Preface

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording or otherwise without the prior written permission of SafeNet.

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person of organization of any such revisions or changes.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address below.

4690 Millennium Drive, Belcamp Maryland 21017, USA

Disclaimers

The foregoing integration was performed and tested only with specific versions of equipment and software and only in the configuration indicated. If your setup matches exactly, you should expect no trouble, and Customer Support can assist with any missteps. If your setup differs, then the foregoing is merely a template and you will need to adjust the instructions to fit your situation. Customer Support will attempt to assist, but cannot guarantee success in setups that we have not tested.

This product contains software that is subject to various public licenses. The source code form of such software and all derivative forms thereof can be copied from the following website: http://c3.safenet-inc.com/

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.
Support

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance, you can contact us directly at:

**Telephone**

You can call our help-desk 24 hours a day, seven days a week:

*USA*: 1-800-545-6608  
*International*: +1-410-931-7520

**Email**

You can send a question to the technical support team at the following email address:

support@safenet-inc.com

**Website**

You can submit a question through the SafeNet Support portal:

https://serviceportal.safenet-inc.com

---

**Publishing history**

<table>
<thead>
<tr>
<th>Date</th>
<th>Part number</th>
<th>Software release</th>
</tr>
</thead>
<tbody>
<tr>
<td>November 2014</td>
<td>007-012834-001</td>
<td></td>
</tr>
</tbody>
</table>
Additional Documentation

We recommend reading the following SafeNet publication:

- SafeNet Authentication Manager Express 8.2 Customer Release Notes
- SafeNet Authentication Manager Express 8.2 Agents Administration Guide
CONTENTS

CHAPTER 1
Introduction .................................................15
Welcome to SAM Express and Enterprise Solution Pack (ESP) ....16
SAM Express components and functions ..........................17
  Core components ........................................17
  Optional servers and components .........................21
  Optional agents .........................................22
The Enterprise Solution Pack (ESP) ............................25
Setting up SAM Express to work for you ......................26
  Managing users in Active Directory .......................26
  Managing users with the SAM Express database ..........26
  Managing users in Active Directory and the SAM Express database . 27

CHAPTER 2
Installing and Activating SAM Express ........................29
Installation prerequisites and requirements ..................30
  Network prerequisites ..................................30
  Hardware/software requirements ..........................30
  Component and optional agent prerequisites ...............31
  Installation topology rules ................................34
Installing SAM Express ......................................35
  Installation details ......................................36
If installing one or more SAM Express agents .................42
Finishing the installation ..................................43
Activating SAM Express ....................................44
  Registering on the portal ................................44
  Activation using ADUC ................................45
  Activating via Website ..................................46
  Activating SAM Express on a remote ADUC installation .....48
Verifying your activation in ADUC ............................48
Verifying activation in the SAM Express Management Console .49
Subsequent token activations ................................49
Extending your support ....................................49
Evaluating MobilePASS tokens ...............................50
The Support Information Center .............................51
# Table of Contents

## CHAPTER 3
**Active Directory Management** .............................................. 53
- Overview ................................................................. 54
- Changing the administrative password in ADUC .................... 55
- Setting up token records and data files ............................. 55
  - Generating MobilePASS records in ADUC ...................... 55
  - Importing token data files ........................................ 58
- Configuring the enrollment policy .................................... 59
- Assigning tokens to users ............................................. 67
  - Assigning tokens with the Token Assignment Wizard .......... 67
- Testing tokens .......................................................... 74
- Adding or changing PINs .............................................. 74
- Resynchronizing Hardware tokens ................................... 75
- Searching for unassigned tokens .................................... 75
- Finding users associated with specific tokens .................... 75
- Generating emergency passcodes ................................... 76
- Reassigning Hardware and Messaging tokens ..................... 77
- Deleting token records from the database ......................... 78
- Delegated administration in Active Directory ..................... 79

## CHAPTER 4
**Basic Administration Tasks** .............................................. 81
- Using the Auto Updater .................................................. 82
- Managing and viewing logs ........................................... 83
  - Configuring ADUC logging ......................................... 83
  - Viewing event logs .................................................. 83
- Database-related tasks ................................................ 85
  - Backing up the database using ADUC ............................. 85
  - Restoring the database using ADUC ............................. 86
- Reinstalling a server or ADUC ........................................ 87
- Configuring alternative group policies ............................. 88

## CHAPTER 5
**Using the MobilePASS Feature** ....................................... 91
- Understanding MobilePASS ............................................ 92
- Software token enrollment ............................................ 93
  - Using the MobilePASS Portal ..................................... 93
  - Changing and updating your admin server credentials ........ 94
- Configuring MobilePASS policies ................................... 97
  - Defining policies ................................................... 101
  - Duplicating policies ............................................... 105
  - Searching existing policies ..................................... 105
  - Editing existing policies ......................................... 105
  - Deleting policies .................................................. 106
- Allowing users to manually self-enroll their tokens ............ 107
- Configuring automatic enrollment for BlackBerry users ......... 108
- Using the Enrollment Portal ......................................... 108
- Configuring re-enrollment for existing MobilePASS tokens .... 111
- Allowing users to self-enroll ......................................... 111
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning a hardware token to the primary account</td>
<td>169</td>
</tr>
<tr>
<td>Testing your primary working account</td>
<td>171</td>
</tr>
<tr>
<td>Changing the default administrator password</td>
<td>172</td>
</tr>
<tr>
<td>What next?</td>
<td>173</td>
</tr>
<tr>
<td>Creating groups</td>
<td>174</td>
</tr>
<tr>
<td>Creating login ACLs</td>
<td>175</td>
</tr>
<tr>
<td>Defining login ACL entries</td>
<td>176</td>
</tr>
<tr>
<td>Editing ACL entries</td>
<td>179</td>
</tr>
<tr>
<td>Ordering ACL entries</td>
<td>179</td>
</tr>
<tr>
<td>Creating roles</td>
<td>180</td>
</tr>
<tr>
<td>Create a role</td>
<td>180</td>
</tr>
<tr>
<td>Creating Web ACLs</td>
<td>182</td>
</tr>
<tr>
<td>Create a Web ACL</td>
<td>182</td>
</tr>
<tr>
<td>Passing personalization data</td>
<td>190</td>
</tr>
<tr>
<td>What now?</td>
<td>193</td>
</tr>
<tr>
<td>Managing authenticators</td>
<td>194</td>
</tr>
<tr>
<td>Generating and importing MobilePASS software tokens</td>
<td>194</td>
</tr>
<tr>
<td>Assigning MobilePASS Software tokens with the Enrollment feature</td>
<td>195</td>
</tr>
<tr>
<td>Assigning hardware tokens manually</td>
<td>198</td>
</tr>
<tr>
<td>Resynchronizing hardware tokens</td>
<td>199</td>
</tr>
<tr>
<td>Modifying token profiles</td>
<td>201</td>
</tr>
<tr>
<td>Fixed password profiles</td>
<td>203</td>
</tr>
<tr>
<td>Managing users</td>
<td>205</td>
</tr>
<tr>
<td>Creating user accounts manually</td>
<td>206</td>
</tr>
<tr>
<td>Adding unprivileged users with the user wizard</td>
<td>213</td>
</tr>
<tr>
<td>Assigning role(s) to multiple users</td>
<td>215</td>
</tr>
<tr>
<td>Deleting a user record</td>
<td>218</td>
</tr>
<tr>
<td>Understanding personalization data</td>
<td>219</td>
</tr>
<tr>
<td>Data elements</td>
<td>219</td>
</tr>
<tr>
<td>The data dictionary</td>
<td>219</td>
</tr>
<tr>
<td>Creating personalization data</td>
<td>219</td>
</tr>
<tr>
<td>Using the Attack Lock feature</td>
<td>222</td>
</tr>
<tr>
<td>Editing personalization data attributes</td>
<td>223</td>
</tr>
<tr>
<td>Removing personalization data attributes</td>
<td>223</td>
</tr>
<tr>
<td>Modifying user personalization data</td>
<td>224</td>
</tr>
<tr>
<td>Importing user records from a third-party user database</td>
<td>225</td>
</tr>
<tr>
<td>Managing and viewing audit logs</td>
<td>227</td>
</tr>
<tr>
<td>Querying audit logs</td>
<td>227</td>
</tr>
<tr>
<td>Searching the audit logs</td>
<td>228</td>
</tr>
<tr>
<td>Viewing a specific user’s authentication activity</td>
<td>229</td>
</tr>
<tr>
<td>Viewing the last successful user login attempt</td>
<td>229</td>
</tr>
<tr>
<td>Viewing specific entry details</td>
<td>230</td>
</tr>
<tr>
<td>Troubleshooting with the Audit Log Monitor</td>
<td>230</td>
</tr>
<tr>
<td>Launching the Audit Log Monitor</td>
<td>230</td>
</tr>
<tr>
<td>Choosing logs to monitor</td>
<td>231</td>
</tr>
</tbody>
</table>
Table of Contents

Managing audit log archives ........................................ 231
Loading an archived audit log file ............................... 232
Unloading an archive set ........................................... 232
Deleting an archived audit log file .............................. 233
Configuring the archival of audit logs ......................... 233
Using advanced archiving features ......................... 234

Reporting ................................................................. 235
Creating reports ...................................................... 235
Report templates ...................................................... 236
Report worksheet generation ..................................... 237
Generating reports from the command line .................. 237
Using the command line reporting tool ....................... 238
Exporting data into Excel worksheets ......................... 239

Database-related tasks ............................................... 240
Backing up your database .......................................... 240
Restoring your database .......................................... 240
Backing up your database using the command line ........ 242

Customizing SAM Express ........................................... 243
Configuring General settings ..................................... 245
Configuring the log server ........................................ 246
Configuring sessions ............................................... 247

Other admin tasks ...................................................... 248
Finding entries ....................................................... 248
Exporting data ....................................................... 248
Editing admin group properties .................................. 248
Session management ............................................... 249
Revoking sessions ............................................... 249

CHAPTER 9

Advanced Administration Tasks ................................. 251

SAM Express server-related tasks ............................... 252
Stopping and starting servers .................................... 252
Changing component ports ....................................... 252
Logging server diagnostics ....................................... 253
Monitoring server status .......................................... 255
Adding servers to the monitored servers list ............... 255
Removing servers from the monitored servers list ........ 256
Cloning servers ....................................................... 256
Configuring the Administration Server ....................... 257

Configuring RADIUS, and RADIUS Accounting servers 258

Authentication Engine related tasks .......................... 259
Authentication Engine performance settings ................ 259
Configuring the Authentication Engine for SoftPIN use ... 259
Managing the Admin and Authentication Engine keys .... 260

Custom user management configuration ....................... 261
Changing the user database post installation ............... 261
Changing agent-specific user information .................... 261
### Table of Contents

- Configuring SAM Express for AD lockout support ........................................ 263
- Configuring the Authentication Policy ..................................................... 264
- Launch the Group Policy window (all agents) ......................................... 264
- Agent configuration screens ................................................................. 265
  - Configuring the Authentication Engine .............................................. 265
  - Changing agent logging settings ....................................................... 266
- Increasing performance ........................................................................... 269
  - Archiving during minimal activity periods .......................................... 269
  - Using multiple database connections ................................................. 269
  - Running without an archive log master .............................................. 270
- Running Repair ....................................................................................... 271

### CHAPTER 10 Replication ................................................................. 273

#### 1. Overview of replication ................................................................. 274
  - Ring topology architecture ................................................................. 274
  - The change log ................................................................................... 275
  - Differences between SAM Express and AD replication ....................... 275
#### 2. Pre-replication setup considerations ............................................... 276
  - General considerations ...................................................................... 276
  - Special considerations ....................................................................... 276
#### 3. Adding peers to a new replication ring .............................................. 277
  1. Verify SAM Express server software is installed .................................. 277
  2. Verify time sync on peer machines ..................................................... 277
  3. Designate a Log Master .................................................................... 278
  4. Back up the database ........................................................................ 278
  5. Restore the backed up database to machines in the ring ..................... 279
  6. Stop the Admin server and Authentication Engine .............................. 279
  7. Edit the sccservers.ini file .................................................................. 280
  8. Run the AddReplPeer.bat file ............................................................. 280
#### 4. Adding a new peer into an existing replication ring ............................ 282
#### 5. Verifying SAM Express server replication ....................................... 284
  - Testing replication setup ..................................................................... 284
  - Checking server replication state ....................................................... 284
#### 6. Troubleshooting ............................................................................... 284

### CHAPTER 11 Managing the RADIUS Servers ........................................ 285

#### 1. Overview of the SAM Express RADIUS server .................................... 286
  - RADIUS protocol ............................................................................... 286
  - The RADIUS server .......................................................................... 286
  - RADIUS server features .................................................................... 286
#### 2. Prerequisites .................................................................................... 288
#### 3. SAM Express RADIUS configuration files .......................................... 288
#### 4. Authorization and configuration groups ............................................. 289
  - Creating a login ACL entry and role for RADIUS ............................... 289
  - Configuring the groups in the Users file ............................................ 289
  - Configuring the RADIUS proxy ......................................................... 290
Table of Contents

Authenticators ......................................................... 292
  RADIUS-encrypted memorized passwords ....................... 292
  Memorized passwords appended to usernames .................. 293
  RADIUS-encrypted synchronous dynamic passwords ............ 293
  Synchronous dynamic passwords appended to usernames ..... 293
  Shared tokens with memorized passwords ...................... 294
  Asynchronous dynamic password authenticators ............... 295
  CHAP-encoded encapsulated dynamic passwords ............... 295

References ...................................................................... 296
  Sample Dictionary file .............................................. 296
  Sample Users file ..................................................... 298
  Sample authfile ....................................................... 300

Understanding the RADIUS Accounting server .................. 301

How the server works .................................................. 302
Configuring the server .................................................. 302
Starting the server ...................................................... 302
  Example: Enabling accounting on Cisco router .............. 303
Sample accounting data ............................................... 303

Troubleshooting .......................................................... 303
  General troubleshooting ............................................ 306
  Troubleshooting AD lockout support .............................. 310
  Troubleshooting Replication ....................................... 311
  Troubleshooting the RADIUS server .............................. 318
  General troubleshooting ............................................ 318
  Check the radius.cfg configuration files ....................... 318
  The clients file ....................................................... 319
  The users file ........................................................ 319
  The dictionary file ................................................... 319
  Conflicts with other RADIUS servers ............................. 319
  Launch the SAM Express RADIUS server in debug mode .... 320
  Diagnostic traces during correct operation ..................... 321
Uninstalling SAM Express ............................................. 321

CHAPTER 12

Troubleshooting .......................................................... 305
  General troubleshooting ............................................ 306
  Troubleshooting AD lockout support .............................. 310
  Troubleshooting Replication ....................................... 311
  Troubleshooting the RADIUS server .............................. 318
  General troubleshooting ............................................ 318
  Check the radius.cfg configuration files ....................... 318
  The clients file ....................................................... 319
  The users file ........................................................ 319
  The dictionary file ................................................... 319
  Conflicts with other RADIUS servers ............................. 319
  Launch the SAM Express RADIUS server in debug mode .... 320
  Diagnostic traces during correct operation ..................... 321
  Uninstalling SAM Express ......................................... 321
CHAPTER 1

Introduction

In this chapter...

Welcome to SAM Express and Enterprise Solution Pack (ESP)....16
SAM Express components and functions........................................17
The Enterprise Solution Pack (ESP) ............................................25
Setting up SAM Express to work for you..................................26
Welcome to SAM Express by SafeNet (referred to throughout the remainder of this guide as SAM Express), the two-factor authentication solution for Microsoft Windows platforms.

SAM Express includes easy-to-use software and hardware tokens. It seamlessly integrates with your existing Microsoft Windows management tools, and makes it easy to deploy multi-factor authentication to protect your most important assets and applications. Additionally, SAM Express components and agents come ready to support Internet Protocol versions (IPv) IPv4 and IPv6.

SafeNet MobilePASS relieves users from using cumbersome hardware tokens, instead allowing them to generate software token passcodes on their iPhone/iPad/iPod touch, BlackBerry, J2ME, Android devices, and Windows Desktops. And when the Enterprise Solution Pack is installed, seamless SAM Express strong authentication is extended to users of Google Apps, Salesforce.com, and other third-party applications via the Cloud Authentication Server and Portal component. MobilePASS Messaging allows users stored in Active Directory to request and receive authentication passcodes via SMS and SMTP.

SAM Express is designed to be extremely easy to install and manage. You can be up and running in a short period of time. Take advantage of the SAM Express Auto Updater Agent to ensure that any future software updates can be easily added. This guide will introduce you to these and all the other SAM Express administrative concepts.

To get SAM Express up and running in your environment, simply:

- Install and activate the software
- Configure the product
- Assign and distribute SAM Express software or hardware tokens to your users

Every effort has been made to provide you with the information you need to easily install and configure SAM Express. The Quick Start Guide (included in the product package) provides overview information about the SAM Express features, as well basic installation information (detailed installation information is contained in this Administration Guide). After SAM Express is installed, information-rich online help is available any time you specific information.

Documentation detailing SafeNet MobilePASS software and hardware authentication information is available for download at [http://www.safenet-inc.com/support/SAMx-documentation/](http://www.safenet-inc.com/support/SAMx-documentation/).
This section describes the SAM Express core and optional components and their functions. If you prefer, you can skip this section and proceed to “Installation prerequisites and requirements” on page 30.

Core components

A basic SAM Express installation has several required core components:

• SAM Express Servers
• Management consoles: either the Active Directory Users and Computers (ADUC) Management Console and/or the SAM Express Management Console.

**Note:** You will need a valid license with the ESP feature enabled in order to use the SAM Express Management Console.

• Auto Updater Agent (AUA)
Additional capabilities can be added by installing optional servers and agents that offer tremendous flexibility in securing critical network resources.

**Figure 1: SAM Express core components**

The SAM Express server

The SAM Express server is comprised of the SAM Express database, the Authentication Engine (AAA), the Administration Service (or Administration Server), and the User Center (UC).

- The SAM Express database serves as the repository for token records.
- The Authentication Engine (sometimes referred to as the AAA, or Auth server) verifies that the passcode supplied with an access request is correct for the token assigned to a specific user.
- The Administration Service (Server) is used by the console to perform the tasks initiated by administrators or users, and synchronizes SAM Express database data in configurations with multiple servers.
- The User Center allows end users to enroll their SafeNet tokens, which saves administrative time when a large number of users will be authenticating with SafeNet tokens. Users can also change or assign their PIN, resync their tokens, and test their tokens after enrollment.
Active Directory Users and Computers Management Console

User management in an Active Directory environment is handled from Active Directory Users and Computers (ADUC) Management Console, which is accessed via the standard Windows Start menu.

After installing the ADUC Management Console, the standard user properties dialog will include the SAM Express tab (Figure 3). You can associate SafeNet tokens, including MobilePASS tokens with AD users, assign PINs, generate emergency passcodes, and test and resynchronize tokens assigned to individual users on this tab.
The SAM Express Management Console (included with ESP)

This console handles users (stored in the SAM Express database) and authenticator management, security policy administration, group management, viewing logs, and generating reports. It can be installed either locally (with the SAM Express server) or on a remote client machine.

The Auto Updater Agent (AUA)

SAM Express Auto Updater provides automatic notification of patches and updates as they become available. The feature installs on every host in the distributed system. When updates are available, a message displays to notify the user. The user will only be notified if there are updates that do not already exist on their system. The Auto Updater runs automatically when the Active Directory Users and Computers console is accessed. On other SAM Express components, it can be launched manually. The Auto Updater allows you to view, download, and install the available updates (if there are any) whenever you desire. Only the updates that you have not already installed will be visible in the list of available updates.

Note: If you do not have internet access, updates must be applied from an FTP image. Contact Technical Support at 1-800-545-6608 (US Toll Free), or 1-410-931-7520 (International) to get the necessary image.

Important: Manually downloading and installing updates is not recommended. This can leave your system in an unstable state. If you download and run the updates manually, be sure to install them in the order in which they are listed in the Auto Updater.
Optional servers and components

You may also choose the following optional servers and features:

**SAM Express RADIUS server (requires ESP license)**

The RADIUS server allows VPNs, routers, and comm servers using the RADIUS protocol to communicate with SAM Express. It also sends user’s names and passwords to the authentication engine where their credentials are either verified or denied.

**SAM Express RADIUS Accounting server (requires ESP license)**

The RADIUS Accounting server listens for properly formatted information packets, and keeps track of all types of user requests.

**SafeNet MobilePASS Portal**

SafeNet MobilePASS provides end-users with SAM Express authentication passcodes without the need to carry a hardware token with them. There are two kinds of MobilePASS authenticators: Software tokens and Messaging tokens. The MobilePASS Software allows users to generate SAM Express passcodes from their iPhone/iPad/iPod touch, BlackBerry, J2ME, and Android devices, and from their Windows Desktops. MobilePASS Messaging token users stored in Active Directory can request and receive SAM Express passcodes via messages to their SMTP and SMS accounts.

**Cloud Authentication Server and Portal (requires ESP license)**

The Cloud Authentication Server and the Cloud Portal component provide seamless SAM Express strong authentication for SAM Express token users accessing the SaaS (Software as a Service) applications Google Apps and Salesforce.com. When a user accesses the Cloud Portal as initiated by either the Identity Provider (SAM Express) or the Service Provider (Google Apps or Salesforce.com), they are prompted for their credentials, authenticated, and logged in to the SaaS application. The Cloud Server can run on Windows Server 2003 and 2008. The Cloud Server should be installed internally, but the user-facing Cloud Portal can be installed in a DMZ for external access.
Optional agents

Agents are software modules that intercept user login or access requests to protected resources, and prompt the user to provide SAM Express credentials (password, authenticator passcode) before access is granted. Agents provide strong authentication for users seeking access to critical resources.

Figure 5 shows a network several possible server combinations and associated SAM Express agents installed.

![Network with possible server / agent combinations]

Configuration details for each of these agents can be found in the Agent Administration Guide, which is located at [http://www.safenet-inc.com/support/SAMx-documentation/](http://www.safenet-inc.com/support/SAMx-documentation/).
The SAM Express Internet Authentication Service (IAS/NPS) Agent

**Note:** Though listed in this guide as the IAS Agent, it also covers the Network Policy Server (NPS).

SAM Express provides strong authentication to SSL VPNs, IPSec VPNs, commservers, and other RADIUS (Remote Authentication Dial-In User Service) devices. Simply install and configure SAM Express’s IAS/NPS Agent, which works with Microsoft’s IAS RADIUS, to provide strong authentication to RADIUS devices through the Microsoft IAS RADIUS server.

Once the IAS Agent is installed and configured, VPN and RADIUS users who remotely access their network and are designated as requiring strong authentication must enter a SAM Express token-generated passcode for access. Users in the SAM Express database may also use a fixed password.

For more information about Microsoft’s IAS, see:


The SAM Express Agent for Web Interface

The SAM Express Agent for Web Interface is for use with Citrix. It resides on the same Citrix server on which the Citrix Web Interface is installed, and provides the link to the SAM Express server. It intercepts user access requests and routes them to the Authentication Engine for user name and passcode verification. Once properly authenticated, users are allowed access; otherwise access is denied.

The Citrix Access Gateway (CAG) Agent

SAM Express adds strong authentication to Citrix Access Gateway through the SAM Express CAG Agent. The agent uses the standard SAM Express administration tools, and installs directly on top of Advanced Access Control (AAC) when the CAG Agent is configured with the AAC option.

**Note:** If CAG does not have the AAC option, the gateway appliance can be configured for RADIUS authentication using the IAS/NPS Agent.
The Outlook Web Access (OWA) Agent

SAM Express’s Outlook Web Access Agent works with the Microsoft Exchange Server to provide SAM Express strong authenticated access through the Microsoft Exchange Outlook Web Access (OWA) component. When this option is chosen at installation, users who access their e-mail account remotely using Outlook Web Access will be prompted for a SAM Express token-generated passcode in order to access the network.
The SAM Express Enterprise Solution Pack (ESP) includes several components that extend the capabilities of SAM Express:

- Extended Windows application protection including strongly authenticated access to Windows resources (Domain login, Remote Desktop, Terminal Services)
- SAM Express Management Console for managing some or all of your users outside of Microsoft Active Directory
- Cloud Authentication Server and Cloud Portal
- RADIUS and RADIUS Accounting

Your SAM Express package includes a 30-day evaluation of ESP. To purchase a valid ESP license, please contact your SAM Express reseller, or browse to the SafeNet corporate site at http://safenet-inc.com.
Setting up SAM Express to work for you

SAM Express is a highly-flexible solution that can be tailored to the specific needs of your organization. A brief description of the most common use scenarios are included below.

Managing users in Active Directory

If you have an existing Active Directory database of users, the Active Directory Users and Computers (ADUC) Management Console allows you to use the familiar ADUC console to assign SafeNet tokens and SoftPINs to your existing users, and to generate records and configure MobilePASS. In this case, you would:

• Install and activate SAM Express
• Install the MobilePASS Portal
• Install the Cloud Server and Portal (Optional)
• Launch and secure ADUC with a new password
• Import hardware token data records or generate MobilePASS records
• Assign tokens to users
• Configure MobilePASS Messaging (Optional).

Managing users with the SAM Express database

If your users will be stored in the SAM Express database, you will be managing them with the SAM Express Management Console which is available as part of ESP. This model may be used to manage users directly in SAM Express. It may also be used to test users and tokens independent of your Active Directory, such as during evaluation or after installation. In this case, you would:

• (If not already done) Install and activate SAM Express
• Install the MobilePASS Portal (Optional)
• Install the Cloud Server and Portal (Optional)
• Launch and secure the SAM Express Management Console
• Import hardware token data records or generate MobilePASS records
• Create groups, login ACLs, Web ACLs, and roles
• Add users and assign tokens.
Managing users in Active Directory and the SAM Express database

In some cases, you may choose to have a mixture of user management options. The User Center allows end users stored in Active Directory or in a stand-alone SAM Express database to enroll and manage their SafeNet tokens. It is easy to use, and saves administrative time when a large number of users will be authenticating with SafeNet tokens. The User Center allows users to enroll their hardware tokens, to change or assign their PIN, to resync their tokens, and test them after enrollment. In this case, you would:

• (If not already done) Install and activate SAM Express
• Launch and secure the User Center
• Provide users with the User Center URL and information about how to enroll and manage their tokens with it.
Chapter 1: Introduction

Setting up SAM Express to work for you
CHAPTER 2

Installing and Activating SAM Express

In this chapter...

Installation prerequisites and requirements.................................30
Installing SAM Express ..................................................................35
Activating SAM Express.................................................................44
Evaluating MobilePASS tokens......................................................50
The Support Information Center.....................................................51
The following are the prerequisites necessary to install, configure, and use this product. Some components are required for all configurations, others are required only if you will be using a specific agent. For specific agent information, refer to the Agent Administration Guide, which is located at http://www.safenet-inc.com/support/SAMx-documentation/.

Network prerequisites

Before installing SAM Express your users must be able to make a successful connection to secure network resources by a secure Web or VPN session. Your network must also have the following required components:

- One of the following 32 or 64-bit Windows servers:
  - Windows Server 2003 (Standard or Enterprise)
  - Windows Server 2008 (Standard or Enterprise)
  - Windows Server 2012 (Standard or Essentials)
  - Windows Server 2012 R2 (Standard or Essentials)

  Note: Windows 2008 Core is not supported. Windows 2003/2008 Small Business Server is not supported.

- Active Directory populated with users (unless user management will be handled exclusively through the SAM Express Management Console)

  Note: A Domain Controller is required for use with Active Directory.

- Internet access (to receive product updates not on your installation CD)

  Note: If you do not have internet access, updates must be applied from an FTP image. Contact Technical Support at 1-800-545-6608 (US Toll Free), or 1-410-931-7520 (International) to get the necessary image.

Hardware/software requirements

Table 1 lists minimum system hardware and software (operating system) requirements for installing and running SAM Express.

Table 1: Hardware/software requirements

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Pentium IV or AMD @ 1.8 GHz (minimum), 2 GHz (recommended)</td>
</tr>
</tbody>
</table>
Chapter 2: Installing and Activating SAM Express

Installation prerequisites and requirements

Component and optional agent prerequisites

Table 2 lists the prerequisites for installing and using SAM Express components and the available optional agents.

Note: Before installing, you should decide which database you will use to manage users.

Table 2: Component and optional agent prerequisites

<table>
<thead>
<tr>
<th>Component</th>
<th>Specification</th>
</tr>
</thead>
</table>
| OS                                             | **Server:** 32 or 64-bit Windows Server 2003 (R2 SP2) or Windows 2008 (R2 SP1) or Windows Server 2012 (Standard or Essentials) or Windows Server 2012 R2 (Standard or Essentials)  
**Desktop:** 32 or 64-bit Windows XP (SP2), Windows 7, and Vista |
| RAM                                            | 1 GB (min) 4GB (recommended)                                                   |
| Disk Space                                     | 3-5 GB (min) 10 GB (recommended) on NTFS-formatted drive                      |

Component and optional agent prerequisites

Table 2 lists the prerequisites for installing and using SAM Express components and the available optional agents.

Note: Before installing, you should decide which database you will use to manage users.

Table 2: Component and optional agent prerequisites

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement(s)</th>
</tr>
</thead>
</table>
| SAM Express server                             | This component is always available as an installation option. If you install it on a non-domain controller, you must provide domain administrator credentials that have the privilege to log on as a service. **Due to the sensitive data stored in the SAM Express server component, it must be a physically secure machine where only administrators have access to the SAM Express installation directory.**  
**Note:** Port 5030 and/or Port 5031 must be open for successful configuration. |
| Active Directory Users and Computers Management Console | • .NET Framework 2.0 or greater installed  
• MMC 3.0 or greater installed  
• This component is only available when the installation machine is part of a domain.  
**Note:** For a Win2008 non-Domain Controller and a Windows 2008 R2 non-Domain Controller, the Active Directory Remote Server Administration Tools feature needs to be enabled before installing the Management snap-in.  
**Note:** Port 5040 must be open between the remote ADUC server and the server running the Admin Service. You may customize this port. |
### Component

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement(s)</th>
</tr>
</thead>
</table>
| MobilePASS Portal (including the MobilePASS Enrollment Portal and the MobilePASS Messaging Application) | • This Web component is supported by the same Windows operating systems as the core SAM Express servers.  
• Internet Explorer 7.0 or higher (for configuring the portal)  
  **Note:** You must set the Administration Server password from the localhost machine.                                                                                                                                                                                                              |
| Cloud Server and Portal                                                 | • SAM Express ESP license  
• This Web component is supported by the same Windows operating systems as the core SAM Express servers.  
• .NET Framework 2.0  
• IIS with ASP.NET 2.0 enabled  
  **Note:** The SAM Express installation will attempt to install these prerequisites if they are not already present.                                                                                                                                                                                                                     |
| IAS/NPS Agent                                                           | • IAS/NPS must be functioning and configured for RADIUS authentication (policies, secret keys, firewall ports, and user permissions must be set correctly, and users must be able to successfully authenticate to IAS/NPS) before installing this agent. See Microsoft documentation.  
• RemoteAccess permissions (Dial-in and VPN) must be set to **Allow Access** on Microsoft Windows 2003 and earlier. Permissions can be set to **Allow Access** or to **Control Access through NPS Network Policy** for Microsoft Windows 2008.  
  **Note:** **Allow Access** always allows user access. **Control Access through NPS Network Policy** can be used to create complicated access points.  
• Port 1812 must be open in any firewalls between the RADIUS clients and the IAS/NPS Server.  
• Internet Explorer 7.0 or higher (for configuring the agent)                                                                                                                                                                                                                      |
| SAM Express Agent for Citrix Web Interface                               | • Web Interface 5.4 (with XenApp 7.5 back-end) 5.2, 4.6 or 4.5 installed  
• Internet Explorer 7.0 or higher (for configuring the agent)                                                                                                                                                                                                                                                                                     |
## Chapter 2: Installing and Activating SAM Express

### Installation prerequisites and requirements

**Important:** For hierarchical domain topologies, you must be logged on as a parent domain administrator.

<table>
<thead>
<tr>
<th>Component</th>
<th>Requirement(s)</th>
</tr>
</thead>
</table>
| OWA Agent | • Microsoft Exchange Server 2003, 2007, or 2010  
• Internet Explorer 7.0 or higher (for configuring the portal)  

**Note:** You must be logged on as a domain administrator for this agent to be available during installation. |
| SAM Express RADIUS and SAM Express RADIUS Accounting Servers | • SAM Express ESP license  
• Internet Explorer 7.0 or higher (for configuring the agent) |
| CAG Agent | • Must have the Citrix Access Gateway appliance configured with the Advanced Access Control (AAC) option  
• Internet Explorer 7.0 or higher (for configuring the agent) |
| Universal Web Agent/Web Login Server | • Available as an optional component  
• New users can install the components from the UWA_WLS install directory on the CD. Existing users should contact Technical Support for the components. |
| SafeNet RADIUS Server | • Available as an optional component  
• SAM Express ESP license  
• New users can install the component from the RADIUS install directory on the CD. Existing users should contact Technical Support for the component. |
Chapter 2: Installing and Activating SAM Express

Installation prerequisites and requirements

Installation topology rules

SAM Express offers a variety of options for installing and using its components to best suit existing installation topologies.

You may install all SAM Express components on one machine (if that machine has the capacity to handle your organization’s authentication and management load), or the components can be installed on separate machines which will share the operational load. The SAM Express installer will not allow you to install a component if it cannot correctly operate on the target machine. All other installation combinations are supported, as long as they conform to the following rules.

- **Rule 1**: SAM Express agents must be installed on the same machine as the component they will protect. Agents are tightly integrated with their respective component and cannot operate as standalone pieces.

  *Note: If your network contains multiple component installations (OWA, IAS-NPS, Web Interface, etc.), each installation must also have its corresponding SAM Express agent installed on the same machine.*

- **Rule 2**: Because of the tight integration with Active Directory, the ADUC Management Console must be installed on a machine that has ADUC.

- **Rule 3**: To avoid creating a race condition between servers when assigning software or messaging tokens, in environments with multiple MobilePASS portals and multiple ADUC consoles (for example, one for each domain controller), or in environments with a combination of MobilePASS portals and ADUC consoles, all portals and consoles must point to an administration server that is designated for token assignments.

If you install on a non-domain controller machine that is part of the domain, you may access ADUC by selecting **Start > Programs > SafeNet > SAM Express > Active Directory Users and Computers**.

*Note: ADUC can be installed on Windows XP and Windows 2003 non-domain controllers if the Administration Tools Pack (Adminpak.msi) is installed. For Windows Vista and Windows 7, install or enable the Remote Server Administration Tools (RSAT). Both can be downloaded from www.microsoft.com.*
A SAM Express installation will not interfere with your existing topology. You can install it directly in your existing environment. Figure 6 shows a flow chart-type snapshot of the installation process, with no Agents selected for installation. Detailed instructions corresponding to the numbered steps are found in “Installation details” on page 36. (Some steps are not included in the installation flow diagram.)

**Figure 6: SAM Express installation flow diagram, page 1**

**Note 1:** If not installing the SAM Express Server on a DC, you will be prompted for Admin Credentials later.
Figure 7 completes the process started in Figure 6 when one or more Agents are selected for installation.

**Figure 7**: SAM Express installation flow diagram, page 2

```
2
IAS selected?
Yes
```

**Installation details**

The installer should start automatically once the SAM Express CD is placed in the machine on which the software is being installed. If it does not autostart, browse to and explore the CD, and launch the *Setup.exe* file.

After the installation wizard windows appear, the SAM Express serial number window appears.

*Note: Only screens that require explanation are shown in this document.*

**Enter the product serial number**
1. Enter your product serial number (located on your product package and/or on the Activation Certificate is in the format NSXX-XXXX-XXXX-XXXX), then click **OK**.

2. Review the License Agreement, then click **Yes** to accept it.

3. When the Choose Destination Location window appears, accept the default installation location (or browse to select another), then click **Next**.

   If you choose to install in a location different than the default location, you must ensure that the following permissions are set:
   - Administrators – full control
   - Authentication users – read and execute
   - CREATOR OWNER – full control (subfolders and files only)
   - Server Operators – modify
   - SYSTEM – full control

4. For SAM Express, select the Authentication and Management Server, the Management Snap-in for Active Directory (if managing users in Active Directory), the MobilePASS Portal (if testing or deploying MobilePASS authenticators), the Cloud Authentication Server (if you will require users to authenticate with SAM Express strong authentication before they can access Google Apps and/or Salesforce.com), and any agents you want to install in your system.
If you are adding ESP components and will be managing some or all of your users in the SAM Express database, select the SAM Express Management Console, the Cloud Server (if you will require users authenticate with SAM Express strong authentication before they can access Google Apps and/or Salesforce.com), and any ESP agents you want to install.

**Note:** Only components that can be installed on your system will display.

**Important:** To avoid creating a race condition between servers when assigning software or messaging tokens, in environments with multiple MobilePASS portals and multiple ADUC consoles (for example, one for each domain controller), or in environments with a combination of MobilePASS portals and ADUC consoles, all portals and consoles must point to an administration server that is designated for token assignments.

If a particular Agent is not listed, refer to Table 2 on page 31 to verify that your system meets the requirements for that Agent.

If you are installing the SAM Express server on a machine that is not a domain controller, a Setup window appears requesting domain administrator credentials with the privilege to log on as a service. In this case, continue to the next step to provide the proper credentials.

**Note:** Domain administrator credentials and the privilege to log on as a service are required so the SAM Express server can write to Active Directory.

5 Make your selections, then click **Next**.

6 Make any needed changes in the Select Program Folder window, then click **Next**.

7 Review the information in the Start Copying Files window, then click **Next**.

If you did not select the SAM Express Server for installation, skip to ““Finishing the installation” on page 43. Otherwise, continue to the next section.
Select preferred user management

8 If you are not using SAM Express with ESP to manage your users, leave the default setting I will manage users in Active Directory, then click Next.

