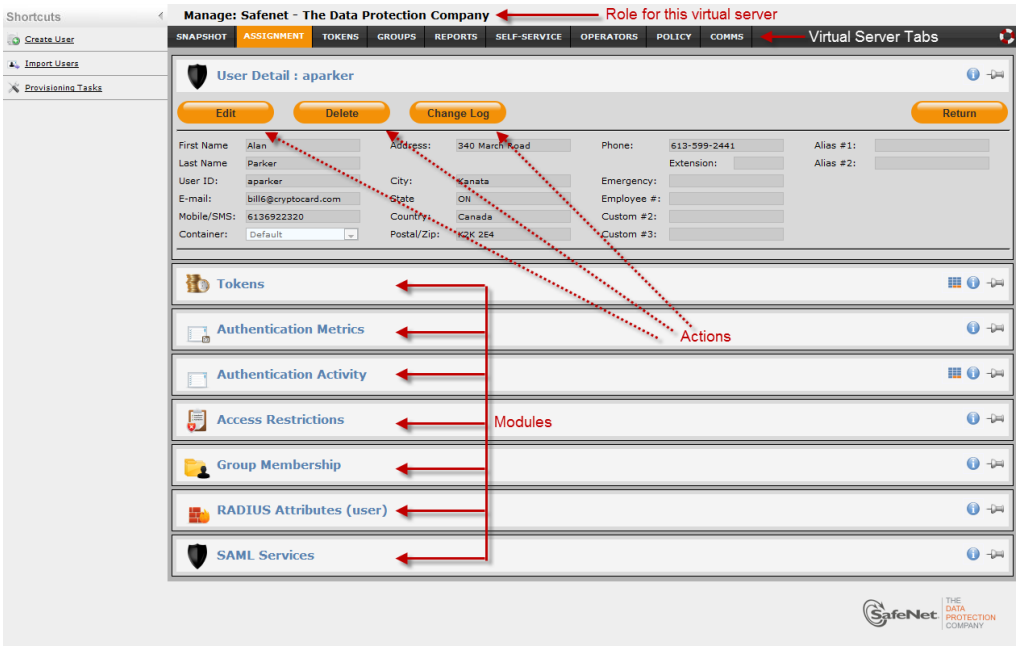


Figure 229: Virtual Server Tabs, Modules and Actions

For example:

De-selecting “Add” in the Tokens module on the Assignment tab and de-selecting “Access” in the Provisioning module removes the ability to assign or provision a token.

Disabling “Operators tab” removes access to this tab and all of its modules.

This high degree of granularity means that Operational Security can easily be customized for each Virtual Server and role.

The Operator role is always assigned to the person added through the Create Operator module on the On-boarding tab. If a different role is required, create the user from within the Virtual Server (Assignment tab, Create User shortcut), then promote the user to Operator status from the Operators tab, selecting an appropriate role.

Roles are specific to the Virtual Server in which they are configured.

The “Operator” role grants unrestricted rights to manage the Virtual Server.

Existing roles are displayed in the roles list. Use the edit or remove hyperlinks to edit or remove the corresponding role.

Creating an Operator Role

Begin by selecting the Role Management hyperlink. This will display the Operator Roles list.

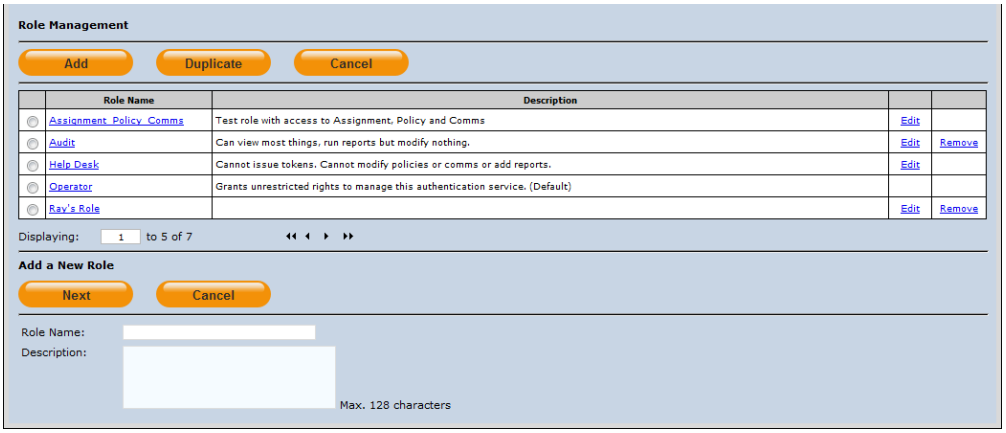


Figure 230: Role Management Policy

Clicking the Role hyperlink displays the list of tabs, modules and actions available for the selected role. All roles except the default “Operator” role can be edited or removed by clicking the Edit and Remove hyperlinks respectively. For similar roles, use the Duplicate button to make a copy of an existing role, and then edit the duplicate as necessary.

Adding or Editing a Role

To add a role or edit an existing role, click the Add button or Edit hyperlink respectively. If adding, you will be prompted to create a role name and a role description, after which you’ll be presented with the Role configuration page.

The Role configuration page (Figure 231: Configuring a Role228) is split into several horizontal sections, each representing a different Virtual Server tab. Within each section is a table listing all modules available on the tab and a corresponding set of actions available for each module.

Clearing a check box removes the tab, module or action from the role.

Module Actions

There are seven possible actions:

- **Access**
  If checked, the module will be displayed.
- **Edit**
  If checked, the Role will have access to all edit functions available in the module.
- **Delete**
  If checked, the Role will have access to all delete or remove functions available in the module.
- **Add**
  If checked, the Role will have access to all Add functions available in the module.
- **Import**
  If checked, the Role will have access to all import functions available in the module.
- **Export**
  If checked, the Role will have access to all export functions available in the module.
- **View Log**
  If checked, the Role will have access to the View Log function available in the module.

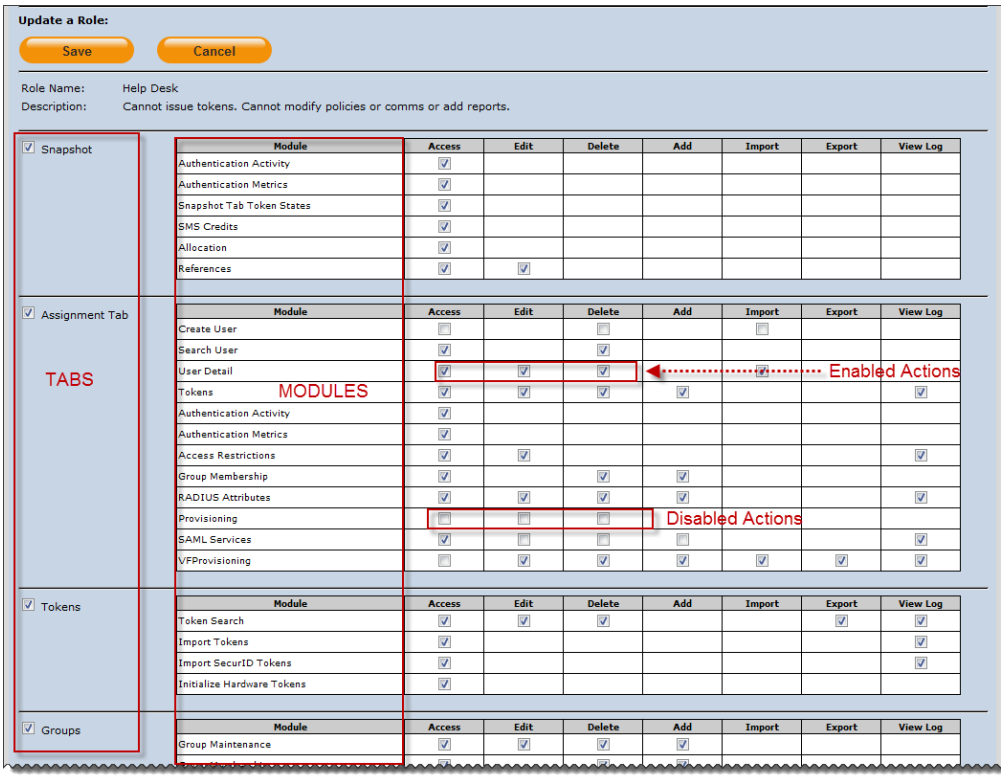


Figure 231: Configuring a Role

Click the Save button to commit the role configuration.

Alert Management Policy

The Virtual Server can generate alerts when a condition or threshold is detected or exceeded. By default an alert policy with all alerts disabled is attached to every role when the role is created. Edit the default policy for each role to enable the desired alert and delivery method.

To configure alerts, begin by clicking the Alert Management policy hyperlink, and then clicking the Edit hyperlink corresponding to a role.

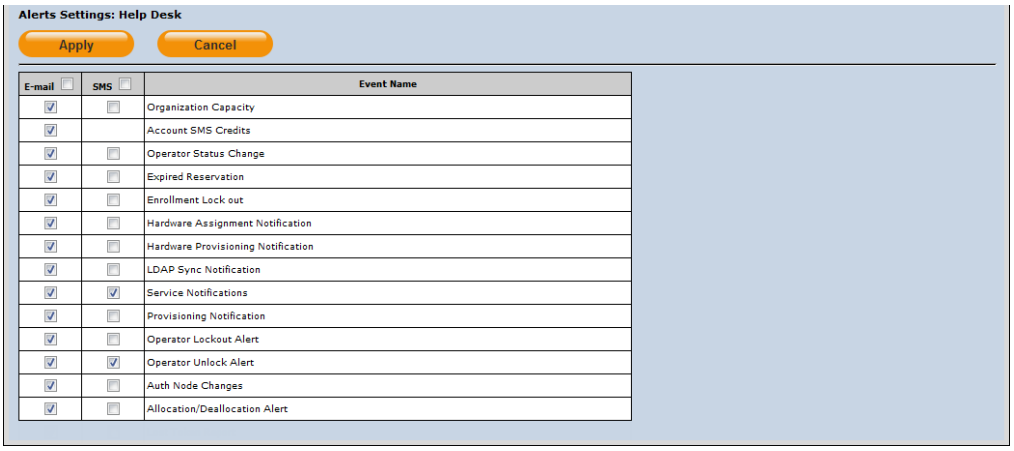


Figure 232: Alert Management Policy

Alerts can be delivered by e-mail and/or SMS message. To enable an alert, check the corresponding option box according to the method of delivery. Commit the changes by clicking the Apply button.

- **Organization Capacity**
  If enabled, an alert will be sent when the Virtual Server capacity falls below the threshold. (Refer to Alert Management Policy on page 228)

- **Account SMS Credits**
  If enabled, an alert will be sent when available SMS Credits falls below the threshold.

- **Operator Status Change**
  If enabled, an alert will be sent when an Operator's status is changed to/from Active, Suspended, Removed.

- **Expired Reservation**
  If enabled, an alert is generated for each user in a provisioning task who has not enrolled their token before the stop date.

- **Enrollment Lockout**
  If enabled, an alert is generated if the user exceeds the maximum number of attempts to enroll their token. (Refer to Self-enrollment Policy on page 235)

- **Hardware Assignment Notification**
  If enabled, an alert including the User detail is sent when a hardware token is assigned to a user.

- **Hardware Provisioning Notification**
  If enabled, an alert including the User detail and address is sent when a hardware token is assigned to a user. This option is useful for alerting a 3rd party fulfillment service with information necessary to deliver the hardware token to the user.

- **LDAP Sync Notification**
  If enabled an alert is sent each time LDAP synchronization results in an update to the server.

- **Service Notification**
  If enabled, service notifications are delivered by the selected method. Note that service notifications are created by the Service Provider and are always published to the management logon page.

- **Provisioning Notification**
  If enabled, an alert is delivered by the selected method each time a provisioning task is created.

- **Operator Lockout Alert**
  If enabled an alert is delivered by the selected method when an Operator account becomes locked.

- **Operator Unlockout Alert**
  If enabled an alert is delivered by the selected method when an Operator account becomes unlocked.

- **Auth Node Changes**
  If enabled an alert is delivered by the selected method when an Auth Node is added, modified or removed from the virtual server.

- **Allocation/Deallocation Alert**
  If enabled an alert is delivered by the selected method whenever inventory (Capacity, tokens, SMS credits, ICE) are add to or removed from the virtual server.

External Alert Recipients Policy

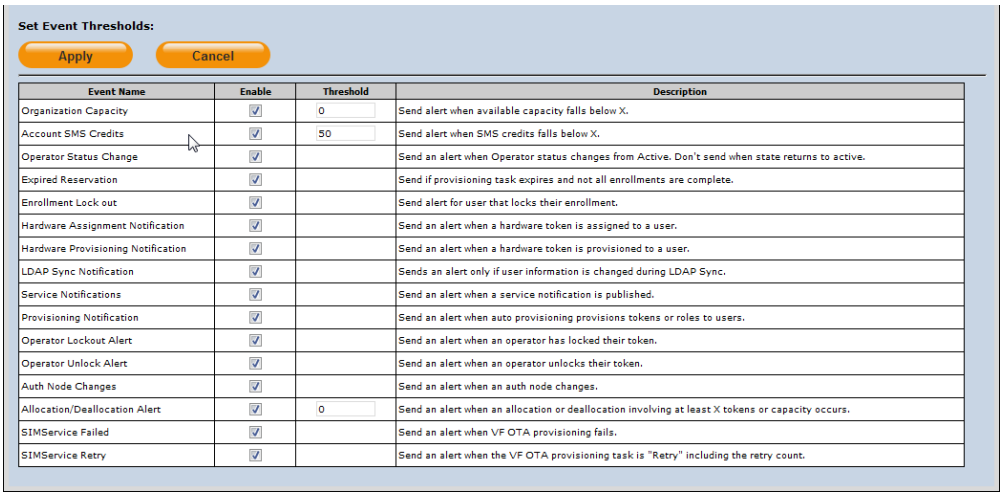
Use this policy to configure alerts and delivery method for recipients that are not Operators. Configuration of this policy is identical to Alert Management Policy with the following exceptions:

- **Alert Name**
  Use this to classify the set of alerts.

- **Alert Recipients**
  This is a list of recipients. A valid address or mobile number must be entered if alert delivery will be by email or SMS message respectively. Click the add button to update the recipient list.

Event Thresholds

Use this policy to configure the server to monitor for specific alerts and thresholds where:



Event Name	Enable	Threshold	Description
Organization Capacity	☑	0	Send alert when available capacity falls below X.
Account SMS Credits	☑	50	Send alert when SMS credits falls below X.
Operator Status Change	☑		Send an alert when Operator status changes from Active. Don't send when state returns to active.
Expired Reservation	☑		Send if provisioning task expires and not all enrollments are complete.
Enrollment Lock out	☑		Send alert for user that locks their enrollment.
Hardware Assignment Notification	☑		Send an alert when a hardware token is assigned to a user.
Hardware Provisioning Notification	☑		Send an alert when a hardware token is provisioned to a user.
LDAP Sync Notification	☑		Sends an alert only if user information is changed during LDAP Sync.
Service Notifications	☑		Send an alert when a service notification is published.
Provisioning Notification	☑		Send an alert when auto provisioning provisions tokens or roles to users.
Operator Lockout Alert	☑		Send an alert when an operator has locked their token.
Operator Unlock Alert	☑		Send an alert when an operator unlocks their token.
Auth Node Changes	☑		Send an alert when an auth node changes.
Allocation/Deallocation Alert	☑	0	Send an alert when an allocation or deallocation involving at least X tokens or capacity occurs.
SIMService Failed	☑		Send an alert when VF OTA provisioning fails.
SIMService Retry	☑		Send an alert when the VF OTA provisioning task is "Retry" including the retry count.

Figure 233: Set Event Thresholds

- **Organizational Capacity**
  This is related to the capacity of the virtual server. If enabled an alert is generated if the value falls below the threshold.

- **Account SMS Credits**
  This is related to the number of SMS credits in inventory. If enabled an alert is generated if the value falls below the threshold.

- **Operator Status Change**
  If enabled an alert is generated whenever an Operator account is created or removed and whenever the state of the Operator account changes between Active and Suspended.

- **Expired Reservation**
  This is related to provisioning tasks. If enabled an alert is generated when user has not enrolled a token prior to the task expiring.

- **Enrollment Lockout**
  This is related to enrolment tasks. If enabled an alert is generated if the user exceeds the maximum number of allowed attempts to enroll.

- **Hardware Assignment Notification**
  If enabled an alert is generated each time a hardware token is assigned to a user. The alert contains the UserID and User Detail.

- **Hardware Provisioning Notification**
  If enabled an alert is generated each time a hardware token is provisioned to a user. The alert contains the UserID and User Detail. Use this alert to automate distribution of hardware tokens, including use with 3rd party fulfillment.

- **LDAP Sync Notification**
  If enabled an alert is generated if one or more user records are updated during a LDAP synchronization.

- **Service Notifications**
  If enabled an alert is generated if a service notification is published by the Service Provider.

- **Provisioning Notification**
  If enabled an alert is generated when a provisioning task is generated.

- **Operator Lockout Alert**
  If enabled, the system will generate an alert whenever an Operator account becomes locked.

- **Operator Unlock Alert**
  If enabled, the system will generate an alert whenever an Operator account becomes unlocked.

- **Auth Node Changes**
  If enabled, the system will generate an alert whenever an Auth Node is added, modified or removed from the virtual server.

- **Allocation/Deallocation Alert**
  If enabled an alert is generated whenever inventory (Capacity, tokens, SMS credits, ICE) are add to or removed from the virtual server.

- **SIMService Failed**
  If enabled and the account has licensed SAE integration and OTA SIM provisioning, an alert will be generated if this is unable to provision the SIM/OTA server.