If you are installing the SAM Express Server, the Server Components window appears and displays the default ports over which SAM Express components will communicate.

Set server component ports and encryption keys

9 Accept the default port settings or specify your own port settings.

Tip: A small exclamation point displayed next to a Port field indicates that port is already in use by another process, and you must select a different port.

You will also be personalizing your SAM Express installation by defining a unique Encryption Key and Signing Key on the Database Security pane. Each key must be 16 characters in length, and must remain the same for the life of the installation.

Note: If you are installing multiple servers, they must all have the same keys as are used here.

Security Alert: It is important to enter your own custom encryption key and signing key for your SAM Express database. This helps to insure the integrity of data, uniquely distinguishing it from all other SAM Express installations.

10 Click Next when all choices have been made.

Set the host address

11 When the Host Address window appears, enter the Fully Qualified Domain Name to which this machine belongs, and then click Next.
12 If...

a your SAM Express Server is being installed on a Domain Controller, or

b you selected SAM Express Management Console

...then skip to “Select Cloud Server installation preference” on page 41.

13 If your SAM Express Server is not being installed on a Domain Controller, you will be prompted to provide the administrator’s credentials for the machine on which the SAM Express Server is to be installed, then click Next.

**Important:** If no credentials are specified, the local system credentials will be used. Clicking Next will cause the Choose Destination window to appear.

14 If you are not installing the Cloud Server, skip to “If installing one or more SAM Express agents” on page 42, otherwise, continue to the next section.
Select Cloud Server installation preference

If you will be using Cloud Authentication, review Table 3, “Cloud Installation Recommendations,” before setting your cloud installation preferences.

Table 3: Cloud Installation Recommendations

<table>
<thead>
<tr>
<th>Environment</th>
<th>Installation</th>
</tr>
</thead>
<tbody>
<tr>
<td>All users are inside the firewall</td>
<td>Install Cloud Server and Cloud Portal inside the firewall.</td>
</tr>
<tr>
<td>Some users are inside the firewall and others are outside the firewall</td>
<td>Install Cloud Server inside firewall. Install Cloud Portal outside the firewall.</td>
</tr>
<tr>
<td>All users are outside the firewall</td>
<td>Install Cloud Server inside firewall. Install Cloud Portal outside the firewall.</td>
</tr>
</tbody>
</table>

**Note:** To use Cloud Authentication, the Cloud Server must be installed on at least one machine in your network.

15 Choose the Cloud Server installation preference:

- Select **Cloud Portal and Server** if you will be installing the Cloud Portal and Server on the same machine. For security purposes, the Cloud Server should only be installed internally.
- Select **Cloud Portal only (for installation in DMZ)** to install the Portal only. The Cloud Portal can be installed alone in a DMZ to allow users to access it externally.

16 If you selected **Cloud Portal only (for installation in DMZ)**, continue to the next step. If you selected **Cloud Portal and Server**, skip to step 18.
Chapter 2: Installing and Activating SAM Express

Installing SAM Express

17 If you are installing the Cloud Portal outside the firewall, you must create a user name and password that the Cloud Server will use to authenticate the Cloud Portal. Enter a Name in the Username field, and then enter a Password in the Password field.

Note: Please remember these credentials. You will need to present them when configuring the Cloud Portal to connect to the Cloud Server.

18 Click the Next button.

If you did not select any Agents for installation, skip to “Finishing the installation” on page 43, otherwise, continue to the next section.

If installing one or more SAM Express agents

Among the agents you may have selected for installation, the IAS/NPS Agent has some additional installation windows.

Note: Complete Agent configuration and use instructions can be found in the SAM Express Agent Administration Guide at http://www.safenet-inc.com/support/SAMx-documentation/.

19 If you selected the IAS/NPS Agent for installation on Server 2003, you will be prompted to restart the IAS service by clicking Yes.

Note: If installing on Server 2008, the Restart IAS window will not appear, and you may skip to “Finishing the installation”.

Figure 13: Create Cloud Server credentials window

![Create Cloud Server credentials window](image)
Installing SAM Express

Once you click Yes, the IAS service will restart, and you can skip to “Finishing the installation” on page 43.

Finishing the installation

During installation, windows will appear and disappear, and installation will take several minutes to complete. The InstallShield Wizard Complete window appears when the installation is finished.

If IAS/NPS was installed on Server 2008 or later, and/or the DLA was selected for installation, you will be prompted to restart the machine.

The basic software installation is now complete, but you must activate your SAM Express software before you can use it.

Refer to the section, “Activating SAM Express” on page 44 to complete the procedure.

Note: If you do not have internet access, updates must be applied from an FTP image. Contact Technical Support at 1-800-545-6608 (US Toll Free), or 1-410-931-7520 (International) to get the necessary image.
Activating SAM Express

By default, SAM Express comes with a 30-day evaluation license. If you want to continue using it, activation is required. The Activation Certificate that came with your software contains the SAM Express Serial number and Token Group ID that allow you to download the activation key and token data records, and are in the following formats:

- **SAM Express Software Serial Number**—The serial number is a 16-digit alphanumeric code in the form of this example: NSxx-xxxx-xxxx-xxxx. You will need the serial number to obtain your product activation key.

- **Token Group ID**—Your Token Group ID is a 16-digit alphanumeric code in the form of this example: TKxx-xxxx-xxxx-xxxx.

---

**Important:** Keep your Activation Certificate in a safe location. You will need the Software Serial Number when/if you purchase additional SafeNet tokens.

---

Registering on the portal

There are two methods for activating SAM Express: using ADUC, or directly from our website if ADUC is not being used (see “Activating via Website” on page 46).

In either case, you must sign in and register on the SafeNet portal before you can complete and submit an activation form. After activating, your information will be verified, and the activation key and token records will be downloaded automatically for ADUC, and manually if you are not using ADUC.

---

**Security Alert:** The prompt to download the activation key and token data records is a one-time only prompt. For security reasons, you are only allowed one attempt to download these files. See www.safenet-inc.com/support for information on how to contact Customer Service to request a CD with these records.
Chapter 2: Installing and Activating SAM Express

Activating SAM Express

Activation using ADUC

To activate the product from ADUC (have your activation certificate handy):

1 In ADUC, click on the SAM Express folder.

   The first time you right-click on the SAM Express folder, you will be prompted to enter and re-enter (to verify) an Administrator password. This Administrator password is not your Windows Administrator password. If you have (or plan to have) multiple management consoles, you must use the same Administrator password for all installations.

   **Note:** The default User Name **Administrator** can only be changed if using the delegated administrators feature (see “Delegated administration in Active Directory” on page 79).

2 Click **OK** when done.

3 Right-click on the SAM Express folder and select **Activate Product**.

4 Log in to the portal using the credentials received when you registered.

   **Important:** Token Group IDs that have not been activated may be entered at this time. All upgraded Token records have already been activated.

   **Note:** You may be required to create a login the first time you visit the activation site.

5 Complete the activation form, then click **Submit**.

   The SAM Express Activation window appears showing the license activation and token import progress. Upon completion, the activation file **key.html** is downloaded to `<Install_Dir>\ImportData`. This is the key to activate your software and your token data records. You should back up these files in case you need to reactivate the product or re-import token records later.

   The Administration Server and Authentication Engine services will restart.

6 To verify the activation, browse to `<Install_Dir>\SERVERS\AdminServer\activation`.

   The successfully processed license file is renamed **key.activated.html**.

7 Relaunch ADUC.
Activating via Website

To manually activate SAM Express, do either of the following:

1 Create an **RCR.txt** file manually by doing the following:
   a On the SAM Express installation server, select **Start > Programs > SafeNet > SAM Express > SAM Express Management Console**.
   b Log in to the Administration Server using the default user name **Administrator** and the default password **Administrator**.
   c From the Configuration menu, select **Support**. The Support Information Center page appears.
   d Click the **Save** button to automatically save the RCR.txt file to a temporary directory.

   Or
   a On the SAM Express installation server, select **Start > Programs > SafeNet > SAM Express > Active Directory Users and Computers**.
   b Right-click the SAM Express folder in the left directory tree and select **Support**.
   c Click the **Save** button to automatically save the RCR.txt file to a temporary directory.

2 Browse to the **SafeNet Portal** and log in using the username and password that were sent to you when you registered.

   **Note:** You may be required to create a login at your first visit to the activation site.

3 Enter your SAM Express Software serial number in the appropriate field. (The serial number format is **NSXX-XXXX-XXXX-XXXX**.)

4 Click **Continue**.
   The SAM Express Activation page appears.

   **Important:** Token Group IDs that have not been activated may be entered at this time. All upgraded token records have already been activated.

5 Import the required support data (**RCR.txt**) by browsing to the RCR.txt file that you saved in step 1.

6 Complete the activation form, then click **Submit**.
   You can now download the files that contain the key to activate your software and your token data records. You should back up these files in case you need to reactivate the product or re-import token records later.

7 Copy **key.html** into the following subdirectory on the SAM Express system:
   `<Install_Dir>\SERVERS\AdminServer\activation`. 
Chapter 2: Installing and Activating SAM Express

Activating SAM Express

Important: Ensure the file name is key.html. Using any variation (key.htm or key.html.html, for instance) will cause the activation to fail.

8 Restart the SAM Express Administration Server and Authentication Engine by browsing to Start > Programs > Administrative Tools > Services, right click on SAM Express Administration Server and select Restart (repeat for the Authentication Engine).

9 To verify the activation, browse to <Install_Dir>\SERVERS\AdminServer\activation. The successfully processed license file is renamed key.activated.html.
Activating SAM Express on a remote ADUC installation

If ADUC is installed on a machine different than the machine on which the SAM Express server is running, the following additional activation steps are necessary:

*Note:* If SAM Express is installed on a 64 bit OS, the server's installation directory and the SAM Express Management Console are found in the C:\Program Files (x86) directory structure.

1. On the system where ADUC is installed, browse to the location where the key.html file is stored (<Install_Dir>\Import Data).
2. Copy key.html into the following subdirectory on the SAM Express system: <Install_Dir>\SERVERS\AdminServer\activation.

*Important:* Ensure the file name is key.html. Using any variation (key.htm or key.html.html, for instance) will cause the activation to fail.

3. Restart the SAM Express Administration Server and Authentication Engine by browsing to Start > Programs > Administrative Tools > Services.
4. Right click on SAM Express Administration Server and select Restart (repeat for the Authentication Engine).

The successfully processed license file will be renamed key.activated.html.

Verifying your activation in ADUC

Your SAM Express registration and activation are complete, but you may verify the success of the activation by doing the following:

1. (If not already open) Launch ADUC.
2. Right-click the SAM Express folder in the Console, and select About SAM Express.
3. Verify that the Product Serial Number in the Serial Number field is correct and that the Expiration Date is set to None.
4. Browse to <Install_Dir>\SERVERS\AdminServer\activation. The successfully processed license file is now renamed key.activated.html.
Verifying activation in the SAM Express Management Console

1. Launch the Console by selecting **Start > Programs > SafeNet > SAM Express > SAM Express Management Console**.
2. Log in as “administrator,” password “administrator.”

   **Important**: If ADUC was previously launched the default administrator password will have been changed, and that new password must be used here.

3. Select **Configuration > Activation**.
4. Verify that the Product Serial Number is correct and that the Expiration Date is set to **None**.

Subsequent token activations

When you purchase additional tokens, you activate them using the original Product Serial Number and the Token Group ID from the newly purchased token pack. Follow the same steps outlined in the activation instructions, “Activating SAM Express” on page 44. In this case, even if the management console is installed separately from the SAM Express server, it is not necessary to activate the server using the **key.html** file.

Extending your support

When you extend your product support, and then reactivate your software, updated support information, including the new expiration date, the activation date, and whether or not ESP is enabled, appear in the About Sam Express window. You can view this information by selecting **Help > About SAM Express** from the SafeWord Management Console and from ADUC.

To renew or extend your product support, re-activate SAM Express by doing the following:

- Right-click the SAM Express node (in ADUC) and select **Activate Product**, or
- Go to the **Portal**, login, and provide your SAM Express serial number. Download the **key.html license key**. You will need to confirm that this key is named **key.html**. Place it in your SAM Express activation folder, and then restart the SAM Express Administration Server service. Upon successful activation, this license will be renamed to **key.activated.html**.
Evaluating MobilePASS tokens

New installations and auto updates of SAM Express include four evaluation tokens. Two of these tokens are Software tokens and two are Messaging tokens. The Software tokens are named **EVAL-SOFTWARE-1** and **EVAL-SOFTWARE-2** and the Messaging tokens are named **EVAL-MESSAGING-1** and **EVAL-MESSAGING-2**.

The four tokens are located in two import files located in the SAM Express folder. One of the files is named **SoftwareEvalTokens.dat** and the other is **MessagingEvalTokens.dat**. The four token records are included in two .dat files located in the SAM Express folder. The evaluation Software tokens are valid tokens. They can be used like any other licensed Software tokens.

---

**Important:** As valid tokens, the evaluation Software token records are included in the pool of available tokens and will be auto-assigned to users. If you do not want evaluation Software tokens auto-assigned, delete the records from your database.

---

The evaluation Messaging tokens are **not** intended for use in production environments; they contain known keys and are therefore insecure. They are intended for evaluating the Messaging feature. Upon evaluation, if you wish to order additional Messaging tokens, please contact your SAM Express reseller, or browse to the corporate site at [www.safenet-inc.com](http://www.safenet-inc.com).
Information about SAM Express support expiration date, renewal options, authenticator counts, and more, can be found by using SAM Express’s Support Information Center.

To access the Support Information Center:

- **From ADUC**, right-click on the SAM Express folder, and select **Support...**
- **From the SAM Express Management Console**, select **Configuration > Support**.

*Note:* From either console, clicking the **Save** button in the **Support** window will save support data to a file named **rcr.txt** (needed for activation) to the system you will be activating.
CHAPTER 3

Active Directory Management

In this chapter...

Overview ..........................................................54
Changing the administrative password in ADUC ..................55
Setting up token records and data files ...............................55
Configuring the enrollment policy ....................................59
Assigning tokens to users .............................................67
Delegated administration in Active Directory .....................79
Overview

This section describes managing users who are stored in Active Directory. It includes details about software token self enrollment, assigning Messaging and Hardware tokens to users, assigning PINs to tokens, generating emergency passcodes, and testing and resynchronizing tokens. Additionally, it provides instructions for delegating certain management functions to administrative users based on their assigned privileges.

SAM Express provides Active Directory users with a variety of software and hardware tokens and options. MobilePASS Software tokens run on iPhone/iPad/iPod touch, BlackBerry, J2ME, and Android devices, and on Windows and Mac Desktops. MobilePASS Messaging tokens deliver passcodes in messages via SMS or e-mail via SMTP. Traditional hardware tokens provide secure one-time use passcodes, and are available in a variety of form factors.

⚠️ **Important:** Before proceeding to user management, you should change the administrative password in ADUC.
Changing the administrative password in ADUC

The first time you access SAM Express in ADUC, you will be prompted to change your administrative password. If for some reason, you need to change that password again, do the following:

1. Right-click on the **SAM Express** node in the directory tree.
2. Select **Change Administrative Password**.
3. Enter the new **password**, and confirm it.
4. Close the dialog box.

Setting up token records and data files

If hardware tokens are being distributed, the token data files that were downloaded during activation must be imported. If Software and Messaging tokens are being distributed, MobilePASS records must be generated. If you need to import hardware token data files, see “Importing token data files” on page 58. If you are generating MobilePASS records for software or Messaging tokens, continue to the next section.

Generating MobilePASS records in ADUC

Before enrolling MobilePASS tokens, the token records must be generated in the SAM Express database. You configure these records on the Active Directory Users and Computers (ADUC) MobilePASS window. To launch the window:

1. Open ADUC by selecting **Start > Programs > SafeNet > SAM Express > Active Directory Users and Computers**.
2. Select the **MobilePASS** folder under the **SAM Express** node. The MobilePASS window appears with the Licensing pane displayed in the upper portion of the window.
Software Tokens allow users to generate passcodes on their iPhone/iPod touch/iPad, BlackBerry, Android, and J2ME devices, as well as on their Windows and Mac Desktops. Messaging Tokens allow users to request and receive passcodes in the form of messages and e-mail via SMS and SMTP respectively.

3 Select the token type for which you wish to generate records (Software Tokens or Messaging Tokens), then click the Configure Licensing button. The Licensing window appears. If you are generating Software tokens, the Passcode Length field is preset to 6 and is inactive on this window, as Software token passcode lengths are not configurable.

Note: For details about configuring providers, refer to “Editing provider information” on page 118.
4 Referring to your MobilePASS/SofToken® II Activation Certificate, enter the following information on the Licensing window:

a Enter the serial number from your MobilePASS/SofToken® II Activation Certificate in the Serial Number field.

b Enter the total number of units from your certificate in the Units field.

c Enter the Seed value in the Seed field.

d Enter your authorization code in the Authorization Code field.

e Enter your activation code in the Activation Code field.

f (Messaging tokens only) Under Generation Options, select the desired Passcode Length. Default length is 6 and range is 6 to 8 characters.

Note: By default the passcode length for Software tokens is set to 6 and is not configurable.

g Select the Overwrite Existing on Import option check box to overwrite existing import records when new records are generated. If you do not want to overwrite existing records, leave the check box cleared.

h Select Generate All or Generate Range.

If Generate All is selected, all available units associated with this license will be generated. In this case, continue to step 5 to generate and import the records.

If Generate Range is selected, the Start Serial Number field, and the Count field are activated. In this case, do the following:

- In the Start Serial Number field, enter the serial number of the first unit in the range of units that will be generated.
- In the Count field, enter the number of units to generate.

5 Click the Generate and Import button. The desired records are generated.
and imported into the SAM Express database.

**Importing token data files**

Before you can assign and use hardware tokens, the token data records downloaded during activation must be imported. To import token data files:

**Note:** If you purchased additional tokens, the token data files will be contained on the CD that came with your tokens. The procedures for importing those token records are the same as listed below.

1. Launch ADUC by selecting **Start > Programs > SafeNet > SAM Express > Active Directory Users and Computers**, expand the **SAM Express node**, and click on the **Import/Backup/Restore** node.

   ![Figure 17: ADUC import](image)

2. Browse to and open the token data file (*importAlpine.dat*).

3. Click the **Import** button, and then click **OK** when the Import Successful window appears.
Configuring the enrollment policy

Before assigning MobilePASS software tokens to users, or allowing users to self enroll, you must configure the enrollment policy. This policy communicates the specific capabilities of a token device between the MobilePASS clients and the MobilePASS portals and servers. The enrollment policy that you configure is a single, global enrollment policy that will apply to all your AD users. Table 4 provides the parameters that are available for configuring the policy. Please note that features are enabled when they are set to true, and are disabled when set to false.

Table 4: Enrollment policy token types and capabilities

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Parameters</th>
<th>Parameter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Event Sync</td>
<td>Passcode Length</td>
<td>6 digits (fixed)</td>
</tr>
<tr>
<td></td>
<td>Collect SoftPIN</td>
<td>True or False</td>
</tr>
<tr>
<td></td>
<td>Use Device PIN</td>
<td>True (fixed)</td>
</tr>
<tr>
<td></td>
<td>Device PIN Length</td>
<td>4 digits (fixed)</td>
</tr>
<tr>
<td></td>
<td>Use Attack Lockout</td>
<td>True (fixed)</td>
</tr>
<tr>
<td></td>
<td>Attacks Before Lockout</td>
<td>10 (fixed)</td>
</tr>
<tr>
<td></td>
<td>Use Attack Delay</td>
<td>False (fixed)</td>
</tr>
<tr>
<td></td>
<td>Attacks Before Delay Begins</td>
<td>8 (fixed)</td>
</tr>
<tr>
<td></td>
<td>Force Device PIN Change</td>
<td>False (fixed)</td>
</tr>
<tr>
<td></td>
<td>Uses Before PIN Change</td>
<td>128 (fixed)</td>
</tr>
<tr>
<td></td>
<td>Allow Enrollment to Non-poly-based Clients</td>
<td>True or False</td>
</tr>
<tr>
<td></td>
<td>Secure Mode</td>
<td>False (fixed)</td>
</tr>
<tr>
<td>Standard Time Sync</td>
<td>Passcode Length</td>
<td>6 digits (fixed)</td>
</tr>
<tr>
<td></td>
<td>Time Sync Interval</td>
<td>30 (fixed)</td>
</tr>
<tr>
<td></td>
<td>Collect SoftPIN</td>
<td>True or False</td>
</tr>
<tr>
<td></td>
<td>Use Device PIN</td>
<td>True (fixed)</td>
</tr>
</tbody>
</table>

Note: Feature is enabled when set to true. Default is false (disabled).
## Configuring the Enrollment Policy

### Device PIN Length
- **4 digits (fixed)**

### Use Attack Lockout
- **True (fixed)**

### Attacks Before Lockout
- **10 (fixed)**

### Use Attack Delay
- **False (fixed)**

### Attacks Before Delay Begins
- **8 (fixed)**

### Force Device PIN Change
- **False (fixed)**

### Uses Before PIN Change
- **128 (fixed)**

### Allow Enrollment to Non-policy-based Clients
- **True or False**

### Secure Mode
- **False (fixed)**

### Standard Challenge Response
- **Passcode Length**
  - **8 digits (fixed)**

### Challenge Length
- **8 (fixed)**

### Collect SoftPIN
- **True or False**

### Use Device PIN
- **True (fixed)**

### Device PIN Length
- **4 (fixed)**

### Use Attack Lockout
- **True (fixed)**

### Attacks Before Lockout
- **10 (fixed)**

### Use Attack Delay
- **False (fixed)**

### Attacks Before Delay Begins
- **8 (fixed)**

### Force Device PIN Change
- **False (fixed)**

### Uses Before PIN Change
- **128 (fixed)**

### Allow Enrollment to Non-policy-based Clients
- **True or False**

### Secure Mode
- **False (fixed)**

More...
### Configuring the enrollment policy

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Parameters</th>
<th>Parameter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Event Sync</td>
<td>Passcode Length</td>
<td>6 or 8</td>
</tr>
<tr>
<td></td>
<td>Collect SoftPIN</td>
<td>True or False</td>
</tr>
<tr>
<td></td>
<td>Use Device PIN</td>
<td>• True or False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, PIN length: 4, 6 or 8</td>
</tr>
<tr>
<td></td>
<td>Use Attack Lockout</td>
<td>• True or False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, attacks before lockout: 3, 6, or 10 invalid attempts. <strong>Note:</strong> The number of attacks before lockout should always be greater than the number of attacks before an attack delay.</td>
</tr>
<tr>
<td></td>
<td>Use Attack Delay</td>
<td>• True or False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, attacks before delay begins: 8 invalid attempts (fixed). <strong>Note:</strong> Initial delay is one minute. Increases by one minute for each failed attempt. Delay reaches a maximum at 20 minutes, and resets only upon successful device PIN entry.</td>
</tr>
<tr>
<td></td>
<td>Force Device PIN Change</td>
<td>• True or False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, successful uses before device PIN change: 128 (fixed).</td>
</tr>
<tr>
<td></td>
<td>Allow Enrollment to Non-policy-based Clients</td>
<td>True or False</td>
</tr>
<tr>
<td></td>
<td>Secure Mode</td>
<td>True or False</td>
</tr>
</tbody>
</table>
### Configuring the Enrollment Policy

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Parameters</th>
<th>Parameter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Time Sync</td>
<td>Passcode Length</td>
<td>6 or 8</td>
</tr>
<tr>
<td></td>
<td>Time Sync Interval</td>
<td>20, 30, or 60 seconds</td>
</tr>
<tr>
<td></td>
<td>Collect SoftPIN</td>
<td>True or False</td>
</tr>
<tr>
<td></td>
<td>Use Device PIN</td>
<td>• True or False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, 4, 6 or 8 digits.</td>
</tr>
<tr>
<td></td>
<td>Use Attack Lockout</td>
<td>• True or False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, attacks before lockout: 3, 6, or 10 invalid attempts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The number of attacks before lockout should always be greater than the number of attacks before an attack delay.</td>
</tr>
<tr>
<td></td>
<td>Use Attack Delay</td>
<td>• True or False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Attacks before delay begins: 2, 4, or 8.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> Initial delay is one (1) minute, and increases by one minute for each failed attempt. Delay reaches a maximum at 20 minutes, and resets only upon successful device PIN entry.</td>
</tr>
<tr>
<td></td>
<td>Force Device PIN Change</td>
<td>True or False</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, successful uses before device PIN change: 128 (fixed).</td>
</tr>
<tr>
<td></td>
<td>Allow Enrollment to Non-policy-based Clients</td>
<td>True or False</td>
</tr>
<tr>
<td></td>
<td>Secure Mode</td>
<td>True or False</td>
</tr>
</tbody>
</table>

*More...*
To configure the enrollment policy for users stored in Active Directory, use the policy parameters from Table 4 and do the following:

1. Open ADUC by selecting **Start > Programs > SafeNet > SAM Express > Active Directory Users and Computers**.

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Parameters</th>
<th>Parameter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Challenge Response</td>
<td>Passcode Length</td>
<td>6 or 8</td>
</tr>
<tr>
<td></td>
<td>Challenge Length</td>
<td>6 or 8</td>
</tr>
<tr>
<td></td>
<td>Collect SoftPIN</td>
<td>True or False</td>
</tr>
</tbody>
</table>
|                             | Use Device PIN       | • True or False
|                             |                      | • When enabled, PIN length: 4, 6 or 8. |
|                             | Use Attack Lockout   | • True or False
|                             |                      | • When enabled, attacks before lockout: 3, 6, or 10 invalid attempts. |
|                             | Use Attack Delay     | • True or False
|                             |                      | • Attacks before delay begins: 2, 4, or 8 |
|                             |                      | *Initial delay is one (1) minute, and increases by one minute for each failed attempt. Delay reaches a maximum at 20 minutes, and resets only upon successful device PIN entry.* |
|                             | Force Device PIN Change | • Enable or Disable |
|                             |                      | • When enabled, successful uses before device PIN change: 128, 256, or 384. |
|                             | Allow Enrollment to Non-policy-based Clients | True or False |
|                             | Secure Mode          | True or False                      |

*Note: The number of attacks before lockout should always be greater than the number of attacks before an attack delay.*
2 Select the MobilePASS folder under the SAM Express node. The MobilePASS window appears with the Configure Policy pane displayed in the lower portion of the window.
3 Click the **Configure Policy** button. The MobilePASS Enrollment Policy window appears.

![Enrollment Policy window](image)

Figure 19: Enrollment Policy window

4 Table 4 on page 59 provides the policy parameters available with each token type. Using this information, select the type of token to which you will be applying this policy. You may choose from the following:
   - Standard Event-Synchronous
   - Standard Time-Synchronous
   - Standard Challenge-Response
   - Custom Event-Synchronous
   - Custom Time-Synchronous
   - Custom Challenge-Response.

5 Select a passcode length from the **Passcode Length** list. You may choose a 6-digit or an 8-digit passcode. If you choose a standard policy, the length of passcode option is disabled, and the default setting displays.

6 Select whether or not to require users associate a SoftPIN with this token by clicking **Collect SoftPIN**, and then selecting **True** or **False** from the drop down menu. Features are enabled when you select true, and disabled when you select false.

7 (For custom challenge-response tokens only.) Select a challenge length from the list. You may choose a 6-digit or an 8-digit challenge length.

8 (For custom time-synchronous tokens only.) Select the interval (in seconds) before a new passcode is available from the Time Sync Interval list. You may choose 20 seconds, 30 seconds, or 60 seconds.

9 (For custom event-synchronous and time-synchronous tokens only.) Under **Device PIN Policy**, do the following:
   a Device PINs refer to the optional PINs that are set on software tokens when MobilePASS is activated. When enabled, device PINs must be
entered on the MobilePASS application or device in order to generate passcodes. Highlight **Use Device PIN** to enable this feature, and then select a PIN length from the PIN Length list (4, 6, or 8 digits).

**b** The attack lockout feature allows you to set the number of attacks before lockout. The number of attacks before lockout should always be greater than the number of attacks before an attack delay. Highlight **Use Attack Lockout** to enable this feature, and then select the number of attacks before lockout occurs (3, 6 or 10).

**c** The attack delay feature allows you to set the number of invalid attempts that can be made before attack delay begins. Highlight **Use Attack Delay** to enable this feature, and then select the number of attacks to allow before delay begins (2, 4, or 8 attacks).

---

**Note:** The initial delay is one minute. The delay increases by one minute for each failed attempt. Delay reaches a maximum at 20 minutes, and resets only upon successful device PIN entry.

---

**d** The Force Device PIN Change feature allows you to set the number of successful PIN uses before the device PIN must be changed. Highlight **Force Device PIN Change** to enable this feature, and then select the number of successful uses before a change is required (128, 256, or 384).

**10** Under Policy Options, select whether to allow client devices that do not support policies to enroll and ignore the specified policy options. The feature is enabled by selecting true, and disabled by selecting false.

**11** (For custom tokens only.) Secure mode allows SafeNet to react to security vulnerabilities of client devices on a case by case basis. Select the Secure Mode check box to allow SafeNet to possibly modify MobilePASS client behavior when security vulnerabilities become known.

**Note:** When secure mode is enabled, application updates may result in MobilePASS disabling clients that do not meet their defined security mode.
Assigning tokens to users

There are two ways to assign SafeNet tokens to Active Directory users. You may use the Token Assignment Wizard, or you can manually enter the token serial number in the serial number field. The Wizard assigns Software, Messaging, and Hardware tokens. It will automatically select and assign the next available Software or Messaging token. You select the Hardware token that you will be assigning with the Wizard.

**Note:** You must use the Token Assignment Wizard to assign Software tokens. If you are manually entering the token serial numbers, the interface will only accept Messaging and Hardware token serial numbers. You cannot assign Messaging tokens with the Token Assignment Wizard if the tokens were generated and imported before SafeWord 2008 version 2.1.0.03.

If you have not already done so, you must generate MobilePASS records before assigning Software or Messaging tokens (see “Generating MobilePASS records in ADUC” on page 55), and/or you must import your hardware token data files before assigning hardware tokens. For details, see “Importing token data files” on page 58.

**Assigning tokens with the Token Assignment Wizard**

The Wizard is located on the SAM Express tab of each user’s Properties window. To assign tokens using the Token Assignment Wizard, do the following:

1. In ADUC, highlight the user to whom you will be assigning a token.

   ![Figure 20: Users node of ADUC](image)

2. Right-click on the the user name and select **Properties**. The Properties window appears.
3 Click the **SAM Express** tab. If this user has not yet been assigned a token, the Token serial number field is empty on the displayed tab. If this user has a token assigned, the window appears with a serial number displayed.

**Tip:** If you get an error while attempting to view a user’s SAM Express tab, the administration service has rejected the user’s client certificate. This occurs when ADUC has been re-installed. Remove the user’s client certificate to access the SAM Express tab of their Properties window (see “Reinstalling a server or ADUC” on page 87).

**Important:** If the user already has a token assigned to them, the existing token will be replaced by a new token when the Wizard is used.

![Figure 21: SAM Express tab of user properties window](image)

**User with no tokens assigned**  **User with a token assigned**

4 Click the **Wizard** button. The Choose authenticator window appears.

![Figure 22: Choose authenticator window](image)

5 Select the type of token to assign. If assigning a Software or Messaging token, and an unassigned token of this type is available in the SAM Express database, the Wizard will automatically assign the next available token of that type and you are prompted to enter an activation code. If you are assigning a Hardware token, you will be prompted to enter the token serial number to assign the token to the user.
6 Continue to the appropriate section for details on assigning specific tokens.
   – If you select **Software token**, continue to “Assigning Software tokens to users” on page 69.
   – If you select **Messaging (SMS/Email) token**, continue to “Assigning Messaging tokens to users” on page 71.
   – If you select **Hardware token**, continue to “Assigning Hardware tokens to users” on page 71.

### Assigning Software tokens to users

Administrators who are assigning Software tokens to Active Directory users should do the following:

a Select the **Software token** option, and then click the **Next** button. The window providing your policy string appears.

![Figure 23: Policy String window](image)

b Enter the policy string onto your device. The Enter Activation Code window appears.

![Figure 24: Enter Activation Code window](image)

**Note:** If there are no Software tokens available, the window appears with the Activation Code field grayed out, and with a message stating there are no tokens available. In this case, generate or import tokens before continuing.
c Enter the 20-digit activation code from your user’s MobilePASS device software, and then click the **Assign** button. The user is assigned a Software token. Confirm the Activation prompt on the device. The device is now ready to be distributed to the user.

d The Wizard closes and the token serial number appears on the User’s SAM Express tab. Continue to “Adding or changing PINs” on page 74.

If you will allow users to self-enroll their Software token, refer to “Allowing users to self-enroll” on page 111.
Assigning Messaging tokens to users

To assign Messaging tokens to users, do the following:

a Select the **Messaging (SMS/Email) token** option, and then click the **Next** button. A new window appears indicating that there are Messaging tokens available.

![Figure 25: Messaging tokens available window](image)

b Click the **Assign** button. The user is assigned the next available Messaging token.

c The Wizard closes and the token serial number appears on the User’s SAM Express tab. Continue to “Adding or changing PINs” on page 74.

Assigning Hardware tokens to users

To deploy Hardware tokens to your Active Directory users, you must import the token data files that were downloaded during activation, or import them from the CD that came with your token pack (see “Importing token data files” on page 58). Once the token data files have been imported, you can associate tokens to users using the Wizard or by manual assignment.

**Assigning Hardware tokens with the Wizard**

To assign Hardware tokens with the Wizard, do the following:

a Select a hardware token.

b Launch the Token Assignment Wizard, select the **Hardware token** option, and then click **Next**. The Hardware token enter serial number window appears.
Chapter 3: Active Directory Management

Assigning tokens to users

Figure 26: Hardware token enter serial number window

- Enter the hardware token serial number (found on the back of the token) into the field, and then click **Assign**. The token is now assigned to the user and you are returned to the User's Properties window.

- Give the token to the user. After a token is assigned by the Wizard, its serial number appears in the Serial Number field of the user’s SAM Express tab. Continue to “Adding or changing PINs” on page 74.

If you wish to allow users to self-enroll their Hardware token, refer to “Allowing users to self-enroll” on page 111.

Assigning tokens manually (“shortcut” method)

You can directly assign Messaging and Hardware tokens using the token serial number. This direct assignment method provides a “shortcut” for quickly assigning tokens. To directly assign a token to a user:

- Launch ADUC.

- On the left side of the window, highlight the **Users** folder.

- Locate the user to whom you will be assigning a token, right-click the user’s name and select **Properties**, then in the user’s Properties window click the **SAM Express tab**.

---

**Tip:** If some of your users will share a token, assign the same token serial number to each user who will share it.
Tip: If you get an error while attempting to view a user’s SAM Express tab, the administration service has rejected the user’s client certificate. This occurs when ADUC has been re-installed. Remove the user’s client certificate to access the SAM Express tab of their Properties window (see “Reinstalling a server or ADUC” on page 87).

d In the **Token serial number** field (found in the SAM Express tab), enter the token’s serial number, and an optional four-digit PIN.

Requiring a PIN with a user passcode adds a second layer of security to your system. If you will require users to authenticate with a token passcode and PIN, they must append the PIN to the end of the passcode. If they do not know their PIN, they will be denied access.

e Click **Apply**.

**Note:** See “Configuring the Authentication Policy” on page 264 for information on configuring group memberships.

Clicking **Apply** activates the lower portion of the window, allowing you to test the token (see “Testing tokens” on page 74).

f If you will not be testing the token now, click **OK** to close the window.

g Distribute the token to the user (be sure to tell them if they will need to append a PIN to the end of their passcode).
Assigning tokens to users

Testing tokens

Once a token has been assigned it should be tested. A token test option is located on a user’s SAM Express tab in ADUC. To test a token, do the following:

1. (If not already open) Open the user’s Properties window and click the SAM Express tab.
2. Confirm that the Token serial number field is populated with the serial number of the token you are testing.
3. Generate a one time passcode using the token and enter it in the Passcode field under Token Test.
4. You do not need to append a PIN to the end of the Passcode in the Management Console, even if the user requires a PIN to log in.
5. Click the Test button.
6. Click OK in the window indicating a successful test.

Adding or changing PINs

Once a token is enrolled into SAM Express, you may also choose to assign a PIN along with token-generated one-time passcodes. As the administrator, you can use ADUC to add or change PINs for users.

You can add PINs for all users, or you can give all or some users the option to decide for themselves whether or not they want to use a PIN. To add or change a PIN with ADUC, do the following:

1. In ADUC, double click the user to whom you are assigning a PIN.
2. When the user’s Properties window appears, select the SAM Express tab.
3. To assign a new PIN or change an existing one, enter the desired PIN in the field labeled PIN (appended to their token passcode).
4 Click **Apply** or **OK**. The PIN is now required each time this user authenticates using passcodes generated with the assigned token.

5 If the user does not require a PIN, simply clear the existing PIN from the field labeled **PIN (appended to their token passcode)**.

---

**Resynchronizing Hardware tokens**

There are occasions when a SAM Express token will get out of synchronization and its generated passcodes will not function properly. If this occurs, you will need to resync the token. To resync a token, do the following:

1 In ADUC, select the **Users** folder on the left side of the window.

2 Right-click the user whose token you need to resync, then select **Properties**.

3 Click the **SAM Express** tab.

4 In the Token Maintenance area, click the **Re-sync**... button to display the Re-synchronize token window, then enter two sequential token passcodes (plus appended PINs, if assigned), and click the **Re-sync** button.

---

**Searching for unassigned tokens**

To search for unassigned tokens, do the following:

1 In ADUC, expand the **SAM Express** node in the left pane.

2 Click the **Tokens** icon.

   Token serial numbers and assigned users appear in the right pane. Unassigned tokens appear with **[Not Assigned]** under the Assigned to User list.

---

**Finding users associated with specific tokens**

To use the SAM Express Search utility to find users and their tokens, do the following:

1 In ADUC, expand the **SAM Express node** in the left pane, and select the **Search** node.
2 Enter the token serial number in the **Token serial number** field, and then click the **Search** button.

**Tip:** Entering a partial token serial number will find all users whose token serial numbers begin with the entered number. Leaving the field blank will retrieve all users who have tokens assigned.

The Search Results list the Full Name, User Logon Name, and Token Serial Numbers.

---

**Generating emergency passcodes**

Emergency passcodes can be generated for event-synchronous tokens. For tokens programmed as time-synchronous, the Emergency Passcode functionality will be disabled on the SAM Express tab of the user’s property window.

**Important:** When you generate an emergency passcode for a user who has forgotten their token (or whose token passcode is not working properly), the token will have to be resynchronized. If you have generated five emergency passcodes, the token will produce five identical passcodes when it is used again. The user should generate the same number of token passcodes as emergency codes generated for them. Generating these passcodes with their token without using the passcodes will resynchronize the token.

To generate emergency passcodes for a user, do the following:

1 In ADUC, select the **Users** folder in the left pane, and double-click the name of the user(s) requiring an emergency passcode(s).

2 In the User Properties window, click the **SAM Express** tab.

3 In the Emergency Passcodes section, set the number of one-time passcodes to generate. You may generate up to nine emergency passcodes.

**Note:** The same sequence of passcodes is generated every time you press the **Generate** button until one of them is successfully used for authentication.

4 Under Emergency Passcodes, click the **Generate** button. SAM Express automatically generates the number of passcodes you request, and they appear in the order in which they must be used.

5 Inform the user of the emergency passcodes.

**Important:** Emergency passcodes must be used in the same sequential order in which they were generated. Emergency passcodes are exactly like token-generated one-time passcodes, and cannot be used more than once.
Reassigning Hardware and Messaging tokens

When users leave your organization or no longer need to authenticate with SAM Express, their SAM Express token and its records can be reassigned to another user. You reassign Hardware tokens by removing the token serial number from the departing user’s properties, then adding that serial number to the new user’s properties and giving the token to the new user. Removing a serial number disassociates the token records from the user. It does not remove that information from your database. When you assign the token serial number to a new user, a new association is created. Once the token is given to the new user, that user can use this token to generate passcodes for authentication to access your protected resources.

Important: When a token is lost, stolen, or broken you must completely remove the token records from your database (as token records are obsolete without the token). See “Deleting token records from the database” on page 78 for information about deleting token records.

When Software or Messaging tokens are unassigned, they are placed back in the pool of available tokens, and can be assigned to another user.

Note: For Messaging tokens, remove the Messaging token from the user properties, and assign a new Messaging token using the Wizard.

To reassign a token, do the following:

1. In ADUC, select the Users folder in the left pane.
2. Locate the user, right-click on the user name for whom you are disassociating token records, then select Properties.
3. Select the SAM Express tab in the user’s Properties window.
4. Clear the serial number from the Token serial number field, and then click the Apply button.
5. If the Delete PIN message appears, click Yes to delete the PIN associated with this token, or click No to leave the PIN assigned to the user from whom this token is being disassociated.

Note: Deleting a token PIN gives that user the option to add a new PIN when receiving the new token. If you do not delete the PIN from a user’s Properties, that user will need to use the assigned PIN even when receiving a new token.

6. Click OK.
7. Open the Properties window for the user to whom you are reassigning the token, assign the same serial number using the Wizard, or enter the token’s serial number into the Token serial number field.
8. Click OK.
Assigning tokens to users

You have now created a new association between this user and the token records, and may give the token to its new user.

Deleting token records from the database

There are situations when you will need to delete token records from the database. If a token is lost, stolen, or broken, its token records are obsolete since you will not be able to reassign the token to another user. You should delete obsolete token records from your database. Deleting them provides space to add new token records when your organization purchases additional SafeNet tokens.

1. In ADUC, expand the SAM Express node in the left pane, and select the Tokens icon.

2. From the Token serial number list on the right side of the window, select one or more tokens to delete and right-click the selection, and select Delete.

   If the token is already assigned to a user, the Token Assigned message appears to confirm that you really want to delete the token record.

   **Important:** If you delete tokens at this point, and then restore the database, all token user associations will be lost.

   **Tip:** Multiple token records can be selected and deleted simultaneously. You can also highlight a token and use the Delete button on the toolbar to delete token records.

3. Click Yes.

4. The token records are deleted from the database. If you want to unassign the token without removing the records from the database, see “Reassigning Hardware and Messaging tokens” on page 77.
SAM Express allows you to create administrative users to whom you can delegate certain AD user and token management responsibilities. Responsibilities are based on the administrative privileges (ability to view and change user records, change and assign PINs, import, assign and test tokens, etc.) that you select for them.

**Note:** The following configurations are set up using the SAM Express Management Console (described in Chapter 8 of this book), which is included with SAM Express ESP.

- **System administrators:** Full Read/Write privileges on all AD user records/token management functions
- **Local administrators:** Selectable Read-Write/Read-Only privileges on AD user records/token management functions

**Note:** Only system administrators can modify the MobilePASS configuration.

The basic process for setting up this configuration in the SAM Express Management Console would be:

- Create (or select) a group for AD administrators (see “Creating groups” on page 174)
- Create AD users (see “Creating user accounts manually” on page 206)
- Assign a token or password (see “Authenticators tab” on page 207)
- Assign System or Local admin privileges (see “Privileges tab” on page 209)

Table 5 gives a mapping of Local Admin settings in the Create User window (SAM Express Management Console) to ADUC setting equivalents.
Table 5: Create User window, privilege settings to ADUC equivalents

<table>
<thead>
<tr>
<th>Create User, Privilege Tab</th>
<th>Local Admin settings</th>
<th>ADUC equivalent</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Record: Read-Only</td>
<td>SAM Express</td>
<td>Read-Only</td>
</tr>
<tr>
<td></td>
<td>User Tab: Read-Only</td>
<td>Read-Only</td>
</tr>
<tr>
<td>User Record: Read-Write</td>
<td>SAM Express</td>
<td>Read-Write</td>
</tr>
<tr>
<td></td>
<td>User Tab: Read-Write</td>
<td>Read-Write</td>
</tr>
<tr>
<td>Authenticator Mgt:</td>
<td>Token Management:</td>
<td></td>
</tr>
<tr>
<td>unchecked</td>
<td>Read-Only</td>
<td></td>
</tr>
<tr>
<td>Authenticator Mgt:</td>
<td>Token Management:</td>
<td></td>
</tr>
<tr>
<td>checked</td>
<td>Read-Write</td>
<td></td>
</tr>
<tr>
<td>Other settings</td>
<td>No effect</td>
<td></td>
</tr>
</tbody>
</table>

After the users have been created, they can log into ADUC with only those administrative privileges that were assigned by you.

**Important:** Helpdesk users created in the SAM Express Management Console are not supported for delegated administrative privileges in ADUC.

**Note:** Login to ADUC will fail if the newly created user record is still open in the SAM Express Management Console.

Checking the **Remember my password** box will store login credentials on a per-user basis (that is, each user on the same machine can have different login credentials stored on the machine for automatic logins to ADUC).

Additionally, the current administrative user can be changed mid-session by using the **Connect as different user** menu option (available when right-clicking the **SAM Express** node in ADUC).

The following functions are not supported in ADUC delegated administration:

- Challenge response tokens
- Emergency fixed password profiles set in the SAM Express Management Console
- User must change password with first login feature set in SAM Express Management Console
- Multiple authenticators.
CHAPTER 4

Basic Administration Tasks

In this chapter...

Using the Auto Updater .............................................................................................................82
Managing and viewing logs .........................................................................................................83
Database-related tasks ..................................................................................................................85
Reinstalling a server or ADUC ......................................................................................................87
Configuring alternative group policies .........................................................................................88
Using the Auto Updater

The Auto Updater allows you to view and/or automatically update your SAM Express software with new features and patches as they become available. By default, SAM Express installs with the Auto Updater set to run each time ADUC is accessed if updates are available.

Disabling the Auto Updater

You may disable or re-enable the Auto Updater at any time by doing the following:

1. In the left pane of ADUC, right-click the **SAM Express** node and select **Configure**.
   
   At the bottom of the window is the check box called **Check for SAM Express updates automatically**.

2. To disable the Auto Updater, clear the check box. To re-enable it, select the check box.

Manually downloading and installing updates

On other SAM Express components, the Auto Updater can be launched manually. You can download and install any or all updates at anytime.

To manually run the Auto Updater or view the available updates, do the following:

1. Select **Start > Programs > SafeNet > SAM Express > Update SafeNet Products**.

   **Note:** If a new version of the Auto Updater is available, you will be prompted to *download the newer version*.

2. Click **Yes** to see the features that are available.

3. Review the list of new features, and then click **Install**. The updates are downloaded to your computer, and a Download Complete window appears when finished.

   **Note:** Selecting **Get Updates** will download all available updates for existing components. The Auto Updater does not allow you to choose which updates to download. New features will not automatically be updated unless you select the component. Accept available updates before adding new features using the Auto Updater.

4. To install the updates, click **OK**.

   **Tip:** To find the list of updates that have been installed on your system, click the **History** button.
SAM Express records various events to logs that you can view for troubleshooting or server maintenance.

## Configuring ADUC logging

You may choose to log specific information from one of the SAM Express Agents, the SAM Express server components (the Authentication Engine, and/or the Administration Server), or from ADUC.

To log ADUC connections to the Administration Service:

1. In ADUC’s left pane, right-click the **SAM Express** node, select **Logging Settings**, and check the **Enable Logging** check box.

![Figure 28: Configure Logging window](image)

**Note:** By default, logs are stored in `<Install_dir>\Agentlogs`.

2. Select the types of messages to log from the following options:
   - Errors
   - Errors and information
   - Errors, information, and diagnostics

3. Click **OK**.

## Viewing event logs

You can audit various system authentication and administrative events such as authentication attempts, the starting and ending of administrative sessions, and modifications to entries in the SAM Express database. Viewing these event records is done using the standard Windows Event Viewer.

Open the Event Viewer by selecting **Start > Programs > Administrative Tools > Event Viewer**, then select **SAM Express** in the left pane.
Figure 29: Event Viewer window

SAM Express events are listed in the right pane according to their list criteria (Type, Date, Time, etc.).
When using an AD user database, the SAM Express database serves as a repository for token records. It should be backed up on a regular basis, or anytime a change has been made to token records.

**Backing up the database using ADUC**

To back up your SAM Express database, do the following:

1. In ADUC, expand the **SAM Express** node and select **Import/Backup/Restore**.

   *Tip:* You can also back up your database with the **Backup Database** icon on the toolbar.

2. Under Backup Database, click the **Browse** button to locate the file to which you will write the backup data.

3. When the file name is shown, click the **Backup** button, then click **OK**.
Chapter 4: Basic Administration Tasks

Database-related tasks

Restoring the database using ADUC

When you restore the database, token records are reset back to their state at the time of the last backup and may be out of sync with their associated tokens. Sometimes the Authentication Engine is able to resynchronize the database records to the physical tokens automatically at the next authentication. Other times, the users need to log into the system twice. The first attempt to login will fail, but the second (assuming a correct one-time passcode is given) will succeed and resynchronize the token record. This behavior is by design. If the tokens are too far out of sync, they may need to be manually resynchronized as described in “Resynchronizing Hardware tokens” on page 75.

**Important:** All configuration data is overwritten when you restore your database. If your current license is different from the license in effect at the time of database backup, you must reapply your license and reactivate following restoration of your database.

1. In ADUC, expand the **SAM Express** node and select the Import/Backup/Restore icon, then click the **Browse** button to locate the file from which to restore data.

   **Tip:** You can also restore the database by selecting the **Restore Database** icon on the toolbar.

2. Click **OK**.

3. When the file name appears in the field labeled **Select a database backup file to restore from**, click the **Restore** button.

4. Restart the Authentication Engine and the Administration Server.

5. Close, then re-open ADUC.

**Important:** Failing to close then re-open ADUC after a database restore will result in one or more error messages.
Reinstalling a server or ADUC

ADUC communicates with the SAM Express server (specifically, the Administration Service), and each generates an SSL certificate (stored with the component) to provide connection security and verify component identity. When the server and ADUC are installed on the same machine, these certificates remain synchronized. However, if they are installed on different machines, and either component is reinstalled, the certificates may not remain synchronized, and may need to be regenerated. An error message stating that ADUC could not connect to the server typically indicates that certificates require regeneration. There are two variations of this situation:

Reinstall the console, and keep the existing server installation

Reset the server's record of the old console's certificate:

1. Locate and open (in a text editor) the file called clients.ini in directory \<Install_Dir>\SERVERS\AdminServer\certificates
2. Locate and remove the line that looks like the following:
   
   HOST_OR_IP_ADDRESS\:CN=ScADUser-
   Ext=DB\:A3\:E9\:4D\:7A\:A6\:A2\:8D\:A5\:B8\:3D\:4E\:E0\:CD
   
   where HOST_OR_IP_ADDRESS is the location of ADUC.
3. Save the file.
4. Restart the Administration Server.

Reinstall the server, and keep the existing ADUC installation

Reset the console's record of the old server's certificate:

1. Locate and open (in a text editor) the file called servers.ini in directory \<Install_Dir>\SERVERS\Shared
2. Locate and remove the line that looks like the following:
   
   
   where HOST_OR_IP_ADDRESS is the location of the SAM Express server (for multiple servers, locate the line with the correct server address). If the server was installed on a port other than 5040, then that port will appear in place of 5040.
3. Save the file.
4. Restart ADUC.
Configuring alternative group policies

SAM Express’s default configuration should suit the majority of network topologies and use cases. The SAM Express Agent is responsible for checking group membership and submitting authentication requests to the Authentication Engine (see Figure 31).

Occasionally, the default configuration may not fit a particular network topology or management policies. If computers in a network DMZ do not have anonymous access to Active Directory, the SAM Express Agent is unable to contact Active Directory and read group membership information in order to determine which users require SAM Express authentication. You can configure SAM Express to handle such a scenario (see Figure 32).

In this configuration, group membership checking is done by the SAM Express server (rather than the agent). Since the server will typically be running inside the trusted network, it should have no difficulty obtaining the necessary information from Active Directory.
To configure the alternative network topology, do the following:

1. On the computer in the DMZ running the SAM Express Agent, use the group configuration window (refer to “Configuring the Authentication Policy” on page 264) to force all users to authenticate using SAM Express. This will forward ALL authentication requests to the SAM Express server.

2. On the computer inside the network running the SAM Express server, locate the file `<Install_Dir>\SERVERS\Shared\sccservers.ini`.

3. Locate the line that starts with
   
   `#GroupsAuthenticationRequiredClass=securecomputing.yellows tone...`

4. Modify the line by removing the “#” sign from the beginning of that line.

5. Navigate to `<Install_Dir>\SERVERS\AAAServer\GroupDiscrimination`.

6. Locate and open the HTML file called `ConfigureGroupPolicy.html`.

   **Figure 33: Group Discrimination configuration page**

   This page will launch configuration dialog boxes to specify logging and authentication policy settings. This enables the server, if configured, to decide the authentication policy that determines a user’s need for authentication. To enable this functionality you must edit the `<INSTALLDIR>\SERVERS\Shared\sccservers.ini` file and uncomment the line that specifies the setting for `GroupsAuthenticationRequiredClass`.

   Configuration Settings for:
   
   **Logging:**
   
   Change logging setting including file name, maximum size and types of logged messages.
   
   **Authentication Policy:**
   
   Configure authentication policy by specifying the groups whose users require strong authentication.

7. Change the logging and authentication policies as needed. Refer to “Configuring the Authentication Policy” on page 264 for additional information.

8. Restart the SAM Express Authentication Engine service.

**Note:** Please note that in this topology it is vital that your SAM Express Authentication Engine service is up and running constantly; otherwise, neither the SAM Express nor the non-SAM Express users will be able to log onto your system. The best way to ensure this is to set up your system with multiple SAM Express servers, as described in section “Replication” on page 273.
CHAPTER 5

Using the MobilePASS Feature

In this chapter...

Understanding MobilePASS ...........................................................92
Software token enrollment..............................................................93
Configuring MobilePASS policies ...................................................97
MobilePASS Messaging ..................................................................112
SafeNet MobilePASS is a software version of a hardware token. MobilePASS provides users with two additional authentication options: software tokens and messaging tokens. The software token is an application that generates passcodes on the desktop and on mobile devices. The messaging token delivers passcodes via e-mail (SMTP) or text messages (SMS).

MobilePASS provides you with two ways to generate software tokens. You can use the integrated MobilePASS product, which is included with SAM Express, and/or you can use the stand-alone device-specific MobilePASS Factory application product.

The integrated product supports iPhone/iPod touch/iPad iOS 4.2.0 and higher devices, BlackBerry OS 4.3 and higher devices, J2ME and higher devices (CLDC 1.1/MIDP 2.0 and higher), and Android OS 1.6 and higher devices, as well as Mac OS X 10.6.4 and higher, Windows XP, Windows Vista, Windows 2003, Windows 2008 Desktops, and Windows Phone version 7.0. The stand-alone product provides device-specific applications for use with earlier J2ME-enabled devices, earlier BlackBerry device models, specific smart phones, and older versions of Windows Desktops.

The MobilePASS Portal includes the Enrollment Portal, where users can enroll their software tokens, and can use the Messaging application. The MobilePASS Portal can be installed on the same machine as SAM Express, or it can be installed on another machine in the same network. It is supported on all Windows operating systems that support the core SAM Express servers.

For detailed information about SafeNet MobilePASS, refer to the SafeNet MobilePASS Software Administration Guide, which is available for download from the SAM Express Documentation page. For information about SafeNet hardware tokens, refer to the Authenticators Administration Guide, which is also available on the SAM Express Documentation page.
The MobilePASS Portal component includes an Enrollment Portal, where users can enroll their software tokens without the aid of an administrator. The sections that follow describe how to configure and use MobilePASS Portal and the Enrollment Portal.

Using the MobilePASS Portal

The MobilePASS Portal and its Enrollment Portal provide end users with a convenient interface for enrolling software tokens. For organizations with a large number of users, this self-enrollment feature lightens the administrative effort when assigning tokens to users.

Additionally, BlackBerry MobilePASS users can automatically enroll their MobilePASS tokens over their wireless network directly from their device. For details, refer to “Configuring automatic enrollment for BlackBerry users” on page 108.

Note: To configure automatic enrollment for BlackBerry MobilePASS users, administrators must add the necessary auto enrollment parameters into the .jad file or to their BES policy.

Once software tokens are enrolled, users can request token passcodes from their device, and then use those passcodes to log into resources protected by SAM Express. The MobilePASS Messaging application allows users who are assigned Messaging tokens to request passcodes be sent to them via e-mail or SMS. The passcodes they receive can be used to log into resources protected by SAM Express.

To use the MobilePASS Portal, you must have already set your administrative password. This is the password you should have changed the first time you accessed the ADUC Management Console. If you have not already changed your administrative password, refer to “Changing and updating your admin server credentials” on page 94 before continuing with configuring MobilePASS.
Chapter 5: Using the MobilePASS Feature
Software token enrollment

Changing and updating your admin server credentials

The first time you access the Management Console, you are required to change the default administrative server password. If you have not done so yet, you must before users can access the MobilePASS Portal. To change or update your administrator server credentials:

1. From the Windows Start menu, select Programs > SafeNet > SAM Express > MobilePASS Enrollment.
   - If this is a new SAM Express installation, the Admin Credentials window appears (Figure 34 on page 94) with instructions for changing your administration server credentials. In this case, continue to step 2.
   - If this is an update to an existing installation, and you have changed the administrative password, the Update Admin Server Credentials window appears (Figure 35 on page 95). In this case, skip to step 3.

Figure 34: Change Default Admin Server Credentials window

2. Before continuing, change the password for the administrator account on the administration server by doing the following:
   a. Launch the ADUC Management Console by selecting Start > Programs > SafeNet > SAM Express > Active Directory Users and Computers.
   b. Highlight the SAM Express node and right-click on it.
   c. Select the Change Authenticator Password option.
   d. Change the default administrator password. (For details see “Changing the default administrator password” on page 172.)

Note: You can also change the password for the administrator account by launching the SAM Express Management Console and editing the account profile.
Chapter 5: Using the MobilePASS Feature

Software token enrollment

e Restart the SAM Express Administration Server service. (For details see “Stopping and starting servers” on page 252.)

f Update the webapps/portal/WEB-INF/conf/datastore.txt on this MobilePASS Portal to reflect the updated Admin Server credentials. Enter the password as plain text. It will automatically be encrypted later.

g Restart the SAM Express MobilePASS Portal service.

3 Update the administrative server credentials.

Note: The MobilePASS Portal will only allow access to the administrative password pages from a localhost connection.

4 Enter your Admin Server user ID and your Admin Server password.

5 Click the Update Credentials button. The next SAM Express MobilePASS Portal window appears with a prompt to restart the SAM Express MobilePASS Portal service. Close the Web browser.

6 To restart the MobilePASS Portal service:
   a Open the Windows Services Control Panel.
b. Locate the **SAM Express MobilePASS Portal** service in the list of services.

c. Right-click the status field and select **Restart**.

d. Close the Services Control Panel. The Enrollment Portal and the Messaging application are ready to use.

**Note:** If the administrative password is set incorrectly, the Set Password page will display again after the service has been restarted.
Configuring MobilePASS policies

Before you can assign MobilePASS tokens to users, or allow users to self-enroll with MobilePASS, you must create MobilePASS policies. Policies communicate the specific capabilities of a token device between the MobilePASS clients and the MobilePASS portals and SAM Express servers.

Token capabilities are based on a device token's type, (event synchronous, time synchronous, or challenge response). MobilePASS includes standard and custom policies. Standard policies allow you to set a minimum of policy options, while custom policies present an array of options, including passcode and challenge lengths, time sync intervals (ticks), allow policy downgrade, secure mode, transaction signing mode, SoftPIN, and device PIN options. Table 15 lists policy parameters available with each token type.

**Note:** In SAM Express, **SoftPIN** refers to optional PINs that administrators may choose to require users to append to their passcodes when users authenticate. Additionally, the term **device PIN** is used to refer to the optional PINs that are set on software tokens when MobilePASS is activated. When enabled, device PINs must be entered on the MobilePASS application in order to generate passcodes.

**Table 6:** MobilePASS token types and capabilities

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Parameters</th>
<th>Parameter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard Event Sync</strong></td>
<td>Passcode Length</td>
<td>6 digits (fixed)</td>
</tr>
<tr>
<td></td>
<td>Device PIN Length</td>
<td>4 digits (fixed)</td>
</tr>
<tr>
<td></td>
<td>Use Attack Delay</td>
<td>Disabled (fixed)</td>
</tr>
<tr>
<td></td>
<td>Use Attack Lockout</td>
<td>Enabled 10 (fixed)</td>
</tr>
<tr>
<td></td>
<td>Force Device PIN Change</td>
<td>Disabled (fixed)</td>
</tr>
<tr>
<td></td>
<td>Collect SoftPIN</td>
<td>Select</td>
</tr>
<tr>
<td><strong>Standard Time Sync</strong></td>
<td>Passcode Length</td>
<td>6 digits (fixed)</td>
</tr>
<tr>
<td></td>
<td>Device PIN Length</td>
<td>4 digits (fixed)</td>
</tr>
<tr>
<td></td>
<td>Use Attack Delay</td>
<td>Disabled (fixed)</td>
</tr>
<tr>
<td></td>
<td>Use Attack Lockout</td>
<td>Enabled 10 invalid attempts (fixed)</td>
</tr>
<tr>
<td></td>
<td>Force Device PIN Change</td>
<td>Disabled (fixed)</td>
</tr>
<tr>
<td></td>
<td>Time Sync Interval</td>
<td>30 seconds (fixed)</td>
</tr>
<tr>
<td></td>
<td>Collect SoftPIN</td>
<td>Select</td>
</tr>
</tbody>
</table>
### Configuring MobilePASS Policies

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Parameters</th>
<th>Parameter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Challenge Response</td>
<td>Passcode Length</td>
<td>8 digits (fixed)</td>
</tr>
<tr>
<td></td>
<td>Challenge Length</td>
<td>8 (fixed)</td>
</tr>
<tr>
<td></td>
<td>Device PIN Length</td>
<td>4 (fixed)</td>
</tr>
<tr>
<td></td>
<td>Use Attack Delay</td>
<td>Disabled (fixed)</td>
</tr>
<tr>
<td></td>
<td>Use Attack Lockout</td>
<td>10 (fixed)</td>
</tr>
<tr>
<td></td>
<td>Force Device PIN Change</td>
<td>Disabled (fixed)</td>
</tr>
<tr>
<td></td>
<td>Collect SoftPIN</td>
<td>Select</td>
</tr>
<tr>
<td>Custom Event Sync</td>
<td>Passcode Length</td>
<td>6 or 8</td>
</tr>
<tr>
<td></td>
<td>Use Device PIN</td>
<td>• Enable or Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, PIN length: 4, 6 or 8</td>
</tr>
<tr>
<td></td>
<td>Use Attack Delay</td>
<td>• Enable or Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, attacks before delay begins: 2, 4, or 8 invalid attempts</td>
</tr>
</tbody>
</table>

**Note:** *Initial delay is one minute. Increases by one minute for each failed attempt. Delay reaches a maximum at 20 minutes, and resets only upon successful device PIN entry.*

*More...*
## Configuring MobilePASS policies

### Use Attack Lockout
- **Enable or Disable**
- **When enabled, attacks before lockout:** 3, 6, or 10 invalid attempts for MobilePass client version 8.2 and earlier. For later clients, the available values for attacks before lockout are from 3 to 20.

**Note:** The number of attacks before lockout should always be greater than the number of attacks before an attack delay.

### Force Device PIN Change
- **Enable or Disable**
- **When enabled, successful uses before device PIN change:** 128, 256, or 384

### Collect SoftPIN
- **Select**

### Custom Time Sync
- **Passcode Length**
  - 6 or 8
- **Time Sync Interval**
  - 20, 30, or 60 seconds
- **Use Device PIN**
  - **Enable or Disable**
  - **When enabled, 4, 6 or 8 digits**
- **Use Attack Delay**
  - **Enable or Disable**
  - **When enabled, attacks before delay begins:** 2, 4, or 8 invalid attempts

**Note:** Initial delay is one minute. Increases by one minute for each failed attempt. Delay reaches a maximum at 20 minutes, and resets only upon successful device PIN entry.

More...
## Configuring MobilePASS policies

### Use Attack Lockout
- **Parameters:**
  - Enable or Disable
  - When enabled, attacks before lockout: 3, 6, or 10 invalid attempts for MobilePass client version 8.2 and earlier. For later clients, the available values for attacks before lockout are from 3 to 20.

  **Note:** The number of attacks before lockout should always be greater than the number of attacks before an attack delay.

### Force Device PIN Change
- **Parameters:**
  - Enable or Disable
  - When enabled, successful uses before device PIN change: 128, 256, or 384

### Collect SoftPIN
- **Parameters:**
  - Select

### Custom Challenge Response
- **Parameters:**
  - **Passcode Length:** 6 or 8
  - **Challenge Length:** 6 or 8
  - **Use Device PIN:** Enable or Disable
    - When enabled, PIN length: 4, 6 or 8
  - **Use Attack Delay:** If attack delay is enabled:
    - Attacks before delay begins: 2, 4, or 8

  **Initial delay is one (1) minute, and increases by one minute for each failed attempt. Delay reaches a maximum at 20 minutes, and resets only upon successful device PIN entry.**
Defining policies

To define policies, do the following:

1. Launch the SAM Express Management Console.
2. Select **Configuration > MobilePASS Policy**. The MobilePASS Policy Configuration window appears. There are no existing policies at this time.

### Configuring MobilePASS policies

To define policies, do the following:

1. Launch the SAM Express Management Console.
2. Select **Configuration > MobilePASS Policy**. The MobilePASS Policy Configuration window appears. There are no existing policies at this time.

<table>
<thead>
<tr>
<th>Token Type</th>
<th>Parameters</th>
<th>Parameter Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Attack Lockout</td>
<td></td>
<td>• Enable or Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, attacks before lockout: 3, 6, or 10 invalid attempts for MobilePass client version 8.2 and earlier. For later clients, the available values for attacks before lockout are from 3 to 20. <strong>Note:</strong> The number of attacks before lockout should always be greater than the number of attacks before an attack delay.</td>
</tr>
<tr>
<td>Force Device PIN Change</td>
<td></td>
<td>• Enable or Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When enabled, successful uses before device PIN change: 128, 256, or 384</td>
</tr>
<tr>
<td>Collect SoftPIN</td>
<td></td>
<td>Select</td>
</tr>
</tbody>
</table>
Chapter 5: Using the MobilePASS Feature

Configuring MobilePASS policies

Figure 37: MobilePASS Policy Configuration window

3 Specify a name for the MobilePASS Policy. You may use Default or specify a name of your choosing.

4 In MobilePASS, **Standard** policies are fixed and cannot be customized. **Custom** policies allow you to create device tokens that meet individual organizational needs. Table 6 on page 97 provides the policy parameters available with each token type. Using this information, select the type of token to which you will be applying this policy. You may choose one of the following:
   - Standard Event Sync
   - Standard Time Sync
   - Standard Challenge Response
   - Custom Event Sync
   - Custom Time Sync
   - Custom Challenge Response

5 Select a desired passcode length from the **Passcode Length** list. You may choose a 6-digit or an 8-digit passcode. If you choose a standard policy, the length of passcode option is disabled, and the default setting displays.

6 (For custom challenge-response tokens only) Select a challenge length from the list. You may choose a 6-digit or an 8-digit challenge length.

7 (For custom time-synchronous policy tokens only) Select the interval (in seconds) before a new passcode is available from the **Time Sync Interval** list. You may choose 20 seconds, 30 seconds, or 60 seconds.

8 Under **PIN Options**, select **Collect SoftPIN (appended to MobilePASS passcode) during self-enrollment** to require users associate a SoftPIN with this token. If you will not require a SoftPIN, leave this check box cleared.
Chapter 5: Using the MobilePASS Feature

Configuring MobilePASS policies

Note: When you choose to collect SoftPINs, users will be required to set up a SoftPIN when they enroll their token. They will be required to append or prepend this SoftPIN to their token-generated passcode each time they authenticate using MobilePASS. This is not the user’s device PIN.

9 (Custom Policies Only) Secure mode allows SafeNet to react to security vulnerabilities of client devices on a case by case basis. Select the Secure Mode check box to allow SafeNet to possibly modify MobilePASS client behavior when security vulnerabilities become known.

Note: When secure mode is enabled, application updates may result in MobilePASS disabling clients that do not meet their defined security mode.

10 Transaction Signing provides the ability to encrypt and verify the integrity of online transactions for supported MobilePASS clients. Select the Enable Transaction Signing Mode check box to enable this feature.

11 Under PIN Options, do the following:

a SoftPINs refer to optional PINs that administrators may require users set up when they enroll their token, and then append to their passcodes when they authenticate with their tokens. Please leave the Collect SoftPIN check box cleared.

Tip: Using SoftPINs and transaction signing together is not recommended.

b Device PINs refer to the optional PINs that are set on software tokens when MobilePASS is activated. When enabled, device PINs must be entered on the MobilePASS application or device in order to generate passcodes. Select the Use Device PIN check box, and then select a PIN length from the PIN Length list (4, 6, or 8 digits).

c The attack delay feature allows you to set the number of invalid attempts that can be made before attack delay begins. Select the Use Attack Delay check box, and then select the number of attacks to allow before delay begins (2, 4, or 8 attacks).

Note: The initial delay is one minute. The delay increases by one minute for each failed attempt. Delay reaches a maximum at 20 minutes, and resets only upon successful device PIN entry.
d The attack lockout feature allows you to set the number of attacks before lockout. The number of attacks before lockout should always be greater than the number of attacks before an attack delay. Select the **Use Attack Lockout** check box to enable this feature, and then select the number of attacks before lockout occurs (a value between 3 and 20).

**Note:** The attack lockout feature works on devices in disconnected mode (no transaction signing and basic challenge response) as well as on those in connected mode.

e The Force Device PIN Change feature allows you to set the number of successful PIN uses before the device PIN must be changed. Select the **Force Device PIN Change** check box, and then select the number of successful uses before a change is required (128, 256, or 384).

12 Select the **Legacy Clients** tab.

13 If you are using client devices that do not support policies (MobilePASS version 8.0), and you wish to allow these devices to enroll and ignore the specified policy options, select the **Allow enrollment to non policy-based clients** check box.

14 If client devices accept policies (MobilePASS versions 8.1 and 8.2), but do not accept the attack lock values as specified for your policy (values other than 3, 6, or 10), to allow enrollment, select the **Allow enrollment** check box, and then select a value (3, 6 or 10) from the 8.1/8.2 Attacks before lockout list.
15 Click the **Save** button. You have finished creating policies for this token type. You may configure another token policy, or you may close the window.

**Note:** Standard policies include the most commonly used features and are easy to implement. Customized policies will lengthen the policy strings. Shorter policy strings are easier for users to enter, and may result in less user entry errors.

---

**Duplicating policies**

To duplicate an existing policy, do the following:

1. Launch the SAM Express Management Console.
2. Select **Configuration > MobilePASS Policy**. The MobilePASS Policy Configuration window appears.
3. Select the policy to duplicate from the list of existing policies.
4. Click the **Duplicate** button.
5. Rename the copy with an appropriate name.
6. Click the **Save** button.

---

**Searching existing policies**

To search for an existing policy, do the following:

1. Launch the SAM Express Management Console.
2. Select **Configuration > MobilePASS Policy**. The MobilePASS Policy Configuration window appears.
3. Enter the desired policy number into the Policy field. Policy numbers can be found on the token device’s About window.
4. Click the **Search** button. The list of desired policies appears.

---

**Editing existing policies**

To edit an existing policy, do the following:

1. Launch the SAM Express Management Console.
2. Select **Configuration > MobilePASS Policy**. The MobilePASS Policy Configuration window appears.
3 Select the desired policy name to edit from the list of existing policies, click the **Edit** button, make the desired changes, and then click the **Save** button.

---

**Deleting policies**

To delete a policy, do the following:

1 Launch the SAM Express Management Console.

2 Select **Configuration > MobilePASS Policy**. The MobilePASS Policy Configuration window appears.

3 Select the policy to delete from the list of existing policies.

*Tip:* You will not be able to delete a policy if there are any users assigned it for self-enrollment.

4 Click the **Delete** button.

5 Click the **Yes** button to confirm the deletion.

Click **OK**. The policy is successfully deleted.
Allowing users to manually self-enroll their tokens

All users can manually self-enroll and test their software tokens via their client device or via a web browser and the Enrollment Portal. When users manually self-enroll, they must first authenticate on the Portal using their Windows credentials or their SAM Express user ID and passphrase provided by their administrator. They must also provide the Activation Code generated by the MobilePASS application on their device. To allow users to manually self-enroll their software tokens, do the following:

1. Confirm the users are stored in the Active Directory database or the internal SAM Express database.

   **Note:** If a user is stored in both the Active Directory and the SAM Express database, the Portal can only be used for one database or the other. You cannot use the Portal to enroll a user from both databases.

2. Ensure that there are sufficient software token records available for each user who will be self-enrolling. (see “Generating MobilePASS records in ADUC” on page 55.)

3. Provide software token users with the following:
   - The URL for the MobilePASS application download site, and instructions for installing MobilePASS on their device.


   - The URL for the Enrollment Portal: [https://<servername:port>/portal/enroll](https://<servername:port>/portal/enroll). By default, port 5444 is used.
   - Instructions for using the Enrollment Portal. See “Using the Enrollment Portal” on page 108. (This feature is optional, and applies to manual activations only.)
Configuring automatic enrollment for BlackBerry users

SafeWord 2008 version 2.1.0.04 includes features that allow BlackBerry users to automatically enroll their software tokens directly from their device via the wireless network. Additionally, if configured, your BES can allow Active Directory users to automatically authenticate. To allow AD users to auto-enroll their tokens, the automatic enrollment parameters in the .jad file or in a BES policy must be configured. For specific configuration information, refer to the SafeNet MobilePASS Software Administration Guide, a PDF available at www.safenet-inc.com/safeword/docs/2008.

Note: Auto-activation is available only with BES, and only supports Active Directory users. It must be configured in the BES. For details, refer to the SafeNet MobilePASS Software Administration Guide.

Using the Enrollment Portal

Software token users can manually activate, enroll, and test their tokens using the MobilePASS Enrollment Portal.

To open the portal, manually activate, and then enroll and test their tokens, inform users to do the following:

1. Enter your Windows credentials or your SAM Express user ID and passphrase provided by your administrator, and then click **Authenticate**. The Activation Code window appears.

   **Note:** You will use your Windows credentials or your SAM Express user ID and passphrase depending upon how SAM Express is set up.

   ![Activation Code window](image)

2. (Conditional) If your token supports policy string entry, enter the policy number that is provided into the Policy field on the token. If the token does not support policies, continue to the next step.

3. Enter the 20-character activation code that displayed on your device when you ran the MobilePASS software in the Enter your activation code field on the Portal.

4. Click **Enroll Software Token**. The Test Software Token window appears.

   ![Test Software Token window](image)

5. Confirm the activation on your device. After confirming the activation, MobilePASS will generate a passcode. Enter this passcode in the browser’s Software Token Passcode field, and then click the **Test Token Software** button.
Configuring MobilePASS policies

Chapter 5: Using the MobilePASS Feature

Figure 42: Token Test Results windows

Either a successful window or a failed window appears.

- If your test is successful, you may close the browser.
- If your token test fails, the Failed Results window appears. In this case, enter a new passcode in the Enter software token passcode field, and then click the Test Software Token button again. If the passcode again fails the token test, contact your administrator and request that the token be removed from your user record. Removing the token from the user record allows the user to re-enroll the token.