- **SIMService Retry**
  If enabled and the account has licensed SAE integration and OTA SIM provisioning, an alert will be generated if the provisioning retry attempts threshold is exceeded.

Language

Use this policy to set the language of the UI. Currently English is the only option.

Automation Policies Module

Automation policies are used to auto-provision users with tokens and control the self-enrollment and self-service functions.

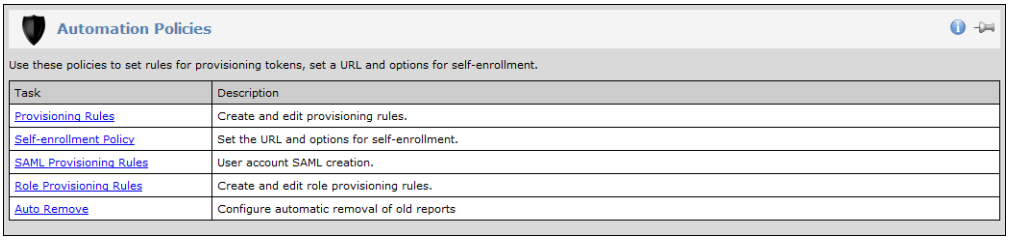


Figure 234: Automation Policies Module

Provisioning Rules

One of the most powerful features of the server, provisioning rules determine under what conditions tokens will be automatically issued and revoked. Rules are triggered when group memberships and other user attributes change. This means that if a user becomes a member of a group included in a rule, the user will be provisioned with a token. Conversely, when the user is no longer a group member, the token will be automatically revoked.

Provisioning rules can be used with internal groups or LDAP synchronized groups. By combining provisioning rules with LDAP synchronization or integration, the server can automatically issue and revoke tokens based on changes made in LDAP. In other words an Operator need not log into the management UI to create users and provision users with tokens as the combination of LDAP synchronization or integration and provisioning rules can achieve the same result.

To create a provisioning rule, begin by clicking the rules hyperlink, and then clicking the New Rule button.

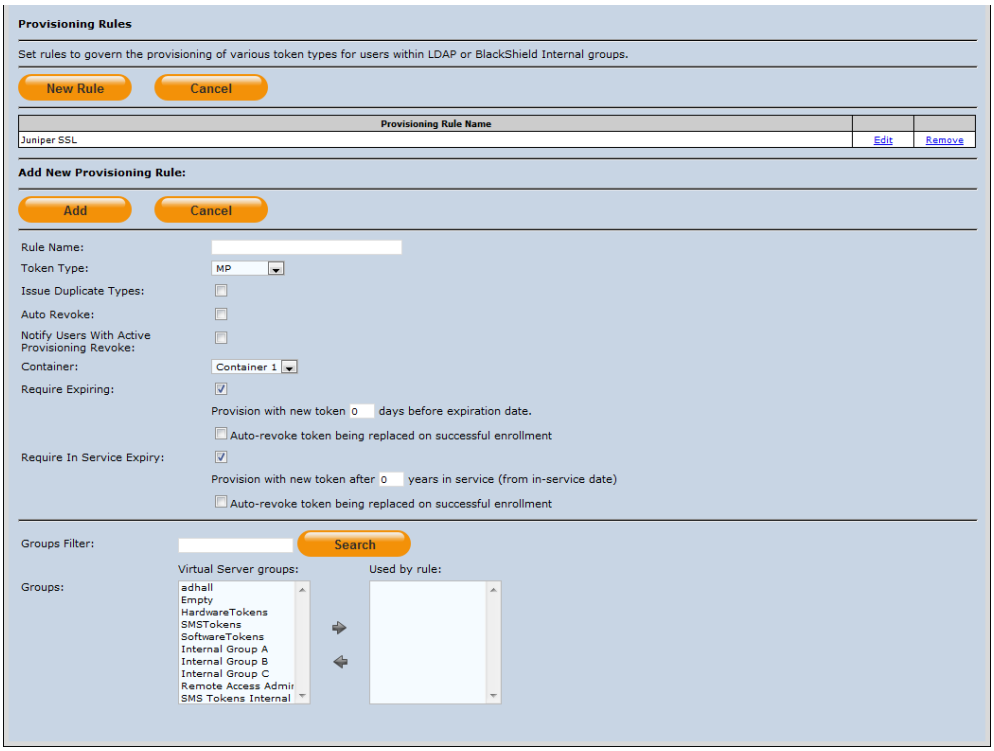


Figure 235: Provisioning Rules

- **Rule Name**
  This is a unique, descriptive name for the rule.

- **Token Type**
  This is the type of token to be provisioned when the rule evaluates true.

- **Issue Duplicate Types**
  If unchecked a user will not be provisioned with the selected token type if they already have one of the same type as a result of manually assigning a token or a different rule evaluating true.

- **Auto Revoke**
  If checked, the token issued by this rule will be revoked if the rule evaluates false for the user such as when a user has been removed from the monitored group(s).

- **Container**
  The user must reside in the selected container for the rule to evaluate true.

- **Require Expiring**
  Enable this option to provision a replacement token N days before the expiration date of any assigned tokens. Enabling the Auto-revoke sub-option results in the replaced token being revoked immediately upon the user completing enrollment of the replacement token.

Require In Service Expiry

This option is used to replace tokens that have been in the field for an extended period of time and are likely to need battery replacement. Enable this option to provision a replacement token for any assigned tokens that has been in use for more than N years. Enabling the Auto-revoke sub-option results in the replaced token being revoked immediately upon the user completing enrollment of the replacement token.

- **Assign as ICE Token**
  If checked, the user will be provisioned with an ICE token which after enrollment can only be used to authenticate during the life of the ICE license. This option is available only if ICE capacity has been added to the server.

- **Groups Filter**
  Use this option with "*" wildcard to limit the groups displayed in the Groups list.

- **Groups**
  A list of internal and synchronized groups. Server Groups represent groups that are not used by the rule whereas Rule groups represent groups to which users must belong for the rule to evaluate true. Highlight a group and use the appropriate arrow to move it between the group windows.

Combine provisioning rules with Pre-authentication rules to seamlessly migrate users from static passwords to token authentication without service interruption and with little to no administration.

Self-enrollment Policy

Use this policy to control self-enrollment thresholds and alerts.

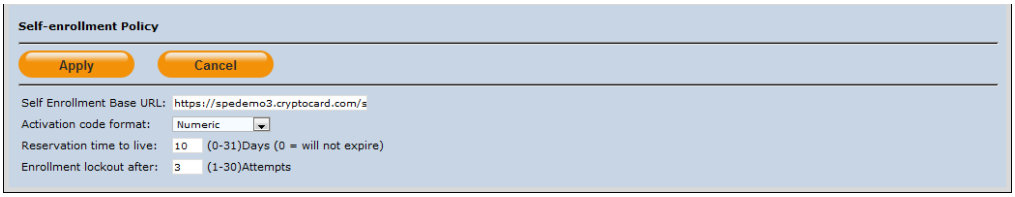


Figure 236: Self-enrollment Policy

- **Self-enrollment base URL**
  This is the URL to which the user will be directed as a result of a provisioning task and is included in the enrollment email instructions to the user. Do not modify this value unless you have installed a stand-alone enrollment web server.

- **Self-Enrollment over SSL**
  To enforce self-service over SSL, replace http with https in the self-enrollment base URL. Do not modify this value unless you have installed a stand-alone enrollment web server and have a valid certificate installed.

- **Activation Code Format**
  This option determines the strength of the activation code included in the enrollment message and encoded in the enrollment URL. Options are numeric, alphabetic or Alphanumeric formats.

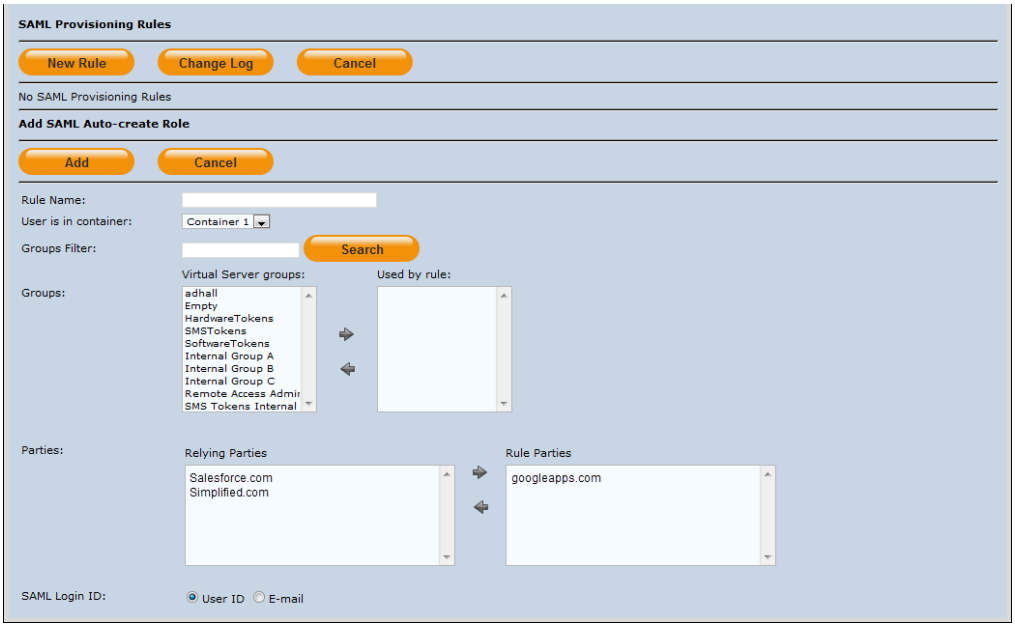
- **Reservation time to live**
  This is the maximum number of days the user has to complete enrollment commencing with the start date of the provisioning task. This value is added to the provisioning task start date to generate the provisioning task stop date. If set to 0, a provisioning task will never expire. The default value is 10 days.

- **Enrollment lockout after**
  This value determines the number of failed enrollment attempts by a user. When this threshold is exceeded, the user will be unable to enroll their token.

SAML Provisioning Rules

For a user to authenticate against a SAML Service Provider (e.g. Google Apps, Salesforce…), they must be given the appropriate rights. SAML Provisioning Rules are designed to replace the manual process (refer to SAML Services on page 128) of creating SAML associations. In effect, a rule automatically creates the appropriate associations based on user attributes such as group membership. For example, the action of adding or removing a user from an Active Directory security group will cause the rule to automatically create or remove SAML associations affected by the rule.

To configure or edit a rule, begin by click the New Rule button or edit hyperlink respectively.



- **Rule Name**
  This is a name that describes the rule.

- **User is in container**
  Users affected by this rule must be in the selected container.

- **Server Groups**
  Users in these groups are not affected by this rule.

- **Rule Groups**
  Users must be in one or more of these groups to be affected by this rule.

- **Relying Parties**
  Service Providers in this section are not affected by this rule. This list contains all configured SAML Service Providers (refer to SAML Service Providers Module on page 288).

- **Rule Parties**
  Users that belong to one or more of the Rule Groups will be able to authenticate against Service Providers in this section.

- **SAML Login ID**
  This is the UserID that will be returned to the Service Provider in the SAML assertion. Options are UserID or E-mail. A custom UserID can be configured manually for each user.

Auto Remove

Auto remove is used to automatically remove reports and alerts that are no longer required based on their age. This function only removes the entries in the various lists. Data is retained in the system and available by rerunning the report if necessary.

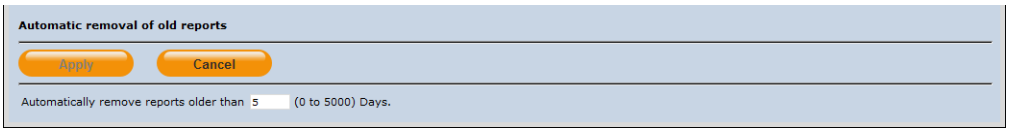


Figure 237: Auto Remove

Comms Tab

On this tab:

- **Communications Module**
  Configure and customize SMS gateways, SMTP email and content of outbound SMS and Email messages.

- **LDAP Module**
  Configure LDAP user source and schema mapping

- **Authentication Processing**
  Configure Pre-authentication rules, LDAP Synchronization and Agent key files.

- **Auth Node Module**
  Configure Auth Nodes, sharing and Realms

- **Custom Branding**
  Customize the appearance of the management UI.

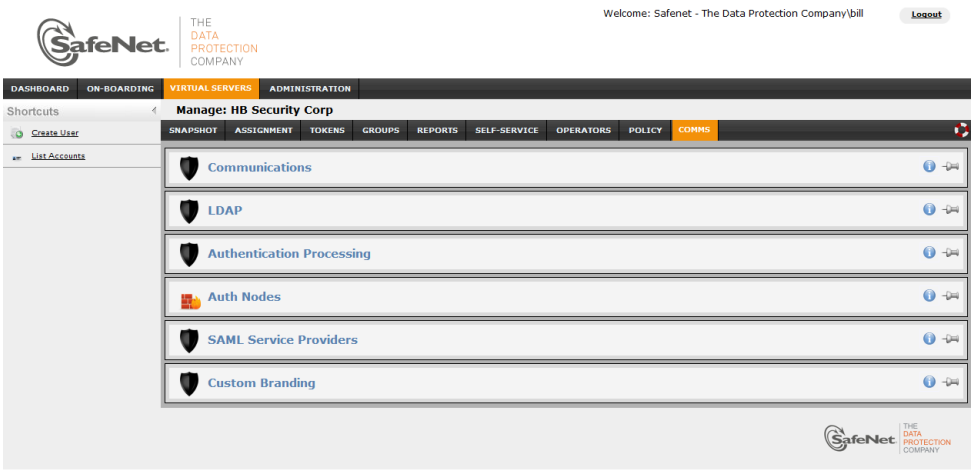


Figure 238: COMMS Tab and Modules

Communications Module

- **SMS Settings**
  SMS gateways are used to send SMS/OTPs and alerts. There are two options for sending SMS messages:

- **Default**
  In this option, SMS messages will be sent via your Service Provider's SMS gateway. This option can

be used only if you have been allocated SMS credits by your Service Provider. You can verify this from the Allocation Module on the Snapshot tab under the SMS Credits column.

- **Custom**
  Select this option to configure the Virtual Server to send SMS messages via a gateway service to which you've subscribed or SMS modem installed at your site. You can verify the ability to send SMS messages by entering the number of a device capable of receiving SMS messages in the SMS Mobile Number field. SMS phone numbers must contain only digits and must begin with a country code.

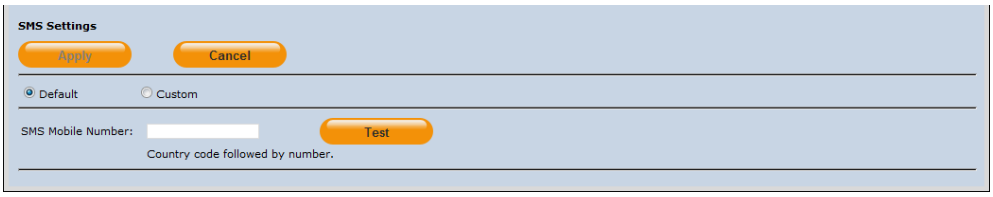


Figure 239: SMS Gateway Configuration

Custom SMS Settings

To configure the Virtual Server to use an SMS gateway service or modem, start by selecting the Custom option:

- Gateway
  Select to configure a primary and failover SMS service provider.

- SMS Plugin
  The list includes a number of preconfigured providers. For unlisted providers, select the Generic HTTP(s) SMS Plugin option.

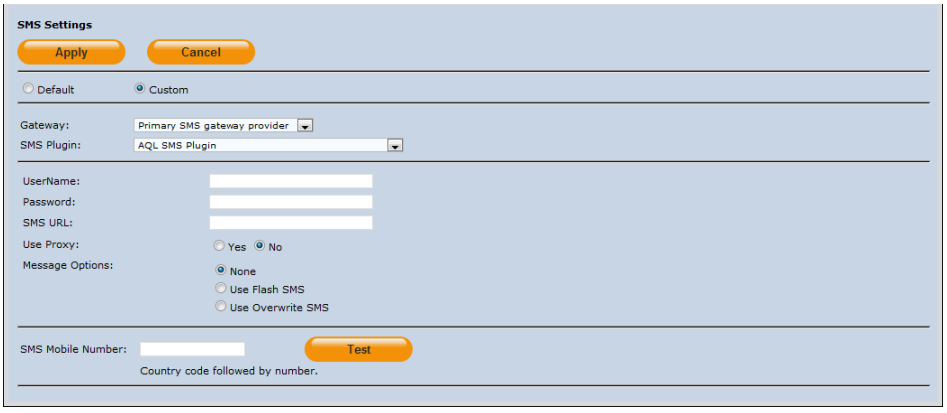


Figure 240: Custom SMS Settings

The options for configuration will vary depending on your SMS plug-in selection. Your gateway service provider will supply the necessary configuration information.

Other configuration options that may be available, depending on your network and SMS gateway service provider:

- **Use Proxy**
  If you will be sending SMS messages via a Proxy Server, select the "Yes" option and add the Proxy URL, Port number, User Name and Password.

- **Use Flash SMS**
  Use this option if the gateway supports Flash SMS and you do not want SMS messages stored on the receiving device.

- **Use Overwrite SMS**
  Use this option if the gateway supports Overwrite SMS, causing the previous SMS message stored on the receiving device to be overwritten by each new message.

Selecting the Generic HTTP(s) SMS Plugin provides options to configure communications with SMS service providers not included in the drop down list. Refer to the provider's documentation for guidance on formatting entries in SafeNet Authentication Service

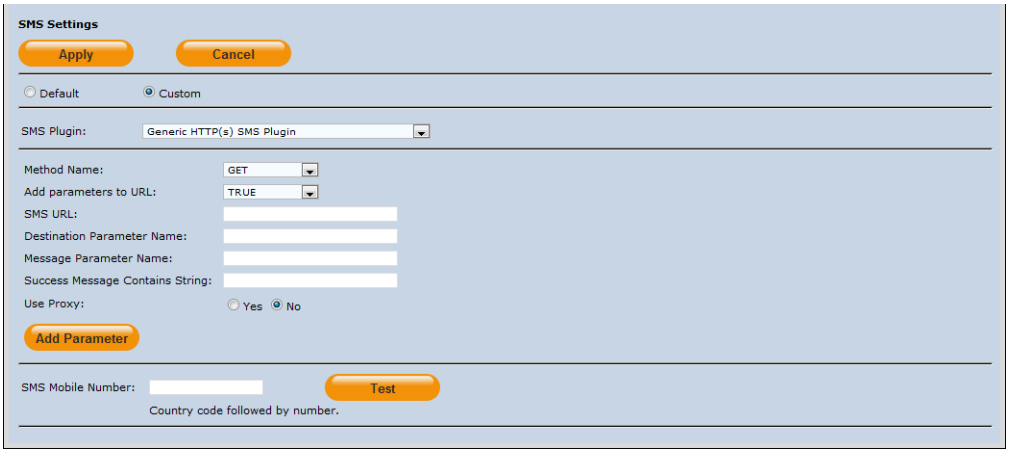


Figure 241: SMS Settings - Custom HTTP(s) SMS gateways

E-mail Settings

SMTP servers are used to send enrollment messages and alerts. There are two options for sending e-mail messages:

- **Default**
  In this option, email messages will be sent via your Service Provider's SMTP server.

  Note that e-mail sent via the Service Providers SMTP server will not appear to come from your account. In addition, any failed deliveries (e.g. Invalid e-mail address) will be sent to the Service Provider's e-mail server.

- **Custom**
  Select this option to configure the Virtual Server to send email messages via the account's SMTP server. E-mail sent via the account's SMTP server will appear to come from the account. Any failed

delivery notices will be sent to the account's e-mail server. You can verify the Virtual Server's ability to send e-mail messages by entering a valid e-mail address in the Test To Address field, and then clicking the Test button.

If using a 3rd party email server, you can modify the "From Address" by choosing the Custom option in the From Address group then enter a custom address.

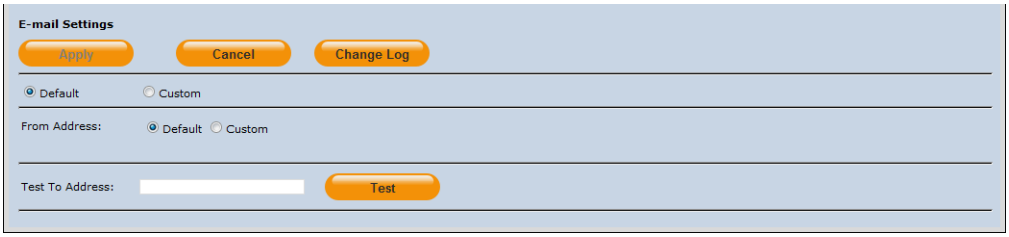


Figure 242: E-Mail Configuration

Custom E-mail Settings

To configure the Virtual Server to use the account's SMTP server, start by selecting the Custom option.

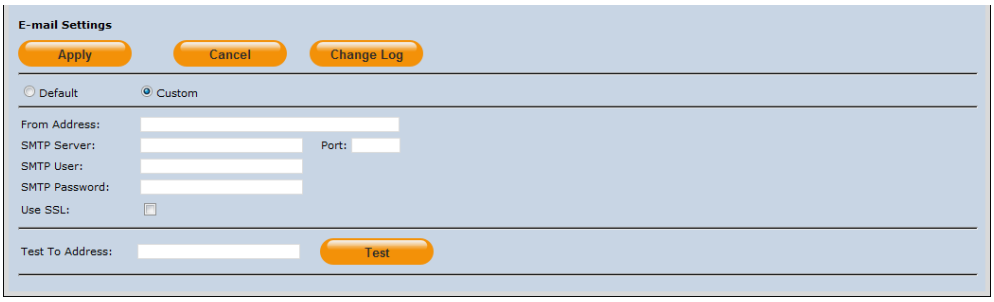


Figure 243: Custom E-mail Settings

- **From Address**
  This is the "From" name (e.g. "System Administrator") and valid account (e.g. account@myco.com) on your SMTP server from which e-mail will be sent. For example: System Administrator (account@myco.com)

- **SMTP Server and Port number**
  This is the SMTP server name or IP address and port number (e.g. Name: smtp.myco.com Port #: 25).

- **SMTP User and SMTP Password**
  If the SMTP server requires authentication, enter an account and password in these fields.

- **SSL**
  Select this option if your SMTP server is configured to use SSL.

SMS Messages

You can customize the various SMS/OTP messages that are sent by the Virtual Server. Start by selecting the Custom option, and then select an SMS Message Type from the dropdown list. The message content is displayed in the Message window.

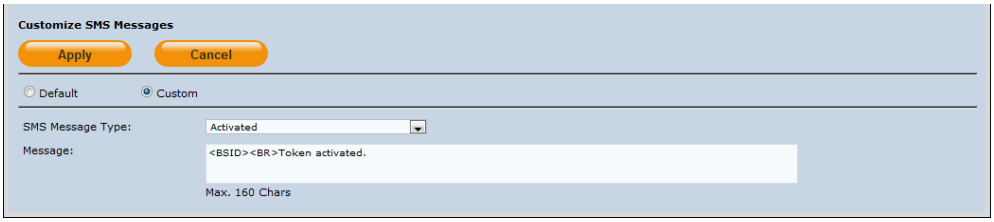


Figure 244: Customize SMS Messages

Custom SMS Messages

Message content can be modified as required bearing in mind that SMS messages greater than 160 characters in length (including spaces) will be split into 2 or more messages.

Tags are used to insert information from the Virtual Server into your message content. The following tags may be used:

Tag	Use
** **	Text following this tag is on a new line.
<NEW_PIN>	New PIN value set by Operator or via Self-Service
<NEXT_OTP>	OTP (Refer to SMS/OTP Policy on page 214)
<USER_ID>	User ID
<PIN>	PIN
<TEMP_PIN>	Temporary Password (Token suspended by Operator)
<BSID>	This value is replaced by the values in the Custom Product Name field.

The following is a list of SMS messages and corresponding events that cause the messages to be sent.

Message	Event	Valid Tags
Activated	Sent when suspended token is Unlocked by Operator	<BSID>
Activated New PIN	Sent when suspended token is Unlocked by Operator and a New PIN is set.	<BSID> <NEW_PIN>
New Challenge/Response	Sent when SMS token in challenge/response mode is provisioned.	<BSID> <USER_ID>
New Challenge/Response with no PIN	Sent when SMS token in challenge/response mode is provisioned and no PIN is required.	<BSID> <USER_ID>
New PIN	Sent when a new PIN is set by an Operator.	<BSID> <NEXT_OTP><PIN>
New PIN Change Next	Sent when a new PIN is set by an Operator and PIN change on first use is required.	<BSID> <NEXT_OTP><PIN>
New QUICKLog	Sent when SMS token in QUICKLog mode) is provisioned.	<BSID> <USER_ID><NEXT_OTP><PIN>
New QUICKLog with no PIN	Sent when SMS token in QUICKLog mode is provisioned and a PIN is not required to use the token.	<BSID> <USER_ID><NEXT_OTP>
Next OTP	Sent after successful SMS/OTP authentication for tokens in QUICKLog mode.	<BSID> <NEXT_OTP>
Next OTP with no PIN	Sent after successful SMS/OTP authentication for tokens in QUICKLog mode and a PIN is not required to use the token.	<BSID> <NEXT_OTP>
Suspended	Sent when the SMS/OTP token is Suspended.	<BSID>
Suspended Temp Password	Sent when the SMS/OTP token is Suspended and a temporary password is set for the user.	<BSID> <TEMP_PIN>
Test Successful	Sent when testing SMS Settings.	<BSID>

E-Mail Messages

You can customize the various e-mail messages that are sent by the Virtual Server. Start by selecting the Custom option, and then select an e-mail Message Type from the dropdown list. The message content is displayed in the Message window.

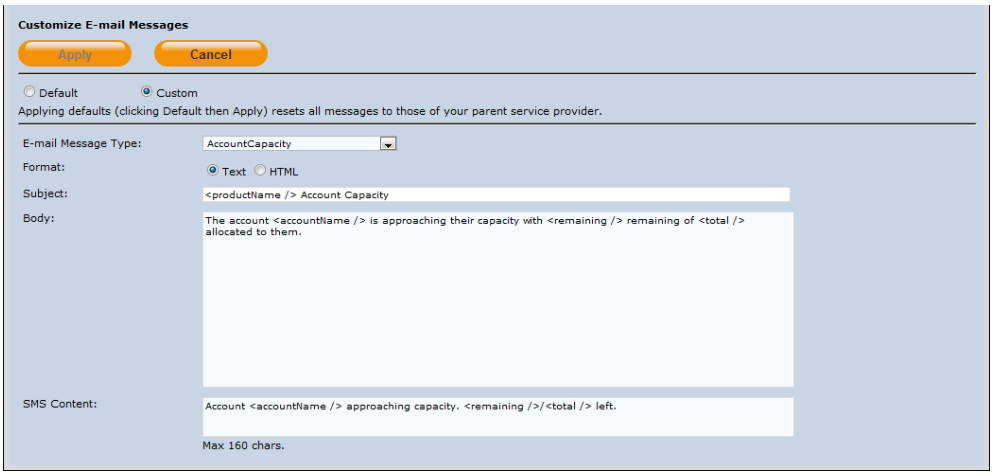


Figure 245: Customize E-mail Messages

Messages that are sent in response to an Alert can be sent by e-mail, SMS or both (Refer to Alert Management Policy on page 228). The SMS Content field is presented for messages that support both types of delivery. SMS messages greater than 160 characters including spaces will span multiple SMS messages.

- Note that an SMS Credit is consumed for each SMS alert message unless the Virtual Server is configured to use an SMS gateway.

Custom E-mail Messages

Message content can be modified as required. Select the Text or HTML option to send content using plain text of HTML respectively.

Tags are used to insert information from the Virtual Server into your message content. Many tags are available for specific messages only. The following tags may be used:

Tag	Use
** **	Text following this tag is on a new line.
<accountName />	Company name associated with Virtual Server
<remaining />	The remaining (unused) capacity in the Virtual Server.
<total />	The total capacity allocated to the Virtual Server
<active />	Virtual Server service as set by Service Provider (enabled / disabled)
<type />	Virtual Server service type (account, Virtual Service Provider, Evaluation)
<daysLeft />	Day before Service stop date.
<stepDate />	Service stop date as set by Service Provider
<dateTime />	Timestamp of an event
<firstName>	First name of a User
<lastName>	Last name of a User
<blackberryURL />	Unique URL for self-enrollment of MP-1 token on BlackBerry generated by Virtual Server.

Tag	Use
<reportName />	Name of a report
<name />	User ID
<taskeID />	Provisioning task number generated by Virtual Server.
<count />	Number of users that did not complete self-enrollment before the Provisioning Task expiration.
<username />	A User's UserID (User Detail)
<Uaddress />	Address (User Detail)
<Ucity />	City (User Detail)
<Uprovince />	State/Province (User Detail)
<Upostal />	Postal/Zip (User Detail)
<Ucountry />	Country (User Detail)
<orgName />	Account Name (Virtual Server)
<Oaddress />	Account address (Virtual Server)
<Oprovince />	Account State/Province (Virtual Server)
<Opostal />	Account Postal/Zip (Virtual Server)
<Ocountry />	Account country (Virtual Server)
<otaURL />	Unique URL for self-enrollment to install MP-1 generated by Virtual Server.
<tokenPIN />	PIN for MP-1 token enrollment on Java phone.
<capLeft />	Remaining Virtual Server license capacity.
<capTotal />	Total Virtual Server license capacity.
<expiryDate />	Server license expiration date
<expiryTime />	Days remaining before license expires.
<capLeft />	Service capacity remaining.
<capTotal />	Service capacity total.
<tokenList />	Serial numbers of tokens no longer associated with users.
<freeSpace />	Disk space remaining.
<diskSize/>	Total disk space.
<percentageFree />	Percentage of available space versus total disk size .
<consoleLink />	Unique URL for Operator Validation and logon to management UI.
<username />	Unique UserID used by Operator to logon to management UI.
<unlockTime/>	Time a user account will automatically unlock.
<organization />	Account to which a user belongs.
<state />	Operator account status. (active, pending, suspended)
<remaining />	Quantity of SMS Credits in Virtual Server inventory.
<selfEnrollURL />	Unique URL sent to user for self-enrollment.
<addList />	List of users added by synchronization with an external user data source.
<ignoreList />	Total number of users not updated during synchronization as users already exist in the Virtual Server.
<updateList />	Total number of users removed by synchronization as users no longer exist in the external data source.
<removeList />	List of users removed by synchronization as users no longer exist in the external data source.

Tag	Use
<totalMarkforRemoval />	Total number of users not found in external data source during synchronization. These users will be removed from the Virtual Server after 24 hours have elapsed.
<markedList />	List of users not found in external data source during synchronization. These users will be removed from the Virtual Server after 24 hours have elapsed.
<tokenType />	Type of token. (KT, MP…)
<time />	Date/Time of request by user to be issued a token.
<oldState />	State of token (assigned, active…) when token was assigned to user.
<newState />	The State a token is moved to by the Virtual Server when the user to which it was assigned can no longer be found.
<serial />	Serial number of a token.
<remaining />	Quantity of a type of token remaining in inventory.
<total />	Total quantity of tokens registered in the Virtual Server.
<failAttempts />	Quantity of consecutive failed logon attempts.

The following is a list of SMS messages and corresponding events that cause the messages to be sent where:

- **SP Alert**
  These alerts are only available to accounts where the Service Type is Virtual Service Provider.
- **Alert**
  These alerts are available in all account Service Types.
- **HAlerts**
  These are system alerts and are valid only for the hosting service.
- **Enrollment**
  These messages are sent as part of a Provisioning and/or Self-enrollment process.

Custom Email Messages

Account Capacity

Type
SP Alert
Event
Sent when Virtual Server capacity falls below configured event threshold.
Subject
SafeNet Authentication Service Account Capacity
Body
The account <accountName /> is approaching their capacity with <remaining /> remaining of <total /> allocated to them.
SMS Content

Account <accountName /> approaching capacity. <remaining />/<total /> left.

Account Removed

Type
SP Alert
Event
Sent when an Account (Virtual Server) is removed.
Subject
SafeNet Authentication Service Account Removed
Body
The account <accountName /> has been removed by <operator />.
SMS Content
Account <accountName /> removed by <operator />.

Account Status Change

Type
SP Alert
Event
Sent when a Virtual Server account is enabled or disabled.
Subject
SafeNet Authentication Service Account Status Change
Body
The account <accountName /> has changed to an <active /> <type />
SMS Content
Account <accountName /> changed to an <active /> <type />.

Account Stop Date

Type
SP Alert
Event
Sent X days in advance of Service stop date.
Subject
SafeNet Authentication Service Account Stop Date
Body
The account <accountName /> is approaching their stop date. There are <daysLeft /> day(s) till the stop date on <stopDate />.
SMS Content
<daysLeft /> day(s) till stop on <stopDate /> for account <accountName />.

Active Evaluation Stop Date

Type
SP Alert
Event
Sent X days in advance of Service stop date for evaluation accounts.
Subject
SafeNet Authentication Service Evaluation Stop Date
Body
The account <accountName /> is approaching their evaluation stop date. There are <daysLeft /> day(s) till the stop date on <stopDate />.
SMS Content
<daysLeft /> day(s) till stop on <stopDate /> for eval account <accountName />.

Android Token

Type
Enrollment
Event
Sent to User enrolling MP-1 on an Android device.
Subject
Over-The-Air (OTA) Installation for Android Device
Body
<firstName /> <lastName />: Follow these 2 easy steps to install the MP-1 token on your Android device: Step 1: Tap the icon below to download the MP-1 from Android Market.   Step 2: Now that the MP-1 is installed, you can click the URL below to install the MP-1 token profile.   <otaURL />
SMS Content
The MP-1 token Download URL: <otaURL />

Auth Service Down

Type
SP Alert
Event
Sent if an element of the service is downgraded or unavailable.
Subject
SafeNet Authentication Service Authentication Service Error
Body
This message is to report that the SafeNet Authentication Service authentication service was found to be unresponsive at <dateTime />, during a scheduled check of the service.
SMS Content
SafeNet Authentication Service authentication service down at <dateTime />

AuthNode Changes

Type
SP Alert
Event
Sent if an element of the service is downgraded or unavailable.
Subject
SafeNet Authentication Service Auth Node Changes
Body
The Auth Node <nodeName /> in account <accountName /> was <action /> by <changedBy />.
SMS Content
Auth Node <nodeName /> in <accountName /> <action /> by <changedBy />.

Blackberry PIN

Type

Enrollment

Event

Sent to Users receiving BlackBerry token by e-mail. First of two messages.

Subject

SafeNet Authentication Service Auth Node Changes

Body

<firstName /> <lastName />:

This e-mail will assist you in the installation and activation of your new SafeNet Authentication Service token into your Blackberry. Step one is to install the Token Authenticator and Token Attachment handler application on your BlackBerry. Step two is the installation and activation of the actual token. Please make note of the PIN below, as it is required to activate your token.

To install the Token Authenticator "Over-the-Air", browse to the URL below with your BlackBerry. If the application is installed via Desktop Manager (USB) or Blackberry Enterprise Server, this step is not necessary. Again, please make note of your token activation PIN. Your token will be issued to you shortly.