Note: If the Enrollment Portal has been configured to allow MobilePASS users who are stored in Active Directory to re-enroll currently enrolled tokens, the administrator does not need to remove the token from the user’s record. The user can simply re-enroll the token again. To configure the Enrollment Portal to allow users to re-enroll their own tokens, see “Configuring re-enrollment for existing MobilePASS tokens” on page 111.
Configuring re-enrollment for existing MobilePASS tokens

To allow Active Directory MobilePASS users to re-enroll their software tokens without administrative assistance, a new parameter must be added to the \textit{sccservers.ini} file, and the parameter must be set to true. To add the parameter, do the following:

1. Locate the \textit{sccservers.ini} file. It can be found at $\texttt{<Install\_Dir>\SERVERS\Shared}$.
2. Open the \textit{sccservers.ini} file using a text editor.
3. Add the following parameter to the bottom of the file:
   \texttt{AllowMobilePassReEnroll=true}
4. Ensure that the parameter is set to \texttt{true}.
5. Restart the SAM Express Administration Server in Microsoft Services.

Allowing users to self-enroll

To allow users to self-enroll their Software tokens, do the following:

1. Confirm the users are stored in the Active Directory database or the internal SAM Express database.

   \textbf{Note: If a user is stored in both the Active Directory and the SAM Express database, the Portal can only be used for one database or the other. You cannot use the Portal to enroll a user from both databases.}

2. Ensure that there are sufficient Software token records available for each user who will be self-enrolling. (See “Generating MobilePASS records in ADUC” on page 55.)

3. Provide software token users with the following:
   - The URL for the MobilePASS application download site, and instructions for installing MobilePASS on their device.
   - The URL for the Enrollment Portal: \texttt{https://<servername:port>/portal/enroll}. By default, port 5444 is used.
   - Instructions for using the Enrollment Portal. See “Using the Enrollment Portal” on page 108. (Optional, applies to manual activation only.)

The MobilePASS Messaging application is the component of MobilePASS that allows users to request and receive authentication passcodes via e-mail (SMTP) and text messages (SMS). Before Active Directory users can request passcodes, administrators must configure the Messaging providers who will deliver these passcodes.

Configuring Messaging providers

MobilePASS Messaging defines and supports two delivery methods, e-mail (SMTP) and SMS (Short Message Service). Before using MobilePASS, you must configure the Messaging providers who will deliver the SAM Express passcodes. One provider must be chosen as the default. This will be the provider that you want messages to be sent to first when a user requests a passcode. The alternate provider can either be disabled, or enabled. When the alternate provider is enabled, if the initial passcode message is not received, the user will be able to request another message be sent to them via the alternate provider. The provider settings that are chosen, will apply to all the Active Directory users who receive passcodes via Messaging.

By default, MobilePASS Messaging ships with all providers disabled. You may choose from the following options:

- “E-mail delivery with SMS as the alternate” on page 114.
- “SMS delivery with e-mail as the alternate” on page 115.
- “Delivery via e-mail only” on page 116.
- “Delivery via SMS only” on page 117.
- To disable passcode delivery, clear the check boxes for all providers on the Configure Providers dialog box.

Whichever scenario you choose, you will also need to edit provider information on the Edit Provider window (see “Editing provider information” on page 118).
Setting passcode timeouts

Administrators may choose to set timeouts for passcodes, or to allow that passcodes never time out. If a timeout is set, passcodes will timeout or expire when the set time period (between 1 and 15 minutes) has passed. The timeout option is available on the Providers configuration window. To set up timeout options, do the following:

1. Launch ADUC by selecting Start > Programs > SafeNet > SAM Express > Active Directory Users and Computers.
2. Click on the SAM Express node to expand the node.
3. Click on the MobilePASS folder.
4. Click the Configure Providers button.
5. If you wish to set a timeout for passcodes confirm that the Use passcode timeout check box is selected. To disable timeouts, clear the check box.

Security Alert: Please be aware that there are security implications if you do not use the passcode timeout option.

6. In the Timeout (mins) box, select the duration (in minutes) before passcodes will expire.
7. Click OK.
8. Continue to one of the following sections to set up Provider information:
   – E-mail delivery with SMS as the alternate
   – SMS delivery with e-mail as the alternate
   – Delivery via e-mail only
   – Delivery via SMS only
E-mail delivery with SMS as the alternate

To configure e-mail as the default delivery method and SMS as the alternate, do the following:

1. From the MobilePASS configuration window in ADUC, click the **Configure Providers** button.
2. Highlight the **E-mail** option.
3. Select the **E-mail** check box.
4. Click the **Set default** button.
5. Select the **SMS** check box.

![Figure 43: Providers window, E-mail and SMS delivery](image)

6. Click the **Edit** button and continue to “Editing provider information” on page 118 to specify provider information.
7. To configure passcode timeout expiration settings, refer to “Setting passcode timeouts” on page 113.
8. Click **OK** to save the changes.

*Important: You must restart the AAA server in Services to enable these changes.*
SMS delivery with e-mail as the alternate

To set SMS as the default delivery method and e-mail as the alternate:

1. From the MobilePASS configuration window in ADUC, click the Configure Providers button. The Providers window appears.
2. Highlight the SMS option.
3. Select the SMS check box.
4. Click the Set default button.
5. Highlight the E-mail option.
6. Select the E-mail check box.
7. Click the Edit button and continue to “Editing provider information” on page 118 to specify provider information.
8. To configure passcode timeout expiration settings, refer to “Setting passcode timeouts” on page 113.
9. Click OK to save the changes.

Important: You must restart the AAA server in Services to enable these changes.
Delivery via e-mail only

To set e-mail as the default delivery method without an alternate:

1. From the MobilePASS configuration window in ADUC, click the **Configure Providers** button. The Providers window appears.

   ![Figure 45: Providers window, e-mail delivery only](image)

   - Available providers:
     - **Email (Default)**
     - **SMS**
   - Use passcode timeout:
     - Timeout (mins): 5

2. Highlight the **E-mail** option.
3. Select the **E-mail** check box.
4. Click the **Set default** button.
5. Ensure that the **SMS** check box is cleared.
6. Click the **Edit** button and continue to “Editing provider information” on page 118 to specify provider information.
7. To configure passcode timeout expiration settings, refer to “Setting passcode timeouts” on page 113.
8. Click **OK** to save the changes.

**Important:** You must restart the AAA server in Services to enable these changes.
Delivery via SMS only

To set SMS as the default delivery method without an alternate:

1. From the MobilePASS configuration window in ADUC, click the Configure Providers button. The Providers window appears.

![Figure 46: Providers window, SMS delivery only](image)

2. Highlight the SMS option.

3. Select the SMS check box.

4. Click the Set default button.

5. Ensure that the E-mail check box is cleared.

6. Continue to “Editing provider information” on page 118 to specify provider information.

7. To configure passcode timeout expiration settings, refer to “Setting passcode timeouts” on page 113.

8. Click OK to save the changes.

**Important:** You must restart the AAA server in Services to enable these changes.
Chapter 5: Using the MobilePASS Feature

MobilePASS Messaging

Editing provider information

To edit the provider information:

1. Launch ADUC by selecting Start > Programs > SafeNet > SAM Express > Active Directory Users and Computers.
2. Click on the SAM Express node to expand it.
3. Click on the MobilePASS folder.
4. Click the Configure Providers button.
5. Click the Edit button.
   a. To configure the e-mail provider, continue to “Editing e-mail provider information” on page 118.
   b. To configure the SMS provider, continue to “Editing SMS provider information” on page 119.

Editing e-mail provider information

To edit e-mail provider information, highlight the E-mail provider and click the Edit button. The Edit Provider windows appears.

![Edit Provider window](image)

**Figure 47:** Edit Provider window

*Note:* The semicolon character (“;”) is not an accepted character in the Edit Provider text fields.
1. (Optional) On the Edit Provider window, enter a description of the e-mail provider in the Description field.

2. To specify the AD user attribute to use to determine the delivery route, select an option from the drop-down list under Look up route in the following Active Directory user attribute. The specified AD attribute must be populated with relevant information (i.e., e-mail address or mobile phone number) in the AD user accounts for each Messaging token user.

3. Highlight the Value field next to E-mail Server (IP Address or Host Name), and then enter the IP address or the host name of the e-mail server.

4. Highlight the Value field next to E-mail Subject, and then enter the text you wish to display in the subject line of the message that will be sent.

5. Highlight the Value field next to E-mail from Address, and then enter the address from which passcodes will be sent.

6. Highlight the Value field next to Message Prefix, and then enter the first part of the message that will be sent to the user when they receive their passcode.

7. When your settings are complete, click OK.

**Editing SMS provider information**

To edit SMS provider information, on the Configure Providers window, highlight the SMS provider, and click the Edit button. The Edit Provider window appears.

![Figure 48: Edit Provider, Clickatell example](image)

**Note:** The semicolon character (";") is not an accepted character in the Edit Provider text fields.
Chapter 5: Using the MobilePASS Feature

MobilePASS Messaging

1. (Optional) On the Edit Provider window, enter a description of the e-mail provider in the **Description** field.

2. To specify the AD user attribute to use to determine the delivery route, select an option from the drop-down list under **Look up route in the following Active Directory user attribute**. The specified AD attribute must be populated with relevant information (i.e., e-mail address or mobile phone number) in the AD user accounts for each Messaging token user.

3. Select the Value field next to **SMS Account username**, and then enter the **account username** that the provider set for you.

4. Select the Value field next to **SMS Account password**, and then enter the **account password**.

5. Select the Value field next to **API ID**, and then enter the provider’s **API ID**. This field may be left blank.

6. Select the Value field next to **API URL** to change the provider’s URL. The URL format should be entered based on your SMS providers requirements. Below is the default URL, based on the ClickaTell SMS provider. Note that SAM Express will replace all placeholders surrounded by $ symbol when sending the SMS message with the correct values.

   ```
   https://api.clickatell.com/http/sendmsg?user=$USER$&password=$PASSWORD$&api_id=$API_ID$&to=$TO$&from=$FROM$&text=$MESSAGE$
   ```

   - $USER$ - will be replaced with the “SMS Account username” field value
   - $PASSWORD$ - will be replaced with the “SMS Account password” field value
   - $API_ID$ - will be replace with the “API ID” field value
   - $FROM$ - will be replaced with the “SMS Originator” field value
   - $MESSAGE$ - will be replaced with the “Message Prefix” field value, plus the SAM Express passcode.
   - $TO$ - will be replaced with the route information looked up for the passcode recipient from Active Directory

   Please format the above placeholders into the URL format from your SMS provider in order for these values to be correctly posted. You may test that the formatting is correct and/or that the credentials are correct by editing

   ```
   https://api.clickatell.com/http/sendmsg?user=$USER$&password=$PASSWORD$&api_id=$API_ID$&to=$TO$&from=$FROM$&text=$MESSAGE$
   ```

   with the values from a messaging provider account.
7 Select the Value field next to **SMS Originator**, and then enter the name you wish to display as the originator.

8 Select the Value field next to **Message Prefix**, and then enter the text you wish to display to users when they receive passcodes.

9 Select the Value field next to **SMS return result**, and then enter the value you received from your provider in the ID field. This value indicates successful delivery. This field is dependent on your provider. Refer to your provider’s information for specific details.

---

**Requesting Messaging passcodes via the MobilePASS Portal**

The Messaging application is supported on Windows Server 2003 and Windows Server 2008 operating systems.

*Security Alert:* SAM Express recommends using an SSL certificate for public-facing MobilePASS Portals.

To request a passcode using the MobilePASS Messaging application:

1 Open the passcode request window by doing one of the following:
   - Launch a Web browser and navigate to `https://<machinename:port>/portal/sms`. By default, port 5444 is used.
   - From the machine where Messaging is installed, select **Start > Programs > SafeNet > SAM Express > MobilePASS Messaging**.

The MobilePASS Messaging Webpage window displays.

*Note:* If you wish that users pre-authenticate with their Messaging token PIN, you may set up pre-authentication in the Messaging Application configuration file. See details in “Using PIN pre-authentication” on page 124.

---

**Figure 49: MobilePASS Messaging window**

2 Enter your SAM Express user ID in the **User ID** field.
Note: The SAM Express user ID can be entered in the following formats: username@DOMAIN.xxx, or DOMAIN\username. This only applies when the user is not part of the domain where the AAA server is installed.

3 Click the Send Passcode button. Your passcode will be sent to you via the default provider.
Customizing the Messaging application

You may choose to customize the Messaging application to meet your organization’s specific needs. Customization occurs in the configuration files that are included with the MobilePASS Messaging application. To access the files browse to: `<install_dir>\WEB\messaging\webapps\portal\WEB-INF\conf`.

The following files are available for customizing the Messaging application:

- **smswebapp.ini** - main configuration file for MobilePASS Messaging
- **webconfig.ini** - file used to customize the “look and feel” of the web pages
- **swec.conf** - swec configuration file (contains the AAA address and port if you need to change them)
- **datastore.txt** - file used to specify the admin server user name and the admin server password to connect the MobilePASS Portal with the Administration Server.

Each file contains explanatory text. You may open the files using Microsoft Notepad or Wordpad.

**Important:** You must restart the MobilePASS Portal service after making any changes to the configuration files.

The **smswebapp.ini** file is the main configuration file for the Messaging application. The following options can be customized in the file:

- PIN pre-authentication
- URL redirect

The sections that follow provide configuration details.
Using PIN pre-authentication

The MobilePASS Messaging application is configured with the pre-authentication mode disabled. This means that users will not need to enter a token PIN with their user ID when requesting passcodes via the Messaging application. Pre-authentication must be enabled in the `smswebapp.ini` file.

By default, Messaging tokens do not have PINs assigned. Administrators must assign a PIN for each Messaging token user on the ADUC User dialog page (SAM Express tab) before enabling PIN authentication.

Using the URL redirect option

Administrators may choose to redirect users to a Web login page after the user has requested a passcode. This option is configured in the `smswebapp.ini` file. The file contains explanatory text for configuration.

Requesting Messaging passcodes via OWA

To request a Messaging passcode using the Outlook Web Access Agent:

1. Browse to the OWA Agent login page. The initial SAM Express Login window appears.

   If your users will primarily be using Messaging, you may choose to hide the SAM Express Passcode field. See “Changing OWA timeouts” on page 267 for details about hiding the passcode field.

   If the OWA Agent is configured to hide the initial SAM Express passcode, the SAM Express login window appears without a SAM Express passcode field (as shown in the upper image. Otherwise, the lower image displays with a SAM Express passcode field.
2 Enter your username in the **Username** field.

3 Enter the name of the domain in the **Domain** field.

4 Enter your Windows password in the **Password** field.

5 If the SafeNet Passcode field displays, enter a passcode here to authenticate, or click the Login button and continue to the next step.
Chapter 5: Using the MobilePASS Feature

MobilePASS Messaging

6 If Messaging was set up with passcode expirations, your SAM Express login window displays with the time remaining before the passcode expires. Close the Message window in this case.

7 Enter the SAM Express passcode that you received via e-mail into the SAM Express Passcode field.

8 To change to the alternate provider, click the drop-down button under Alternate delivery methods, and select the alternate delivery method.

9 Click the Resend button. This button can be used when your passcode has expired, and when you are changing to the alternate delivery method and need the passcode to be resent.
CHAPTER 6

Using the Cloud Authentication Portal

In this chapter...

Overview ...................................................................................... 128
Configuring cloud portals.............................................................. 128
Logging onto the portal................................................................. 143
Overview

The following provides instructions for using the Cloud Authentication Portal for logging onto service providers such as Google Apps and Salesforce.com. When either of these applications has been configured to require SAM Express credentials, the user must authenticate using the SAM Express Cloud Portal before they are logged onto the application.

Note: The Cloud Server and the Cloud Portal require a valid ESP license. Contact your SAM Express reseller or browse to the SafeNet corporate site at http://safenet-inc.com to purchase a valid license.

Configuring cloud portals

SAM Express provides a seamless strong authentication experience for enterprise users remotely accessing the SaaS (Software as a Service) applications Google Apps and Salesforce.com (SFDC). When a user browses to the portal or either cloud application, they are automatically redirected to the SAM Express Server for authentication via the Cloud Portal. The user must provide a username and either their SAM Express credentials or their Active Directory password at the Cloud Portal before gaining access to the specific application.

Adding a portal connection

A connection to the Cloud Server must be added for the Cloud Portal. This connection is configured using the Portals Configuration tool on the machine where the Cloud Portal is installed.

The following prerequisites must be present for the Cloud Authentication feature:

- .NET Framework 2.0
- IIS with ASP.NET 2.0 enabled

Note: During installation, SAM Express automatically installs these prerequisites if they are not present during installation. The prerequisites must be installed manually if the installation server cannot access the update.safenet.com site.

To open the Portals Configuration tool, do the following:

1. On the machine where the portal is installed, from the Windows Start menu, select All Programs > SafeNet > SAM Express > Portals Configuration. The SafeNet Authentication Manager Portals Configuration window appears.
2 Select the **Connections** tab, and then click the **Add** button. The Connection Details window appears.

**Tip:** Ensure that Ports 5030 and/or 5031 are open for successful authentications.

This is the connection to the Cloud Server where strong authentication occurs via the Cloud Portal. You configure the Cloud Portal to communicate with the Cloud Server here.

**Note:** The Cloud Server does not have to reside on the same machine as the machine where SAM Express is installed. The Cloud Server must be installed on a machine somewhere in your network.

3 Complete the following fields:

- Enter a logical name for this connection in the Connection Name field.
- Enter the **Cloud Server URL** in the Backend Server URL field. This is the host name of the Cloud Server in URL format.
c Enter the **Username** in the Username field. These are the credentials for connecting to the Cloud Server. These credentials were specified during the installation process.

d Enter the **Password** in the Password field. This is the password that is used for logging on to the Cloud Server. This password was set during installation.

e Click the **Select** button. The Select SAM Instance window appears.

---

**Figure 53:** Select SAM Instance window

4 Select the **SAM Express** Instance Name from the SAM Instance Name menu.

5 Click **OK**.
A message window may appear informing you to restart the SAMPortalsAppPool IIS Application Pool for the configuration changes to take effect. Click **Yes** on the Configuration Changed message window.

![Configuration Changed window](image)

**Important:** When the configuration is changed, the SAMPortalsAppPool IIS Application Pool will automatically restart upon closing the Portals Configuration window.

The new connection is added to the list of connections in the Portals Configuration window.

![New connection window](image)

Continue to the next section “Configuring portal connections” on page 132 to configure portal connections to the desired cloud applications.
Configuring portal connections

To configure a portal connection to the desired cloud application, open the Portals Configuration tool by selecting **Start > Programs > SafeNet > SAM Express > Portals Configuration**, and then do the following:

1. On the Portals Configuration tool, click the **Cloud Configuration** tab.

   ![Cloud Configuration tab - Portals Configuration window](image)

2. Click the **Add** button. The Add Configuration window appears.

   ![Add Configuration window](image)

3. On the Add Configuration window, enter a name for this configuration in the **Configuration Name** field.

4. Select one of the following service providers:
   - **Google Apps**
   - **Force.com**

   **Note:** The user must have an account at the service provider.
When users log onto the Cloud Portal, they enter their usual SAM Express username. The username that is passed to the Cloud application can be configured to be the same name as the SAM Express username, a personalization data attribute for users stored in the SAM Express database, or an attribute stored in Active Directory.

5 Select how the username will be passed to the service provider:

- If the **Username entered in the cloud portal** option is selected, ensure that the SAM Express username is exactly the same as the name used in Google Apps or Salesforce.com, and then continue to step 6.

- If the **User attribute in the user store** option is selected:
  - For users stored in the SAM Express database, select an attribute from the fixed set of attribute values (**CloudName1** through **CloudName5**). Also, ensure that the personalization data attribute name matches the name used in the SAM Express database. For more information about associating user attributes using the Administration Console, see “Associating user attributes with the Administration Console” on page 138.
  - For users stored in Active Directory, select the attribute name (**mail** for example) from the list. Also, ensure that the user attribute value (**mail**) matches the users’ cloud ID.

![Figure 58: Attribute Name list in Edit Configuration window](image-url)
Chapter 6: Using the Cloud Authentication Portal

Configuring cloud portals

6 Select who will initiate authentication by selecting one of the following:
   • **Authentication requests must be initiated by the Service Provider only** - Select this option when the user will log in using the Service Provider URL.
   • **Authentication requests can be initiated by either the Service Provider or the SafeNet Identity Provider** - Select this option when the user will log in using the SafeNet Cloud Portal URL or the Service Provider URL. (Supported in the Salesforce.com environment only.)

7 Click **OK**. You are returned to the Cloud Configuration tab. The new configuration(s) appear under the Name column.

8 Restart the **SAMPortalsAppPool** for the changes to take effect.
Setting Cloud Portal options

The Portal Settings feature allows you to customize your Cloud Portal.

Configuring displayed links

To customize the Portal to send the OTP in a message, do the following:

1. From the Cloud Configuration tab, select one of the provider names to highlight it, and then click the Portal Options button. The Portal Settings window appears.

![Portal Settings window](image)

**Figure 61:** Portal Settings window

*Note:* The settings in this window are optional. They apply to Google Apps and Salesforce.com. The option to send the OTP in a message is only available when using a Messaging token. The Challenge Code option is not available with SAM Express at this time.

2. In the Displayed Links pane, select **Send me the OTP in a message**.
Configuring SSO

On the Portal Settings window, the lower pane contains the SSO (Single Sign-on) option. By default the single sign-on feature is OFF. To configure SSO and use the signout feature, do the following:

1. Browse to the `sccservers` file at: `<install_dir>\SERVERS\Shared\sccservers.ini`.
2. Set the SSO feature to ON by adding the lines below to the `sccservers` file:
   
   ```
   Cloud_Enable_SSO=on
   Cloud_SSO_Timeout=30
   ```

   **Note:** The SSO timeout unit is minutes.

3. Save and close the `sccservers` file.
4. Open the Portal Settings window by selecting a provider name on the Cloud Configuration tab.

   **Figure 62:** SSO pane

   ![SSO pane](image)

5. Select the End SSO session upon sign-out check box. The users’ browser will now delete the cookie when the user logs out of their cloud application session, and the user will be forced to re-authenticate when accessing multiple cloud providers. If this check box is left clear, users authenticate once and are able to access multiple cloud providers without re-authenticating.

   **Security Alert:** For security purposes, SafeNet recommends selecting the End SSO session upon sign-out option, and forcing the user to re-authenticate when they sign out of one cloud provider and access another.

6. Click OK. You are returned to the Cloud Configuration tab.

7. Select the required provider from the list, and then click the Info for Service Provider... button. The selected service provider’s Cloud Configuration Information window appears, along with the Domain URL window (see the active window in Figure 63 below).
Chapter 6: Using the Cloud Authentication Portal

Configuring cloud portals

In the Domain URL field, enter the URL of the server where you installed the Cloud Portal, and then click OK. The Cloud Configuration window appears with your information displayed.

Exporting server certificates

To export a cloud certificate, do the following:

1. From the Cloud Configuration Info window, click the Export Certificate button in the lower pane. The Save As window appears.
2. Enter a file name for this certificate, and then click the Save button. The certificate is imported into the Google Apps or the Force.com portal when you configure SSO for that provider.
3. You are returned to the Cloud Configuration Info window. Click Close.

Using arbitrary attributes

Administrators may set an arbitrary attribute in the user record by customizing the web.config file. To add an arbitrary attribute, do the following:

1. Locate and open the web.config file. The file is located at:
   
   `<install_dir>\Authentication\SAM\x64\Web\samwebapi`
   (for 64-bit systems)
   `<install_dir>\Authentication\SAM\x32\Web\Web\samwebapi`
   (for 32-bit systems)
Chapter 6: Using the Cloud Authentication Portal

Configuring cloud portals

Note: The web.config file is located on the machine where the backend server is installed.

Figure 65: Web Configuration file

```xml
<?xml version="1.0"?>
<configuration>
  <appSettings>
    <add key="CloudIDMappings" value="department=department;division=division"/>
  </appSettings>
</configuration>
```

2 Add the following line at the end of the appSettings module in the file (the location is indicated by the arrow in Figure 65 above):

```xml
<add key="CloudIDMappings" value="department=department;division=division"/>
```

3 Restart the IIS server (for the changes to take effect).

If your users are stored in ADUC, the new attribute appears in the menu on the Edit Configuration screen (see Figure 58 on page 133). If your users are stored in the SAM Express database, continue to the next section to associate the attribute with the Administration Console.

Associating user attributes with the Administration Console

To associate a user attribute for a user stored in the SAM Express database, use the Administration Console to do the following:

1 Create a personalization data attribute that matches the user attribute in the Portal Configuration window. (See “Understanding personalization data” on page 219.

2 Assign that attribute to the user. the value of the attribute should match that including the cloud users’ cloud identity.
Setting up SSO in Google Apps

Once the Google App cloud portal is configured, SSO may be set up for it. To set up SSO, do the following:

1. Browse to Google Apps, and select Advanced Tools > Authentication > Set up Single Single-on (SSO).
2. Select the Enable Single Sign-on option.
3. Using the information displayed in the Cloud Configuration Info window (see Figure 64 on page 137), do the following:
   a. Enter the Sign-in page URL in the Sign-in page field.
   b. Enter the Sign-out page URL in the Sign-out page URL field.
   c. Enter the Change password URL in the Change password URL field.

   _Note: The sign-in URL, sign-out URL, and change password URL fields must be exactly the same as those used on the Cloud Configuration tab._

4. In the Verification Certificate field, click the Browse button, and then do the following:
   a. Navigate to the verification certificate.
   b. Select the certificate. The verification certificate is the certificate exported in the Cloud Configuration Info window.

Setting up SSO in Force.com

Once the Force.com cloud portal is configured, SSO may be set up for it. To set up SSO, do the following:

1. Browse to Force.com and log in.
3. Select SAML Enabled.
4. Select SAML version 2.0.
5. Click the Browse button (located next to the Identity Provider Certificate field), and then navigate to the certificate that was exported in the Cloud Configuration Info window.
6. Enter the Issuer into Issuer field. This is the issuer shown on the Cloud Configuration Info window (Figure 64 on page 137).

   _Note: The field is case-sensitive; ensure that the information is exactly as displayed in the Cloud Configuration window._
7 Click the **Save** button. The salesforce.com login URL is displayed.

8 If you are using the Identity Provider-initiated setup, copy the **salesforce.com login URL**, and then paste it into the Service provider’s login URL field on the Edit Configuration window.

---

**Manually configuring the AAA Server for the Cloud Portal**

You may manually configure the AAA Server to communicate with the Cloud Portal using the Internet Information Services (IIS) Manager tool. The process varies slightly between Windows 2008 and Windows 2003. If you are configuring the AAA Server on a Windows 2008 machine, continue to the next section. If you are configuring on a Windows 2003 machine, skip to “Windows 2003” on page 142.

**Windows 2008**

To manually configure the AAA Server to communicate with the Cloud Portal, you must add the do the following:

1 On a Windows 2008 machine where the Cloud Server is installed, select **Start > All Programs > Administrative Tools > Internet Administrative Services (IIS) Manager**.

2 Expand the directory tree in the far left column, and then highlight the **samwebapi** icon.
3 Double-click the **Application Settings** icon.

**Figure 66: Application Settings window**

4 On the Application Settings window, select the **AAAHost** line, and then click **Edit** on the far right-side of the pane under the Actions column.

5 Set the desired host name or IP address value for the **AAAHost**.

6 Click **OK**.

7 Restart **IIS**.
Windows 2003

1 On a Windows 2003 machine where the Cloud Server is installed, select Start > All Programs > Administrative Tools > Internet Administrative Services (IIS) Manager.

2 Expand the directory tree in the far left column, and then highlight the samwebapi virtual directory.

3 Right-click on the virtual directory, and then select Properties.

4 Select the ASP.NET tab, and then click the Edit Configuration button. The ASP.NET Configuration Settings appears.

5 Click the General tab.

Figure 67: General tab

6 Select the AAAHost line, and then click the Edit button.

7 Set the desired host name or IP address value for the AAAHost.

8 Click OK.

9 Restart IIS.
Logging onto the portal

Once an application has been configured for cloud portal authentication (see “Configuring cloud portals” on page 128), the administrator should provide users with the following instructions for logging onto the portal:

1. Open a web browser, and do one of the following:
   - If the authentication request is being initiated by the Service Provider, navigate to the SaaS application’s website.
   - If the authentication request is being initiated by the Identity Provider, navigate to the Cloud Authentication Portal Logon Page.

   The Cloud Authentication Portal window appears.

   **Tip:** Ensure that the Web browser is configured to accept cookies for successful authentications to the Cloud Portal.

2. Enter your **username** in the Username field.

3. Depending on the type of token you are using, do one of the following:
   - For software or hardware token users, generate a new passcode on the device.
   - For messaging token users, click **Send me an OTP in a message** on the logon page. A passcode is sent to your mobile device or email address, and a Message Sent confirmation displays.
   - If you do not have a token assigned, enter your memorized password (users in the SAM Express database) or your Active Directory password.
4. Enter the passcode into the OTP Authentication Code field.

5. Select the **Remember username** check box if you want this computer to remember your name the next time the Cloud Authentication Portal opens.

6. Click the **Log on** button. You are authenticated to the application’s site.
In this chapter...

- About the User Center .......................................................... 146
- User Center Initialization ....................................................... 146
- User Center features ............................................................. 148
- Adding user authentication during enrollment ...................... 155
- Configuring the User Center for a SAM Express Database .... 156
- Configuring the User Center to reassign tokens .................... 157
The User Center allows Messaging and Hardware token users stored in Active Directory or in a stand-alone SAM Express database to enroll and manage their SafeNet tokens. The User Center is easy to use, and saves administrative time when a large number of users will be authenticating with SafeNet tokens. The User Center also allows users to change or assign their PIN, resync their tokens, and test their tokens after enrollment.

This section contains administrative post-installation procedures that help ensure the security of the User Center.

### Enabling the User Center

The SAM Express User Center is installed as a Windows service with the core SAM Express servers. By default, the User Center is not enabled; its service startup profile is set to Manual startup mode. To enable the User Center you must manually start the service by setting the startup mode to Automatic the first time you access it.

To set the User Center to automatically start:

1. Open the Windows Services Control Panel.
2. Change the startup mode of the SAM Express User Center service to Automatic.
3. Start the service.

### Setting the User Center password

The first time you access the User Center, you will automatically be prompted to enter its administrative password. You will only have to set this password the first time you open the User Center. You can only set the administration password from the machine where the User Center is installed.

To customize the administration password, do the following:

1. Browse to the User Center by launching the Web page: https://localhost:<port>/usercenter (port will vary based on the machine and the port being used).
When prompted, enter the Administration password that is used by the “administrator” user.

Ensuring password security

In order to allow the User Center to connect to the Administration Service automatically, passwords are stored as part of the component’s configuration. Because of this, the physical and network security of the computers where you install the SAM Express server component is of paramount importance. You must ensure that these machines are physically secure and that they do not have any publicly-accessible directories. Specifically the usercenter_<install_dir>SERVERS\Web\Tomcat\webapps\usercenter\WEB-INF directory must not be publicly accessible.
Users can perform a number of tasks related to their tokens without administrative assistance in the User Center. Users have the ability to perform the following:

- Enroll tokens
- Test tokens
- Change user PINs
- Resync tokens

Before any of these tasks can be accomplished, you must give users access to the User Center. The sections that follow describe how you provide access to the User Center, and how users complete the User Center features.

### Giving users access to the User Center

Since users browse to the User Center, the administrator must provide them with the User Center URL in the following format:

```
https://<machinename:port>/usercenter/toc.jsp
```

( the machine and port will vary based on the machine and the port being used).

*Note: You may also choose to require users authenticate when they enroll their tokens with the User Center. See “Adding user authentication during enrollment” on page 155.*

### Enrolling tokens

To enroll their tokens, instruct your users to:

1. Open the User Center by launching the following Web site:
   ```
   https://<machinename:port>/usercenter/toc.jsp
   ```

   In the URL, `<machinename>` is the computer where the SAM Express server is installed, and `<port>` is the port on which the User Center is installed. The default port is 8443.

   *Tip: As an alternative, you can use the IP address in place of the machine name in the URL.*

   The User Center home page appears.
2 Click **Enroll Token**. The Enroll Token window appears.

3 Enter your user name in the **User Name** field.
4 Enter the token serial number found on the back of the token into the **Token Serial Number** field.

5 Click the **Submit** button. The Successfully enrolled token window appears.

![Successful enrollment window](image)

The token is now enrolled in SAM Express. If you want to test the token, click **Test Token** and refer to Testing tokens.

## Adding or changing PINs

PINs add another layer of security to your system. Choosing to add a PIN means each time users authenticate using a token generated one-time passcode, they must append their PIN to the end of their passcode.

PINs can be added by administrators or by users after a token has been enrolled. If your users will be adding their own PINs, provide them with the following information:

**Note:** If you will allow your users set their own PIN, you must supply them with the URL for the User Center. (See “Giving users access to the User Center” on page 148.) If the user already has a PIN associated with their token, they will also need the current PIN in order to change to a new PIN.

1 Open the User Center by launching the following Web page:

   ```
   ```

   **Note:** In the URL, `<machinename>` is the name of the computer where the SAM Express server is installed, and `<port>` is the port on which the User Center is installed. The default port number is 8443.

   **Tip:** As an alternative, you can use the IP address in place of the machine name in the URL.
2 When the User Center home page appears, click Change PIN. The Change PIN window appears

Figure 74: Change PIN window

3 Enter the token serial number from the back of your token into the Token Serial Number field.

4 Enter a token passcode in the Token Passcode field. Be sure to include your PIN if applicable.

5 Enter your desired four-digit PIN in the New Token PIN field.

6 Click the Submit button.

Figure 75: Successful PIN Change window

The Successfully changed PIN window appears. You must use the new PIN when logging in with token-generated passcodes.

Testing tokens

Once a token has been assigned and enrolled, it should be tested. Users can test their token using the User Center. To test a token with the User Center, instruct your users to do the following:
Chapter 7: Working with the User Center

User Center features

1. Open the User Center by launching the following Web page:

   **Note:** In the URL, `<machinename>` is the name of the computer where the SAM Express server is installed, and `<port>` is the port on which the User Center is installed. The default port number is 8443.

   **Figure 76:** User Center Home Page window

   ![User Center Home Page window](image)

   - **User Center**
   - **Re-sync Token**
   - **Enroll Token**
   - **Change PIN**
   - **Test Token**

2. When the User Center home page window appears, click **Test Token**.
   The Test Token window appears.

   **Figure 77:** Test Token window

   ![Test Token window](image)

   If you have an assigned PIN, append it to your token passcode.

   - **Token Serial Number:** 
   - **Token Passcode:** (including PIN, if assigned)

3. Enter the token serial number in the **Token Serial Number** field.
4 Enter a token-generated passcode in the **Token Passcode** field. Remember that if a PIN has been added to this token, it must be appended to the end of the passcode on this field.

5 Click the **Submit** button.

**Figure 78:** Successful Token Test window

6 A Successful Token Test window appears, informing you that this token has been successfully tested.
Resynchronizing tokens

There are occasions when a SAM Express token will get out of sync and its generated passcodes will not function properly. If this occurs, and you allow users to resync their own tokens, provide them with the following information:

1. Launch the User Center.

2. On the main menu, select Re-sync Token. The Re-sync Token window appears.

3. Enter the out-of-sync token’s serial number in the Token Serial Number field.

4. Generate a passcode and enter it in the first Token Passcodes field. If this token has a PIN assigned to it, add it to the end of the passcode.

5. Generate a second passcode and enter it in the second Token Passcodes field. Add a PIN if applicable.

6. Click the Submit button. The token is now synchronized.
Adding user authentication during enrollment

You may require your users to authenticate before they can gain access to the User Center. To set up pre-enrollment authentication, you must configure the LDAP server that will be queried by doing the following:

1. Browse to `<Install_DIR>\SERVERS\Web\Tomcat\webapps\usercenter\WEB-INF`, and open the `EnrollAuth.bsh` file with a text editor.

2. Change the `hostname`, `domain`, `domain suffix` (example: `host.domain.com`), and the `LDAP port` to the following parameters:
   - HOST = `<your host>`
   - DOMAIN = `<your domain>`
   - DOMAIN_SUFIX = `<your domain suffix>`
   - PORT = `<your port>`

3. Change the account credentials for the LDAP search to the following parameters:
   - ADMIN_USER = `<your account name>`
   - ADMIN_PASS = `<your account password>`

   Do not change any other setting in this file.

4. Browse to `<Install_DIR>\SERVERS\Web\Tomcat\webapps\usercenter\WEB-INF`, and open the `login.conf` file.

5. Ensure that `REQENROLLAUTH` = true, and then save the file.

*Note: If you changed the `login.conf` file, you must restart the SAM Express User Center in Services.*

When users access the User Center, they now must enter their username and Windows password, along with their token serial number and PIN before they can enroll their tokens.

**Figure 81:** Windows Authentication window
The Admin Server plugin "SccTokenASPlugin", used by the User Center can function with the user database in Active Directory (the default) or with the SAM Express database.

**Note:** If Active Directory was initially used to enroll tokens, and then enrollment is switched to the SAM Express database, you must re-enter those Active Directory users into the SAM Express Management Console. The users must also re-enroll their tokens.

To switch from users in Active Directory to users in the SAM Express database, use the following steps:

1. Browse to `<Install_Dir>\SERVERS\Shared`, and open the `sccservers.ini` file with a text editor.
2. Add the following line to the bottom of the file:
   ```
   userDBType=securecomputing.nbt.tokenasplugin.SWUserDBMapper
   ```
3. During enrollment, if you want to allow new users to be created in the SAM Express database based on the user name entered, add the following to the `sccservers.ini` file:
   ```
   SWUserDBMapper_CreateUsers = true
   ```
4. Save the file.
5. Restart the SAM Express Admin Server and Authentication Engine Services.
To allow users to reassign a token, modify the `login.conf` file by doing the following:

1. Browse to `<Install_Dir>/SERVERS/Web/Tomcat/webapps/usercenter/WEB-INF`, and open the `login.conf` file with a text editor.