<blackberryURL />

Your token activation PIN is: <tokenPIN />

SMS Content

Blackberry Token

Type

Enrollment

Event

Sent to Users receiving BlackBerry token by e-mail. Second of two messages.

Subject

SafeNet Authentication Service Blackberry Token

Body

<firstName /> <lastName />:

Your new SafeNet Authentication Service BlackBerry token is attached.

To install the token, move the cursor to the attached file at the bottom of this message. Click the trackwheel or trackball and then select the Load Token option on the menu. It will pop up the SafeNet Authentication Service BlackBerry token installation wizard and prompt for the user name and activation PIN. Use the activation PIN received in the previous e-mail. If you have not received an activation PIN, contact your HELP Desk.

SMS Content

SafeNet Authentication Service MP Token

Type
Enrollment
Event
Sent to Users receiving MP-1 token by e-mail.
Subject
SafeNet Authentication Service MP Token
Body
<<firstName /> <lastName />: Your new SafeNet Authentication Service MP token is attached. To install, double click on the attached token. This will launch the MP-1 Software Tools installation wizard and prompt you for the activation PIN. Use the activation PIN received in the previous e-mail. If you have not received an activation PIN, or you do not have the MP-1 Software Tools installed, please contact your Help Desk or Administrator.
SMS Content

Completed Report

Type
Alert
Event
Sent to recipients receiving reports by e-mail.
Subject
SafeNet Authentication Service Report Results
Body
<accountName /> Results of the report <reportName /> are attached.
SMS Content

Enrollment Lockout

Type
Alert
Event
Sent when a User exceeds the maximum number of attempts to self-enrol. (Refer to Self-enrollment Policy on page 235)
Subject
Enrollment Lockout
Body
<accountName />, The user <name /> has been locked out of self enrollment at <dateTime /> because there have been too many failed attempts to enroll.
SMS Content
User <name /> has been locked out of self enrollment

Enrollment Out of Band

Type
Enrollment
Event
Sent when a User during enrollment of a token provisioned using a shipping authority.
Subject
Enrollment Validation
Body
This e-mail is to validate an ongoing enrollment attempt. Your validation code is <code />. If you are not in the process of enrolling a token, this e-mail can be ignored.
SMS Content
Your enrollment validation code is <code />.

Expired Reservation

Type
Alert
Event
Sent when a Provisioning Task expires before all Users in the task have completed self-enrollment.
Subject
SafeNet Authentication Service Reservation is Expired
Body
Provisioning task <taskID /> has expired in account <accountName /> with <count /> users still pending enrollment. They will no longer be able to complete enrollment.
SMS Content
Reservation expired for user <userName />

Hardware Assignment Notification

Type
Alert
Event
Sent when manually assigning a hardware token.
Subject
SafeNet Authentication Service Token Assignment Notification
Body
A hardware token has been assigned <firstName /> <lastName />: <userName /> At: <Uaddress /> <Ucity /> <Uprovince /> <Upostal /> <Ucountry /> In company: <orgName /> At: <Oaddress /> <Ocity /> <Oprovince /> <Opostal /> <Ocountry />
SMS Content

Hardware Provisioning Notification

Type
Alert
Event
Sent when auto-provisioning a hardware token.
Subject
SafeNet Authentication Service Token Provisioning Notification
Body
A hardware token has been provisioned <firstName /> <lastName />: <userName /> At: <Uaddress /> <Ucity /> <Uprovince /> <Upostal /> <Ucountry /> In company: <orgName /> At: <Oaddress /> <Ocity /> <Oprovince /> <Opostal /> <Ocountry />
SMS Content

iPhone Token

Type
Enrollment
Event
Sent to User enrolling MP-1 on iPhone or iPad.
Subject
Over-The-Air (OTA) Installation for iPhone Device
Body
<firstName /> <lastName />: Follow these 2 easy steps to install the MP-1 token on your iPhone, iPod, iTouch or iPad: Step 1: Tap the icon below to download the MP-1 from App Store.   Step 2: Now that the MP-1 is installed, you can click the URL below to install the MP-1 token profile.   <otaURL />
SMS Content
The MP-1 token Download URL: <otaURL />

Java ME OTE

Type
Enrollment
Event
Sent to User enrolling MP-1 on Java phone.
Subject
SafeNet Authentication Service MP Token for Java-enabled Mobile Device
Body
<firstName /> <lastName />: This e-mail will assist you in the Over-the-Air (OTA) installation and activation of your new SafeNet Authentication Service Multi-Platform (MP) token on your Java-enabled Mobile Device. Initial PIN: <tokenPIN /> Download URL: <otaURL />
SMS Content
New SafeNet Authentication Service MP token: PIN:<tokenPIN /> Download URL: <otaURL />

Java ME USB

Type

Enrollment

Event

Sent to User enrolling MP-1 on Java phone via USB desktop connection.

Subject

SafeNet Authentication Service MP Token for Java-enabled Mobile Device

Body

<firstName /> <lastName />:

This e-mail will assist you in the desktop suite (USB) installation and activation of your new SafeNet Authentication Service Multi-Platform (MP) token on your Java-enabled Mobile Device.

Initial PIN: <tokenPIN />

==========

Download Nokia PC Suite:
http://www.nokia.ca/get-support-and-software/software/pc_suite/download

MP token installation on Nokia Phone:
<nokiaHelpURL />

==========

SMS Content

License Capacity

Type

HAlert

Event

Sent when Service capacity falls below minimum threshold.

Subject

SafeNet Authentication Service License Capacity Warning

Body

This message is a warning that your SafeNet Authentication Service system is nearing its maximum license capacity.

Remaining Active Token Capacity: <capLeft /> / <capTotal />

If you require more capacity, contact SafeNet Authentication Service to expand your license.

SMS Content

System Capacity warning: <capLeft /> / <capTotal />

License Expiry

Type
HAlert
Event
Sent X days before license expires.
Subject
SafeNet Authentication Service License Expiry Warning
Body
This message is a warning that your SafeNet Authentication Service system is nearing its license expiry. Your license expires on <expiryDate />. You have <expiryTime /> day(s) left before SafeNet Authentication Service shuts down. Contact SafeNet Authentication Service to get your license extended.
SMS Content
License expiry warning: Your license expires on <expiryDate />

License Accounts

Type
Alert
Event
Sent when remaining account capacity falls below minimum threshold.
Subject
SafeNet Authentication Service License Capacity Warning
Body
This message is a warning that your SafeNet Authentication Service system is nearing its maximum account capacity. Remaining account capacity: <capLeft /> / <capTotal /> If you require more accounts, contact SafeNet to expand your license.
SMS Content
System Account Limit warning: <capLeft /> / <capTotal />

List of Token Users Not Found

Type
Alert
Event
Lists token(s) no longer associated with users caused when users are removed from external user source before revoking token.
Subject
List of SafeNet Authentication Service Token Users Not Found
Body
The following list contains tokens that have had their state set to <newState /> because the users they were assigned to can no longer be found by SafeNet Authentication Service <tokenList />
SMS Content
Tokens have been orphaned in SafeNet Authentication Service Log in to see the details.

Low Disk Space

Type
HAlert
Event
Sent when disk space falls below minimum threshold.
Subject
SafeNet Authentication Service Low Disk Space Warning
Body
This message is to report that the free disk space on system drive <driveLetter /> is low. Details: Time of Report: <dateTime /> Free Space: <freeSpace /> bytes. Disk Size: <diskSize /> bytes. Percentage Free: <percentageFree />
SMS Content
Low disk space warning. <percentageFree />% free on <driveLetter />

Mail Test

Type
Alert
Event
Sent when testing email/smtp settings.
Subject
SafeNet Authentication Service E-mail Configuration Test
Body
E-mail configuration is correct if you have received this message.
SMS Content
SMS configuration is correct if you have received this message.

MP PIN

Type
Enrollment
Event
Sent to users receiving MP-1 token by email. First of two messages.
Subject
SafeNet Authentication Service MP Token PIN
Body
<firstName /> <lastName />: This e-mail will assist you in the installation of your new SafeNet Authentication Service MP token. Please make note of the PIN below, as it is required to activate your token, which will be issued to you shortly. Your token activation PIN is: <tokenPIN />
SMS Content

Operator E-mail Validation

Type
Enrollment
Event
Sent to user when promoted to Virtual Server Operator.
Subject
SafeNet Authentication Service E-mail Validation
Body
To activate your Operator account in the SafeNet Authentication Service Authentication Manager you must logon by following the link and using the e-mail address indicated below: Logon link: <consoleLink /> E-mail: <userName />
SMS Content
Welcome to SafeNet Authentication Service. Logon at <consoleLink />

Operator Lockout Alert

Type
Alert
Event
Sent to Operator when a user account becomes locked. (Account Lockout/Unlock Policy)
Subject
SafeNet Authentication Service User Lockout Alert
Body
Attention: The following user has been locked out of authentication access until <unlockTime />, following <failedAttempts /> consecutive failed logon attempts: Name: <firstName /> <lastName /> Username: <userName /> Account: <organization />
SMS Content
Account <userName /> in organization <organization /> has been locked.

Operator Unlock Alert

Type
Alert
Event
Sent to Operator when a user account becomes unlocked. (Account Lockout/Unlock Policy)
Subject
SafeNet Authentication Service User Unlock Alert
Body
Attention: The following user's authentication access has been unlocked: Name: <firstName /> <lastName /> Username: <userName /> Account: <organization />
SMS Content
Account Unlock Alert: User: <userName /> Organization <organization />

Operator Status Change

Type
Alert
Event
Sent when an Operator’s status changes. (active, pending, suspended)
Subject
Operator Status Change
Body
Attention: The following operator's state has been changed to <state /> User Account: <userName /> Account: <accountName />
SMS Content
<organization />: <userName />'s operator status changed to <state />

Organization Capacity

Type
Alert
Event
Sent when Virtual Server capacity falls below threshold.
Subject
SafeNet Authentication Service Capacity
Body
<accountName /> You are approaching your maximum capacity. <remaining /> left out of <total />
SMS Content
Approaching capacity: <remaining /> left of <total />

Organization SMS Credits

Type
Alert
Event
Sent when Virtual Server SMS Credits falls below threshold.
Subject
SafeNet Authentication Service SMS Credits
Body
<accountName />, Your available SMS credits are getting low. You have <remaining /> left.
SMS Content
SMS Credits low. <remaining /> left

Provisioning Cancelled

Type
Alert
Event
Sent to users that have not completed self-enrollment when the corresponding provisioning task is cancelled.
Subject
SafeNet Authentication Service Provisioning Cancelled
Body
<First /> <Last />, your pending token provisioning has been cancelled. The enrollment link you received in a previous E-mail is no longer active.
SMS Content
Your token provisioning has been cancelled.

Self Enrollment

Type
Enrollment
Event
Self-enrollment instructions sent to users as part of a provisioning task.
Subject
SafeNet Authentication Service Self-enrollment
Body
<firstName /> <lastName />: Your self-enrollment account has been created. If you are enrolling a hardware token, and do not have your token yet, please contact your system administrator. Please, go to the following URL to enroll with SafeNet Authentication Service: <selfEnrollURL /> If the above link does not work, please copy and paste this url to your web browser.
SMS Content
SafeNet Authentication Service Self Enrollment: Enroll at <selfEnrollURL />

Self Service Report Lost Token

Type
Enrollment
Event
Self-service Confirmation of Lost Token
Subject
SafeNet Authentication Service Self-enrollment
Body
<firstName /> <lastName />: Please click the following link to confirm your lost token report. <url /> If the above link does not work, please copy and paste this url to your web browser. Please confirm your lost token report within the next 10 minutes.
SMS Content
Please click the following link to confirm your lost token report. <url />. Please confirm your lost token report within the next 10 minutes.

Self Service Request Token

Type
Enrollment
Event
Sent when a user initiated token request is received from self-service.
Subject
Self-service Confirmation of Token Request
Body
<firstName /> <lastName />: Please click the following link to confirm that you requested a token. <url /> If the above link does not work, please copy and paste this url to your web browser. Please confirm your request within the next 10 minutes.
SMS Content
Please click the following link to confirm that you requested a token. <url />. Please confirm your request within the next 10 minutes.

Self Service Temp Password

Type
Enrollment
Event
Sent when a user requests a sign-in credential for the self-service site.
Subject
Self-service Temporary Sign in Password
Body
<firstName /> <lastName />: Your self-service temporary sign in password is: <password /> Please use this password to sign in within the next 10 minutes.
SMS Content
Your self-service temporary sign in password is: <password />. Please use this password to sign in within the next 10 minutes.

Service Notification

Type
Alert
Event
Sent when a service notification is enabled by a Service Provider and delivery method is email.
Subject
SafeNet Authentication Service Notification
Body
SafeNet Authentication Service Notification – contents of this message should be changed to reflect the notification.
SMS Content
SafeNet Authentication Service Notification

SIM Service Failed

Type
Alert
Event
Sent when a SIM/OTA service is unable to provision a user.
Subject
SIM Provisioning Failed
Body
Task <taskID /> to MSISDN <MSISDN /> for user <userName /> has failed after <attempts /> attempt(s).
SMS Content
Task <taskID /> for <userName />@<MSISDN /> has failed after <attempts /> attempt(s).

SIM Service Retry

Type
Alert
Event
Sent when a SIM/OTA service retries a provisioning task.
Subject
SIM Provisioning requires retry
Body
Task <taskID /> to MSISDN <MSISDN /> for user <userName /> has not been completed after <attempts /> attempt(s). It will be attempted <remaining /> more times.
SMS Content
Task <taskID /> for <userName />@<MSISDN /> has failed after <attempts /> attempt(s).

Sync Notification

Type
Alert
Event
Sent whenever an LDAP sync task updates the virtual server.
Subject
LDAP Sync notification
Body
The following actions have been processed for <orgName />: The following <totalAdded /> new users have been added: <addList /> The following <totalUpdated /> existing users have been updated: <updateList /> The following <totalRemoved /> users have been removed: <removeList /> The following <totalMarkForRemoval /> users have been marked for deletion: <markedList /> They will continue to exist for 24 hours, during which period they have been marked as disabled. If this was a result of a misconfiguration, fixing the configuration will re-enable the users. Note: If you have deleted a user in LDAP, re-creating a new user with the same user name will NOT restore the existing user.
SMS Content
Task <taskID /> for <userName />@<MSISDN /> has failed after <attempts /> attempt(s).

Token Request Ack

Type
Enrollment
Event
Sent to user to acknowledge request to be issued a token.
Subject
SafeNet Authentication Service Token Request Acknowledged
Body
This message is to confirm that your request for a <tokenType /> token has been received as of <time />.
SMS Content
Your request for a SafeNet Authentication Service token has been received.

Token Request Deny

Type
Enrollment
Event
Sent to user when request to be issued a token is denied.
Subject
SafeNet Authentication Service Token Request Denied
Body
This message is to inform you that your request for a <tokenType /> token has been denied.
SMS Content
Your request for a SafeNet Authentication Service token has been denied.

Token User Not Found

Type
Alert
Event
Sent when token state is change when the user to which it was assigned is not found.
Subject
SafeNet Authentication Service Token User Not Found
Body
The token <serial /> which was assigned to user <userName /> has been changed from state <oldState /> to <newState /> This has occured because the user <userName /> can no longer be found by SafeNet Authentication Service
SMS Content
Token <serial /> has been orphaned as user <userName /> can not be found.

Token User Replaced

Type
Alert
Event
Sent when a User (UserID) with an assigned token is overwritten with a user from a different user source with an identical UserID. For example, a manually created userID is overwritten during LDAP synchronization which includes an identical UserID.
Subject
SafeNet Authentication Service Token User Replaced
Body
The token <serial /> which was assigned to user <userName /> has been changed from state <oldState /> to <newState /> This has occured because the user <userName /> has been overwritten by a new user <userName />.
SMS Content
Token <serial /> orphaned because user <userName /> was over written.

Token Request Approval 1

Type

Enrollment

Event

Sent to Approver 1 Authorities when a token request is received from the self-service site.

Subject

<productName /> Self-service token request

Body

LEVEL 1 APPROVAL

The following user has requested a token in <accountName />.

User: <userName />
First Name: <firstName />
Last Name: <lastName />
E-mail: <email />

Token type requested: <typeRequested />

To approve this request click on this link: <approveURL />.

To reject this request click on this link: <rejectURL />.

This request can also be approved or rejected by logging into the SafeNet Authentication Service Manager.

SMS Content

Self-service token request <taskID />. Click URL or logon to approve or reject.

Token Request Approval 2

Type

Enrollment

Event

Sent to Approver 2 Authorities when a token request is approved by an Approver 2 Authorities (if enabled)

Subject

<productName /> Self-service token request

Body

LEVEL 2 APPROVAL

The following user has requested a token in <accountName />.

User: <userName />
First Name: <firstName />
Last Name: <lastName />
E-mail: <email />

Token type requested: <typeRequested />

To approve this request click on this link: <approveURL />.

To reject this request click on this link: <rejectURL />.

This request can also be approved or rejected by logging into the SafeNet Authentication Service Manager.

SMS Content

Self-service token request <taskID />. Click URL or logon to approve or reject.

Token Request Issuer

Type

Enrollment

Event

Sent to Issuing Authorities when a token request has all necessary approvals.

Subject

<productName /> Self-service token request

Body

The following user has requested a token in <accountName />.

User: <userName />
First Name: <firstName />
Last Name: <lastName />
E-mail: <email />

Token type requested: <typeRequested />

To issue this request click on this link: <issueURL />.

This request can also be issued by logging into the SafeNet Authentication Service Manager.

SMS Content

Self-service token request <taskID />. Click the URL or logon to issue or reject.

Token Request Receipt

Type

Enrollment

Event

Sent to the requesting user to confirm receipt of the request from the self-service site.

Subject

<productName /> Token request receipt notification

Body

REQUEST RECEIPT PROCESSING

<firstName /> <lastName />,

Your request for a token has been received and is awaiting approval. Your request will be processed within the next <expireLength /> days.

SMS Content

Your request for a token has been received.

Token Request Shipper

Type
Enrollment
Event
Sent to the shipping authority once the token request has received the Issuing Authority approval (if enabled.)
Subject
<productName /> Self-service token request
Body
The token for the following request needs to be shipped in <accountName />. User: <userName /> First Name: <firstName /> Last Name: <lastName /> E-mail: <email /> Token type requested: <typeRequested /> After the token required for this request has been shipped, the request can be marked as shipped by logging into the SafeNet Authentication Service Manager.
SMS Content
Self-service token request <taskID /> ready for shipping.

Token Request Validation

Type
Enrollment
Event
Sent to the requesting user to require their confirmation of a request for a token from the self-service site.
Subject
Token Request Validation
Body
<P>Click on the link below or paste link into a browser to validate your token request.</P> <P>Requests that are not validated with <Days /> are automatically rejected.</P> <P>Validation URL: <URL /></P>
SMS Content
Go to <URL /> to validate token request.

Token Sub Capacity

Type
Alert
Event
Sent when remaining quantity of tokens in inventory falls below the minimum threshold.
Subject
SafeNet Authentication Service Token Capacity
Body
<accountName />, You are approaching your remaining capacity available to you. <remaining /> left out of <total /
SMS Content
Approaching capacity: <remaining /> left of <total />

User Lockout Alert

Type
Alert
Event
Sent to user when their account becomes locked due to excessive failed consecutive logon attempts
Subject
SafeNet Authentication Service User Lockout Alert
Body
<firstName /> <lastName />, you have been locked out of authentication access until <unlockTime />, following <failedAttempts /> consecutive failed logon attempts.
SMS Content
Your SafeNet Authentication Service account has been locked until <unlockTime />

User Unlockout Alert

Type
Alert
Event
Sent to user when their account becomes unlocked.
Subject
SafeNet Authentication Service User Unlock Alert
Body
<firstName /> <lastName />, you can again attempt to logon to the authentication service.
SMS Content
Your SafeNet Authentication Service account has been unlocked.

Windows Phone 7 Token

Type
Enrollment
Event
Sent to User enrolling MP-1 on Windows Phone 7 device.
Subject
Over-The-Air (OTA) Installation for Windows Phone 7 Device
Body
<firstName /> <lastName />: Follow these easy steps to install the MP-1 token on your Windows Phone 7 device: Step 1: Tap the icon below to download the MP-1 from Windows Phone Marketplace.   Step 2: Now that the MP-1 is installed, please complete the following steps: 1. Copy the code below by tapping it, and then drag the arrows at each end of the highlighted text to include the first and last characters, up to and including the trailing BSID characters at the end of the code.   <otaURL />   2. Tap Copy.   3. Open the MP-1, and then tap the Import button.   4. Tap inside the text box and then tap the Paste button to paste the download code.   5. Tap the Done button to complete the installation of the token.
SMS Content
The MP-1 token Download code: <otaURL />

LDAP Sync Server Settings

Used to change the default location to for the LDAP Sync Server. Sync agents will transmit to this location. Do not modify the default settings unless you have installed and configured as separate sync server.

FTP/SFTP/SCP Settings

Reports generated by the virtual server can be sent by FTP, SFTP or SCP on generation. This module defines the location and connection information to the remote FTP/SFTP/SCP server.

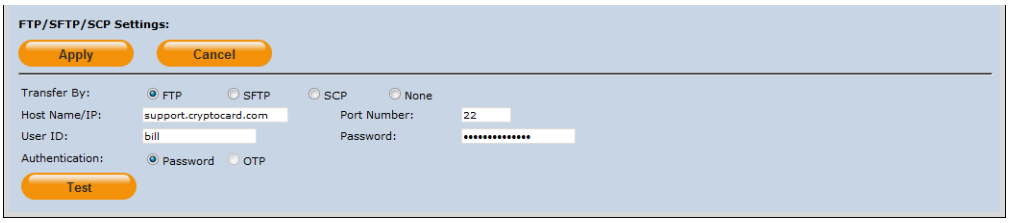


Figure 246: FTP/SFTP/SCP Settings

Configure the connection information by selecting the type of transfer, server location and connection method. Choose the OTP option if you have configured the server to require OTP authentication. The In this case the UserID must have an active MP-1 token.

Use the test button to test the connection to the server.

LDAP Module

The LDAP module is used to configure LDAP integration.

- LDAP Integration should only be configured where a high speed, permanent connection is assured and LDAP failover is configured. Loss of connection between the Virtual Server and all LDAP user sources will result in authentication service outage.
- This feature is only available on SafeNet Authentication Service SPE and PCE Editions. For SafeNet Authentication Server (SAS) refer to LDAP Sync Server Settings on page 273.
- If your LDAP/AD is not using a default schema, you must configure a compatible schema in the Virtual Server before configuring the LDAP User Source. Do this from the Schema Management hyperlink. (Refer to Schema Management on page 276)

LDAP User Source

To configure LDAP Integration, begin by clicking the LDAP User Source hyperlink, and then follow the steps to configure the Virtual Server to connect directly to your LDAP/Active Directory.

- **Host name or IP**
  This is the FQDN host name or IP address of your LDAP/AD.
- **Port**
  This is the port number allowed to connect to LDAP/AD.
- **Use SSL**
  Check this option if you have a properly installed and configured certificate on your LDAP/AD server.
- **Number of Failover hosts**
  Indicates the number of failover LDAP/AD servers to which the Virtual Server will attempt to connect in the event the primary LDAP/AD cannot be reached.

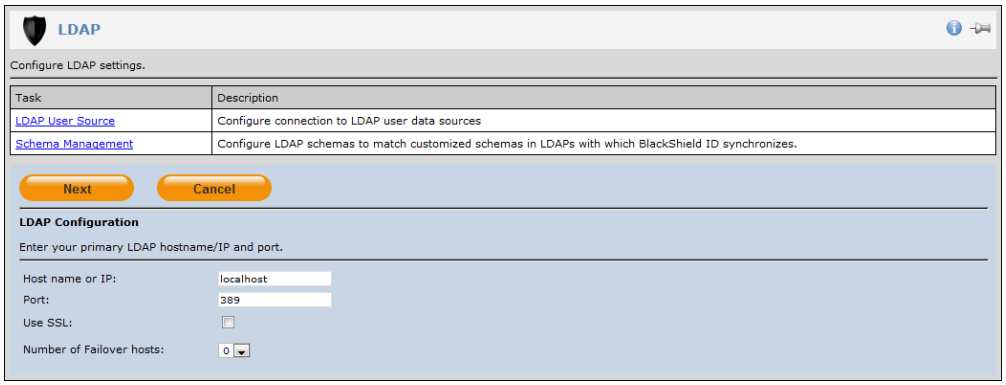


Figure 247: LDAP Module

Once a connection has been established, you must choose an LDAP Schema from the dropdown list. The list contains default schemas.

LDAP/Active Directory Integration

If your LDAP/AD is not using a default schema, you must configure a compatible schema in the Virtual Server before configuring the LDAP User Source. Do this from the Schema Management hyperlink. (Refer to Schema Management on page 276)

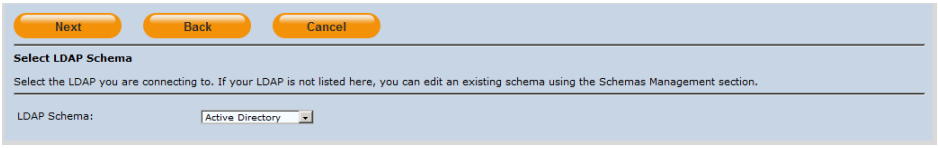


Figure 248: Select base LDAP Schema

Next provide a valid user account that can be used by the Virtual Server to connect to your LDAP/AD.

The Virtual Server will not write to LDAP. The account privileges need only be sufficient to allow the Virtual Server to connect and browse the schema.

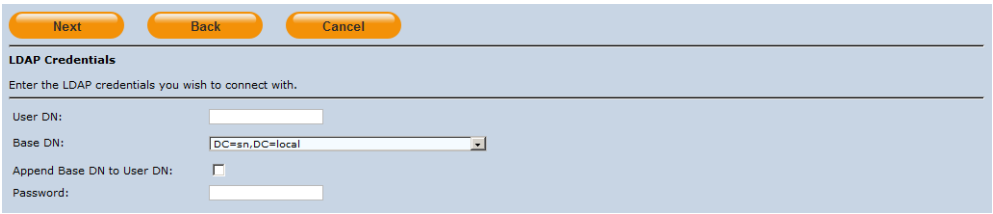


Figure 249: LDAP Credentials

Once a connection has been established, the Virtual Server will automatically detect all DNs containing users that will be integrated with the Virtual Server. Users added or removed from these DNs will automatically be added or removed from the Virtual Server.

Use the Manually edit searched containers option to remove DNs from integration with the Virtual Server.

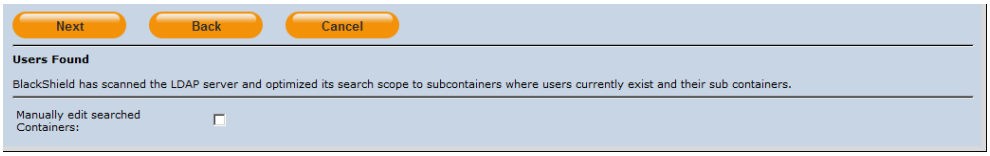


Figure 250: Select DNs

The Virtual Server can simultaneously support LDAP Integration or LDAP Synchronization and creation and management of users in its SQL database. If you intend to use the Virtual Server to authenticate users in your LDAP/AD user source as well as users that are not in that user source, check this option.

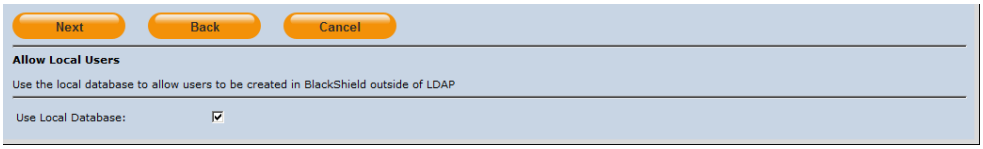


Figure 251: LDAP and Virtual Server User Sources

Click Done to save the configuration. Users in your LDAP/AD will automatically be populated in the Virtual Server.

Schema Management

You can add a custom schema to the Virtual Server. Start by clicking the Schema Management hyperlink, and then choose a default schema that is most like your custom schema by selecting from the Schema dropdown list.

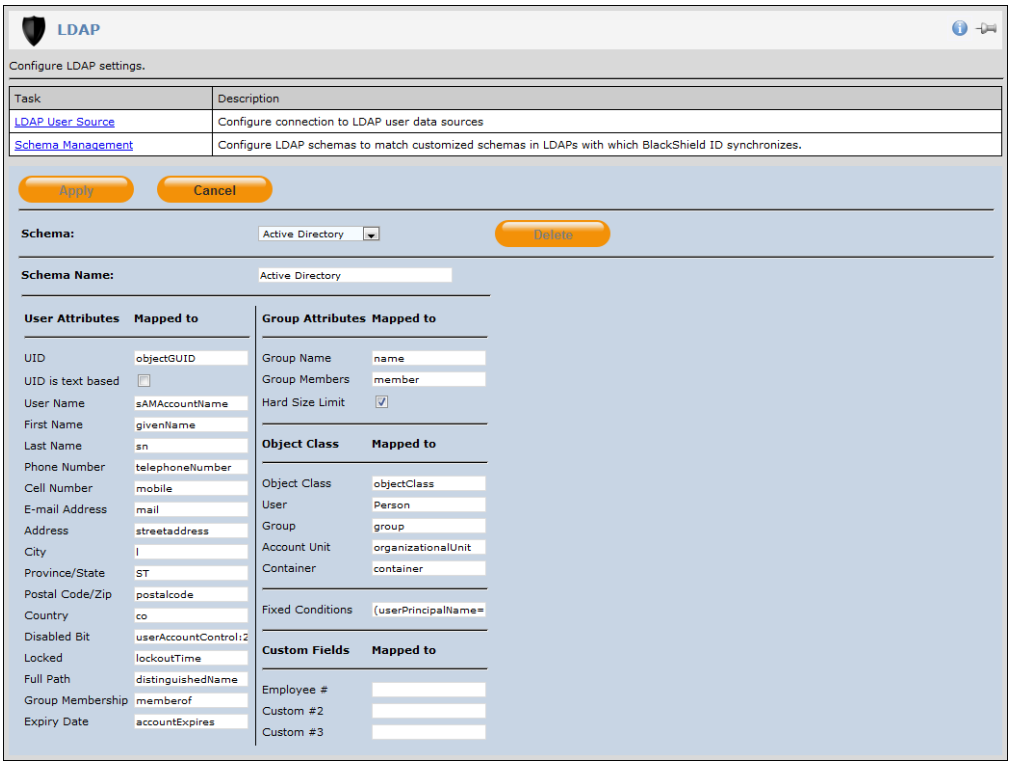


Figure 252: Custom Schemas

The page displays the default schema mappings. Adjust the defaults to map your schema to the User and Group Attributes, Object Class and Custom Fields where:

- **User Attributes and Custom Fields**
  These are the fields that appear in the User detail.

The Virtual Server in conjunction with LDAP Pre-auth Rules can take advantage of additional attributes found in Active Directory including:

- **userAccountControl**
  The Virtual Server will not authenticate a User whose account is disabled in Active Directory.
- ***lockoutTime***
  The Virtual Server will authenticate a user only during the Days/Times set in Active Directory.
- **memberOf**
  The Virtual Server will authenticate a user based on their Active Directory group membership. This is usually combined with source IP and other attributes in Pre-authentication rules.
- **accountExpires**
  The Virtual Server will not authenticate an expired Active Directory user account.

Authentication Processing Module

In this module:

- **Pre-Authentication Rules**
  Determines the conditions that must be satisfied before a user is allowed to authenticate.
- **Authentication Agent Settings**
  Generates a unique encryption file used by agents to authenticate against the Virtual Server.
- **Remote Service Settings**
  Generates a unique encryption file to be used by Remote Services against the Virtual Server.
- **LDAP Sync Agent Settings**
  Generates a unique encryption file to be used by the LDAP Sync Agent to synchronize LDAP/AD user sources with the Virtual Server.
- **ICE Activation**
  Activates ICE capacity allowing MP-1 ICE tokens and capacity to be used to accommodate a short term requirement to increase the number of users that can authenticate against the system.
- **LDAP Sync Agent Hosts**
  Use this to add allowed LDAP sync agents to the virtual server by name and source IP address.

Task	Description
Pre-authentication Rules	Set filter attributes to be evaluated before validating credentials.
Authentication Agent Settings	Generate encryption keys required for remote authentication agents.
Remote Service Settings	Generate encryption keys required for remote service agents.
LDAP Sync Agent Settings	Confirm or clear LDAP Sync Agent settings.
LDAP Sync Agent Hosts	List of all remote host names/IPs of servers syncing to BlackShield ID

Figure 253: Authentication Processing Module

Pre-authentication Rules

Just because a user is able to provide a valid one-time passcode does not necessarily mean that they should be granted access to the network. Other conditions such as network access point, group membership, account status and other attributes might be important in allowing or denying access.

Security Administrators can use Pre-authentication Rules to apply additional conditions that must be met for authentication to succeed.

The key advantages of Pre-authentication Rules are:

- Rules can be applied to LDAP/Active Directory user account attributes.
- Rules can be applied to user accounts maintained in the internal SQL user data source.
- Rules can be applied based on network access points (source IP, Agent).

- Rules can be used to modify the authentication sequence (OTP, LDAP, LDAP + OTP).
- Changes to user attributes made in LDAP or the internal user data source are immediately effective on SafeNet Authentication Service.
- Rules can have a fixed start and/or stop date; a useful feature for transitioning from static passwords to OTP authentication.

There are few limitations to how Pre-authentication Rules can be used. Rules can be relatively simple, checking a single attribute such as time of day restrictions or can be complex, checking multiple attributes such as group membership, network access point and token state.

The authentication proceeds in the following sequence:

1. UserID is validated. If valid:
2. Pre-authentication rules are applied. If any rule is satisfied:
3. Password is validated. If valid, access is granted.

The key concepts to consider when creating rules are:

Multiple rules may be configured, however a user's attributes need only satisfy one rule for authentication to proceed.

Initially SafeNet Authentication Service is configured with an "Allow All" rule. Pre-Authentication Rules must be enabled to provide the restrictions.

Configure Pre-Authentication Rules

Begin by clicking the Pre-authentication Rules hyperlink, and then clicking the New Rule button. Enter a name and description for the rule, and then select a filter from the drop down list. Possible filters are:

- Agent is
- Date Restrictions
- IP
- LDAP Password pass through
- User is a member of

Figure 254: Pre-authentication Rules

Agent is

This attribute is used to specify which agents are allowed to authenticate against the Virtual Server. For example, Agent is IAS would allow RADIUS authentication from all Microsoft IAS/NPS servers with the appropriately configured SafeNet Authentication Service IAS/NPS agent.

Filter: Agent is	Description
Authentication API	Required to allow authentication from 3rd party applications that added authentication using the SafeNet Authentication Service Authentication API.
Citrix	Required to allow authentication via the SafeNet Authentication Service Agent for Citrix Web Interface.
Console	Required to allow remote management connections to SafeNet Authentication Service server
IAS	Required to allow authentication via the SafeNet Authentication Service Agent for IAS / NPS
IIS	Required to allow authentication via the SafeNet Authentication Service Agent for IIS
Remote Management API	Required to allow the Command Line Interface (CLI) to connect to SafeNet Authentication Service server.
Juniper / Funk SBR	Required to allow authentication via the SafeNet Authentication Service Agent for Juniper/Funk Steel Belted RADIUS
Windows Logon	Required to allow authentication via the SafeNet Authentication Service Agent for Windows Domain Logon.