2. Add the following line to the bottom of the file: `ALLOWREENROLL = true`. If the line is already in the file, change it from `false` to `true`.

3. Save the file and close it.

4. Restart the SAM Express User Center in Services.
Chapter 7: Working with the User Center

Configuring the User Center to reassign tokens
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control concepts overview</td>
<td>160</td>
</tr>
<tr>
<td>Quick authentication demo</td>
<td>165</td>
</tr>
<tr>
<td>Setting up the SAM Express Management Console</td>
<td>166</td>
</tr>
<tr>
<td>Creating groups</td>
<td>174</td>
</tr>
<tr>
<td>Creating login ACLs</td>
<td>175</td>
</tr>
<tr>
<td>Creating roles</td>
<td>180</td>
</tr>
<tr>
<td>Creating Web ACLs</td>
<td>182</td>
</tr>
<tr>
<td>Managing authenticators</td>
<td>194</td>
</tr>
<tr>
<td>Managing users</td>
<td>205</td>
</tr>
<tr>
<td>Understanding personalization data</td>
<td>219</td>
</tr>
<tr>
<td>Importing user records from a third-party user database</td>
<td>225</td>
</tr>
<tr>
<td>Managing and viewing audit logs</td>
<td>227</td>
</tr>
<tr>
<td>Reporting</td>
<td>235</td>
</tr>
<tr>
<td>Database-related tasks</td>
<td>240</td>
</tr>
<tr>
<td>Customizing SAM Express</td>
<td>243</td>
</tr>
<tr>
<td>Other admin tasks</td>
<td>248</td>
</tr>
</tbody>
</table>
Though users and groups are familiar concepts to administrators who use Active Directory, there are slight differences in the way they are implemented in the SAM Express Management Console.

If you wish, you may skip this overview and turn to “Setting up the SAM Express Management Console” on page 166.

### Users

In the SAM Express Management Console, users are categorized into one of three administrative levels: system administrators, group administrators (which includes local administrators and helpdesk staff), and regular users. These three levels of users fit into two categories, those with administrative privileges (system administrators, local administrators, and helpdesk staff), and those without administrative privileges (regular users). Table 7 summarizes these levels and their privileges.

<table>
<thead>
<tr>
<th>Level</th>
<th>Privileged</th>
<th>Unprivileged</th>
</tr>
</thead>
<tbody>
<tr>
<td>System administrators</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Group administrators (local administrators and helpdesk staff)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Regular users</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

**Important:** If you are also going to use Active Directory as part of your installation, only System and Local Administrators will be able to log on to the ADUC snap-in.

#### Privileged users

Privileged users can administer some portion of the SAM Express system. The extent of their administration depends on their level of permissions. In general, administrators can create, modify, and manage groups and users that are under their control. There are three types of administrative users: system administrators, local administrators, and helpdesk staff. Table 8 shows user type permissions.

**Important:** Helpdesk users created in the SAM Express Management Console are not supported for delegated administrative privileges in ADUC.

**Note:** Local administrators and helpdesk staff are collectively known as group administrators because their administrative permissions are restricted to those admin groups specifically assigned to them by the system administrator.
### Unprivileged users

Users who are not given system administrator, local administrator, or helpdesk staff privileges are referred to as unprivileged users. Most of your users will be unprivileged users who can not perform any administrative or system-related tasks.

### Groups

Groups are virtual containers that can hold users or objects such as tokens, ACLs, or roles, etc. Groups allow you to more easily organize and manage large numbers of users, and you can delegate the administrative duties of particular groups within the hierarchy of an organization to local administrators.

### Groups and subgroups

You can create groups and organize them alphabetically, by department, or geographic region, etc. You can also nest groups within groups to further subdivide them into a parent-child group hierarchy that resembles your organization. Group affiliation is required since every object must belong to a group.
Chapter 8: Using the SAM Express Management Console

Access control concepts overview

Note: A user’s placement in a group has no bearing on their authorizations within SAM Express. A SAM Express group should not be confused with groups as defined within Windows operating systems. SAM Express roles are analogous to Windows groups.

Types of groups

There are two kinds of groups: global and non-global.

- **Global groups**: contain data, such as ACLs, roles, and profiles, that you want other administrators to view and access. Placement in a global group makes these objects visible, but not modifiable to all administrative users. Users cannot be placed in global groups so local administrators won’t have unintended access to users in other groups. Global groups and the objects within them can only be created and modified by system administrators.

- **Non-global groups**: visible to system-level administrators, local administrators, and helpdesk staff with specific management duties over those specific groups. This gives system administrators the ability to assign local or helpdesk administrators to specific groups without also granting them access to other groups. These groups normally contain users, but can also contain roles, ACLs, tokens and authenticator profiles, and reservations that are relevant only to users in that local group. By placing users in non-global groups, you are able to divide a large number of users into smaller groups that are independent of groups at the same hierarchical level, then assign group-level administrators to manage those groups.

Note: You should probably only have one global group in your deployment. The majority of your groups will be non-global groups because users can only reside in non-global groups.

Access Control Lists (ACLs)

All access requests are processed through one or more ACLs, which are a collection of access rules defined for a set of protected resources. Low-risk resources can have less restrictive rules, while highly-sensitive resources will have stricter rules. ACLs define and store your security policies. Login ACLs store the rules that control access to your network services and Web ACLs govern access to your Web resources. All users must be authorized by a login ACL before they are permitted access to your Web servers.

SAM Express comes pre-populated with a default login ACL and a default Web ACL. You can use the default ACLs as templates when you create your own ACLs. The default login ACL is named DEFAULT_ACL, and the default Web ACL is named DEFAULT_WEB_ACL. Both are stored in the GLOBAL DATA group in the Management Console.
Important: We strongly recommend that during testing of new security policies, you place those policies in a new login ACL or a new Web ACL, and leave the default ACLs intact and unmodified.

ACL entries

ACL entries are the access rules that make up an ACL. They specify the user access permissions of your security policy, and are the most important parts of an ACL. When an authenticated user attempts access into your network, the circumstances of that attempt must meet the permission criteria of at least one matching ACL entry before successful authorization and authentication will occur.

You define permission criteria when you create your ACL entries. For instance, in a login ACL, you can set up entries that allow access to particular resources, to all users, or to limited users based on role, IP address, SAM Express agent or custom application, or specific user name. This information is the subject of your entry. Once you have defined the subject part of the entry, you set the restrictions that will be applied to the users who are targeted by the subject. You can restrict all access, allow unrestricted access, or grant access based on authenticator strength, date range, and day and time.

Roles

In ESP, roles are tags or labels that identify groups of users who share common access privileges. In other words, roles define collections of access rules applicable to particular groups of users.

You may choose to categorize users into roles based on their relationship to your organization. For example, you might set up roles for management, accounting, human resources, IT, and administrative staff members. Another possibility is to create roles with names that denote user authorization, for instance, “nightshift users”. You may also have roles for accessing servers (by server name or IP address), with a role for your mail server, your HR, Finance, and Sales servers. You would then create ACL entries for each of these resources.

Important: Every role must be associated with a supporting login ACL in order for it to have any meaning within your ESP security policy.

Figure 82 on page 164 shows groups of users with multiple roles, their relationship to a login ACL, and the ACL entries that map role-based access restrictions.
Figure 82: Role to login
ACL relationship

Though not a required user attribute, roles are valuable because they offer a quick means of applying or modifying uniform sets of access permissions to large numbers of users.
The SAM Express Management Console allows you to configure flexible access control mechanisms specifically tailored to the needs of your organization. If you want to set up a test of the SAM Express token authentication process independent of AD, you would do the following (assuming the SAM Express Management Console has been installed and configured):

- Import token records with the Console (refer to “Importing hardware authenticator files” on page 168)
- Create a user in the SAM Express database (refer to “Creating user accounts manually” on page 206)
- Assign a token to that user (refer to “Assigning hardware tokens manually” on page 198)

A SAM Express token authentication can then be performed from the SAM Express RADIUS server or a SAM Express Agent, such as the OWA Agent.

Agent configuration information can be found in the SAM Express Agent Administration Guide, a downloadable PDF found on the corporate Web site at: www.safenet-inc.com/safeword/docs/2008.
Setting up the SAM Express Management Console

Before you import your users, you should customize your installation and secure the SAM Express Management Console by changing the default login username and password, and then create a working administrative account. Next, you will need to create the groups into which your users will be placed, one or more login Access Control Lists (ACLs), Web ACLs, and roles that support your company's security policy.

Launching and securing the Console

The first time you launch the SAM Express Management Console, you will log in using the default username (administrator) and password (administrator) before you enter your custom password.

**Important:** If ADUC was previously launched and a custom password was assigned, the administrator password will already have been set.

Start > Programs > SafeNet > SAM Express > SAM Express Management Console

Verifying the list shows the machine on which Admin Server is installed.

![Connection Progress]

Enter the default username: **administrator**

![Connection in Progress]

Enter the default password: **administrator**

Creating a primary working administrator account

The default system administrator account is designed for several purposes, including troubleshooting your primary working account, and should not be changed. Instead, you should clone the default account and then customize the clone. By maintaining the default system administrator account in its original state with a new password, you have a tool for troubleshooting authentication issues should they occur.
To clone the default system administrator account, do the following:

1. **Expand the Reserved Admin Group folder.**
   
   Reserved admin groups should be used for administrative-level users only so you can delegate the administrative duties of specific groups to specific administrators.

2. **Highlight Users.**
   
   **Note:** User icons that appear in color indicate an unprivileged user with an enabled account. A grayed out icon indicates a user account that is disabled or not completely set up.

3. **Right-click Administrator, then select Duplicate.**
   
   The Create a New User window appears.

4. **Enter information.**
   
   This name will identify your primary working account; its name should be something that will make it recognizable as such.
   
   It is recommended that you leave the default Admin Group RESERVED selected and un-edited.

   **Important:** Since you are creating your primary working account, we recommend that you do not edit the group properties unless there are custom changes you are certain you want to apply to this admin group.

5. **Assign the default role to the primary working account by clicking Select.**
   
   The Pick Role(s) window appears with DEFAULT_ROLE highlighted. Clicking the Select button will assign the default role to your working account, and take you back to the Create a New User window. The DEFAULT_ROLE appears under Roles.
You have now created a primary working account. To more tightly secure your account, you should generate MobilePASS records and secure the working account with a Software or Hardware token, import your token data records and assign a Hardware token to the working account, or assign a fixed password to the primary account. Additionally, you may choose to assign a SoftPIN to this account to add another layer of security.

- To generate MobilePASS software tokens, see “Generating and importing MobilePASS software tokens” on page 194
- To import hardware files, refer to “Importing hardware authenticator files” on page 168

---

**Importing hardware authenticator files**

Hardware tokens can only be used if there is an association between the token serial number and corresponding cryptographic algorithm in SAM Express. This is done by importing the token programming file. The token programming file (for example, `importAlpine.dat`) you need to import was downloaded at activation time.
Assigning a hardware token to the primary account

You can ensure security of your primary working account by assigning a hardware token to the account, and then strictly limiting use of that token to administrators who are responsible for administration of the primary working account. You will be using the authenticator programming files you imported earlier in order to assign a hardware token to the account.
Figure 86 shows the process of assigning a token (and optional SoftPIN) to your primary working account.

You may require that administrators enter a SoftPIN in addition to the token-generated passcode they must supply in order to access the primary working account. SoftPINs are optional; they consist of 4-character numerical strings that are generally appended to the end of the passcode each time an administrator accesses the account. SoftPINs add an additional layer of security to your account.

Security Alert: When you deploy SAM Express operationally, we strongly recommend assigning a hardware token or a software authenticator for every user.
Verify your account expiration and privileges

You should verify that your primary working account will never expire, and has System Administrator privileges.

1. Right-click your account name, and select Edit.
2. Click the Advanced tab, verify Never is selected in Account Expires.
3. Click the Privileges tab, verify System Administrator is selected.

Testing your primary working account

It is important to test your primary working account and the token you have assigned to it once you are finished setting them up. To test the account you will need to log out and then log back in under your new primary working account username, using the token and softPIN if required. To test the account:

1. Log out of the session by clicking the Server Disconnect icon, then click Yes.
2. Click the Server Connect icon.
3. Enter your primary working account username.
4. Enter the requested information for the assigned token.

**Success:** If you are able to successfully log in, your primary working account is functioning properly, and you can now safely change the default system administrator account’s password. See “Changing the default administrator password”.

**Failure:** If you are unable to successfully log in, log out again and log back in under the default system administrator user account to troubleshoot your primary working account.
Changing the default administrator password

The default login password ("administrator") is the same for all SAM Express installations, and you should change the default password to a newer, more lengthy one and keep that password locked in a safe place.

**Important:** Do not change the default administrator password until you have logged out and successfully logged back in under your primary working account.

To assign fixed password, do the following:

1. Right-click the default Administrator account, and select **Edit**.
2. In the **Edit User: ADMINISTRATOR** window, click the **Authenticators** tab, highlight the existing fixed password, and click the **Properties** button.
3. Clear the **User must change password...** checkbox so you are not forced to change passwords again at the next login.

   **Note:** Typically, you would only check this box when you are assigning a fixed password to a user OTHER than yourself.

4. Enter a new password in the **Fixed Password** field, then re-enter in the **Confirm Password** field.
   - Use a lengthy and difficult password that is not easily hacked or guessed.

   **Note:** The available default profiles are **fixed** and **Emergency**. Table 9 lists the attributes of the two default password profiles.

<table>
<thead>
<tr>
<th>Fixed password profile name</th>
<th>Strength</th>
<th>Minimum password length</th>
<th>Minimum password Age</th>
<th>No. of warning days</th>
</tr>
</thead>
<tbody>
<tr>
<td>fixed</td>
<td>5</td>
<td>4</td>
<td>Never expires</td>
<td>N/A</td>
</tr>
<tr>
<td>Emergency (see note)</td>
<td>20</td>
<td>12</td>
<td>3 days</td>
<td>3</td>
</tr>
</tbody>
</table>

   **Note:** The Emergency fixed password profile should only be used by administrators or helpdesk staff to temporarily assign a fixed password when a user has lost or otherwise compromised their hardware authenticator.

**Tip:** You can modify the default fixed password profile settings at any time, or create a new fixed password profile with different settings.

5. Click **OK** to finish, then click **OK** in the Edit User window to return to the Console.

6. Log off and then log back on using your new system administrator name and fixed password.
What next?

At this point, token data files have been imported, and basic account and console security configurations have been finished for the SAM Express Management Console.

Next, you should set up groups, login Access Control Lists (ACLs), roles (optional), and Web ACLs (optional), before distributing tokens. Procedures for these additional configurations begin in the section called “Creating groups” on page 174.
Creating groups

There are two types of admin groups in SAM Express, global and nonglobal. Global groups contain data that any administrator, no matter what level they have been designated, can access. This means system level administrators, local administrators, and helpdesk staff can all view data contained in these groups. Non-global groups contain data whose access is restricted to system and lower-level administrators with specific management duties for the particular groups. When you create a new group, you specify whether or not it will be global.

⚠️ Important: Users cannot be placed into global groups, thus preventing local administrators and helpdesk staff from having unintended access to data they do not have permission to access.

To create a new admin group or subgroup, do the following:

1. In the SAM Express Management Console, highlight the Admin Group under which you want the new group or subgroup to appear (USERS, for example).
   - If the group is to be a top-level group, select the top-most group folder (for instance, Admin Groups).
   - Subgroups are groups nested beneath admin-level groups (which become the Parent group to that subgroup). Administrators who manage a group also manage the subgroups inside their group.

2. Select Insert > Admin Group.

3. Enter a name in the Admin Group field.

4. (Optional) Select the Globally Visible check box if this is a group that will not contain users. This allows other administrative-level users access to this group’s contents.

5. Click OK to create the group.
Creating login ACLs

Login Access Control Lists contain the access rules (entries) that restrict user access into your network. SAM Express has a default login ACL that you can use as a template for creating ACLs. Figure 87 shows the process of creating a Login ACL with page references for additional information (if needed).

**Important:** We strongly recommend that DEFAULT_ACL be left intact. This will keep you from accidently locking yourself out of your system.

Login ACLs work with non-Web-related SAM Express agents to restrict access to your network services. You can restrict access based on:

- **A Subject:** One or more users, a role, IP address, agent/application; and/or
- **A Restriction:** Authenticator strength, time of day, range of dates

You can also specify a **Return** value to be sent in response to success or failure of an authentication attempt.

From the SAM Express Management Console, select **Insert > Login ACL**

![Create a New Login ACL](image)

**Figure 87:** Create a new Login ACL

- **Restriction:** Authen. Strength
- **Restriction:** Time of day
- **Restriction:** Range of dates

**New ACL Entry:** Subject “Subject” on page 176

**New ACL Entry:** Restrictions “Restrictions” on page

**New ACL Entry:** Return “Return” on page 178
Defining login ACL entries

Login ACL entries specify user access rules, and at least one must be met to gain entry. ACL entries are defined by one or more of the following:

- **Subject**: sets user, role, IP address, or agent information for this entry. See “Subject”.
- **Restrictions**: sets any subject restrictions. See “Restrictions” on page 177.
- **Return**: sets values returned to an agent upon either successful or unsuccessful authentication attempts. See “Return” on page 178.

**Subject**

**Subject**: the users to whom entry Restriction and Return values will apply.

**Tip**: Avoid creating ACL entries that have a single user ID as the subject, and instead define access restrictions common to all users.

Choose from the following options to apply to the entry:

- **Role**: applies this rule to users with a role selected from the Role drop-down list.
- **IP**: restricts user access to a specific resource’s host name, IP address, or resources within a specified range of IP addresses (including wildcards such as 196.168.24.* or 192.168.24.1-100). IPv6 addresses are also acceptable (e.g. 2001:db6:0:1:* or 2001:db6:0:1:A000-AFFF:*).

To prevent users from logging on from the same machine on which core servers are installed, create IP restrictions for both the IPv4 (127:0:0:1) and IPv6 (::1) localhost addresses.

Core servers must have the IPv4 localhost address defined in the hosts file.

**Note**: RADIUS and RADIUS Accounting servers only support IPv4 addresses.
• **Agent/Application:** applies this rule to users attempting to access resources via a particular agent or custom application.

• **User:** permits or deny access to a specific user. You may not specify a user by alias, you must use their primary name.

**Restrictions**

Restrictions are applied to users targeted on the Subject tab.

![Figure 89: New ACL entry (Restrictions tab)](image)

**Important:** Clearing the check box results in no restrictions being defined for this ACL entry. Restrictions will be taken from the next matching ACL entry.

Choose either to allow unrestricted access, to allow no access, or to define access restrictions.

• **Unrestricted Access:** users targeted on the Subject tab will be given access to the requested resource if they pass authentication. No authorization phase will be conducted.

• **No Access:** users targeted in the Subject tab will not be given access to the requested resource, even if they pass authentication.

**Note:** If you select either unrestricted access or no access, continue to “Return” on page 178.

• Click **Grant access if the user meets these restrictions** to define the following restrictions:
  – **Minimum Authentication:** set according to how strong (secure) you want the access requirement to be (based on the strength of individual or combined authenticators).
Chapter 8: Using the SAM Express Management Console

Creating login ACLs

Table 10: Authenticator strengths

<table>
<thead>
<tr>
<th>Authenticator Type</th>
<th>Default Strength</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed password</td>
<td>5</td>
</tr>
<tr>
<td>Emergency fixed password</td>
<td>20</td>
</tr>
<tr>
<td>Alpine Token</td>
<td>10</td>
</tr>
<tr>
<td>MobilePASS authenticator</td>
<td>10</td>
</tr>
<tr>
<td>SofToken II</td>
<td>10</td>
</tr>
<tr>
<td>Gold 3000</td>
<td>20</td>
</tr>
<tr>
<td>Platinum</td>
<td>20</td>
</tr>
<tr>
<td>eTokenPASS</td>
<td>10</td>
</tr>
</tbody>
</table>

- **Range of dates**: Set a range of access dates (this works well for fixed-term contractors or temp employees)
- **Time and day**: Set specific days and times on which access is permitted.

**Return**

To specify return values for this entry (used by a SAM Express Agent, not seen by the user). Generally, this tab is used to define access rules for resources protected by SAM Express agents or a custom agent created using the Authentication SDK, and you will need to specify a return value.

---

**Figure 90: New ACL Entry (Return tab)**

- Select a status (Success or Fail), or leave the **Return a value...** box blank.
- Select a value (0, 1) to return on pass or fail.
- Enter a text string (e.g. “Authorization Passed,” “Authorization Failed”) or for application level role (e.g. “bank_app_admin,” or “bank_app_user”).
- Select a Personalization attribute (if the user has one).
- Select SAM Express to return the user’s role.
**Editing ACL entries**

To edit an ACL entry, select **Find > Login ACLs**.

1. Use either the **Find all available**, or **Find all that match** filters to locate the ACL you created earlier.

2. Select the ACL you want to edit from the list of entries, and click the View button (binoculars).
   
   The View Login ACL window appears.

3. Click the **Edit** button to edit the ACL.
   
   The process for editing an ACL entry is the same as the process for creating entries.

**Ordering ACL entries**

Login ACL entries are evaluated from the first entry in the list to the last. This processing sequence means that any user logon attempt will first be matched against the subject of the first ACL entry. If the subject matches, access and/or authorization will proceed. If not, the next entry in the ACL will be evaluated.

Since the evaluation process goes from the top entry downward, you will want to order your entries from most restrictive (top) to the least restrictive (bottom). Placing the least restrictive entries higher in the list opens your system up to a larger number of users. You may want to insert an ACL entry that targets “All Users” last in the list since it will catch all users. If you do not place an entry that targets “All Users,” and no match is discovered as the ACL is processed, the Authentication Engine will consult the user’s next highest priority role to determine the next ACL to process. This may or may not result in the processing of the same ACL, or an entirely different one. Any entry placed below an “All Users” entry will be ignored.

To change the order of the ACL entries, select **Find > ACLs > Login**. The Find Login ACL entries window appears.

1. Select the **Find all available** filter to locate all ACLs.

2. Click **Find**.
   
   The **Find Results: ACL Entries** list appears.

3. Select the ACL that you want to update.

4. Click the **Edit Entry** button.

5. When the Edit Login ACL window appears, select individual ACL entries and click the arrows to the right of the entry list until your ACL entries are reordered as desired.
Creating roles

Before creating roles, you must have at least one login ACL created, as each role must point to a login ACL. Additionally, a role can only point to one login ACL. As you create each role, you point it to the ACL that provides the security policy definition for it, specifically, the ACL that contains an entry with that role as its subject.

If you have not created a login ACL, refer to “Creating login ACLs” on page 175. When you have created a login ACL, you are ready to start creating roles to assign to your users.

While not required, Roles can be very powerful tools to help manage user access needs. A role is a tag that identifies a user’s access privileges. Roles are generally associated with login ACLs. In SAM Express, a role is only a label, and is generally meaningless without a supporting login ACL.

Tip: When naming your roles, it is helpful to use a naming convention that describes what the role does, or who the role affects. For example, role names such as “Executive_role”, “HR_role”, “Weekday_dayshift_role”, or “No_weekend_role” offer visual clues about the function of those roles. Note however, that this convention only works if the access rules that you define in the associated login ACL provide relevant security policy definitions for that role. For example, a role called “nightshift” should point to an ACL that defines an access rule that maps the “nightshift” role to the blocks of time within the work week that comprise the nightshift within your organization.

Create a role

To create a role, from the SAM Express Management Console, select an Admin Group into which the roles will be placed. Generally, roles are placed in a global group that will be accessible to all administrators. If you want to restrict accessibility, select a non-global admin group.

Select Insert > Role to display the Create a New Role window.
1 Enter a name in the **Role** field.

2 Accept the default RESERVED, or enter a new group.

   The Admin Group is the group to which this new role will be assigned. The default setting is based on the group that was highlighted at the time you began the role-creation process. You can select another if desired.

3 Select a login ACL from the **Login ACL** list.

   A role must point to a login ACL. If no login ACL is selected, the default login ACL, as specified in your SAM Express configuration (see “Reconfiguring the default login ACL” on page 246), will be used.

   **Note:** The Personalization Data tab is discussed in “Understanding personalization data” on page 219.

4 Select a priority from the **Priority** list.

   The valid input range is 1 to 999. Priorities come into play when a user has more than one role assigned to them. During authorization, the Authentication Engine works with only one role at a time. It will choose the highest priority role or the default role if no role was assigned. If no match within the role’s referenced login ACL is found, the next lower priority role is checked. This process continues until a match is found that meets whatever criteria is relevant to the login attempt.

5 Enter any comments in the **Comments** field.

   At this point there is no personalization data available to apply to this role. If you want to add data to the role, see “Understanding personalization data” on page 219. Otherwise your new role is complete.

6 Click **OK** to create the role.
Creating Web ACLs

A Web ACL is a list of Web ACL entries or rules that govern access to individual URLs and their content on your Web servers. Universal Web Agents use Web ACLs to enforce your Web security policy. In order to protect your Web servers, the UWA must be installed on all Web server machines you want to protect.

Each Web ACL entry has three parts:

- the protected URLs - users can specify HTTP hosts and/or path names for specific URLs, or can choose to match all URLs
- restrictions - restrict access to the URLs based on roles, IP address, time of day, date range, or authentication strength
- personalization data (optional) - allows extra information about the user to be sent to the server or back to the client (browser).

The UWA uses exactly one Web ACL to control access to the Web applications and resources that it protects. The UWA checks the rules in order until one matches the URL that is being requested by the user. When a rule matching the URL is found, that rule is checked for any restrictions (such as time of day, or role), and to see if any personalization data has been requested to be sent to the Web application or the Web browser.

For information about installing and configuring the Universal Web Agent, see the *Universal Web Agent Administration Guide*, a PDF available for download from [www.safenet-inc.com](http://www.safenet-inc.com).

Create a Web ACL

To create a Web ACL, from the Admin Console, select **Insert > ACL > Web**. The Create a New Web ACL window appears.

1. Enter a name in the **ACL** field.
2 Select an admin group for this ACL from the **Admin Group** list.

**Tip:** To view the properties of an Admin Group, click the **View** button next to the **Admin Group** field.

3 Click the **New** button under ACL entries. The New Web ACL window appears with the Protected URLs tab displayed.

![Figure 93: New Web ACL Entry window (Protected URLs tab)](image)

**Specifying URLs to protect**

You may choose to protect all URLs on a targeted Web server, or specific URLs. To protect all URLs, select **All URLs**. Choosing this option will disable all other options on this panel. If you choose this option, select the Restrictions tab, and skip to “Setting URL restrictions” on page 185, otherwise select **Specific URLs** and continue with this procedure.

**Note:** If a resource being used is not on the list, it is passed through unprotected.
Chapter 8: Using the SAM Express Management Console

Creating Web ACLs

1. Click the Add button. The Add URL window appears.

2. (Optional) In the Domain Name field, enter the name of the location where the Web server resides. For example, if the Web server location is www.safenet-inc.com, you would enter safenet-inc.com.

   **Important:** If a domain name is not specified, the Web ACL applies to all Web servers. If one is specified, the Web ACL applies only to that Web server.

3. Enter the path part of the URL in the Path field. This may be a path to a directory, or to a specific file or application. If a directory is specified, all subdirectories will be protected too. Asterisks may be used as wildcards. For example: /protected/* will protect all resources in the protected directory, and all resources in the subdirectories. /regforms/register.html will protect only the register.html page. /cgi_bin/bbs* will protect all applications with names beginning with the letters “bbs”.

4. (Optional) In the Arguments field, enter the URL arguments that you want matched. You may use wildcards. If you do not enter a value here, the program automatically matches wildcards. Arguments are matched in the order they are entered.

5. When you enter arguments, you must specify how to treat escape sequences. Choose one of the following options:
   - Treat escape sequences as text (the default)
   - Treat escape sequences as binary data.

6. The UWA automatically adds headers that do not allow protected content to be cached. To turn this feature off for this URL, select the check box labeled Don’t add cache control HTTP headers.

   **Tip:** The UWA does not recognize the ^ symbol in PremierAccess version 3.2.

7. Click OK. You are returned to the Protected URLs tab.

8. Under HTTP Methods:
   - click All to activate all available methods and disable the list. If you choose this option, continue to “Setting URL restrictions” on page 185.
   - click Specific to apply specific HTTP methods for this ACL entry. If you choose the specific option, continue to the following procedure.
Chapter 8: Using the SAM Express Management Console

Creating Web ACLs

9 To activate specific HTTP methods, select the check boxes for the methods that apply.

- **GET** returns whatever data is specified in the Request-URI
- **POST** allows for such actions as posting messages to bulletin boards, news groups, articles, mailing lists, etc., or providing a block of data such as credit card information
- **HEAD** tests hypertext links
- **OPTIONS** informs the client of requirements or capabilities associated with a resource or server without initiating data retrieval
- **PUT** stores supplied information in a specified URI
- **DELETE** requests that the server delete the resource identified by the request URI
- **TRACE** allows the client to see what was received by the target server. This information and is used for testing or diagnostics

By checking any of these check boxes, you are saying that this ACL entry’s restrictions apply to attempts to access the specified URLs with these specified HTTP request methods. GET, POST, and HEAD are the most commonly used methods.

10 When desired settings have been made, click the **Restrictions** tab.

**Setting URL restrictions**

The Restrictions tab defines a set of restrictions that will be applied to all users requesting access. These restrictions will be applied to the URLs and methods specified on the Protected URLs tab.

1 **Select:**

- **Unrestricted Access** to permit all access. This option gives explicit access permission to users who have successfully authenticated with SAM Express.
Chapter 8: Using the SAM Express Management Console

Creating Web ACLs

- **No Access** to deny all access. This option denies all access, even if the user provides correct authentication.
- **Grant access if the user meets these restrictions** to limit access based on restrictions including roles, authentication strength, Web browser, time of day, or range of date.

If you choose either of the first two options, continue to the Personalization tab and “Passing personalization data” on page 190. If you choose Grant access if the user meets these restrictions, the Restrictions and Settings are enabled and you can define your role restrictions. Continue to “Defining restrictions based on roles” on page 186.

**Defining restrictions based on roles**

To restrict access to a resource based on allowed roles, on the New Web ACL Entry window’s Restrictions tab, select **Allowed roles**. This option means users must have one of these specific roles to be granted access to the protected URLs targeted by this ACL entry.

![Figure 96: New Web ACL Entry (Restrictions tab)](image)

1. Click the **Edit** button. The Edit Restriction window appears.

![Figure 97: Allowed roles window](image)

2. Click **Enabled** to activate the window.
3 Select a role from the **Available Roles** list, and then click the **Add** button to move the role to the **Allowed Roles** list. The allowed roles are the roles users must possess in order to access URLs protected by this Web ACL.

**Tip:** The left pane contains the list of all available roles that define the total group of users that can access the selected URLs.

4 When you have added all the roles you want to require, click **OK**.

### Defining restrictions based on authentication strength

To restrict users access to URLs protected by this Web ACL based on authentication strength, from the Restrictions and Settings window, select the **Minimum Authentication Strength** restriction.

1 Click the **Edit** button. The Edit Restriction window appears.

![Figure 98: Minimum authentication strength window](image)

2 Click **Enabled** to activate the window. This panel is used to set a minimum (combined) authenticator strength for access. The allowable range is from 1 to 60. The higher the authentication strength number, the stronger the authenticator or combination of authenticators must be in order to successfully access resources. For instance, if fixed passwords in your system have an authentication strength of 5 and Platinum tokens have an authentication strength of 20, you can restrict a resource to Platinum token users only, by setting a value of 20. Only users with a combined authentication strength of 20 or higher will be able to access this resource.

3 Select an authentication strength from the **Minimum Authentication Strength** list.

4 Click **OK**. You are returned to the Restrictions and Settings window.

### Defining restrictions based on Web browser IP address

To restrict users access to protected URLs targeted by this Web ACL based on Web browser IP address, select the **Web Browser IP** restriction. The Edit Restriction window appears.

1 Click **Enabled** to activate the window.
2 To define specific Web browser IP address(s) from which to allow or deny access, select:
   - **Allow** to designate the computers that will be allowed access to the protected URLs. All other computers will be denied access.
   - **Deny** to designate the computers that will be denied access to the protected URLs listed. All other computers will be allowed access.

3 Click the **Add** button to activate the IP address list.

4 Enter a new IP address in the **IP Address** field.

   **Note:** Wildcards and ranges are allowable. All four parts of the IP address must be specified (for example 192.168.24.* or 192.168.24.2-15).

**Modifying existing IP addresses**

To modify a existing IP address, select it from the **IP address** list on the Edit Restriction window, and click the **Edit** button. Make the desired changes, then click **OK**.

**Removing IP addresses from the list of restrictions**

To remove an IP address from the list of addresses, on the Edit Restriction window, select the entry and click **Remove**. The restriction is removed and the Restrictions and Settings window reappears.

**Defining restrictions based on time of day**

To restrict users access to protected URLs targeted by this Web ACL based on the time of day the user seeks access, from the Edit Restriction window, select the **Time of day** restriction.
Figure 100: Time of day window

1. Click **Enabled** to activate the pane. The **Time of day** pane allows you to designate specific blocks of time when users specified in the Subject of this ACL entry can access protected URLs targeted by this Web ACL.

2. **Click and drag** your mouse to highlight the cells between the access start time and the stop time.

3. When the proper range is highlighted, click **OK**.
Defining restrictions based on range of dates

You may choose a range of dates when specified users can access protected URLs targeted by this Web ACL. To set a range of dates, from the Edit Restriction window, select the Range of dates restriction.

1. Click Enabled to activate the window.

2. Select a month, day and year from the beginning with list.
3. Select a month, day and year from the ending with list.
4. Click OK.

Figure 101: Date range window

Passing personalization data

The Personalization tab allows you to determine if and how personalization data will be passed via HTTP header fields. To pass personalization data, from the New Web ACL window, click the Personalization tab.

Note: The UWA prefixes all personalization data requests with “SafeWord-” when the request is passed through HTTP headers.
1. Configure the Personalization screen by selecting either:
   - **Web Application** from the To list for personalization data to be sent to the Web application.
   
   Or
   
   - **Web Browser** from the To list for personalization data to be sent to the user’s browser.

   Sending personalization data to the Web application is the more common option, as personalization generally takes place in the Web application on the server side, and not in the Web browser.

   **Tip:** You can have personalization data sent to both Web applications and Web browsers. To do so, select the **To Web Application** option, and choose the personalization data to pass there, then select the **To Web Browser** option, and choose the personalization data to pass there.

2. Select the **Pass data to the Web (Application/Browser) (via HTTP header)** check box to activate the available options and allow selected data to be passed as required for this Web ACL entry. Then select any of the following options:
   - **Insert userid in HTTP header** to have the user’s userid included in an HTTP header field called SafeWord-User.
   - **Insert role data in HTTP header** to have role data included in the HTTP header field called SafeWord-Authorization.
   - **Insert no Personalization Data in HTTP header** if you do not wish to have any of the authenticating users’ assigned personalization data inserted into the HTTP messages. If you choose this option, you have completed this procedure. Click **OK**. Otherwise, select one of the following then continue to the next numbered step.
Chapter 8: Using the SAM Express Management Console

Creating Web ACLs

- To instruct the UWA to insert all of the user’s assigned personalization data into the HTTP message, select Insert all Personalization Data in HTTP header, or
- to instruct the UWA to insert only some of a user's assigned personalization data, select Insert some Personalization Data in HTTP header. The Available and Selected list boxes become enabled, and you are able to specify exactly which personalization data should be inserted into the HTTP request or response message.

3. Select the personalization data attribute(s) that should be inserted into the HTTP request or response message from the Available list.

4. Click the Add button to move the attribute(s) to the Selected list.

5. The information in the Available list is set in the Personalization Data Configuration window. To access that window, from the main Admin Console select Configuration -> Personalization Data. For information about creating attributes, see “Understanding personalization data” on page 219.

6. Click OK. The window appears with the Web ACLs listed in the box.

Figure 103: New Web ACL create/edit window

The Web ACL is processed from the top down. Therefore, your most specific Web entries, those that target a narrowly defined group of users, should be placed at the top of your ACL list. More general Web entries should be placed toward the bottom of the list. The most general ACL should be the last one in the list.
Changing the order of protected Web entries

To change the order of the protected Web entries, from the ACL Entries pane of the New Web ACL window, select the URL you want to move, click the arrows to reorder it in the list of Protected URLs, then click OK to close the window.

What now?

At this point, you have created and tested a primary working account and secured it with (at least) a password and/or token, the default Administrator's account login password has been changed, and you have started to create groups, roles, login ACLs, and Web ACLs. Basically, your initial setup and configuration are done, and you can either start assigning tokens or adding users. To assign tokens, see “Managing authenticators” on page 194. To add users, see “Managing users” on page 205.
Managing authenticators

This section describes how to assign, resync, and modify tokens and authenticators from within the SAM Express Management Console.

Generating and importing MobilePASS software tokens

To generate and import MobilePASS software tokens, do the following:

1. Launch the SAM Express Management Console by selecting Start > Programs > SafeNet > SAM Express > SAM Express Management Console.
2. Log into the Console.
3. Click the Configuration menu, and then select MobilePASS Licensing. The MobilePASS Token Generation window appears.

4. Referring to your MobilePASS/SofToken® II Activation Certificate, enter the following information on the Licensing window:
   a. Enter the serial number from your MobilePASS/SofToken® II Activation Certificate in the Serial Number field.
   b. Enter the total number of units from your certificate in the Units field.
   c. Enter the Seed value in the Seed field.
   d. Enter your authorization code in the Authorization Code field.
   e. Enter your activation code in the Activation Code field.
   f. Select the Overwrite Existing on Import option check box to overwrite existing import records when new records are generated. If you do not want to overwrite existing records, leave the check box cleared.
g  Select **Generate All** or **Generate Range**.