Date Restrictions

This attribute is used to limit the lifetime of a rule. This rule is always used in conjunction with another attribute. For example it could be used with the “LDAP password pass through” attribute to facilitate migration from LDAP passwords to token authentication, whereby LDAP passwords would be valid against SafeNet Authentication Service until the rule expires or a token is activated.

Filter: Date Restrictions	Description
Begin this rule on	If enabled, the rule will not be active until the indicated date. If disabled, the rule is immediately effective.
Expire this rule on	If enabled, the rule will stop being enforced on this date. If disabled, the rule will remain active.

IP

If enabled, SafeNet Authentication Service will not process authentication requests from NAS devices such as VPNs and firewalls that have an IP address outside of the defined range. This attribute is usually used in conjunction with another attribute. For example, if combined with a group membership attribute, only members of a specific group could authenticate at a NAS device in the IP range. Conversely, in the absence of any other contravening rule, members of the group would not be able to authenticate at a NAS device not in the IP range. This filter supports IPv4 and IPv6 addressing.

Filter: IP	Description
Is equal to	Specifies a single valid IP address
Is in the range	Specifies an IP address range
Is in mask	Specified and IP address range using a mask

LDAP Password Pass Through

This attribute determines when SafeNet Authentication Service should validate a password or pass it through to LDAP for validation. It also determines how SafeNet Authentication Service will handle LDAP authentications that fail.

The primary purpose of this attribute is transparent migration of users from static passwords to token authentication. For users that meet the conditions, authentication will “pass through” SafeNet Authentication Service to LDAP for validation. There is no need to create, manage or import the LDAP static password into SafeNet Authentication Service. It also determines the action to be taken by SafeNet Authentication Service after LDAP authentication. This attribute is usually combined with Date Restrictions and Agent or IP attributes.

For example, enabling LDAP Password Pass Through if a user has no token or temporary password would mean that any user with a token must use it to authenticate while those without could continue to use their LDAP password until they received or enrolled their token or until the Date restriction disabled this attribute.

Filter: LDAP Password Pass Through	Description
Always	All passwords will be passed to LDAP for validation
When user has no SafeNet Authentication Service Token/Password	Passwords will be passed to LDAP for validation only if the user does not have a token in the Active, Suspended or Locked state.
If LDAP Authentication fails	
Reject the authentication	Access is denied if LDAP authentication fails
Forward request to SafeNet Authentication Service	SafeNet Authentication Service attempts to validate the password.

User is a member of

This attribute is used to require group membership for authentication to proceed. It is normally used in conjunction with Agent or IP attributes so that a user must be a member of a specified LDAP group when authenticating at the defined agent or IP address.

This attribute does not require group membership to be configured in SafeNet Authentication Service. Users LDAP group memberships can be checked with each authentication. This means that group memberships can manage from LDAP. Use "*" as a wildcard to filter available groups.

Filter: User is a member of	Description
User is a member of	User must be a member of the specified group in the list. To create a list, separate LDAP group names with a semi-colon ";"

Authentication Agent Settings

SafeNet Authentication Service agents send authentication requests to the Virtual Server. Security sensitive data sent between the server and agents is protected by AES 256 encryption. To encrypt the traffic and to prevent unauthorized agents, the Virtual Server requires that each agent use an identical encryption key file.

A default encryption key file is automatically created by the Virtual Server.

For optimum security a new encryption key file should be created and used to replace all default Authentication Agent key files.

To create an Agent Key File, begin by clicking the Authentication Agent Settings hyperlink, and then clicking the Create button.

Figure 255: Create Agent Key File

Download the newly created key file and use it when prompted during configuration of any SafeNet Authentication Service agent that will authenticate against the Virtual Server. For information on individual agents and configuration go to www.safenet-inc.com or www.cryptocard.com.

Remote Service Settings

This setting is not available on SafeNet Authentication Service Cloud.

Remote Service allows command line clients to send management instructions to the Virtual Server. Security sensitive data sent between the server and agents is protected by AES 256 encryption. To encrypt the traffic and to prevent unauthorized command line clients, the Virtual Server requires that each client use an identical encryption key file.

A default encryption key file is automatically created by the Virtual Server.

For optimum security a new encryption key file should be created and used to replace all default Remote Service key files.

To create a Remote Service Key File, begin by clicking the Remote Service Settings hyperlink, and then clicking the Create button.

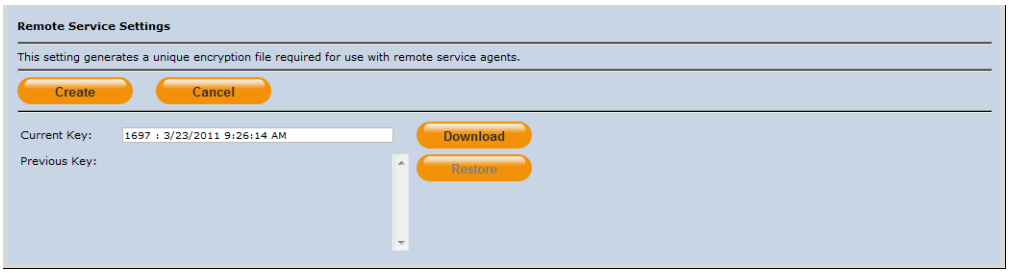


Figure 256: Create Remote Service Key File

Download the newly created key file and use it when prompted during configuration of any SafeNet Authentication Service agent that will authenticate against the Virtual Server.

LDAP Sync Agent Settings

The LDAP Sync Agent Settings generates an encryption key file that is required by the LDAP Sync Agent to encrypt data transmitted between the sync agent and the Virtual Server. This section also includes settings that determine how the Virtual Server handles Operator accounts under certain conditions described below.

Begin by clicking the LDAP Sync Agent Settings hyperlink, enable/disable the options, then download the Sync Agent key file and install with your LDAP Sync Agent.

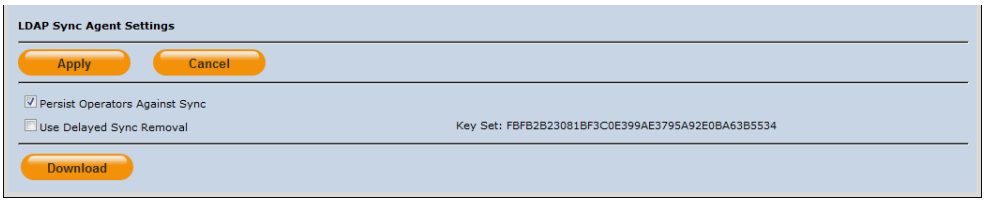


Figure 257: LDAP Sync Agent Settings

- **Persist Operators Against Sync**
  By default, synchronized user accounts are removed from the Virtual Server when removed from a synchronized group in your external data source (LDAP/AD). If this option is unchecked, users that have been promoted to Operator will also be removed. Checking this option ensures that unintended changes to the LDAP account do not prevent the Operator from logging into the Virtual Server management UI. If checked, Operator accounts must be manually removed.

- **Use Delayed Sync Removal**
  This option delays removal of synchronized user accounts from the Virtual Server for 24 hours. It is intended to protect against unintentional user account removal due to a significant but erroneous change at the remote user source. If an event is detected, the Virtual Server can send an Alert to Operators indicating that a change will occur in 24 hours unless they intervene.

ICE Activation

This option is available only if ICE (In Case of Emergency) capacity has been allocated to the Virtual Server. ICE is used to temporarily increase the Virtual Server capacity and quantity of MP-1 tokens and therefore the number of users that can authenticate against the Virtual Server in response to an extraordinary situation or event.

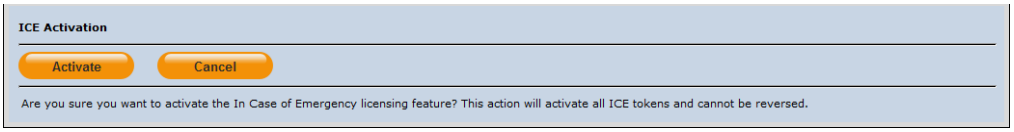


Figure 258: Activating ICE

All ICE licenses are valid for 30 days from activation and can be activated one time only. Once activated the license will persist for 30 days or until overwritten by a new ICE license. Unused time or capacity is not retained.

Users that have been provisioned with ICE MP-1 tokens will be able to self-enroll at any time prior to activation or after activation of the ICE license. However, on expiration of ICE, they will not be able to authenticate. Note that their ICE tokens remain valid for use if a subsequent ICE license is activated.

To activate an ICE license, click the ICE Activation hyperlink, and then click the Activate button.

LDAP Sync Agent Hosts

This lists all LDAP sync agents that are allowed to synchronize with this virtual server.

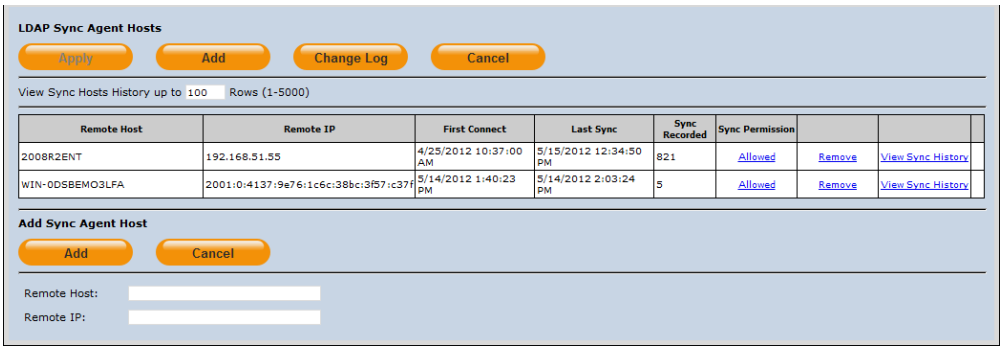


Figure 259: LDAP Sync Agent Hosts

Click Add to create a new entry in the table, then enter the name of the remote agent and its source IP address. The sync agent can send LDAP changes with Sync Permissions are set to “Allowed”. Use the hyperlinks:

- **Sync Permissions**
  Toggles between Allowed and Denied.
- **Remove**
  To remove a sync agent from the list.
- **View Sync History**
  To view synchronization activity.

Auth Node Module

An Auth Node is any RADIUS client, Agent or application (e.g. VPN and web applications such as Outlook Web Access) that will send authentication requests to the Virtual Server. This module displays a list of configured Auth Nodes and allows adding, editing and removal of Auth Nodes.

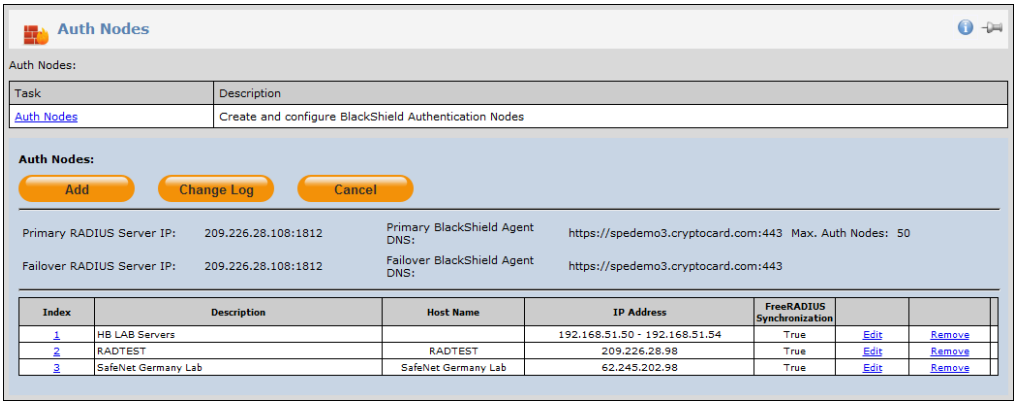


Figure 260: Auth Nodes Module

An entry in the Auth Nodes table must be created for every Auth Node. The number of Auth Nodes cannot exceed the allowed number set by your Service Provider. The Virtual Server will not process authentication requests received from devices or applications that are not in the list.

Configuring Auth Nodes

To configure an Auth Node, click the Add button and enter at least the following:

For RADIUS clients such as SSL VPNs:

- A descriptive name of the device in the Agent Description field
- The IP Address of the RADIUS client
- The RADIUS Shared secret (this must be identical in both SafeNet Authentication Service and the RADIUS client)

For SafeNet Authentication Service Agents such as Agent for Outlook Web Access:

- A descriptive name of the device in the Agent Description field
- The IP Address of the Agent

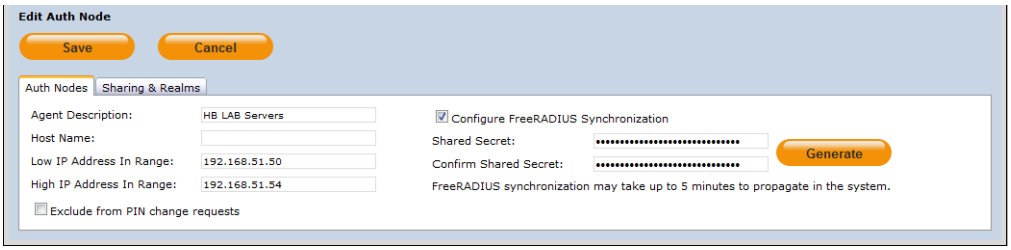


Figure 261: Auth Node Configuration

Some RADIUS Clients are not fully RADIUS compliant and do not support “Challenge-Response” which is a requirement for Server-side PIN changes. If your RADIUS client does not support Challenge-Response and you have configured your Server-side PIN policy to require the user to periodically change their PIN, check the “Exclude from PIN change requests” to prevent a forced PIN change with the non-compliant RADIUS client.

Sharing and Realms

Sharing and Realms is an optional service feature that allows an Auth Node to be shared with two or more organizations or Virtual Servers. Essentially a Realm is a group of Virtual Servers. For example, (referring to Figure 35: Sharing and Realms) Org 1 manages a Web Application and its own users for authentication. Org 1 wants users from 3 of its subsidiaries (Org 2, 3, 4), each with their own Virtual Server to be able to log into the Web App. In addition each Org has protected applications to which only

its users should have access. Using Sharing and Realms, Org 1 can share the Web App with other orgs while restricting access to other Auth Nodes to its own users.

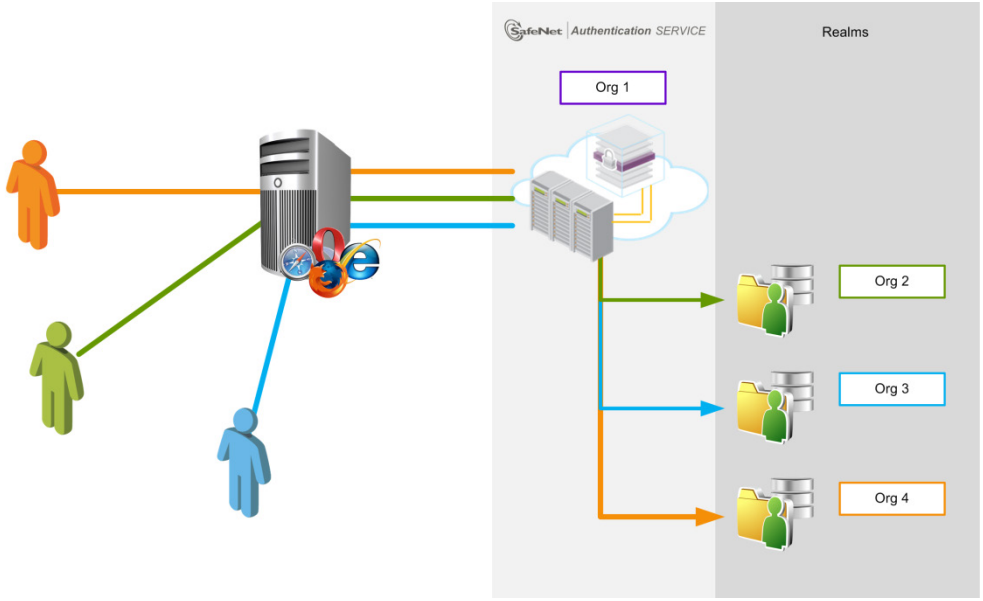


Figure 262: Sharing and Realms

To configure begin by clicking the Sharing and Realms tab, configure as necessary then click Save to commit the configuration where:

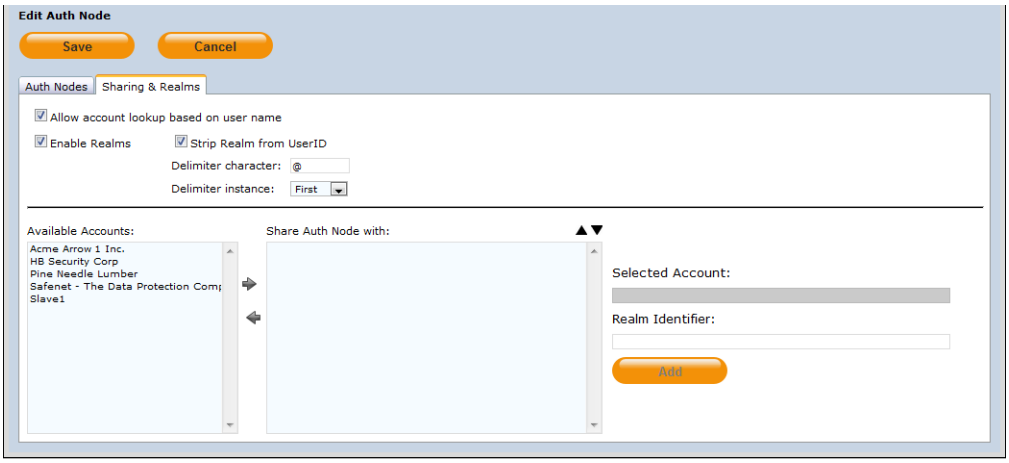


Figure 263: Sharing and Realms

Allow account lookup based on user name

The submitted UserID will be used to authenticate the user. The Virtual Server will search the “Shared Auth Node” list in descending order. The first matching UserID will be used to authenticate the user. Use the up/down arrows to move a selected realm up or down in the priority list. Effectively this means that all UserIDs must be unique across all Realms.

Enable Realms
Use this option where UserIDs may not be unique across all realms. If enabled, additional UserID information will be used to determine to which realm the user belongs. Typically the UserID will be an email address. Use this feature in conjunction with the Selected Account and Realm Identifier options.

Strip Realm from UserID
Strips all data starting with the delimiter character from the UserID. This allows a submitted UserID such as an email address (UserID@myco.com) to be authenticated as UserID.

Delimiter Instance
Uses the first instance of the delimiter (left to right) or last instance of the delimiter (right to left).

For example, consider two users with the identical UserID of BSmith, one belonging to ACME (acme.com), the other belonging to International Light (IL.com). Configured as follows:

- Realms enabled
- Strip realm from UserID
- Delimiter character is “@”
- Selected Realm= ACME, Realm Identifier= ACME.COM
- Selected Realm=International Light, Realm Identifier= IL.COM

The UserID of BSmith@acme.com would authenticate against the Acme Virtual Server with an effective UserID of BSmith while BSmith@IL.com would authenticate against the International Light Virtual Server with an effect UserID of BSmith.

SAML Service Providers Module

SAML Service Providers (e.g. Google Apps, Salesforce, Box.net…) can rely on SafeNet Authentication Service for authentication. Use this module to add Service Providers to the virtual server. For configuration examples using popular cloud applications, refer to the separate document: SAML Authentication with SafeNet Authentication Service Cloud.

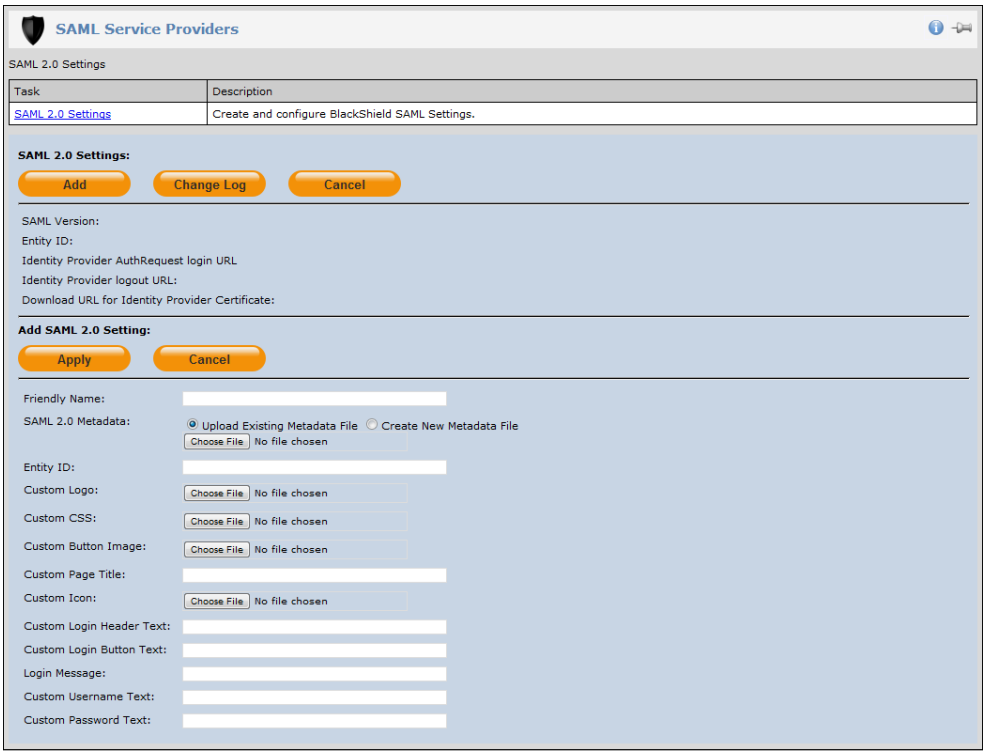


Figure 264: SAML Service Providers

The information displayed below the ADD button will be required by your Service Provider.

Click Add to insert a new provider into the list where:

- **Relying Party ID**
  This is the "Entity ID" of the SAML Service Provider, typically (but not always) in the form of a URL. This value will be provided by the SAML Service Provider or can be extracted from the metadata (XML file) provided by the SAML Service Provider.

  For example:

  <?xml version="1.0" encoding="UTF-8"?>
  <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID=https://mycompany.salesforce.com

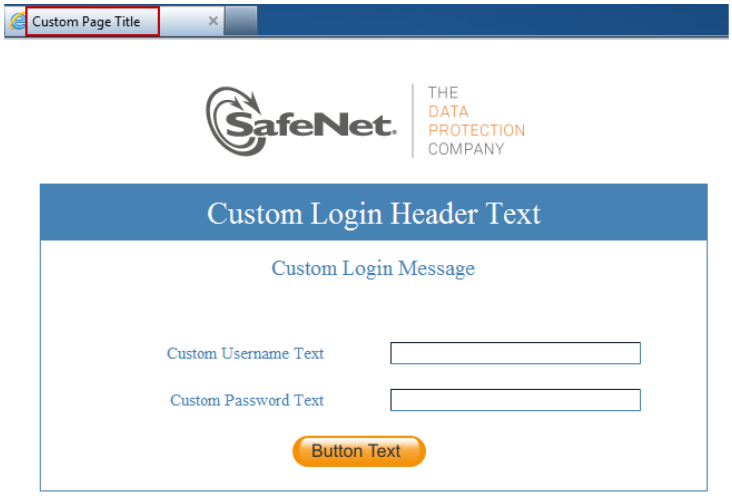
- **Friendly Name**
  This is a name you assign to the Relying Party for easy identification. This name will appear in SAML Services lists on the Assignment Tab | SAML Services Module and on the Policies Tab | Automation Policies | SAML Provisioning Rules.

- SAML 2.0 Metadata

- **Upload existing metadata file**
  This is an XML file that is generated by your SAML Service Provider.

- **Create new metadata file**
  Some SAML Service Providers do not provide a metadata file but instead provide only their Entity ID and Location (essentially the resource being accessed). Use this option to have the virtual server create and add a metadata file based on this information.

The remaining options are used to customize the appearance of the logon page presented to the user.



- **Custom Logo**
  This is the logo you want to appear on the logon form presented to your users during authentication.

- **Custom CSS**
  Modify the default CSS then upload to modify the appearance of the page. The following is the default CSS:

```
.tableBanner
{
   width: 600px;
   border-width: 0px;
   border-spacing: 0px;
   background-color: white;
}

.tableMain
{
   width: 600px;
```

```
    border-width: 1px;
    border-spacing: 0px;
    border-style: solid;
    border-color: #4682B4;
    border-collapse: separate;
    background-color: white;
    padding: 0px;
}

.tdTopSpaceAboveBanner
{
    height: 50px; text-align: center;
}

.tdBanner
{
    height: 100px; text-align: center;
}

.tdSpaceBelowBanner
{
    height: 50px; text-align: center;
}

.tdLoginHeader
{
    height: 50px; text-align: center; font-size: 28px; color: white; background-color: #4682B4;
padding-left: 0px; padding-right: 0px;
}

.tdLoginMessage
{
    height: 50px; text-align: center; font-size:20px; color: #4682B4;
}

.tdUserNameLabel
{
    text-align: right;
    font-size: 15px;
```

```
    color: #4682B4;
    padding-left: 70px;
}

.textUserName
{
    width: 225px; height: 20px; text-align: left; border-color: #4682B4; border-width: 1px;
}

.tdPasswordLabel
{
    text-align: right;
    font-size: 15px;
    color: #4682B4;
    padding-left: 70px;
}

.textPassword
{
    width: 225px; height: 20px; text-align: left; border-color: #4682B4; border-width: 1px;
}
.tdUserName
{
    padding-left: 60px;
}
.tdPassword
{
    padding-left: 60px;
}
.td20PxSpace
{
    height: 20px;
}
.td40PxSpace
{
    height: 40px;
}
.tdUserErrorMessage
{
```

```
    height: 40px; color: red; text-align: center; font-size: 14px;
}
.tdSubmit
{
    text-align: center; height: 30px;
}
.buttonSubmit
{
    background-color: white; background-repeat:no-repeat; border-width: 0px; width: 120px;
height: 28px; text-align: center; font-size: 14px; color: white;
}

.tdSpaceBelowLoginWindow
{
    height: 80px;
}

.relayingParty
{
    text-align: center; font-size: 10px; color:darkblue; height: 20px;
}
.sessionTimeout
{
    text-align: center; font-size: 12px; color:blue;
}
.sessionWarning
{
    text-align: center; font-size: 14px; color:crimson;
}
.copyRight
{
    text-align: center; font-size: 8px; color: darkblue; height: 20px;
}

.td404Error
{
    height: 40px; color: red; text-align: left; font-size: 28px;
}
.tdError
```

```
{
   height: 40px; color: red; text-align: left; font-size: 28px;
}
.tdWarning
{
   height: 40px; color: brown; text-align: left; font-size: 28px;
}
.tdInformation
{
   height: 40px; color: darkblue; text-align: left; font-size: 28px;
}
.tdSignoutMessage
{
   height: 40px; color: red; text-align: left; font-size: 18px;
}
.tdErrorMessage
{
   height: 40px; color: red; text-align: left; font-size: 14px;
}
```

- **Custom Button Image**
  This is the image used for the logon button.
- **Custom Page Title**
  This is the page title displayed on the browser tab.
- **Custom Icon**
  This is the displayed on the browser tab.
- **Custom Login Header Text**
  This is the text displayed in the header of the logon form.
- **Custom Login Button Text**
  This is the text displayed on the logon button.
- **Login Message**
  This is the text, usually containing instructions displayed between the Logon Header Text and the Username field.
- **Custom Username Field**
  This is the label for the user name field

- **Custom Password Text**
  This is the label for the password field.

Custom Branding Module

The appearance and branding of the Virtual Server management UI, Self-service and Enrollment web pages can be customized for colours, fonts, logos and titles.

The Virtual Server generates a unique URL for each customized page:

- **Customized Management UI Logon Page URL**
  This is the "Operator login URL" reference in the custom branding module.
- **Customized Self-service URL**
  This is the "Self Service Unique URL" found in the Self-service Tab | Configuring Self-service module.
- **Customized Enrollment pages**
  This is the "Self Service Unique URL" found in the Self-service Tab | Configuring Self-service module.

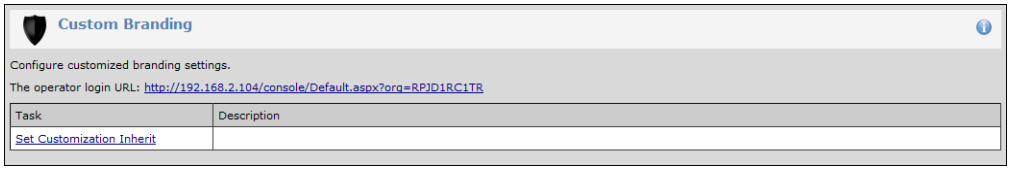


Figure 265: Custom Branding

To customize, begin by clicking the Set Customization Inherit hyperlink, clear the Use Customizations Inherit option, and then click Apply. The module will now display options for customizing Fonts, Colours, Buttons and Logos. Conversely, to discard customizations, check the set customization inherit option.

> Note: if Use Customizations Inherit is re-enabled, the Virtual Server inherits system defaults and not the defaults from the Service Provider.

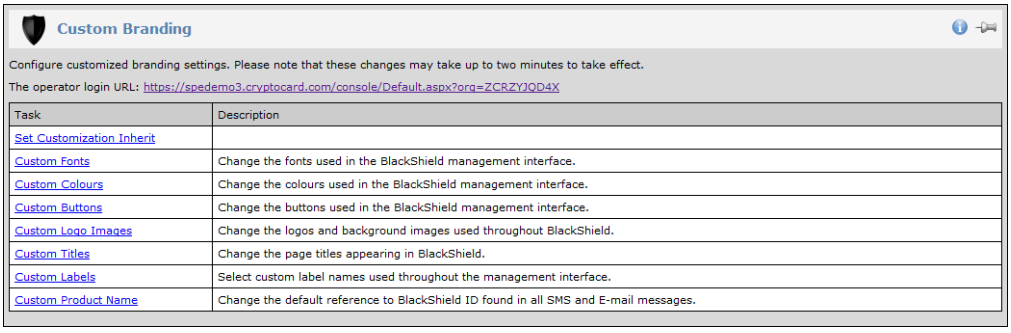


Figure 266: Custom Branding Options

Custom Fonts

To begin, click the Custom Fonts hyperlink. Select the font-family from the dropdown list.

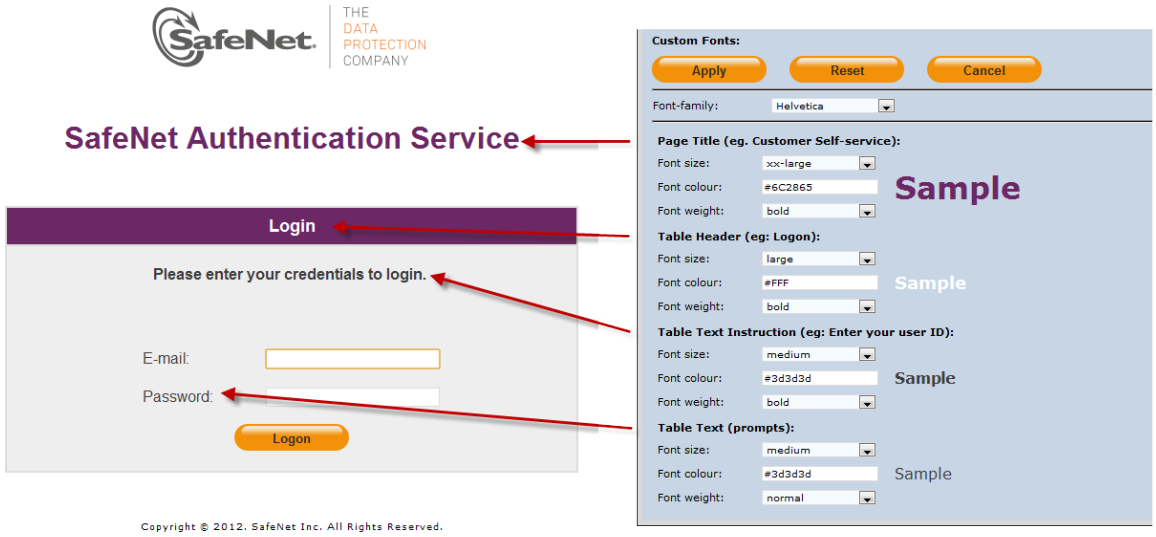


Figure 267: Custom Fonts

Custom Colours

To begin, click the Custom Colours hyperlink. Select the font-family from the dropdown list. Enter colours using standard names (red, green, blue etc.) or use hex values (#F80000, #CC6600 etc.)

Custom Colours – Logon Page

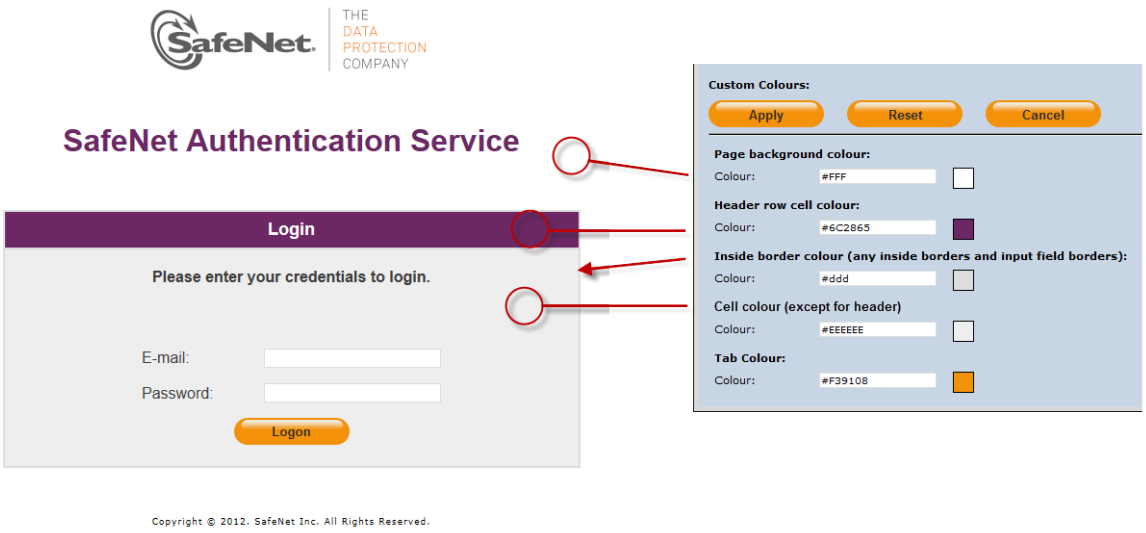


Figure 268: Custom Colours - Logon Page

Custom Colours – Management UI

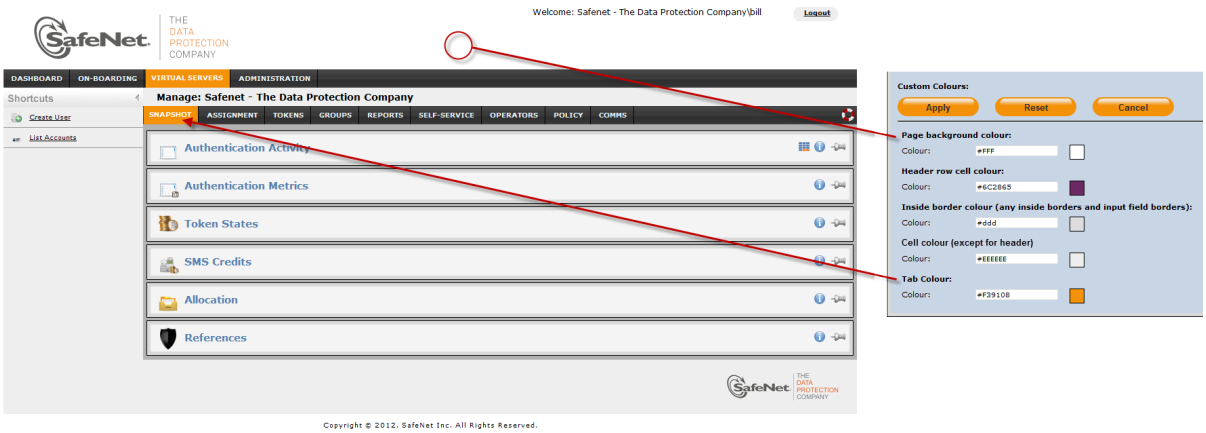


Figure 269: Custom Colours - Management UI

Custom Buttons

To begin, click the Custom Buttons hyperlink. To select a preset graphic button, click the corresponding radio button and click Apply. To use an HTML button, enter a colour value (red, green…) or a colour HEX value (#F80000, #00C800…).