If Generate All is selected, all available units associated with this license will be generated. In this case, continue to step 5 to generate and import the records.

If Generate Range is selected, the Start Serial Number field, and the Count field are activated. In this case, do the following:

- In the **Start Serial Number** field, enter the serial number of the first unit in the range of units that will be generated.
- In the **Count** field, enter the number of units to generate.

5  Click the **Generate and Import** button. The desired records are generated and imported into the SAM Express database.

---

**Assigning MobilePASS Software tokens with the Enrollment feature**

To use the MobilePASS Enrollment feature to assign MobilePASS Software tokens to SAM Express users do the following:

1  Open the SAM Express Management Console by selecting **Start > Programs > SafeNet > SAM Express > SAM Express Management Console**.

2  Locate the user to whom you are assigning a token.

3  Right-click the user entry and select **MobilePASS Enrollment**, or select **Tools > MobilePASS Enrollment**. The MobilePASS Enrollment window appears with the user’s name displayed.

Figure 105 shows two windows, the one that will display when you are enrolling the user now, and the one that will display when you will allow the user to self-enroll.
Figure 105: User Name window

Select the enrollment option for this user.

a. If you will enroll this user, click the **Enroll Now** option, click the **Next** button and continue to step 5.

b. If you will allow this user to self-enroll, select the **User will self-enroll** option, click the **Next** button, and skip to step 7.

c. Select a token policy from the Token Policy list.

d. Click **Next**.

Figure 106: Activation Code window

Enter the **Activation Code** generated from this user’s MobilePASS device, then click **Next**. The Enrollment Status window appears displaying the
enrollment status as Enrolled.

6 Click the **Finish** button.

7 Enter the **MobilePASS enrollment passphrase** that users must enter when they self-enroll, and then click **Next**. (Ensure you tell the user which passphrase they will need to use when self-enrolling.) The Enrollment Status window appears displaying the enrollment status as Pending.
8 Click the **Finish** button. You can notify your user that they should download the MobilePASS application to their device, and then they should go to User Enrollment Portal (see “Using the Enrollment Portal” on page 108). Provide them with the passphrase specified in step 7.

### Assigning hardware tokens manually

To assign tokens to users, do the following:

1. **(If not already open)** Launch the Console by selecting **Start > Programs > SafeNet > SAM Express > SAM Express Management Console**.

2. On the left side of the window, select the **Users** folder (or any admin group also containing users). A list of users appears on the right side of the window.
3 Locate the user to whom you will be assigning a token, right-click the user’s name and select **Edit** to display the **Edit User** window, then click the **Authenticators** tab and the **Pick authenticator** button.

**Tip:** If some of your users will share a token, assign the same token serial number to each user who will share it.

4 Select a SAM Express token, and enter its serial number in the **Serial Number** field of the Edit Serial Number window.

5 If you will be assigning a SoftPIN to this user, enter a four-digit PIN in the **SoftPIN** field. Otherwise, leave the field empty.

   Requiring a PIN with a user passcode adds a second layer of security to your system. If you will require users to authenticate with a token passcode and PIN, they must append the PIN to the end of the passcode. If they do not know their PIN, they will be denied access.

6 Click **OK**.

7 Distribute the token to the appropriate user(s). Be sure to tell them if they will need to append a PIN to the end of their passcode.

8 Repeat the procedure for each SAM Express user.

---

**Resynchronizing hardware tokens**

If a SAM Express token gets out of synchronization and its generated passcodes are rejected, it will need to be resynchronized by doing the following:

1 Locate and right-click on the user to whom the token is assigned, click the **Edit...** button in the **View User: (username)** window.
2 In the **Edit User: (username)** window, click the **Authenticators** tab, then highlight (click) the token you want to re-sync, then click the **Re-sync...** button to display the Re-synchronize Authenticator window (see Figure 111).

![Re-synchronize Authenticator window](image)

3 Enter the first then second token passcode (with appended SoftPIN, if applicable), and click the **Re-sync** button.

**Note:** If the token is a time-sync token, ensure that the time interval between the first passcode has expired before entering the second passcode. The second passcode should be different from the first passcode generated.
Modifying token profiles

This section describes how to modify token profiles, editing attributes such as their strength, group, etc.

To modify an existing token profile, do the following:

1. Select Find > Authenticator Profiles > Software/Hardware Authenticator.
2. Select Find all available, then click the Find button (or use Find all that match, and enter specific criteria).
3. Select the desired profile, right-click and choose Edit.

4. Set the Authenticator Strength for this profile.
   Authenticator strength sets the numerical value for this authenticator type. It can be used by the Authentication Engine to determine whether sufficient strength exists to access a resource protected by a fixed numerical strength.

   Tip: Assigned strengths should reflect how effective you perceive this type of authenticator to be. You may give this profile a higher strength if you also increase the minimum password length, and set passwords to expire in a shorter length of time.

5. Select a group for this profile from the Admin Group list.

   Note: You can view the properties for this group by clicking the View button next to the Admin Group field.

6. The Display Name field allows you to customize the field your users will see when they enter their passcode. Enter your user’s authenticator type.

7. Enter any supportive or defining comments in the Comments field.

8. For Alpine Time and/or Event-Synchronous tokens, the Additional Options fields allow you to set the following token synchronizing values (see “Resynchronizing hardware tokens” on page 199):
   - Sync Window: (time sync) the time span (plus/minus, in minutes) beyond current time in which an un-synchronized token will still authenticate, or (event sync) the number of token button presses (events) before the token becomes unsynchronized.
Chapter 8: Using the SAM Express Management Console
Managing authenticators

- **ReSync Window**: *(time sync)* the time span (in minutes) within which a token outside the Sync window can still authenticate (after an initial failure), or *(event sync)* the number of events beyond the sync window in which the token will still authenticate.

9 Click the **Configure** tab. The configuration settings for this profile appear.

*Note: If you are using tokens other than Gold 3000 and the Platinum, the Configure tab is not available.*

---

**Figure 113**: Hardware Authenticator Profile window (Configure tab)
10 Clear the **Password is echoed on input** check box if you do not want the one-time password for this profile to be displayed by the SAM Express agent while the user is authenticating.

11 Click **OK**.

---

**Fixed password profiles**

A fixed password profile defines the attributes associated with a particular password. These may include the authenticator strength, a minimum password length, and the duration of the password’s validity.

1 Select **Find > Authenticator Profiles > Fixed Password**, then select **Find all available** and click the **Find** button.

2 Select **fixed** (or any other fixed password profile you want to edit) from the Profile list. Fixed is a default fixed password profile that is shipped with your system.

3 Click the **Edit** icon to display the **Edit Fixed Password Profile** window.

![Figure 114: Edit Fixed Password Profile window](image)

**Tip:** When creating profiles, consider using a naming convention that offers visual cues as to the function of the profile (e.g. Medium Strength Fixed, or High Strength Fixed, etc.).

4 Set an **Authenticator Strength** for this profile. This is the numerical strength value for this authenticator type. The strength is used by the AAA Server to determine if sufficient strength exists to access a resource protected by a fixed numerical authenticator strength. For more information about authenticator strengths, see Table 10 on page 178.

**Tip:** The strengths you assign should reflect how effective you consider this type of authenticator to be. You may want to give this profile a higher strength if you increase the minimum password length, and you set passwords to expire in a shorter length of time.

5 Select a group for this profile from the **Admin Group** list.
Tip: To view the group properties, click the View button next to the Admin Group field.

6 Enter a name for this profile in the Display Name field. This might be a user-friendly version of the profile name. This name will be displayed to your users while they authenticate.

7 Enter any supportive or defining comments in the Comments field.

8 Click the Configure tab.

Figure 115: Fixed Password Profile (Configure tab)

9 Set a Minimum Password Length. The higher the minimum length, the more secure the password since it will be harder to guess.

10 Set the Passwords to remember. This is the number of expired passwords that will be remembered by the system. A higher setting means fixed passwords are more secure. A setting of 6, for example, will result in the user having to come up with 7 different passwords before they can use any one of them over again.

Important: The Passwords to remember feature affects administrator removal/replacement of fixed password authenticators. You cannot remove a fixed password and assign the same one to replace it. The user cannot use the same password again until the number of passwords to remember has been exceeded.

11 Select the Passwords are case sensitive check box to make the passwords case sensitive, and more secure.

12 Passwords that expire often are more secure than those that expire infrequently, or not at all. To set the expiration life span of this password, select the Password will expire check box, then choose from the following options:

- after this many days refers to the number of days you set in the Max password age field.
- with this many warning days is the number of days lead time a user will be advised that their password is about to expire.

13 Click OK when done.
Managing users

SAM Express Management Console features allow you to add (either manually or using the User Wizard), edit, assign roles to, and delete users.

If you are only adding a few users, you can manually create user accounts for them in the database (see “Creating user accounts manually” on page 206), or users can be added using the Wizard (see “Adding unprivileged users with the user wizard” on page 213). Finally, if your users are coming from a third-party user database, you can import their records using comma separated values.

Figure 86 shows the process and gives page references for information on each tab.
Creating user accounts manually

To manually create a new user account, do the following:

1. From the Console, select `Insert > User`. The Create a New User window appears.

General tab

2. Enter the user name in the `Username` field and select a group from the `Admin Group` list. The user will be placed in this admin group. The following characters are prohibited in the Username field: `#<>+;:\*/`.

   **Tip:** If the user will have a helpdesk user account, assign them to the highest-level user group in your user group hierarchy. Since they will only be able to assist users in the same group or any subgroup of their group, placing them at the highest level of your group hierarchy allows them to manage the widest distribution of users. If the user is to be designated a local (or group) administrator, assign them to whatever individual group hierarchy they will control.

Assigning roles to a user

3. (Optional) To assign a role to a user, from the General tab of the Create a New User window, click `Select`. The list of roles appears.

4. Choose the role(s) to assign to this user from the list of available roles. Use the Control key while clicking to select more than one role.

5. When you are finished assigning roles, click `OK`.

**Security Alert:** Roles should only be assigned if they conform to your security policy implementation.
Authenticators tab

6 To assign an authenticator to a user, from the Create a New User window, click the Authenticators tab.

Figure 118: Create a new user window, Authenticators tab

7 Choose one of the following options:

- **Add password** to assign a fixed password.

  If you have not created any other fixed password profiles, the default “Fixed” and “Emergency” profiles will be the only ones available. A fixed password profile describes characteristics about a common class of passwords. All passwords that reference the same fixed password profile will have the same properties.

  a Enter the user’s password in the **Fixed Password** field.

  b Re-enter the same password in the **Confirm Password** field.

  c (Optional) Select the **User must change password with first login**. Check box if you want users to change their password at the first login.

  d (Optional) Click the **View** button to see or modify the profile’s properties, or click **OK**.

- **Pick authenticator** to assign a hardware token or software authenticator. The Enter Serial Number window appears. (For MobilePASS release tokens only.)

  Enter the authenticator serial number in the **Serial Number** field. Hardware token serial numbers are located on the back of each token.

  MobilePASS serial numbers come from the MobilePASS authentication generation log file. (For MobilePASS release tokens only.)

  SofToken II serial numbers are listed in the SoftGen II output file, “keyphrase.txt”.
Using SoftPINs with a user account

To add a SoftPIN to this account, in the SoftPIN field, enter the four digit string you want to use as the SoftPIN for this token, then click OK. The authenticator type and the serial number appear under Passwords and Software/Hardware Authenticators.

**Note:** By default, the Authentication Engine allows SoftPINs to be appended to passwords. You can reconfigure the server to allow the SoftPINs to be prepended to passwords instead. For more information about reconfiguring the Authentication Engine so that SoftPINs can be prepended to passwords, see “Configuring the Authentication Engine for SoftPIN use” on page 259.

Advanced tab

(Optional) SAM Express allows you to define an expiration date for a user account, which is useful if you need to create temporary accounts.

8 To set an expiration for a user account, click the Advanced tab.

9 By default, accounts are set to never expire. Select the After option, then enter the desired expiration date and time.

**Note:** If you prefer to set up this account so it never expires, leave the Never option set.

Assigning an alias to a user account

Aliases are additional names, like screen names, that can be assigned to a user for login purposes, and point to the user’s record. Aliases might be variations of the user’s name, such as MSmith might be M_Smith, or SmithM.
Privileges tab

There are three levels of users in SAM Express: system administrators, group administrators (which includes local administrators and helpdesk staff), and unprivileged users. Each level of user has a different set of user privileges. In short, system administrators can perform all tasks, unprivileged users can perform no tasks, and local administrators and helpdesk staff fall in between.

System administrators have full access to all functions of SAM Express. Local administrators cannot modify system configurations, but they can view audit logs and conduct authenticator management tasks (adding, changing, or modifying authenticator profiles, to name a few). Local administrators can have READ/WRITE access to user records and security policy items. Helpdesk staff can be given privileges to assign, remove, and modify fixed passwords and SoftPINs, reset attack-locked accounts, view audit logs, and temporarily disable or enable users.

To define user privileges based on administrative level, do the following:

10 Click the Privileges tab from the Create a New User window.

11 Based on your user’s administrative level, choose the appropriate option from the following:
   - If your user is an unprivileged user, that option is already selected, click OK to complete the user privilege process.
   - If your user is a member of the helpdesk staff, choose Helpdesk staff, then refer to “Defining privileges for helpdesk staff” on page 210.
   - If your user is a local administrator, choose Local administrator, then refer to “Defining privileges for local administrators” on page 211.
   - If your user is a system administrator, choose System administrator, then refer to “Defining system administrator privileges” on page 212.
Defining privileges for helpdesk staff

Helpdesk staff users are able to offer first tier support to your users. A helpdesk staff user should be given enough privileges to handle most of the authentication problems that your users may encounter. Figure 121 displays the privilege selections available for helpdesk staff.

12 Ensure that Helpdesk staff is selected under Administrative Level. Then choose from the following privileges.

- **Remove software/hardware authenticators**: allows this user to remove software and hardware authenticators from a user record. For example, a helpdesk user will be able to remove a user’s hardware token if a user reports that his hardware token has been stolen or destroyed. Clicking this option will check and disable the Temporarily disable/enable hardware authenticators option.

- **Temporarily disable/enable hardware authenticators**: allows authenticators to be disabled or enabled by helpdesk staff. For example, helpdesk staff will be able to temporarily disable a user’s hardware token if that token has been lost or forgotten for a period of time.

- **Add/Remove/Change fixed passwords**: allows helpdesk staff to remove old, compromised, or unneeded fixed passwords from a user record. Helpdesk staff will be able to grant and remove temporary emergency passwords for users who have lost their hardware tokens. Clicking this option will check and disable the Change existing fixed password option.

- **Change existing passwords**: allows helpdesk staff to change user’s existing passwords.

- **Add/Remove/Change SoftPINs**: allows helpdesk staff to add, delete, or remove SoftPINs from a user record. Helpdesk staff will be able to allow a user to secure his token with a SoftPIN. Clicking this option will check and disable the Change existing SoftPIN option.
• **Change existing SoftPINs**: allows SoftPINs be changed for a user. Helpdesk staff will be able to field requests for SoftPIN changes.

• **Select Reset attack lock** to allow a user account that has been attack locked (locked from repeated unsuccessful authentication attempts) to be cleared by helpdesk staff.

• **Select Temporarily disable or enable users** to allow helpdesk staff to temporarily disable or enable users. Helpdesk staff will be able to temporarily disable a user if it is expected that this user will not be authenticating for a known period of time. This feature is useful during a user leave of absence.

• **Select View audit logs** to allow helpdesk staff to view audit logs that show a history of user authentication activity within SAM Express.

When you are finished, click **OK**.

**Defining privileges for local administrators**

Local administrators have considerable administrative authority. They are able to oversee the user management of a subset of the SAM Express user database, and they may be given the authority to create other local administrators with equal or fewer privileges. Figure 122 displays privilege settings for local administrators.

**Figure 122**: Local administrator privilege settings

13 Ensure the **Local administrator** option is selected under Administrative Level if this user will be given local administrator privileges. Then choose from the following options:

- **User records READ-ONLY** allows the local administrator to only read a user’s record. A local administrator would need **READ/WRITE** privileges to create, modify, and delete users within his group hierarchy.
Managing users

- **Security policy READ-ONLY/READ-WRITE** allows the local administrator to read, or create and modify security policy elements (i.e. ACLs, ACL entries, and roles). Local administrators can be given complete control of the security policy within a subset of the your deployment. For instance, if the user population is organized by physical location, the local administrator for that location can be given the authority to create or modify the location’s security policy.

- **View audit logs** allows the local administrator to view audit logs that show a history of user authentication activity within SAM Express.

- **Select Authenticator management** to allow the local administrator to create, modify, and delete authenticator profiles, and import hardware authenticators.

- **Edit local administrators** allows local administrators to create, delete, or edit other local administrators. The local administrator can still view other local administrators if not selected. This option is only available when the local administrator has READ-WRITE privilege on user records.

When you have made all your selections, click **OK**.

**Note:** Local administrators can only use these privileges within their assigned group hierarchy.

Defining system administrator privileges

A system administrator is the highest level of administrator, therefore having complete access to all privileges within SAM Express.

14 Ensure that **System administrator** is selected under Administrative Level, then click **OK**.

![Figure 123: System administrator privilege settings](image-url)
Adding unprivileged users with the user wizard

Unprivileged users are users who do not have administrative-level privileges. They are also referred to as “regular” users in SAM Express. These users can quickly be added into the system using the user wizard. To add an unprivileged user with the user wizard, from the Console, select a non-global group into which you want to add a user, then do the following:

1. Select Insert > User with wizard.

2. Enter the new user’s name in the User field, and click Next.
   The Select an Authenticator Type window appears.

3. Select an authenticator type for this user from the Authenticator Type list.

4. Click Next.
   - If you selected Software/Hardware Authenticator, the Enter Serial Number window appears. Enter the serial number for the authenticator you will be issuing to the new user in the Serial Number field.
   - If you selected fixed password as the authenticator type, the Select a Fixed Password Profile window appears. Select a password type from the Fixed Password Profile list. The available profiles are fixed and Emergency. The Enter a Fixed Password window appears, in which you will enter then re-enter the password.

5. Click Next.
Chapter 8: Using the SAM Express Management Console

Managing users

**Important:** The Emergency fixed password profile should only be used by administrators or helpdesk staff who need to assign a temporary fixed password authenticator to a user whose hardware authenticator has been lost or compromised.

**Tip:** If you want to see the properties of the selected fixed password profile, after selecting it, click the View button.

**Important:** Leave the User must change password with first login check box selected. This forces the user to select a password known only to them when they log in. Users always have the option to change their password, whether or not you check this option. This forces them to do so the first time they log into SAM Express.

6 If you want to add another authenticator (in the Add Another Authenticator window), click Yes and repeat the previous procedure. If you do not want to add another authenticator, click No.

**Tip:** A user can be assigned up to three authenticators in any combination. SAM Express allows a user to possess multiple authenticators for various authentication scenarios. For instance, your security policy might require that a user present a one-time password from a hardware authenticator when authenticating remotely, but that the user only present a fixed password when authenticating internally.

**Figure 126:** Select an Admin Group window

7 When the Select an Admin Group window appears, select the non-global group to which this user will be assigned from the Admin Group list, then click Next.

The Assign Roles window appears.
Assigning roles is optional, and you may prefer to assign them to multiple users at once. For more information about doing so, see “Assigning role(s) to multiple users” on page 215. If no role is to be assigned, click Finish. If you want to assign a role to this user, click Select.

Select the role(s) you want to assign to this user. Use the Control and Shift keys to select more than one role. The Assign Roles window appears with the roles listed under Role Names.

Click Finish to complete the procedure.

Assigning role(s) to multiple users

Occasionally, it may be more convenient to assign them to a large number of users who are already a part of a particular group. The SAM Express Management Console allows this to be done quickly and easily. To assign one or more roles to a particular group of users from the Console, select a user group from the left pane.
1  In the Console, select the users to whom you want to apply a role, then select **Tools > Assign Roles**.

Figure 129 shows the resulting window.

Figure 129: Selected names and Select Users window

**Tip:** If you highlight users directly, their names appear in the Selected Users field of the Select Users window.

2  Or, to locate one or more users who meet some specific criteria, click **Find > Users**, and in the Find User entries window, select **Find all that match**.

**Tip:** The Find all available option is not recommended if you have a large user population. It is best to narrow down your search results by supplying search criteria with the Find all that match option.

3  When you have chosen the search criteria, click **Find**.
4 In the Select Users window, click the **Add** button to move the users to the **Selected Users** list, then click **Next**.

**Figure 130**: Choose Roles window

5 In the Choose Roles window, select one or more roles to assign to these users from the **Available Roles** list and click **Add** to place them in the **Roles to Assign** list.
6  (Optional) Select the **Remove user's current roles** check box to remove any roles the user was previously assigned, then click **Finish**.

---

### Deleting a user record

Certain events, such as an employee leaving an organization, require the deletion of a user record.

1  Select **Find > Users**.

![Figure 131: Find User entries with username](image1)

2  In the Find User window, enter the username in the far right field.

3  Click **Find**.

   The Find results: User entries window appears with the requested username listed.

![Figure 132: Find results window](image2)

4  To delete the user's record, highlight the name, then click the **Delete** icon. The Confirm Deletion window appears, asking if you want to delete the user entry.

5  To permanently delete this user record, click **Yes**.
Understanding personalization data

SAM Express allows you to store personal data about the users who access your resources. Your helpdesk staff might use personalized data to verify information about a user. This could prove helpful before assigning a temporary authenticator, or when you need to change a user’s SoftPIN.

Data elements

Personalized data is configured using specific attribute-value pairs called personalization data elements. Personalization data elements can be stored at the user record level or at the role level. A user may also inherit elements from the roles that he has been granted.

The data dictionary

Before you can begin to assign personalization data elements to users and roles, you must enter the personalization data attributes into the database. By entering these attributes, you create a data dictionary of personalization attributes. Since system administrators are ultimately in control of the kinds of data that are stored about a user, only system administrators are allowed to edit this data dictionary. These administrators will optionally be able to specify a range of allowable values for any given personalization data attribute.

Creating personalization data

To create personalization data attributes, do the following:

1. In the SAM Express Management Console, click Configuration > Personalization Data.

   The Personalization Data Configuration window appears.
2 Enter a name in the **Attribute** field. For example, enter “Full Name” to collect the full names of your users.

3 (Optional) Enter descriptive information in the **Description** field. Descriptions state the purpose of the attribute to fellow administrators.

   Once your data dictionary is complete, you may begin defining data at the user and role record level. You define data by setting up value restrictions for your attributes. For example, you might enter the full names and language preferences of each user on their user records.

You can place restrictions on the values of personalization data attributes. As an administrator you have the choice of allowing any value for a given attribute, or allowing only one value from a set of predefined values.

4 Click **Allow any value** to create an attribute like “Full Name”, that does not lend itself to a discrete set of possible values. If you choose **Allow any value**, click **OK** to complete the attribute.

5 Select **Allow only the following values** to restrict an attribute’s value.

   A good example of an attribute you would restrict is language preference. You would restrict the value of this attribute by defining a set of allowable languages.

   ![Figure 134: Adding values to attributes](image)

   When you restrict a value, you must also supply the list of specific values that are allowable. To add allowable values:

   a Click the **Add** button.

   b Enter an allowable value for the personalization data attribute that you are creating under **Allow only the following values**.

   c Click the **Add** button again to enter additional values.

   d When you are finished adding values, click **OK**.
The attributes and any descriptions appear in the attribute list. Click **OK**.
Using the Attack Lock feature

Attack lock prevents “brute-force” attempts to gain access to a user’s account by repeatedly trying to log in with different passwords. You can determine the number of attempts that are allowed before SAM Express locks the account. Occasionally, a user may inadvertently self-trigger the attack lock feature with repeated unsuccessful login attempts, or be locked out because someone else tried to access their account.

The following actions and results should be noted:

- If the user enters a bad SAM Express OTP, but the proper Windows password, the Active Directory (AD) attack lock will NOT increment.
- If the user enters a bad SAM Express OTP AND a bad Windows password, the AD attack lock will NOT increment.
- If a user enters a valid SAM Express OTP with an invalid Windows password, the AD attack lock will be incremented.

Setting attack lock for individual users

In some cases, you may want to disable the attack lock feature for an individual user rather than as a global user attribute. The process is done as follows:

1. Locate the\servers.ini file (found in <Install_Dir>\SERVERS\Shared).
2. Add the following line to the .ini file:
   Disable_Attack_Lock_Attribute=DisableAttackLock
3. Restart the Authentication Engine.
4. Modify the user’s record to add personalization data = DisableAttackLock.

Resetting a locked account

1. Select Find > Users and locate the user account that needs to be reset.

   **Tip:** A user’s account will automatically reset after a configurable amount of time as long as the **AAA clears attacked -locked accounts** option is selected. This option is on the General tab when you configure SAM Express.

2. Select and right-click the user’s name, and select Edit.

   A window appears stating that this user’s account has been attack locked.

3. Click OK.

   The Edit User window appears.

4. Clear the **Account locked out** check box.

5. Click OK and inform the user their account has been reset.
Editing personalization data attributes

To edit an attribute or its description from the Console, select Configuration > Personalization Data.

1. When the Personalization Data Configuration window appears, select the attribute you want to edit from the list of attributes.
2. Click the Edit button.
3. Change the attribute or its description, then click OK. The edited attribute appears in the list of attributes.

Removing personalization data attributes

To remove an attribute from the list of attributes, from the Console, select Configuration > Personalization Data.

1. When the Personalization Data Configuration window appears, select the attribute you want to remove from the list of attributes.
2. Click the Remove button.
3. Click OK. Once your data dictionary is complete, you may begin defining data at the user and role record level.
Modifying user personalization data

You may choose to store personal information about users in the application. Personalized data is configured using specific attribute-value pairs called personalization data elements. Personalization data elements can be stored at the user record level or at the role level. A user may also inherit elements from the roles that he has been granted. Before you can begin assigning personalization data elements to users, you must define and enter the set of attributes into the SAM Express database. For more information about setting up personalization data attributes, see “Creating personalization data” on page 219.

Modifying a user's attributes

To add, edit, or remove a user’s attributes:

1. Right-click the user’s name, and select Edit, then in the Edit User window, select the **Personalization Data** tab.

2. To add an element to a user's record, click the **Add** button.

   ![Figure 136: Create a New User window (Personalization data tab)](image)

   1. Select an attribute from the **Name** list.
   2. Enter a **Value** or select one from the **Value list** depending upon the attribute you have chosen.
   3. (System Admins only) If you are a system administrator, you can click the **Add New Personalization Data** button to invoke the screen that allows you to introduce new personalization data attributes into the system. This set of attributes can be thought of as a “dictionary” of SAM Express personalization data.
4 When you are finished, click **OK**.

To edit an element in a user’s record, from the Personalization Data tab of the Create a New User window, highlight the element to be edited. Click **Edit**, make the desired changes, then click **OK**.

To remove an element from a user’s record, from the Personalization Data tab of the Create a New User window, highlight the element to be removed. Click **Remove**, then click **OK**.

The SAM Express import feature allows you to move large numbers of users from a third-party user database into SAM Express. When you import a large number of users, you must save the file as an ASCII file, with either a .csv or a .txt extension, and you must use commas as delimiters. The use of commas as delimiters is important because if the user database to be exported has the user name syntax “Last name, First name”, the comma between the last and first name would be interpreted as a delimiter, and the output file would have only last name in the user name field, then first name in the comment field. The only required field in each user record is the user name; all other fields are optional. The following other rules apply:

- These characters are prohibited: #<>+;,*:"?|\n- Blank spaces are allowed
- Maximum length for each userid is 128 characters
- Syntax for each user entry is: **userid,comments**
- If comments are not used, the user record can be terminated after the user name
- If a user record contains aliases, they are allowed by syntax: **userid:alias1:alias2** (For example: **mike_smith:msmith:smithm,comments**)

To import users, do the following:

1 From the Console main menu, select **File > Import > User (CSV)**.
1 Click **Browse** in the Import User - Select File window.
2 **Browse** to locate the previously exported comma separated value- (CSV) formatted user file you want to import.
3 Click the **Open** button when the file has been located and selected. The Import User - Select Admin Group window appears.
4 In the Import User - Select Admin Group window, select a non-global Admin Group from the Admin Group list. All your imported users will be placed into this admin group, then click Next.

5 In the Select Role(s) window, select a role(s) to give to your imported users from the Available Roles list, then click Add to place that role in the Selected Roles list.

6 Click Import.
   The Import Completed window appears with the status of your import.

7 Click OK.
   The Import User Continue window appears and asks if you want to import more users. Click Yes (and repeat the process) to import more users or click No if you are finished importing users.

8 To verify successful import, select the Admin Group where you just imported your user records.
   The right pane shows a list of the users you just imported. Their icons are gray, indicating that they do not yet have authenticators assigned to them. Now that you have imported your user records into the system, you will need to assign authenticators to them.

**Tip:** Once a user is assigned an authenticator, their icon no longer displays in gray, indicating that they can authenticate to SAM Express.
SAM Express records all authentication and administration activity into audit logs. These audit logs are stored in the SAM Express database, and are easily accessible for monitoring enterprise activity and for creating reports (in the SAM Express Management Console). The audit logs are viewable by all system administrators, and by local administrators and helpdesk staff who have been given the appropriate privileges.

**Querying audit logs**

SAM Express allows you to query specific audit logs using a variety of search parameters. You may choose to search for all audit logs, search for those that match a specific date range, and/or search using specific parameter filters that you define. Table 11 lists the search parameter filters and their functions.

**Table 11: Audit Log search parameter filters**

<table>
<thead>
<tr>
<th>Search Parameter Filter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performed by</strong></td>
<td>Use this filter to identify authenticator and administrative activity performed by a specific user (by userid). For authentication audit logs, this specifies the user that attempted authentication to SAM Express. For all other event types, this specifies the user that performed the particular action described by the audit log.</td>
</tr>
<tr>
<td><strong>Event type</strong></td>
<td>Use this filter to search by:</td>
</tr>
<tr>
<td></td>
<td>• Authentication</td>
</tr>
<tr>
<td></td>
<td>• Insertion</td>
</tr>
<tr>
<td></td>
<td>• Deletion</td>
</tr>
<tr>
<td></td>
<td>• Modification</td>
</tr>
<tr>
<td></td>
<td>• Authenticator import</td>
</tr>
<tr>
<td></td>
<td>• Backup or restore</td>
</tr>
<tr>
<td></td>
<td>• Data error</td>
</tr>
<tr>
<td></td>
<td>• Log archive operation</td>
</tr>
<tr>
<td></td>
<td>• Administrative session</td>
</tr>
<tr>
<td></td>
<td>• User session start/stop</td>
</tr>
<tr>
<td></td>
<td>• Resign operation</td>
</tr>
<tr>
<td><strong>Authentication status</strong></td>
<td>Use this filter to specify a search of authentication activity that resulted in either success or failure. Though this filter is relevant only for searches on authentication activity, it is not necessary to specify an ‘Event type’ filter with a value of ‘Authentication’, since it is implicitly assumed.</td>
</tr>
</tbody>
</table>
Chapter 8: Using the SAM Express Management Console

Managing and viewing audit logs

Searching the audit logs

To search the audit logs, from the SAM Express Management Console, select Find > Audit Logs.

The Find Audit Log Entries window appears.

<table>
<thead>
<tr>
<th>Search Parameter Filter</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Admin Group</td>
<td>Use this filter to narrow down the authentication and administration activity specific to a particular admin group.</td>
</tr>
<tr>
<td>Logins where role</td>
<td>Use this filter to specify a search of authentication activity in which users were either granted or denied access due to a particular role. Though this filter is relevant only for searches on authentication activity, it is not necessary to specify an ‘Event type’ filter with a value of ‘Authentication’, since it is implicitly assumed.</td>
</tr>
<tr>
<td>Database entry</td>
<td>Use this filter to narrow down the audit logs that pertain to administrative activity on a specific entry in the database (for instance, a specific user account or token record). This filter is relevant only for audit logs that do not describe authentication attempts, and therefore is ideal for tracking the modification history of specific database entries.</td>
</tr>
</tbody>
</table>

1. Select Find all available, or refine your search using the search filters.
2. Select the Match dates check box to search for audit logs in a date range that you will specify, or clear the Match dates check box to return all available audit logs, regardless of date. You may use the Match dates check box with Find all available or Find all that match.
3. Click the Find button. If the system locates one or more audit log entries that match the search criteria you selected, they will be listed.
Viewing a specific user's authentication activity

To view a specific user’s authentication attempts:

1. Select **Find > Audit Logs**.

2. Select **Find all that match**, then enter the user’s name in the far right box.

3. Select the **More** button.

4. Select an **Event type** from the left side drop-down box, then select **Authentication** from the right side drop-down box.

5. If desired, specify a date and time range to narrow down the results, then click the **Find** button.

Viewing the last successful user login attempt

To activate the last successful user login attempt feature, browse to and locate the file `sccservers.ini` (found in `<Install_Dir>\SERVERS\Shared\`), and do the following:

1. To store the last successful user login attempt in the database, add the line **Store_Last_Access_Time=on** as the last line in the file, save the file, then restart the Authentication Engine.

   The information will be available via the Reporting Tool.

2. To also enable viewing via Personalization Data, add the line **Last_Access_Attribute_Name=Last_Access_Time**, then save the file.

3. Using the SAM Express Management Console, add a Personalization Data Attribute **Last_Access_Time**.

4. Restart the Authentication Engine.
Viewing specific entry details

Log summaries allow you to review the details of an audit log. To review an entry’s details, find the specific log you are interested in, and from the Search Results: Audit Log Entries window, double-click on the entry.

Troubleshooting with the Audit Log Monitor

The Audit Log Monitor allows you to troubleshoot authentication and administration activity in real-time. For example, when an end user calls into a helpdesk about an authentication problem, the helpdesk staff can launch the Audit Log Monitor to display only authentication events concerning that end user. As the user goes through successive authentications, logs describing these attempts automatically appear in the Audit Log Monitor.

The Audit Log Monitor is similar to the traditional mechanism for viewing audit logs, but the difference is that the Audit Log Monitor continues to refresh the log output periodically, sparing administrators from having to manually perform the refresh function.

The Audit Log Monitor is available to the same set of users who are allowed to view audit logs. Therefore, system administrators can use it, and helpdesk staff and local administrators may use it if they have been given the privilege to view audit logs in SAM Express.

*Note:* If the Audit Log Monitor is run on a remote Console (a machine other than the SAM Express Server machine), synchronizing the clocks on the two machines results in optimal performance regardless of differences in time zones.

Launching the Audit Log Monitor

To launch the Audit Log Monitor, select **Tools > Audit Log Monitor**.
Choosing logs to monitor

You may choose to monitor all available audit logs or a particular subset, say, for an end user.

1  To monitor a specific user’s events, specify the user and the types of audit logs that you wish to monitor.

2  Click the Find button. The Monitor Results: Audit Log Entries window appears displaying all authentication activity performed by the user. The administrator can review the authentication process with the end user, and use the audit logs to debug the user’s authentication problem.

**Important:** By default, the Audit Log Monitor refreshes every 60 seconds. You may find that a different refresh period works better for your particular environment. To manually set the refresh period, change the value in the `Monitor_interval_in_seconds` property in the Console’s `client.ini` file (in `<install_dir>/AdminConsole`). After changing the value, restart the Monitoring tool for the changes to take effect.

Managing audit log archives

Every system event is recorded into audit logs which, over time, can become quite large, and can negatively affect system performance. To avoid this, configure SAM Express to remove the log entries from the database and save them to a local file after a set period of time.

The Admin Server handles all archiving operations by constantly monitoring the age of audit logs stored in the database. Once particular audit log entries reach a certain age, they are removed from the database and archived to a local file. Once archived, the Console and the command line reporting tool cannot retrieve them.

Each time audit logs are archived, a file is created and given a name based on the date and time of the first log in the archived set. To manage your audit log archive sets, from the Console, select **File > Log Archives**. The Manage Audit Log Archives window appears.
Managing and viewing audit logs

Figure 140: Manage Audit Log Archives window

The Manage Audit Log Archives window displays all previously archived sets of audit logs. The sections that follow explain how to load, unload, delete, and configure the time when logs are archived.

Tip: If you have not archived any audit logs yet, the list here will be empty.

Loading an archived audit log file

The Manage Audit Log Archives window lists all existing archive sets, and indicates whether or not the sets are currently loaded. When archive sets are loaded, the logs contained in them are available for searches and reports.

To load a previously archived file, select the desired archive set, then click Load. If the load was successful, the word Yes appears in the Loaded column. The audit logs from the archive file are now available in the SAM Express database. Click OK to close the window.

Unloading an archive set

The Manage Audit Logs Archives window allows you to unload archive sets from the database server. Unloading an archive set deletes its previously loaded contents from the SAM Express database, but has no affect on the disk file where the archived set is stored.

To unload a set from the database, select the archive set you want to unload from the list on the Manage Audit Log Archives window, then click Unload. The word No appears in the Loaded column and the log entries from that set are no longer available on the database server, but they are archived on the Admin Server. Click OK to close the window.

Important: Loading and unloading archives start new connections to the Admin Server. Login credentials will be requested again for those new connections if the initial Console login was performed more than eight hours prior.
Deleting an archived audit log file

When you want to completely remove an archive set from the system, you use the Delete button on the Manage Audit Log Archives window.

To delete an archive file, select the file you want to delete, then click Delete and answer Yes to confirm your decision. When the file is successfully deleted, it will be removed from the list. Click OK to close the window.

Important: This will permanently delete the archive set.

Configuring the archival of audit logs

To archive audit logs you must designate a period of time after which audit logs of a chosen age will automatically get archived. The Audit Log Archival pane on the Manage Audit Log Archives window allows you to define the age (in hours) after which the designated logs automatically are archived into an archive set.