To normal and hover button text size, colour and weight can be customized by configuring the Button Text and Button Hover Text options. As above use standard colour values or enter a HEX value for font colour.

Custom graphic buttons can also be used. Buttons must be 120 x 28px in png, jpg or gif format. First upload the button in the Custom Logo Images module, then return to this page and select the button, text, hover etc.

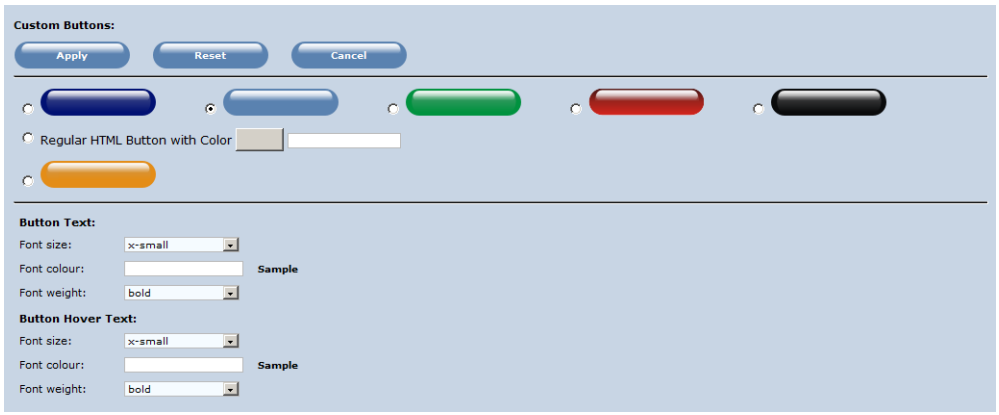


Figure 270: Custom Buttons

Click Apply to commit the changes.

Custom Logo Images

To begin, click the Custom Logo Images hyperlink. Select the images then click the Upload button. Images can be replaced with the defaults by clicking the "X" to the right of any custom image or replaced by simply uploading a new image.

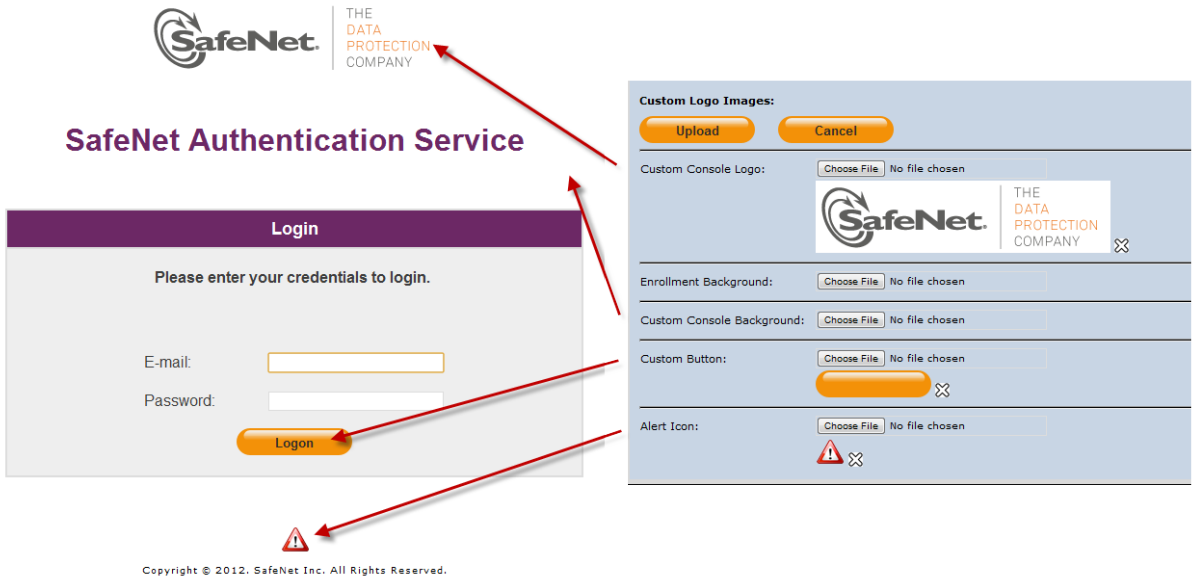


Figure 271: Custom Logo Images (with custom button uploaded)

- Custom Console Logo must be in no larger than 400 x 100 px in png, jpg or gif format.
- Alert Icon must be 30 x 30 px in png, jpg or gif format.

The recommend background size is 1800 x 1100 px in png, jpg or gif format. To maintain page loading speed image size should be less than 50kB.

Custom Logo – Enrollment Pages

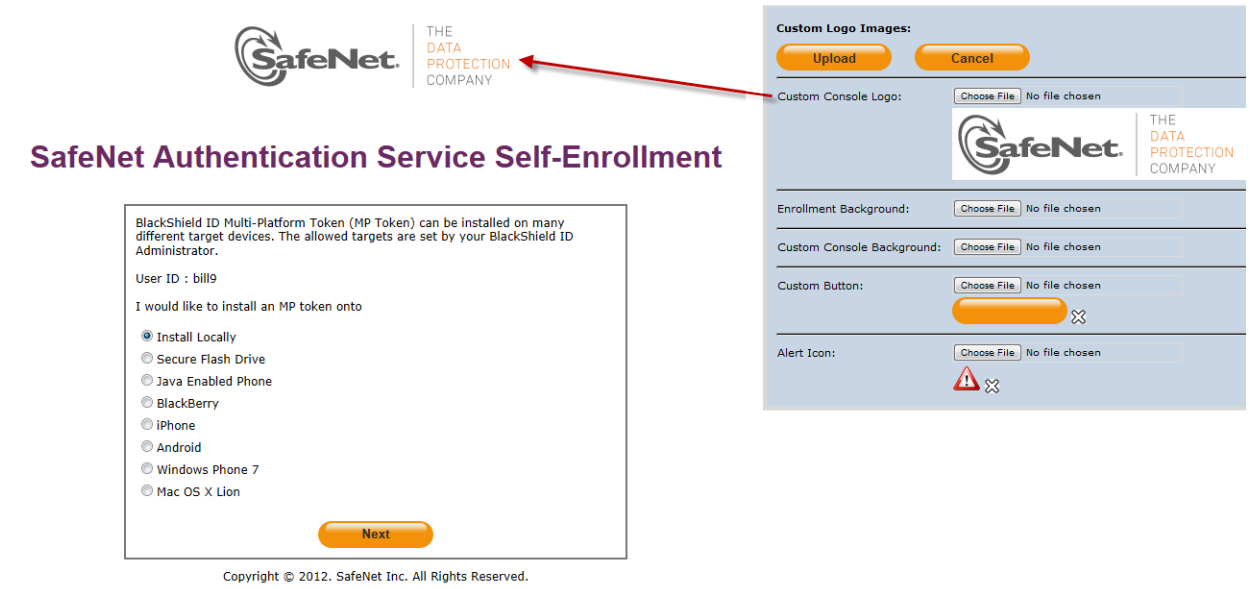


Figure 272: Custom Logo - Enrollment Pages

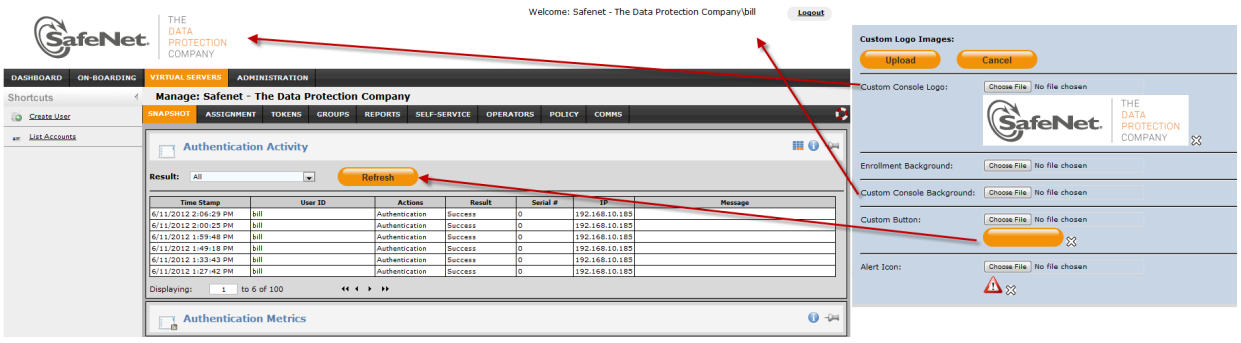


Figure 273: Custom Logo - Management UI

Custom Titles

Modify the text in the corresponding fields to replace the titles on the console management logon, self-enrollment and self-service pages.

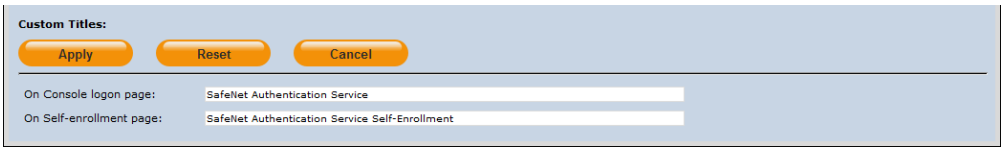


Figure 274: Custom Titles

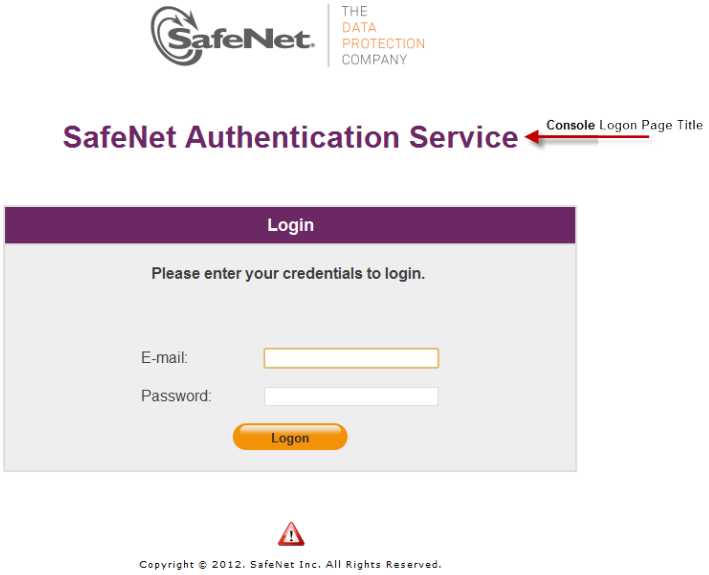


Figure 275: Console Logon Title

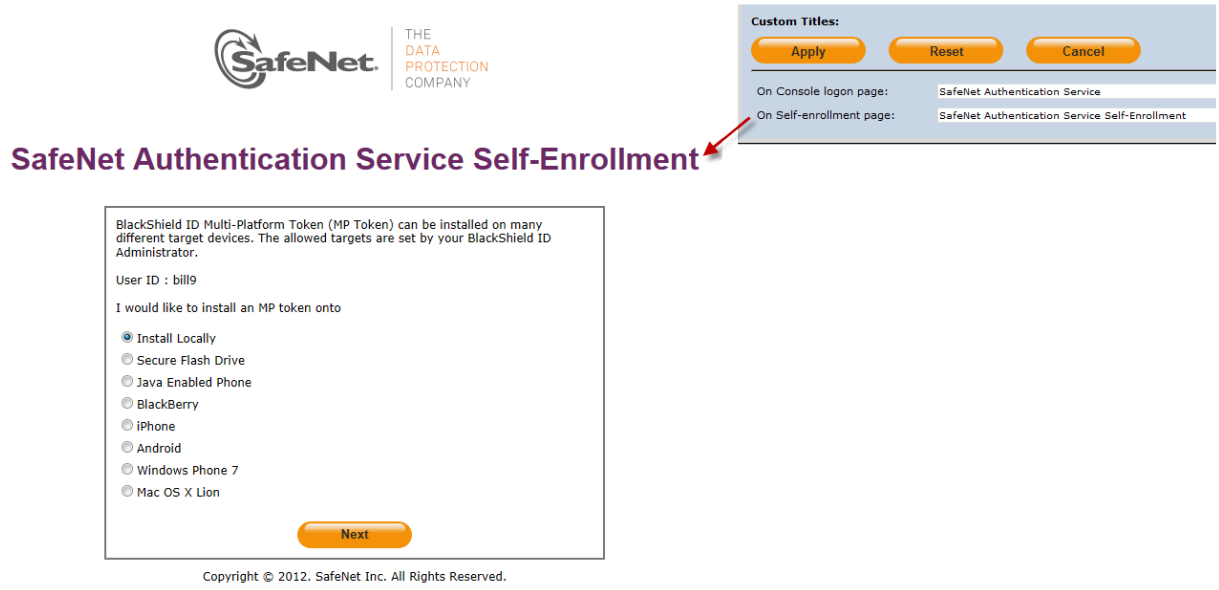


Figure 276: Self-enrollment Page Title

Custom Labels

Use this module to change the Custom # labels displayed in the UI where:

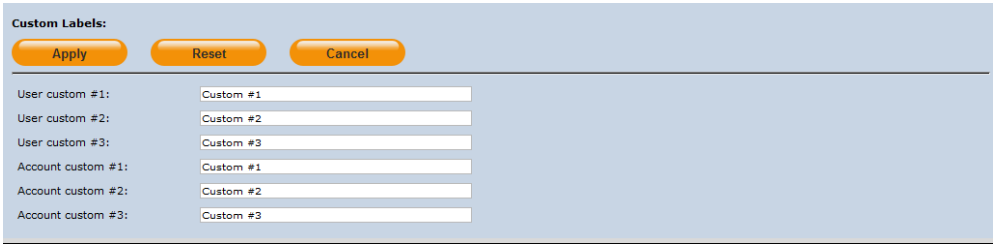


Figure 277: Custom Labels

- **User Custom**
  Refers to Custom #1, Custom #2 and Custom #3 field labels displayed in User Detail (Virtual Server) and in user related reports and tables. An example use would be to change Custom #1 to an employee number or other identifier that could be used to link reports and user information in SafeNet Authentication Service to the external system.

- **Account Custom**
  Refers to Custom #1, Custom #2 and Custom #3 field labels displayed in Accounts Detail (On-Boarding) and in account related reports and tables. An example use would be to change Custom #1 to an account number or other identifier that could be used to link reports and customer information in SafeNet Authentication Service to the external system.

Custom Product Name

Use this module to change all occurrences of the default product name (SafeNet Authentication Service) used in e-mail and SMS templates (refer to COMMS Tab | Communications module | SMS Messages / E-mail Messages).

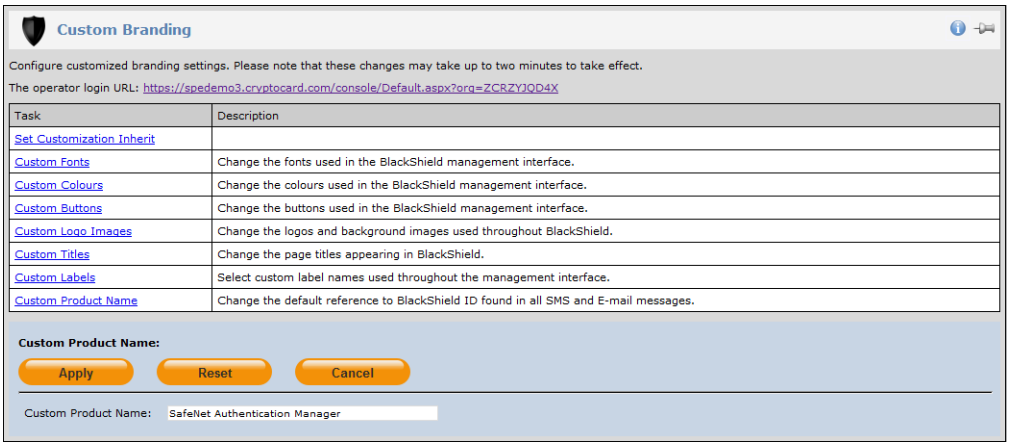


Figure 278: Custom Product Name