Automatically archiving audit logs

To automatically archive audit logs of a certain age, on the Manage Audit Log Archives pane, in the Archive Audit Logs Older Than field enter the number of Hours that logs should exist before they are archived.

Click OK to save this value.

Archiving audit logs immediately

To archive off all the audit logs immediately, click Now on the Audit Log Archive pane. SAM Express archives currently stored audit logs and removes them from the system. This may take a few minutes in larger databases. Once done, the archived log sets appear in the list window.

When you are done, click OK to close the window.

Log archival impact on reporting

The most common reporting scenarios will involve the export of audit log data. With audit logs, you can determine many useful statistics that describe the authentication activity in your organization. However, you must ensure that the appropriate amount of audit log data stays resident within the Admin Server for long enough so that it can be exported through the new reporting mechanism. Specifically, you must ensure that the audit log archival period is sufficiently large. If you intend to run weekly reports based on a week’s worth of audit log data, then you must ensure that your audit log archival period is at least seven days.
Using advanced archiving features

One of SAM Express’s advanced features is the audit logs archives keywords functionality. Table 11 lists keywords that can be used when loading and unloading archive files. The values here can be customized to best suit your environment by changing them in the `sccservers.ini` file, found in `<Install_Dir>\SERVERS\Shared\`.

Table 12: Audit log archives keywords

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Function</th>
<th>Recommended Setting Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>ArchiveWorkerThreads=20</td>
<td>Controls the number of threads used for loading archive sets. The higher the number, the faster the loading operation will work, but the more memory it will require.</td>
<td>Optimum values will vary from system to system, but a range of 5 to 40 threads is reasonable. Set to 0 to revert back to the single thread implementation of versions prior to version 3.1.</td>
</tr>
<tr>
<td>ArchiveLogsInBatch=50</td>
<td>Controls the number of logs in a batch per thread.</td>
<td>Optimum values will vary from system to system, but a range of 20 to 100 logs is reasonable.</td>
</tr>
</tbody>
</table>
SAM Express enables you to generate reports that summarize and detail all administrative and authentication activity, and the SAM Express Management Console allows you to export raw data that can easily be imported into a third-party reporting package. This gives you the ability to convert raw logging data into highly-customized reports describing your organization’s activity.

Along with audit logs, you can export any subset of SAM Express data elements that you have introduced or created, including users, admin groups, roles, and authenticators. For example, you can easily generate reports that identify users who do not yet have an assigned authenticator, and identify the authenticators that remain unassigned to users. Once you have exported your raw data, the reporting possibilities are endless.

SAM Express exports specified raw data into Microsoft Excel worksheet files. Using Excel macros, you may find that a third-party reporting package is not even necessary to generate useful reports. However, if you have a favorite reporting package, it will certainly accept data from either the native Excel worksheet format (XLS), or from the CSV (comma separated value) format (which Excel is capable of generating).

Creating reports

To create reports, connect to an Admin Server and select **Tools > Reports**.

In the Report Definition window you define the categories of raw data that you would like to export (typically audit log data, user data, and perhaps software/hardware authenticator data). For example, to generate reports concerning the authentication activity, you would export authentication audit logs; to generate reports on users who are attack-locked or are otherwise disabled, you would export user data; and to generate reports on unassigned tokens, you would export software/hardware authenticator data.

1. Select the check boxes in the Included column for the categories of raw data that you wish to include in your report.
Tip: To clear all the check boxes, select the Include None button.

2 (Optional) To refine the criteria for this report, select the Refine Criteria button and use Find to refine the category.

3 (Optional) To view a summary of the report criteria, select the Content Summary button. The View Report Filter Details window appears summarizing the report’s contents. When you are finished viewing the summary, click OK.

4 Once the data is in Excel, you can sort rows, or use Excel macros to generate pie charts and bar graphs to summarize authentication activity. You can also move the data to your reporting package.

Report templates

The report generation window allows you to specify the types of raw data to export. By checking the check box associated with a category, you are adding that report filter to a report template. A report template simply defines a set of data to export. This set may comprise a single category (e.g. only audit logs) or several categories (e.g. audit logs, users, authenticators).

Saving a report template

The Save Template button allows you to store the settings of a particular report as a report template. Figure 142 shows the details of a report template that fetches all authentication audit logs, users and authenticators in an admin group called Pacific.

Figure 142: Filter Details window

Loading a report template

The Load Template button on the report generation window allows you to retrieve a report template from disk. Templates allow you to define a report that will be run frequently and thus ensure that you always fetch the same categories of raw data. For example, if on a weekly basis, you would like to analyze the authentication activity of the users in the Pacific admin group, you might create and save a report template called weekly-pacific_auth.tpl that fetches authentication audit logs. Then, once a week, you would invoke the report definition dialog, load this report template, and execute the report.
Report worksheet generation

The SAM Express Management Console will sometimes generate more than one worksheet for a given report template. When a report template contains more than one categories (e.g. users and tokens), an Excel worksheet file will be created for each data type. In addition, the `Number_of_lines_per_Excel_sheet` property in the Console configuration file (`client.ini`) governs the number of rows that will be written to any one particular worksheet file. By default, this property is set to 5000. For example, if you export 15000 audit logs during the report generation process, the first 5000 rows will be stored in one worksheet file (e.g. with the name “weekly-logs.xls”) and the remaining 10000 rows will be stored in a second and third worksheet file with a similar name (e.g. “weekly-logs_0.xls”). The client.ini file is located in the Administration Console directory (`.\SAM Express\AdminConsole`).

Whenever the Console creates more than one worksheet file for a single report, it will also create a **VBScript** file that can be used to merge all of the individual files into one file with a worksheet for each file. This VBScript can only be used on Windows platforms. This script file will be named similarly to the generated worksheet files. To continue the example, this script file would be called “merge-weekly-logs.vbs”. The output of this script would be a single Excel worksheet file called “merged-weekly-logs.xls”.

*Note:* If you change the value of the `Number_of_lines_per_Excel_sheet` property in the Console configuration, you must restart the Console for the new value to take effect.

Generating reports from the command line

In addition to using the Console to generate reports, you may also generate reports using a command line tool that is packaged with the Console. This gives you the ability to create your own shell scripts that can trigger the creation of several reports in one pass. Additionally, you can use your operating system’s native scheduling features to call your custom shell scripts on scheduled intervals. By doing so, you can automate the process of generating periodic reports (for example, to track authentication activity on a weekly basis).

The command line reporting tool, called `report.bat` can be found in the Console installation directory (`.\SAM Express\AdminConsole`). In the same way that the Console can be installed and executed on a remote machine (i.e. executing on a machine other then the SAM Express server machine), so can the command line reporting tool.
As the command line reporting tool is simply a text-based shell script, it is easily configurable. You will need to specify the name of the SAM Express server machine, the port on which the Admin Server is listening, and the userid and password of an administrative user through which the report queries can be executed. Table 13 details the variables that are defined in both versions of the shell script.

**Table 13: Shell script variables**

<table>
<thead>
<tr>
<th>Variable Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADMIN_HOST</td>
<td>Specify the IP address or hostname of the machine on which the SAM Express Admin Server is installed</td>
</tr>
<tr>
<td>ADMIN_PORT</td>
<td>Specify the port number on which the SAM Express Admin Server is listening (By default, this port number is 5040).</td>
</tr>
<tr>
<td>ADMIN_USER</td>
<td>Specify the userid of the administrative user account that will execute the desired report queries. This user account must use a fixed password to authenticate to SAM Express.</td>
</tr>
<tr>
<td>ADMIN_PASSWORD</td>
<td>Specify the password for the named administrative user. This value need not be defined in the shell script as it can be supplied as a command line argument to the reporting tool. If you do decide to define the password in the shell script, you should ensure that the script is properly secured, either via operating system security features or via physical machine security.</td>
</tr>
</tbody>
</table>

**Using the command line reporting tool**


The first two arguments are required. The first argument specifies the location of a saved report template. Refer to “Report templates” on page 236 for instructions on how to define and save a report template. By default, report templates are saved in the “templates” subdirectory of the Console installation. The second argument specifies the location of the target Excel worksheet file. The Console installer creates a subdirectory called “reports” in which all generated reports can be contained.

The third argument is optional and allows you to specify the password of the administrative user that is used to execute the desired report queries. This is useful in situations where it is not appropriate to store the cleartext fixed password in the shell script.
For example, assume you have created a report template called `all-logs.tpl` that fetches all available audit log data in the SAM Express database and you wish to store this data in an Excel worksheet file called `all-logs.xls`.

From the Windows command line, you might use: `report.bat templates\all-logs.tpl reports\all-logs.xls mypassword`.

### Exporting data into Excel worksheets

An additional method exists for exporting data into Excel spreadsheets. The dialogs that appear when you choose categories from the Find menu have a button called Export. Choosing this button causes the Console to export the search results data directly into an Excel spreadsheet. You can export any SAM Express data including audit logs, admin group data, user data, login and data, roles, profiles, tokens, and sessions data.

When you select the Export button, SAM Express prompts you to name the Excel worksheet file it will create. All data resulting from your search is written directly to the new worksheet file.

**Note:** If you are running the Console on a Windows platform that also has Microsoft Excel installed on it, the Console automatically provides you with the option to view your new report in Excel once it is created.
Database-related tasks

The SAM Express database contains all user, token, and access policy data, and should be backed up on a regular basis, or anytime a change has been made.

Backing up your database

**Important:** Backing up, restoring, and log archive operations start new connections to the Admin Server. Login credentials will be requested again if the initial SAM Express Management Console login was performed more than eight hours prior.

1. Select File > Backup Database.

| ![Figure 143: Backup Database window](image)

2. Enter the file name in the **Backup to file** field.

3. (Optional) Select the **Do not backup audit logs** check box if you prefer to not back up these records.

4. (Optional) Select the **Encrypt records** check box if you wish to encrypt the records.

5. Enter and re-enter the entire encryption key string in the **Encryption key** field.

**Note:** The key text string you use here must be used again if you restore your database from this backup file. Be sure to keep the key text string in a safe, but accessible place.

6. Click **OK** in the Export Completed window.

Restoring your database

**Important:** To maintain existing configuration data when there is an LDIF file to be restored on a newly installed database, the backup LDIF file must be restored before doing anything else on the system. This ensures the database will not be corrupted after restoration. If there are already users in the database, before restoring an LDIF file, ensure that the **Overwrite existing entries** check box is cleared. You must also review the list of objects in the reject file that is generated after restore, then update your system.
If your database becomes corrupted, you can use a backup file to restore settings and user information from a previously saved backup file.

**Important:** Backing up, restoring, and log archive operations start new connections to the Admin Server. Login credentials will be requested again for those new connections if the initial SAM Express Management Console login was performed more than eight hours prior.

**Tip:** Before initiating this procedure, log out of then back into the Console. If you have a clean database (or a newly installed database), we recommend that you restore your LDIF file before doing anything (like adding entries) in the database.

1. Select **File > Restore Database**.

   ![Restore Database window](image)

   **Figure 144:** Restore Database window

2. Enter the filename for the backup file to be used.

   Either manually type the full path and filename, or click **Browse** to find the directory and file.

3. If an encryption key was used, check the **Decrypt records with key** check box, and supply the encryption key string.

4. (Optional) Check the **Log restored records** check box if you want a log entry to be created for every record restored from a backup.
5  (Optional) Check the **Re-sign restored records** check box to have the system compute a new signature for each record restored from the backup.

You would want to use this option if, for instance, the Admin Server key used for signing records was compromised (see “Managing the Admin and Authentication Engine keys” on page 260). This is required if the new system has a different signature key than the system that produced this backup file.

By default, the **Overwrite existing entries** box is checked. This setting enables the Admin Server to overwrite existing records in the database with those from the backup file. If cleared, the Admin Server will return “Duplicate Entry Error Messages” during the restore operation.

6  Click **OK**.

A status window appears in which the status of your backup is shown. When the backup is completed, another dialog box will inform you of the number of successfully imported records.

---

**Backing up your database using the command line**

Occasionally, it is convenient to back up or restore data quickly, without the usual data validation and processing overhead of the standard SAM Express Backup/Restore functionality. In such cases, you can use two low-level **QBackup** and **QRestore** utilities that back up and restore the raw database data. These work quickly because they simply export and import the SAM Express tables to a text file. They are convenient as quick utilities that can be scheduled to run periodically to take snapshots of the data.

**Note:** These utilities cannot be used to back up and restore data between different versions of SAM Express. They are not compatible with the file format used by the standard SAM Express Backup/Restore functionality. Files produced by QBackup can only be used by QRestore. These scripts must not be used as a replacement for the standard backup operation performed via the SAM Express Management Console.

The scripts are located in the `<Install_Dir>\SERVERS\Database\bin` directory and can be used as follows: **QBackup filename** to back up the data, and **QRestore filename** to restore it.
Customizing SAM Express

The SAM Express Management Console has several screens that allow you to edit and/or create custom SAM Express configurations that can meet virtually any of your organization's individual needs.

**Configuration > SAM Express** (see Table 14)

*Edit Configuration*
- General Tab
- Servers Tab
- Sessions Tab

- **Attack Lock settings**
- **Max search results**
- **Unregistered user ID**
- **Default Login ACL settings**
- **Logging settings**

- **Log Server settings**
- **Session duration**
- **Session inactivity**

Table 14, “Configuration fields and functions,” lists the tabs, fields, and functions that are available to you.
### Table 14: Configuration fields and functions

<table>
<thead>
<tr>
<th>Tab</th>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>General (see “Configuring General settings” on page 245)</strong></td>
<td>Attacks before lockout</td>
<td>Sets the number of unsuccessful authentication attempts before the user is locked out. This protects your users from brute force attacks. (see “Using the Attack Lock feature” on page 222)</td>
</tr>
<tr>
<td></td>
<td>AAA clears attack locked account</td>
<td>Clears an account that was locked as a result of a brute force attack.</td>
</tr>
<tr>
<td></td>
<td>Clear lockout after (min)</td>
<td>Sets the minimum lockout time value. This is the period after which the attack lock will automatically reset.</td>
</tr>
<tr>
<td></td>
<td>Unregistered User ID</td>
<td>The username under which authentication will proceed if an invalid username is supplied. Changing these values is not recommended.</td>
</tr>
<tr>
<td></td>
<td>Default Role</td>
<td>System default -- points to the default ACL. This value is customizable.</td>
</tr>
<tr>
<td></td>
<td>Default Login ACL</td>
<td>System default -- no restrictions.</td>
</tr>
<tr>
<td></td>
<td>Use verbose logging</td>
<td>Allows for extended log entries.</td>
</tr>
<tr>
<td><strong>Servers (see “Configuring the log server” on page 246)</strong></td>
<td>Log Server</td>
<td>TCP address and port of the Admin Server that functions as the Logging server.</td>
</tr>
<tr>
<td><strong>Sessions (see “Configuring sessions” on page 247)</strong></td>
<td>Duration Timeout (hours/minutes)</td>
<td>Sets the maximum time limit for user sessions in hours and minutes.</td>
</tr>
<tr>
<td></td>
<td>Inactivity Timeout (hours/minutes)</td>
<td>Sets the time limit before automatic logoff for inactive user sessions in hours and minutes.</td>
</tr>
</tbody>
</table>

There are three tabs related to configuration settings. The sections that follow describe how to reconfigure the options on each of them.
Configuring General settings

The General configurations panel allows you to change settings for the Attack Lock feature, Unregistered user ID, Default Role and Login ACL, and logging.

Reconfiguring attack lockout options

If a user account becomes the target of a brute force attack, SAM Express will lock out the user record.

- In the **Attacks before lockout** field, specify the number of consecutive unsuccessful login attempts that will constitute a brute force attack. Once an account has been locked, it will remain so for a configurable amount of time.
- Clear the **AAA clears attack-locked accounts** check box if you do not want SAM Express to clear the locked out user automatically.
- In the **Clear lockout after** field, specify the minimum duration that the account will remain locked.

**Note:** The attack lock will not be cleared until the first successful authentication after the minimum duration has elapsed. Administrative users can clear the lock at any time by editing the locked user account.

Reconfiguring the unregistered user ID

The unregistered user ID field contains the name BAD_USER_ID. When an unregistered user attempts to log in, the BAD_USER_ID is triggered and it prompts the unregistered user to enter a platinum token-generated passcode. In most instances, you would not want to change this field, however some organizations do choose to change the field in order to trigger a prompt that is consistent with that of their other users. In that case you would:

- (Optional) Change the BAD_USER_ID properties so the passcode prompt matches the authenticator used by your other users.
- (Optional) In the **Unregistered User ID** field, specify a user ID under which authentication should proceed if an invalid username is supplied.

Reconfiguring the default role

If a user is not assigned specific roles, they are automatically assigned the default role by SAM Express. To change the default role that gets assigned to these users, in the **Default role** field, highlight the default role, and enter a new role in its place. This is the role that will automatically be assigned to users if they have no roles explicitly assigned.
Reconfiguring the default login ACL

All requests for access to resources are processed through one or more ACLs. These ACLs are a collection of access rules that are defined for a set of resources being protected. All users must be authorized by a login ACL, and if none is explicitly assigned, the default login ACL is applied.

To change the default ACL, in the Default Login ACL field, highlight the existing text, and enter a different login ACL in its place. If none of the user’s roles (explicit or implicit) refer to a login ACL, the Authentication Engine consults the Default Login ACL during authorization.

Reconfiguring logging

Each time there is an access request, the date and time of the request, whether the authentication passed or failed, and any authorization violations are logged in an audit log file. To allow more extended entries in the log file, click the Use verbose logging check box.

Configuring the log server

The Servers tab is used to specify the IP address and port of the log server that handles all audit log archive operations. If your deployment includes more than one admin server, you must designate which one will perform audit log operations. If your deployment only has one admin server in it, that server’s IP address and port number are automatically populated in the hostname log server and port fields. To access the Servers tab, select Configuration > SAM Express, then set or confirm the following Servers tab configurations:

- In the Log Server field, enter one of the following for the Admin Server handling log operations in your network:
  - Hostname: obtained by typing hostname in command prompt (independent of IPV4 or IPV6 configuration).
  - IP Address: obtained by typing ipconfig in command prompt.

  Note: If using IP address and both IPV4 and IPV6 are enabled, the Log Server should contain the IPV4 address. If IPV4 is disabled, the Log Server should contain 127.0.0.1.

- In the Port field, enter the Port that the Admin Server is using.
Configuring sessions

The Sessions tab allows you to set the session duration and the session inactivity timeout. To set these options, select **Configuration > SAM Express**, click the Sessions tab.

1. On the Sessions tab, set the maximum lifetime of a session by selecting the **Number of Hours** and **Number of Minutes** for user sessions.

2. To force a session to expire if the user has been idle or inactive for a period of time, do the following:
   a. Select the **Use session inactivity timeout** check box.
   b. Select the **Number of Hours** and the **Number of Minutes** of inactivity to allow before the session automatically times out.

3. Click **OK**, and then restart your servers.
Chapter 8: Using the SAM Express Management Console

Other admin tasks

This section describes miscellaneous admin functions using the SAM Express Management Console.

Finding entries

The Console allows you to search and find categories of data including users, login ACLs, admin groups, roles, and authenticator profiles. The following procedure outlines how to find login ACLs, but the same procedure applies to any of the object categories.

To find a login ACL (for example):

1. Select Find > ACLs > Login.
2. In the Find Login ACL entries window, use either the Find all available, or Find all that match filters to locate the ACL you created earlier.
   - The filters contain different parameters such as object IDs or admin group IDs that can be filtered upon.
3. Click the More button to use additional filters (if more than one filter is used, you can click the Less button to remove the last filter).
4. Click Find.
   - The Find Results: ACL Entries list appears with the list of login ACLs displayed.

Exporting data

In addition to finding object data, the Console allows you to export that data directly into spreadsheet files. For more information about exporting data, refer to “Exporting data into Excel worksheets” on page 239.

Editing admin group properties

You may edit admin group’s properties to make the admin group more suitable to your needs. Existing admin groups are listed on the left pane of the main Console window. To edit the properties for an existing admin group:

1. Double-click on the admin group you wish to edit.
2. In the Edit Admin Group window, click the View button to display the group’s properties and information about the last group modifications.
3. Click the Edit button to modify the properties for this group.
4. Make desired changes to the group, then click OK.
Session management

When a user authenticates via the Administration Server, UWA/WLS, or SAM Express Authentication SDK, the Authentication Engine creates a session for the user, then stores data about the user in that session. You can view or revoke user sessions using the SAM Express Management Console by selecting **Find >Sessions**.

![Figure 147: Find Session window](image)

1. In the Find Session Entries window, locate the desired session by selecting:
   - **Find all available**.
   - **Find all that match**, then selecting specific search criteria with which to search for the desired session.
   - **Search for sessions based on the Match Session Start Time**.

2. To automatically export this data into a report and save it, click the **Export** button and follow the prompts to save the report. Otherwise, click the **Find** button, then double-click the desired session to display the View Sessions window.

Revoking sessions

You can revoke user sessions from the View Sessions window. To revoke a session, thereby ending this user session, click the **Revoke** button. The Prompt for Revoke window appears. Click **Yes**. The session is revoked, and the Confirm window appears.
Chapter 8: Using the SAM Express Management Console

Other admin tasks
In this chapter...

SAM Express server-related tasks ...................................................252
Configuring RADIUS, and RADIUS Accounting servers ..............258
Authentication Engine related tasks .............................................259
Custom user management configuration .....................................261
Configuring the Authentication Policy...........................................264
Agent configuration screens.........................................................265
Increasing performance................................................................269
Running Repair ............................................................................271
As the administrator, you can change component ports, audit system events, view event logs, set up a different administration server, set up logging, and configure SAM Express servers.

### Stopping and starting servers

If you need to manually stop or start a SAM Express server, do the following:

1. Select **Start > Programs > Administrative Tools > Services**. The Services utility opens.

![Services window with SAM Express servers running](image)

2. Select the name of the SAM Express server you want to stop or start.

3. Select **Action > Start or Stop** button from the tool bar.
   
   Alternatively, double-click the server’s name to display its Properties window, and then click the Service Status **Start or Stop** button.

*Tip:* Restarting the Database Server will restart the SAM Express Admin Server and Authentication Engine.

### Changing component ports

You can change the ports over which your SAM Express components are communicating using the SAM Express Configuration Utility. To change ports:

1. Launch the SAM Express Configuration Utility by selecting **Start > Programs > SafeNet > SAM Express > Configuration > Server Configuration**.
   
   The SAM Express Configuration Utility window appears.
You may change the ports and signing key that the SAM Express components are using on the Server Components tab. Remember that if you change the server port through the Configuration Utility, you must change the corresponding ports for each client that connects to the server.

2 To change an active value, highlight the existing value and enter a new one.

3 When finished using the Configuration Utility, click OK to exit.

**Note:** Restart all SAM Express Services for changes to take effect. For details, see “Service restarts after agent configurations” on page 268.

### Logging server diagnostics

Occasionally it is useful to view a detailed log of operations to the various SAM Express components. To turn on detailed diagnostic logging, do the following:

1 In the SAM Express Configuration Utility, select the **Server Diagnostics** tab.
Figure 150: Server Diagnostics tab of the Configuration Utility

2 Select the check box for any of the following events you want to log:
   – Authentication message exchange
   – Authentication request details
   – Administrative sessions
   – Server synchronization
   – User Center operations
   – Database operations
   – Data signing

3 When done, click OK.

Table 15 specifies the locations of the generated diagnostic logs.

Table 15: Server diagnostic file locations

<table>
<thead>
<tr>
<th>Event Type</th>
<th>File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication-related events</td>
<td>&lt;Install_dir&gt;\SERVERS\AAAServer\SccAAASrvr Log.txt</td>
</tr>
<tr>
<td>Administration and server synchronization events</td>
<td>&lt;Install_dir&gt;\SERVERS\AdminServer\SccAdSrvr Log.txt</td>
</tr>
<tr>
<td>Database and signing events</td>
<td>Files will be distributed between the two locations listed above depending on which component performed the operation</td>
</tr>
<tr>
<td>User Center operations</td>
<td>&lt;Install_dir&gt;\SERVERS\Web\Tomcat</td>
</tr>
</tbody>
</table>

**Important:** Restart all the SAM Express Services for changes to take effect. For details, see “Service restarts after agent configurations” on page 268.
Monitoring server status

To check the status of servers you have selected to monitor:

1. In the SAM Express Configuration Utility, click the Server Status tab to display the Server Status Configuration window.

![](Figure 151: Server Status tab of the Configuration Utility)

The server name, its address, port, and status of the servers you chose to monitor are displayed in the active window.

Adding servers to the monitored servers list

You can add servers to be monitored using the Server Status tab of the Configuration Utility. To add a server to the monitored server list:

1. On the Configuration Utility’s Server Status tab, click the New button.

![](Figure 152: Server Status Configuration window)
2 In the **Server name** field, enter the name of the server you wish to monitor or choose a server from the drop-down list (if the server is not installed on the local machine, enter its host name or IP address and a port number).

3 Click **OK**.

You are returned to the Server Status tab. The new server name, its address, port, and status are displayed in the list of servers.

---

**Removing servers from the monitored servers list**

You can remove servers from the monitored list using the Server Status tab of the Configuration Utility. To remove a server from the list, select a server to remove, then click the **Remove** button.

---

**Cloning servers**

You can clone (copy) servers with their settings to use as templates to create new servers to monitor on the Server Status tab of the Configuration Utility. To clone a server:

1 From the Server list, select a server whose settings are similar to those you want to apply to a new server.

2 Click the **Clone** button.

The new cloned server appears in the Server list.

3 To change settings for the newly cloned server, highlight the server and click the **Edit** button.

4 Edit the cloned server’s name, host name or IP address, and port number, then click **OK**.
Configuring the Administration Server

The SAM Express Snap-in must access the Administration Server. If the SAM Express server is installed on a different machine from ADUC, you may have to configure the console to point to the correct Administration Server as follows:

1. In ADUC (left pane), right-click the **SAM Express** node and select **Configure**.

2. (Conditional) If the Administration Service is on the local machine, select **Administration Service is installed on the local machine** and click **OK**.

3. (Conditional) If the administration service is installed on a remote machine:
   a. Select the **Administration Service is installed on a remote machine** option.
   b. Enter the **IP address** and **Port** for the machine where the SAM Express servers are installed.

   **Important:** The port used for configuring the Administration Service must match the port specified as Administration Service when the SAM Express server was installed.

   c. Click **OK**.
Configuring RADIUS, and RADIUS Accounting servers

If you selected the RADIUS and/or RADIUS Accounting server(s) for installation, you can configure them using the web-based RADIUS/RADIUS Accounting Server configuration window.

1. From the Start menu, select Start > Programs > SafeNet > SAM Express > Configuration > RADIUS Server (or) RADIUS Accounting Server.

- To configure Authentication Engine settings, refer to “Configuring the Authentication Engine” on page 265.

Note: The RADIUS Accounting Server Configuration window is almost identical to the RADIUS Server window, and uses the same Edit clients file screen.

Figure 153: RADIUS Configuration Utility

Enter the required information (hostname/IP, Secret key, and Type), then click Add.
The Authentication Engine (part of the SAM Express Server), may require some additional configuration or performance settings to optimize its operations.

Authentication Engine performance settings

During normal operations, ACL, Authenticator Preference, and Role entries are cached and used until a pre-set refresh time period is reached. They will not be re-read from the database until one is requested by some action, and the refresh time period has elapsed. This may cause a delay between the time you modify an entry and the time the Authentication Engine uses it. To set a faster refresh time and minimize the delay, the following (default) parameters can be modified (to a range of 0 - 3600 seconds) in the sccservers.ini file (found in <Install_Dir>\SERVERS\Shared):

- `AuthenPrefs_Cache_Refresh_Seconds=600`
- `Role_Cache_Refresh_Seconds=120`
- `ACL_Cache_Refresh_Seconds=120`

You must restart the AAA server for any changes to take effect.

Configuring the Authentication Engine for SoftPIN use

SAM Express allows you to use SoftPIN, which requires users to append a PIN number of their choice to a token-generated password. By default, the Authentication Engine is configured to force users to append a SoftPIN to a token-generated password. You can configure the Authentication Engine to force users to prepend (precede) a SoftPIN to the token-generated password.

**Note:** These steps should be followed for every Authentication Engine if running multiple SAM Express servers in a replication ring.

To force users to prepend a SoftPIN, do the following:

1. Locate the sccservers.ini file, found in:
   `<Install_Dir>\SERVERS\Shared`

2. Open the file, and scroll down to the line:
   ```
   # Set this to 'on' to force SoftPin to precede the password
   Pin_Before_Password=off
   ```
   Set the `off` value to `on`.

3. Restart the Authentication Engine for the changes to take effect.
Managing the Admin and Authentication Engine keys

The Admin Server and Authentication Engine hold several cryptographic keys. The Admin Server key signs database entries to assure data integrity. On a regular basis, or if either of these keys is compromised, you should change the key and re-sign all database entries.

To change the Admin Server signing key, back up your system database.

1. At the local machine (where the Admin Server is installed), log on as an administrator, and go to `<Install_Dir>\SERVERS\Shared`.

2. Locate and open the file `signers.cfg` for editing.

   ```
   # Multiple signers are supported for verification, but the first on a name matching a particular component will be used for signing!
   # dbCipher lines should not be modified.
   # Currently supported algorithm types for signing and encryption are “DES” and “3DES” are supported for backwards compatibility only.
   SccAdminServer, AES, 87654321abcdefgh
   SccAuthServer, AES, 87654321abcdefgh
   dbCipher, AES, 12345678abcdefgh
   ```

   **Important:** Do not modify!

3. To change the Admin server key, add a new line above the line `SccAdminServer` that says:

   ```
   SccAdminServer, AES, 87654321abcdefgh
   Or
   SccAdminServer, AES, 12345678defghijk
   ```

4. To change the Authentication Engine key, add a new line above the line `SccAuthServer` that says:

   ```
   SccAuthServer, AES, 12345678abcdefgh
   ```

   **Note:** The key string can be numerics, or a combination of letters and numbers. For signing, the key must contain 16 characters minimum.

   **Important:** Do not modify the `dbCipher` lines.

5. Restart the Admin Server and/or Authentication Engine using the Windows Services Utility.

   Restore the database, with Re-sign restored records checked. This will sign all entries with the new key.

   **Note:** This step is optional. If the database is not completely restored but new keys are assigned, any and all future changes to the database will be resigned with the new key.
During installation you chose to have your users managed either in Active Directory or the SAM Express database, and the installer configured the servers and agents accordingly.

However, there may be cases in which you want or need to have some users in Active Directory and others in the SAM Express database. This requires modifying the server-side configuration file to tell the Authentication Engine where it should look for user information.

### Changing the user database post installation

To switch the database where your users are managed, you must modify the server-side configuration file so the Authentication Engine knows where to look for user information. To modify the file, do the following:

1. Locate the `IdMapper.cfg` file in the `<Install_Dir>\SERVERS\AAAServer` directory, and open the file in a text editor.
2. Locate the following line in the file using the Search tool:
   ```xml
   <isDefaultMapper>true</isDefaultMapper>
   ```
   If the line is present in the file, Active Directory is currently used. If the line is not present in the file, the SAM Express database is currently used.
3. To switch from the Active Directory database to the SAM Express database, delete `<isDefaultMapper>true</isDefaultMapper>` from the file.
4. To switch from the SAM Express database to the Active Directory database, add `<isDefaultMapper>true</isDefaultMapper>` to the location indicated by the arrow below.

```xml
<IdMapper id="propFileIdMapper">
  <IdMapperName>securecomputing.yellowstone authserver:PropFileIdMapper</IdMapperName>
  <agents>
    <agent>Sample agent</agent>
  </agents>
  <configuration>
    <PropFileIdMapperFile>C:\Program Files\Secure Computing\SAM\AAAServer\users.map</PropFileIdMapperFile>
  </configuration>
</IdMapper>

<IdMapper id="ADtoTokenIdMapper">
  <IdMapperName>securecomputing.yellowstone authserver:ADtoTokenIdMapper</IdMapperName>
  <roleMapperName>securecomputing.yellowstone authserver:ADGroups</roleMapperName>
  <agents>
    <agent>test agent</agent>
  </agents>
  <configuration>
    <ADToTokenIdMapperFile>C:\Program Files\Secure Computing\SAM\AAAServer\users.map</ADToTokenIdMapperFile>
  </configuration>
</IdMapper>

<isDefaultMapper>true</isDefaultMapper>
<IdMapper id="internal">
  <IdMapperName>internal</IdMapperName>
  <agents>
    <!-- DO NOT CHANGE Admin server MUST use internal mapping. -->
    <agent>TESTADMIN</agent>
  </agents>
</IdMapper>
</IdMapper>
```

### Changing agent-specific user information

To change how the Authentication Engine looks up user information for a
Chapter 9: Advanced Administration Tasks

Custom user management configuration

particular agent, do the following:

1. Locate the IdMapper.cfg file in the <Install_Dir>\SERVERS\AAAServer directory, and open the file in a text editor.

2. Decide which agent(s) you want to work with users in Active Directory, and enter the agent(s) names in the '<IdMapper= “ADtoTokenSNIdMapper”>' section, as specified in the IdMapper.cfg file’s instructions.

3. Decide which agent(s) you want to work with users in the SAM Express database, and enter the agent(s) names in the '<IdMapper= “internal”>' section, as specified in the IdMapper.cfg file’s instructions.

⚠️ **Important:** Each agent’s name must appear in only one section.
Configuring SAM Express for AD lockout support

The SAM Express AAA server can be configured to work with Active Directory’s user lockout feature. During authentication, the AAA server will verify a user’s lockout status and, if user’s AD account is locked out or disabled, SAM Express authentication will fail.

This feature of SAM Express is disabled by default. To enable, create the following registry key:

**Note:** This must be done for all hosts on which the SAM Express AAA server is installed.

```
HKEY_LOCAL_MACHINE\Software\Secure Computing\SccADHelper
```

Parameter: DenyLockedAccounts
Value Type: REG_DWORD
Valid Range: 1, 0 (enabled, disabled)
Default: 0
Description: This enables or disables the test for locked/disabled Active Directory user accounts when SAM Express is retrieving a user’s token serial number. If enabled, SAM Express authentication for the user will fail if their account is locked or disabled.

**Note:** If ‘DenyLockedAccounts’ is enabled, the SAM Express settings for a user’s account in ADUC are disabled until the user’s account is unlocked or re-enabled. This restriction also applies to users enrolling through the SAM Express User Center.

Troubleshooting steps for this feature can be found in “Troubleshooting AD lockout support” on page 310.
Configuring the Authentication Policy

You can designate special groups of users (as opposed to all users) who will be required to authenticate using a SAM Express token. To require a specific Windows group to log in using tokens, use the native Windows user and group management tools to create a global group called SAM Express_USERS.

By default, built-in AD accounts (such as the Administrator account) do not have an assigned User Principal Name (UPN). To protect AD accounts with the SAM Express Domain Login Agent, a UPN must be assigned to each. Once users are placed in this special group, you must tell the agent what the group is, and how to treat users in it.

**Important:** You must create global groups before you can apply authentication policies to specific users.

---

Launch the Group Policy window (all agents)

**Note:** This configuration only affects groups associated with SAM Express Agents.

1. To require all users authenticate using SAM Express strong authentication, select **All users authenticate using SAM Express**, or
2. Specify users by Group:
   a. Select the **Group** from the drop-down list
   b. Verify the listed, or enter a new domain in the **from domain** field
3. Select one of the following:
   a. **Only users in this group authenticate using SAM Express** - includes all users in the selected group
   b. **Only users NOT in this group authenticate with SAM Express** - excludes all users in the selected group
4. Click **OK** when done
This section contains information on configuring the Authentication Engine, changing logging settings, and changing the authentication policy.

Complete details for configuring and using agents are found in the *SAM Express Agent Administration Guide*.

### Configuring the Authentication Engine

1. For the IAS/NPS, Web Interface, CAG, and Domain Login Agents, click the **Authentication engine** button on the Agent Configuration window. For the OWA Agent, click the **Configure** button on the Authentication Engine portion of the Agent Configuration window. The Authentication Settings window appears.

   ![Authentication Settings window](image)

2. In the **Host name/IP address** field, enter the host name or IP address of the machine to which the agent will send authentication requests (name/IP address of machine on which the SAM Express Server is installed).

3. In the **Port** field, enter the port number on which the Authentication Engine (Authentication Server) will listen for requests.

   This port number must match the port number specified for the Authentication Engine.

4. Click **Save**, and the server appears in the Configured Locations list.

5. Click **OK**.

### Removing servers

To remove servers from the Configured Locations list, select the server name from the list, click the **Remove** button, and then click **OK**.

---

**Important:** If you are configuring multiple servers, repeat the same steps for each server you are configuring.
Changing agent logging settings

Note: This section applies to all SAM Express agents.

You may view log records, manage log records, and modify the messages that are logged using the Windows Event Viewer or any text editor. By default, logging functions are disabled, although errors are still logged to the Windows Event Viewer. You must enable logging before you can reconfigure the settings.

Changing IAS/NPS, Web Interface, OWA, and CAG/SAM logging settings

1. Launch the agent’s configuration screen, and click **Logging**.

![Figure 155: Agent logging window for IAS, WI, and CAG agents](image)

2. Click the **Enable Logging** checkbox to enable the window and have the agent record logging events.

3. Accept the **Logfile name**, or enter a new name (plus full path) to which agent logs will be written.

   The OWA agent logging function records extension logs and filter logs. Extension logs are generated when a non-credentialed user attempts to access an Exchange resource and is required to authenticate. Filter logs are created every time a user accesses an Exchange resource.

   **Note:** By default, IAS, WI, and CAG Agent logs are stored in `<Install_Dir>\Agentlogs`. OWA Agent logs are stored in `<Install_Dir>\OWAAgent\Logs`.

4. Set the **Maximum size in KB per log file**.

5. **Select messages to log** from the following options:
   - Errors
   - Errors and information
   - Errors, information, and diagnostics

   **Important:** Logging diagnostic information may result in lengthy output. Unless you are troubleshooting a problem, diagnostic logging should be disabled.

6. Click **OK** when done.
Changing Domain Login Agent logging settings

1. Launch the agent’s configuration screen, and click **Settings**.
2. Click the **Logging** tab.

![Figure 156: Agent configuration window for DLA](image)

The DLA UI allows log information (type and max file size) to be gathered for various Agent components. If changes are made:

- Sub-auth changes are effective immediately
- For Agent service changes: restart the agent service
- For Workstation Agent changes: re-boot the workstation.

Changing OWA timeouts

In the Agent Configuration window, click the OWA Agent **Configure** button.

![Figure 157: Configure SAM Express OWA Agent window](image)

Modify the following fields as needed:

- **Enable Timeouts** (selected by default – click to clear): enables or disables time limits for an active or idle (inactive) session
- **Session Timeout** (3600 seconds default): the duration (in seconds) for a single session
Agent configuration screens

- **Idle Timeout** (300 seconds default). the duration (in seconds) of an idle (inactive) session
- **Require SSL Connections** (selected by default): requires that all login attempts are via SSL (https) connection
- **Hide initial SAM Express passcode field** (cleared by default – click to hide the field): removes the SAM Express Passcode field from the initial SAM Express Login window

**Note:** The Require SSL Connections option is enabled only if a certificate is present in the Exchange OWA site, in which case the option will automatically be turned on at installation time.

**Security Alert:** Operating an Exchange OWA site without a server certificate and SSL is not recommended.

Service restarts after agent configurations

Some agent configurations require you to restart a corresponding service afterwards. Table 16 on page 268 lists which agents require service restarts.

**Table 16: Agent/service restarts**

<table>
<thead>
<tr>
<th>Agent</th>
<th>Restart</th>
</tr>
</thead>
<tbody>
<tr>
<td>IAS/NPS Agent</td>
<td>IAS-NPS Service</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If Routing &amp; Remote Access Server (RRAS) is on the same machine, stop the IAS service and RRAS, restart RRAS, then restart IAS.</td>
</tr>
<tr>
<td>Web Agent</td>
<td>IIS Service</td>
</tr>
<tr>
<td>CAG Agent</td>
<td>None required</td>
</tr>
<tr>
<td>OWA Agent</td>
<td>IIS Service</td>
</tr>
<tr>
<td>Domain Login Agent</td>
<td>If changes are made:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Sub-auth filter</strong>: changes are effective immediately</td>
</tr>
<tr>
<td></td>
<td>• <strong>Agent service</strong>: restart the agent service</td>
</tr>
<tr>
<td></td>
<td>• <strong>Workstation Agent</strong>: re-boot the workstation.</td>
</tr>
<tr>
<td>Universal Web Agent</td>
<td>UWA Service</td>
</tr>
</tbody>
</table>
Increasing performance

In busy environments, you may have to minimize replication traffic and remove resource contention issues between replication and authentication. The following sections describe how to configure your software for best results.

Archiving during minimal activity periods

One way of increasing performance is by archiving during your organization’s minimal activity periods. For example, if your organization is busiest between the hours of 7 a.m. and 7 p.m., then archiving after 7 p.m. and before 7 a.m. reduces the database conflicts between archiving and authentication.

Changing the default archive value

The `sccservers.ini` file contains the entry that determines when archiving occurs. By default the value is set to archive logs every hour. To change the setting and force log archiving to only occur during minimal activity periods, you must uncomment the attribute and change the range specifier value to the hour or range of hours when you want archiving to occur.

To enable archiving times during minimal activity periods, browse to the `<Install_Dir>\SERVERS\Shared\sccservers.ini` file.

1. Find and uncomment the entry: `#SkipArchivingHours=6-18`.
2. On the same line, specify the hours when you do not want to log archives by entering the specific hour or range of hours. The following rules apply when setting your hours:
   - Archiving hours are 0-based and use a 24-hour clock.
   - Entries can be either a specific number or a dash-separated range of numbers. For example, the value `0, 6-18, 23` would skip archiving during the hours of 11 p.m. and 1 a.m., and from 6 a.m. to 6 p.m.
   - Spaces are ignored and individual entries are comma-delimited.
3. Restart the Administration Server.

**Note:** Use of this feature does not affect how the audit log archives are created. Instead, it only affects when the Administration Server performs the archiving.

Using multiple database connections

You can fine tune database and networking throughput for replication if your network topology has higher than normal network latencies. By default, the number of replication threads is set to one (1). Increasing the number of replication threads may improve replication performance in your environment.

To change the number of replication threads, browse to the `<Install_Dir>\SERVERS\Shared\sccservers.ini` file.
The file contains the entry that sets the number of threads and database connections the replication engine uses to propagate changes to this peer.

1. Find the following entry:
   
   ```
   #ReplPrev_ReplWorkerThreadCount=1
   ```

2. Uncomment the line by removing the # symbol from its beginning.

3. Change the value currently set to one (1) to the number of threads you want to be used for replication. Reasonable values for this attribute are in the range of 1 to 15 threads.

   **Note:** The example in step 1 configures replication thread count for the previous peer in the replication ring. To configure thread count for the next peer, locate and modify the following entry:

   ```
   #ReplNext_ReplWorkerThreadCount=1
   ```

4. Restart the Administration Servers in the system.

   **Tip:** Experiment with the number of threads to determine the best replication throughput for your network.

---

**Running without an archive log master**

Configuring individual server log archiving in a multi-server system allows each server in the ring to perform its own archiving; each effectively becomes a log master on which archive operations can be performed. In this mode, each server in the system archives the local audit logs and removes them from the local database. The deletions are not replicated to other servers in the ring; instead, the archive manager on each server explicitly archives the logs.

Additionally, when you load or unload archive sets, the logs in the archive are only imported into the local machine. Insertions and deletions are not replicated throughout the system. This mode greatly reduces the replication traffic caused by both day-to-day operation of the system and the occasional loading and unloading of archive sets.

   **Note:** Another positive side effect of running without an archive log master is that the archived audit log files are effectively replicated on all servers in the system.

---

**Enabling individual server log archiving**

To enable individual server log archiving, connect to the current log master server.

1. Select Configuration > SAM Express, and select the Servers tab.
2. Select the All admin servers are log servers option.
3. Restart the administration servers in the system.
Running Repair

The repair process creates a sccservers.ini.bak file that contains the customized configuration of the sccservers.ini file. If you run repair, the following files are overwritten and should be backed up prior to running repair.

- For the user center:
  - SERVERS/Web/Tomcat/conf/server.xml
  - SERVERS/Web/Tomcat/webapps/usercenter/WEB-INF/login.conf
  - SERVERS/Web/Tomcat/webapps/usercenter/WEB-INF/EnrollAuth.bsh

- SafeNet\SAM Express\SERVERS\Shared:
  - Sccservers.ini
  - Signers.cfg

- SAM Express\SERVERS\Web\Tomcat\Tomcat\Webapps\usercenter\WEB-INF:
  - EnrollAuth.bsh
  - Login.conf

- SafeNet\SAMx\SERVERS\RADIUS\RADIUSAccountingServer

- SafeNet\SAMx\SERVERS\RADIUS\RADIUSServer:
  - Authfile
  - Clients
  - Dictionary
  - users

- For Admin Console
  - \SAM Express\AdminConsole\SupportExpiration.spe
  - \SAM Express\AdminConsole\client.ini
  - \SAM Express\AdminConsole\Certificates (whole folder)
Replication

In this chapter...

About replication.................................................................274
Pre-replication setup considerations ........................................276
Adding peers to a new replication ring .....................................277
Adding a new peer into an existing replication ring ....................282
Verifying SAM Express server replication .................................284
Troubleshooting......................................................................284
About replication

Replication plays a key part in the fault tolerance scheme within SAM Express. It is the process of duplicating or copying database information from one machine to one or more other remote machines, and is implemented in the Admin Server of each SAM Express installation.

Ring topology architecture

SAM Express uses a bidirectional ring topology architecture. In a ring topology, each machine is known as a replication peer, and these peers are arranged in a logical loop. Each peer has a unique address, and its Admin Server communicates with its own Database Server as well as the Database Servers of up to two neighbors: the logical Next peer, and the logical Previous peer in the ring. Multiple peer replication is shown in Figure 158.

![Multiple peer replication diagram](image)

AS = Admin Server  
DB = Database Server

If there are only two replication peers in the ring, each will only have a Next peer.

**Important:** In a multiple server replication ring, all participating servers must have the same encryption and signing keys, the same management console login password, and the same User Center password (if User Center is installed and being used). If different values are used, errors will occur when attempting to decrypt the databases, and attempts to access management consoles and the User Center will fail.

Additionally, database replication does not happen automatically when replication is initiated, so all participating peers must be in sync (databases restored from a previously backed-up master) before replication is initiated.
The change log

Every local server database action — authentication or administration — is followed by a note of the operation written in real-time into a special file called the change log. Events such as insertions, modifications, and deletions of each relevant record in a SAM Express database are tracked in the change log immediately after the event takes place and in the context of the operation that triggered the event. Concurrent to the main event processing, another thread (hosted by the SAM Express Admin Server) monitors the change log, propagating changes reflected in the change log to the replication peers of the local server.

During replication, timestamps on changes to the local change log are compared against those on the peer nodes, and changes are propagated only if the object on the peer node is older than the local one.

Note: The change log (QueryChangeLog.bat) is not modifiable; it is only available to view database changes. It is an internal mechanism that SAM Express uses to reliably track changes to its database.

Tip: To obtain the total number of change log records without displaying the text of each record that is found, use runsql CheckChangeLogCount.sql or MonitorChangeLog from the Database/bin directory.

Change record creation and change propagation are independent actions, which means you can track database changes, but delay their replication to other replication peers until a later time.

Differences between SAM Express and AD replication

Note: This section applies to ADUC users only.

There are differences between what happens during SAM Express replication and Active Directory replication when using SAM Express with Active Directory.

In AD, user-token assignments are stored only in the AD database and not in the SAM Express token database. As such, AD will automatically replicate user-token assignment records between the domain controllers in your network.

SAM Express, on the other hand, only stores token records in the token database, and not user-token assignments.

A quick method of verifying that token record replication of the SAM Express database is working is by making a change that modifies a token record (see “Testing replication setup” on page 284).
Pre-replication setup considerations

If you plan to use SAM Express’s replication feature, there are some technical issues to be taken into consideration.

---

General considerations

- (Optional) A diagram of your network, with target machine names and IP addresses would be useful.
- Make sure you have at least one stable machine -- one that is up and running with no noted errors or unexpected behavior -- on the network.
- **Accurate time sync between the machines in your replication ring is critical.**
- All peers must have routing to the actual IP of their replicating neighbors no matter what Network Address Translation (NAT) might be occurring between them.
- Replicating servers initiate bi-directional communications, so intervening systems (such as firewalls, packet filters, smart switches, VPN definitions, etc.) must allow bi-directional sessions.
- Make sure the network connectivity between the machines is stable and has sufficient bandwidth for rapid transfer of large amounts of data.
- Make sure your target machines meet the system requirements.
- Install peer machines one at a time and verify that each is in a stable state before installing another peer.

Special considerations

- All servers must be in sync before setting up replication.
- All servers in the ring must use the **same encryption key**, the **same management console password**, and the **same User Center password** (with SAM Express ESP only). Different values among the servers will result in non-decrypting databases, and an inability to access the management console or User Center.
- All SAM Express peers must be at the same version and build.
- Before starting replication, you must back up the database on the master machine and restore it to all other machines that will be part of the ring.

⚠️ **Important:** While the chances of multiple-point failure are low, it should be noted that the risk of replication ring segmentation becomes greater for a ring containing more than 3 machines.

⚠️ **Important:** It is strongly recommended that you run synchronization over a VPN link. If not run over a VPN link, server synchronization traffic is not encrypted.
Adding peers to a new replication ring

The steps for adding machines into a replication ring is described below, in the order in which they should be done.

1. Verify SAM Express server software is installed

   SAM Express server software must be installed on each machine to be added to the ring. If needed, refer to the “Installing SAM Express” on page 35.

   Once all machines have SAM Express server software installed, and all machines are time sync’d, you can start adding peer machines into the replication ring.

2. Verify time sync on peer machines

   To maintain time synchronization, Network Time Protocol (NTP) can be used to synchronize clocks to Universal Coordinated Time (UTC - the international time standard). Any computer on your network can get time from NTP servers on the Internet, and a good source for time synchronization can be found at http://tycho.usno.navy.mil.

   Before adding additional peers to your replication ring, you should ensure that the target machine’s clock is synchronized to a stable, accurate time source.

   1. On the first peer in your replication ring, go to the Windows Time service, found under Start > Programs > Administrative Tools > Services.
   2. Scroll down in the list to locate Windows Time, and verify that its status is Started, and its Startup Type is Automatic.
      
      If not, right-click Windows Time, select Properties, and set the status to Started and/or startup type to automatic.
   3. Close the Services window.
   4. Launch a Command Prompt window, and enter the following command:
      
      c:\net time /setsntp:IP_address
      
      where IP_address is the name of the master time source, or IP address (or fully qualified domain name) of Master server.
   5. In the (still open) command prompt window, enter the command:
      
      c:\w32tm -once
      
      This will execute an immediate time sync to the source you listed in step 4.
   6. Repeat these procedures for each machine in the ring.
3. Designate a Log Master

**Note:** If using ADUC, skip to “4. Back up the database”

The Log Master is a specific machine responsible for archiving off old audit logs. You need to designate a machine to act as Log Master by using the SAM Express Management Console as follows:

1. Launch the SAM Express Management Console from **Start > Programs > SafeNet > SAM Express > SAM Express Management Console**.
2. Select **Configuration > SAM Express > (Edit SAM Express Configuration window) > Servers tab**.
3. Enter IP address and port number for the Log Master.
4. Click **OK** when done.

4. Back up the database

**If using the SAM Express Management Console:**

The Log Master’s database needs to be backed up so it can be restored to all machines in the ring. Back up the database as follows (if needed, see “Backing up your database” on page 240 for more information):

1. In the SAM Express Management Console, select **File > Backup Database**.
2. Enter a file name in the **Backup to file:** field, and (optionally) check (select) **Do not backup audit logs** and/or **Encrypt records** if needed.
3. Enter (then re-enter) the entire encryption key string.
4. Click **OK** when done.

**If using ADUC:**

1. In ADUC, expand the **SAM Express** node (left side, navigation pane) and select **Import/Backup/Restore**.
2. Under **Backup Database**, click **Browse** to select the file to which you will write the backup data.
3. When the file name is shown, click the **Backup** button, then click **OK** when done.

Continue with “5. Restore the backed up database to machines in the ring” on page 279.
5. Restore the backed up database to machines in the ring

If using the SAM Express Management Console:

If the backed up database is not restored to all other machines in the ring, contention problems will arise as the Admin server on each machine will attempt to become the Log Master.

On each machine in the ring, do the following:

1. In the SAM Express Management Console, select File > Restore Database.
2. Enter the filename of the backed up file (from the Log Master backup).
3. Enter the encryption key string used when backing up the file.
4. **Optional** Check the Re-sign restored records checkbox.
5. Click OK when done.

If using ADUC:

On each machine in the ring, do the following:

1. In ADUC, expand the SAM Express node (left side, navigation pane) and select the Import/Backup/Restore icon, click Browse to select the backed up file from which you will restore your data, then click OK.
2. Click the Restore button when the proper file name appears in the Select a database backup file to restore from.
3. Restart the Authentication Engine and Administration Server.
4. Close, then re-open ADUC.

---

**Important:** Failing to close then re-open ADUC after a database restore will result in one or more error messages.

---

6. Stop the Admin server and Authentication Engine

On each peer in the replication ring, Stop the Admin Server and Authentication Engine using Windows Services as follows:

1. Browse to Start > Programs > Administrative Tools > Services, right-click SAM Express Administration Server and select Action > Stop.
2. Repeat for the Authentication Engine.

---

**Important:** Do not stop the Database server.

Continue with “7. Edit the sccservers.ini file” on page 280.
Chapter 10: Replication
Adding peers to a new replication ring

7. Edit the sccservers.ini file

As part of your server replication setup, you will need to edit the sccservers.ini file on every peer in the replication ring.

1. Browse to <Install_Dir>\SERVERS\Shared, and open sccservers.ini.
2. Locate and uncomment the line starting with DBActionListenerClass=.
   This Admin server will now track changes by 'listening' to actions in the database, and recording them as new records in the change log.
3. Scroll down to the section called #Properties for replication connections, and uncomment the line starting with ReplNext_JDBC_URL=.
4. Replace NEXT_HOST on that line with the name or IP address of the peer that will serve as the logical 'next' peer in your replication ring.
   If the database on 'N' was installed on a custom port (other than 5010), make sure to reflect the correct port in this setting.
5. Save the file.

If your replication ring has more than two peers:

1. In the sccservers.ini file section called #Properties for replication connections, uncomment the line starting with: ReplPrev_JDBC_URL=
2. In that same line, replace PREV_HOST with the IP address (or name) of the peer that will serve as the logical 'previous' peer in your replication ring.
   If the database on 'N' was installed on a custom port (other than 5010), make sure to reflect the correct port in this setting.
3. Save the file.

8. Run the AddReplPeer.bat file

The AddReplPeer.bat script identifies to each machine in the ring its next and previous neighbor machines (by IP address). For a replication ring of only two machines, the script is run once per machine, since each machine only has one neighbor. For a replication ring of more than two machines, you would run the script twice on each machine in the ring; once for its next neighbor, once for its previous neighbor.

For example: you have a replication ring of four machines: A, B, C, and D (see Figure 159 on page 281).
Figure 159: AddReplPeer implementation

As shown above, on machine A you would run the script twice: `AddReplPeer B` (allows connection from A's next neighbor, peer B), then again as `AddReplPeer D` (allows connection from A's previous neighbor, D). You will also run the script twice to add previous and next neighbors on all other machines in the ring.

When running this script, you will also run the command-line utility `TSEXEC`. It ensures that the database utility script files continue to work properly when Windows Terminal Services is installed/configured on the server.

To run the `AddReplPeer.bat` script as described above, do the following:

1. Open a console window, and cd to: `<Install_Dir>\SERVERS\Database\bin`, then run the batch file:

```
tsexec AddReplPeer.bat neighbor_IP_address (of neighbor machine)
```

   For example; if you are setting up a peer NEPTUNE.SOLAR.SYS, and its replication neighbor is JUPITER.SOLAR.SYS (with an IP address of 192.168.10.10), then on Neptune you would enter the command:

```
tsexec AddReplPeer.bat 192.168.10.10
```

   This will set the file configuration which allows the database to accept connections from neighbor peers you specify as the line arguments.

   **Note:** While you may specify a neighbor by host name, the name must match its entry in the DNS record exactly or it won’t be recognized. IP address is recommended.

2. Repeat for each peer in the ring.

Before you begin, SAM Express must be installed and running on the machine you intend to add into the ring. In this example, peers “A” and “B” are existing, and you are adding new peer “N” between “A” and “B.”

1 Verify the existing replication ring is in a ‘steady state’ (i.e. state where no changes need to be replicated) by doing the following:
   a Open a console window and cd to 
     <Install_Dir>\SERVERS\Database\bin
   b Run the batch file called tsexec QueryChangeLog.bat
      This file queries the change log in the local database. An empty change log means there are no more changes to be propagated. Do this on at least “A” and “B” (ideally on all peers in the ring).
   c The system is in a steady state once the output indicates: Empty set
2 Back up the database on either “A” or “B” (they should be in sync).
3 Stop the Admin Server and Authentication Engine on “A” and “B” to prevent any further database changes from being propagated.

Important: Do NOT stop the database servers.

Example steps for adding a peer to a replication ring

To add a new peer to an existing (example) replication ring, do the following:

Step 1 of 5: on peer “A”

1 Edit file <Install_Dir>\SERVERS\Shared\sccservers.ini:
   a Locate line starting with ‘ReplNext_JDBC_URL’
   b Replace name or address of Next peer on that line (which should have been “B”) with the name or IP address of “N”.
      If the database on “N” was installed on a custom port (other than 5010), make sure to reflect the correct port in this setting.
   c Save the file.
2 Open a console window and cd to <Install_Dir>\SERVERS\Database\bin.
3 Run the batch file tsexec AddReplPeer.bat N_IP_address with the parameter specifying IP address of “N”.

Step 2 of 5: on peer “B”

1 Edit file <Install_Dir>\SERVERS\Shared\sccservers.ini:
   a In the line starting with ‘ReplPrev_JDBC_URL’, replace name or address of Previous peer on that line (“A”) with the name or IP address of “N”.
      If the database on “N” was installed on a custom port (other than 5010),
Step 3 of 5: on peer “N”

**Important:** Before starting these procedures, make sure you have installed SAM Express on this peer machine.

1. Start your management console, login, and **Restore** the database from the backup set you originally created on “A” or “B”.
   
   The data on “A”, “B” and “N” should now be almost in sync, barring any changes that took place since the backup set was created.

2. **Stop** the Admin Server and Authentication Engine.

**Important:** Do NOT stop the database server.

3. Edit file `<Install_Dir>\SERVERS\Shared\sccservers.ini`:
   
   4. Uncomment line starting with ‘DBActionListenerClass’.
      
      This allows the Admin server to track changes by ‘listening’ to actions in the database and recording them as new records in the change log.

   5. Locate and uncomment line starting with ‘ReplNext_JDBC_URL’

   6. Replace name or address of **Next** peer on that line (which should have been NEXT_HOST) with the name or IP address of “B”.
      
      If the database on “B” was installed on a custom port (other than 5010), make sure to reflect the correct port in this setting.

   7. Locate and uncomment line starting with ‘ReplPrev_JDBC_URL’.

   8. Replace name or address of **Previous** peer on that line (which should have been ‘PREV_HOST’) with the name or IP address of “A”. If the database on “A” was installed on a custom port (other than 5010), make sure to reflect the correct port in this setting.

9. **Save** the file.

10. Open a console window and cd to `<Install_Dir>\SERVERS\Database\bin`.

11. Run batch file `tsexec AddReplPeer.bat A_IP address` with the parameter specifying the IP address of “A”.

12. Run batch file `tsexec AddReplPeer.bat B_IP address` with the parameter specifying the IP address of “B”.

13. **Start** the Admin Server and Authentication Engine.

**Step 4 of 5: on peer “A”**
Chapter 10: Replication

Verifying SAM Express server replication

Start the Admin Server and Authentication Engine so any changes that may have occurred since the backup will be propagated to “N”.

To verify that server replication is working, perform the following tests on any system in the server replication ring.

**Important:** Do not use this process if you have already associated tokens to users. The procedure for testing the token import process is only applicable when you are initially setting up two or more machines.

### Testing replication setup

There are two quick tests you can run to verify that your replication ring is set up and running properly:

- Assign (or unassign) a PIN to a token and verify the token PIN on the other server(s) was correctly added or cleared.
- Import a token and verify that the newly imported token data has replicated on all other server(s) in the ring.

After running one of these two quick tests, check the other servers to see if the change was replicated to each. Then, do the same on each other server to make sure it propagates the change to its neighbors.

### Checking server replication state

To confirm that SAM Express server replication is in a steady state (meaning all changes are replicated), do the following:

**Important:** You must perform the following procedure on each server in the ring.

1. Open a command window and cd to `<Install_Dir>\SERVERS\Database\bin`.
2. Run the batch file called `QueryChangeLog`.
   
   The system has reached steady state once the output reads: **Empty set**.

### Troubleshooting

Troubleshooting steps and corrective actions can be found in “Troubleshooting Replication” on page 311.
Managing the RADIUS Servers

In this chapter...

Overview of the SAM Express RADIUS server ......................... 286
Prerequisites ................................................................................ 288
SAM Express RADIUS configuration files ................................. 288
Authorization and configuration groups .................................... 289
Authenticators .............................................................................. 292
References ................................................................................... 296
Understanding the RADIUS Accounting server ....................... 301
How the server works ................................................................ 302
Configuring the server .............................................................. 302
Starting the server .................................................................... 302
Troubleshooting ........................................................................ 303
As networks grow and branch out to remote locations, network security increases in importance and administration complexity. Customers need to protect networks and network services from unauthorized access by remote users. RADIUS is one of the protocols commonly used to provide these solutions in today's internetworks.

**RADIUS protocol**

Authentication is the process of identifying and verifying a user. Several methods can be used to authenticate a user, but the most common includes a combination of user name and password. Once a user is authenticated, authorization to various network resources and services can be granted. Authorization determines what a user can do, and accounting is the action of recording what a user is doing or has done.

The RADIUS protocols define the exchange of information between these components in order to provide authentication, authorization, and accounting functionality. The RADIUS protocol, as published by Livingston, is a method of managing the exchange of authentication, authorization, and accounting information in the network. RADIUS draft was submitted to the Internet Engineering Task Force (IETF) as a draft standard in June, 1996. RADIUS is a fully open protocol.

**The RADIUS server**

The RADIUS Server is an authentication protocol server daemon that has been interfaced with SAM Express through the EASSP protocol. It supports all of the RADIUS functionality documented in Internet RFC 2138, and all functionality as documented in SAM Express publications, with minor restrictions on multiple simultaneous dynamic password authenticators. The RADIUS Server can be located on a separate computer, distinct from any computer that houses the SAM Express AAA server. It can also be located on the same computer as the AAA server.

**RADIUS server features**

- Fully RFC 2138 compliant
  
  The RADIUS Server is fully RFC 2138 compliant.

- Supports group authorization
  
  The RADIUS Server supports authorization and configuration groups named in the SAM Express directive. The SAM Express record for any user can list the name of a group record defined in the RADIUS users file.

  Most users can be treated as members of a group of users that will receive
identical treatment with regard to network authorization. For example, a company with 500 employees may have a group of 40 salespersons that all need permission to dial into the corporate network via modem, and that all need access to the computer hosting the sales database. This group mechanism allows all 40 of those salespersons to be assigned to the sales group and to be administered simultaneously. Any administrative change to the definition of the sales record will immediately affect all 40 sales users.

• User-specific attributes support
Some RADIUS attributes are closely associated with a specific user, and do not lend themselves well to administration as part of a large group of users. For example, it may be desirable to assign a specific IP address to a specific person every time he or she is attached to the Internet. The RADIUS Server supports user-specific RADIUS attributes matching a user or group name in the user’s file. This user-specific mechanism allows administrators to store arbitrary RADIUS attributes directly inside the return field of the appropriate ACL entry.

• CHAP support
Administrators can manage CHAP authenticators in the same way they support all other authenticator types.

• Vendor-Specific Attributes support
The RADIUS Server provides full support for Vendor-Specific Attributes (VSAs) in accordance with the provisions of RFC 2138. VSAs allow vendors of routers, communication servers, or other RADIUS-compatible clients to take full advantage of the unique features of their equipment. Under the provisions of the current RADIUS protocol, any vendor can teach his RADIUS-compatible client equipment to accept and carry out one or more vendor-specific commands through the RADIUS protocol.

The RADIUS Server is capable of sending any RADIUS-compliant VSA to any RADIUS client after authentication, whenever the data associated with an authenticated user references a VSA.

• RADIUS Proxy support
The RADIUS Server was enhanced with the ability to support informal “RADIUS proxy forwarding”.

• RADIUS accounting support
The RADIUS protocol includes provisions for storing messages from RADIUS clients. These are generally used to keep records of network access activity for accounting purposes. The RADIUS Server can store these messages in a file for offline analysis.

• Extensive diagnostics level
The RADIUS Server provides extensive diagnostic levels to help troubleshoot RADIUS authentication sessions.
Prerequisites

To run the RADIUS Server, you need the following:

- **At least one RADIUS-compatible client**
  The RADIUS Server will listen for RADIUS requests from RADIUS clients. Therefore, at least one RADIUS-compatible client is required. A RADIUS-compatible client may be a router, communication server, VPN, firewall, or an application.

- **SAM Express Authentication, Authorization and Accounting (AAA) Server**
  The RADIUS authentication requests received by the RADIUS Server from the RADIUS client(s) must be forwarded to the SAM Express AAA server daemon.
  The RADIUS Server issues a request that is formatted according to the conventions of the authentication protocol, and transmits it across the network. If an authentications server is listening for such requests, it can be serviced.

- **RADIUS users registered in the SAM Express User database**
  All users that need to be authenticated by SAM Express must be registered in the SAM Express User database. Users must be registered in the SAM Express database if the Authentication Broker is not going to be used.

SAM Express RADIUS configuration files

The RADIUS Server has five configuration files:

- clients
- dictionary
- users
- radius.cfg
- authfile

You can modify the above files from **Start > Programs > SafeNet > SAM Express > Configuration > RADIUS Server Configuration**.

The RADIUS configuration files, clients, and the `radius.cfg` can be found in `<Install_Dir>\SERVERS\RADIUS\RADIUSServer`, and can be edited manually, if needed.
The RADIUS Server supports authorization and configuration groups named in the SAM Express databases.

### Creating a login ACL entry and role for RADIUS

The following steps will take you through the process of adding a login ACL entry and role for your RADIUS users.

To create a login ACL entry, create either a new ACL just for RADIUS users, or add a RADIUS-specific entry to an existing ACL (see “Creating login ACLs” on page 175).

1. Create a role for this set of users (see “Creating roles” on page 180).
2. In the ACL entry, click the **Subject** tab, and set the following parameters:
   - Some Users.
   - Role = (whatever role you created in step 1).
3. Click the **Restrictions** tab, and set restrictions for these users.
4. Click the **Return** tab, and set the following parameters:
   - Authentication Status = Success
   - Select the **Return a value on successful authentication** box
   - Click the **Text** option
   - Enter **group=Develop** in the text field.

**Note:** The Develop group must exist in the users file. It is case-sensitive.

5. Create the users that will use the role you have created.

### Configuring the groups in the Users file

The *Users* file defines the names of all users and the type of authentication that will be demanded of each user. Everything handled by the industry-standard Livingston RADIUS Server is handled in the same way by the RADIUS Server. In addition, the following items can be inserted into the *users* file when used with the RADIUS Server:

- SAM Express (as a password indicator)
- Authorization and configuration group records

When the special keyword “SAM Express” is inserted into the *users* file, it must follow the special keywords “Password =”. This indicates that authentication for the user described in the associated record must come from SAM Express.

Authorization and configuration group records (or **group records**) are unique to the RADIUS Server, and are not familiar to administrators that have been working with the Livingston RADIUS Server. Like the familiar “user” records
that dominate the bulk of Livingston’s *Users* file, group records always begin with a name. However, instead of representing an individual with a name like “fred,” group records represent multiple people and tend to use descriptive names, such as “Developers” or “Sales.” Unlike user records, group records never contain a “Password =“ attribute, because they are always authenticated through SAM Express. Group records can contain any combination of legal RADIUS attributes, and are used to configure data communication parameters and authorization privileges for groups of users after their identities have been positively authenticated by SAM Express.

**The DEFAULT user record**

The record in the *Users* file that specifies the username as “DEFAULT” deserves special attention. It is used to handle all users whose names do not match the names of any other user records in the *Users* file. Thus, the DEFAULT record can be set up to demand SAM Express authentication and is sometimes the only user record in the *Users* file. Most administrators take full advantage of this mechanism to simplify their administrative duties. The sample *Users* file on page 298 illustrates this type of setup. This arrangement minimizes the need to edit the *Users* file.

Although the RADIUS Server supports all of the features of the Livingston users file, in practice the *Users* file in RADIUS Server situations is generally much simpler than the corresponding file used by Livingston RADIUS Servers. This is because the high-performance SAM Express database can better handle user authentication, assigns each user to an appropriate group record, and can supplement the group record attributes with any required user-specific attributes. Therefore, a typical *Users* file might contain only one “DEFAULT” user record and a small number of group records that are rarely changed.

**Configuring the RADIUS proxy**

The RADIUS Server supports the proxy mechanism to another RADIUS Server. The *authfile* is used in support of the increasingly popular “RADIUS proxy forwarding” mechanism.

When present, the *authfile* defines the relationships between cooperating pairs of RADIUS Servers so that they can use “RADIUS proxy forwarding” to send RADIUS requests and replies to one another. SafeNet’s interpretation of the contents of *authfile* is a compatible subset of the well-known conventions established by Merit Networks Incorporated and has been distributed as a part of their free enhanced RADIUS Server since they introduced RADIUS proxy forwarding to the RADIUS community.

Understanding RADIUS proxy forwarding and the *authfile* requires prior understanding of the following concepts and definitions:

- Specially formatted usernames
If a username contains an embedded @ sign, then the RADIUS Server will interpret it in two separate portions in support of RADIUS proxy forwarding. Any text to the left of the @ will be interpreted as the SAM Express-compatible user name. Any text to the right of the @ represents what Merit calls a “realm” and, after an authfile lookup, leads to the location of another RADIUS Server, which should know how to proceed further. Thus, if the RADIUS username field contained “Bob@NYC,” then the name of the realm is “NYC.” You can override the default site character by running RADIUS with the argument -r <char>. By default, it is “-r @”.

- Realms

The authfile associates realm names with specific RADIUS Servers. Inside the authfile, separate lines of printable text always begin with the name of separate realms. After the realm name, each line also contains the special keyword “RADIUS” (indicating that the RADIUS protocol will be used to authenticate users associated with this realm) and then the DNS name or IP address of a RADIUS Server where requests can be forwarded to satisfy the authentication requirements of that realm.

The destination RADIUS server is the one whose name matches the realm part of the username. It follows the site character. For example, in the auth file entry “NYC RADIUS 192.168.14.23”, for the user Bob@NYC, NYC is the realm. Packets will be forwarded to the IP address 192.168.14.23 on the port (taken from the users file) of 1812.

It is possible to proxy to other RADIUS servers running on a different port. To enable this, the clients file is consulted.

<table>
<thead>
<tr>
<th>IP [:port]</th>
<th>Keyword</th>
<th>[NAS: PROXY]</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.100</td>
<td>1234</td>
<td>NAS</td>
</tr>
<tr>
<td>192.168.14.23</td>
<td>MySecret</td>
<td>PROXY</td>
</tr>
<tr>
<td>192.168.14.23:1812</td>
<td>TooManySecrets</td>
<td>PROXY</td>
</tr>
</tbody>
</table>

**Note:** The Network Access Server (NAS) field of the previous table is for clients (if one client has a NAS, all other clients must also), and PROXY is when this server will become a “middle man” and needs to send data to another RADIUS server.

- Server position

When RADIUS proxy forwarding is in use, each RADIUS Server can be a member of a chain of cooperating RADIUS servers, and within that chain, each server can perform any of three distinct roles, depending on whether its position is first in the chain, last in the chain, or somewhere in between. The first RADIUS Server in the chain is the only one that ever communicates directly with the originating RADIUS client. The “middle” RADIUS Servers simply forward RADIUS requests to the next member of the chain after adding a tiny place-marker attribute to the packet. The RADIUS
Servers remove their own place marker attributes from the resulting response packets on the return trip, before forwarding those responses back to the next link of the chain in the opposite direction. Therefore, although “later” links in the chain can see the place markers of earlier links, earlier links in the chain never see any of the attributes of the later links, and by the time the response packet arrives back at the originating RADIUS client, all routine proxying information is removed so it can look just like a “normal” packet that has never been forwarded.

The last link in the chain of RADIUS Servers determines that it is the last link by consulting the authfile and identifying its own name as the RADIUS Server associated with the realm in use. The RADIUS Server will then make the final determination as to the identity of the requesting user, construct the reply packet granting or denying access, and return it to the RADIUS Server that sent the request packet.

Authenticators

The RADIUS Server supports all hardware and software authenticators that are compatible with SAM Express, which allows you to assign up to three authenticators per user. You can specify their use in any combination, but you may only require any combination of two authenticators per authentication. For more information on assigning authenticators to a user’s record, refer to “Creating user accounts manually” on page 206.

You can assign two authenticators to a user by assigning a memorized password and a dynamic password authenticator. However, you cannot assign two memorized passwords or two dynamic passwords to a user.

RADIUS-encrypted memorized passwords

A memorized password is best handled by typing it at the RADIUS password prompt. For example:

Username: Fred
Password: ******

In the above example, the user, Fred, typed his memorized password at the RADIUS password prompt. The RADIUS client obscures unauthorized viewing of the password response by displaying asterisks in place of the actual keystrokes.
Memorized passwords appended to usernames

A memorized password can be handled by typing it into the RADIUS username field, separated from the username by a comma. For example:

Username: **Fred,merchantmarine**
Password: 

In the above example, a user, Fred, typed his memorized password, “merchantmarine” at the RADIUS username prompt, separating it from his username with a comma. The password prompt was left blank. This method does not obscure memorized passwords from view of passerbys. The entire contents typed at the username prompt, including the password in this case, are always transmitted in clear text across the network inside RADIUS packets. For these reasons, this method is not recommended for general use, but may be useful when troubleshooting a system if it is necessary to trace accurate delivery of a password.

*Note: Neither a username nor memorized passwords can contain a comma because a comma is a special character used to separate usernames from passwords.*

RADIUS-encrypted synchronous dynamic passwords

A synchronous dynamic password may be typed into the RADIUS password prompt. For example:

Username: **Fred**
Password: ******

In the above example, Fred obtains the proper synchronous dynamic password by activating a button on his hardware or software authenticator, and enters the displayed value into the RADIUS password field after seeing the Password prompt. The RADIUS client obscures the password by displaying asterisks in place of Fred's actual keystrokes.

Synchronous dynamic passwords appended to usernames

As an alternative, a synchronous dynamic password may be typed into the RADIUS username prompt, separated from the username by a comma. For example:

Username: **Fred,139ac2**
Password: 

In the above example, Fred typed his dynamic password at the RADIUS username prompt, separating it from his username with a comma. The password prompt was left blank.

This method does not obscure dynamic passwords as they are typed, and the entire contents of the Username field, including the password in this case, are always transmitted in clear text across the network inside RADIUS packets. However, this does not present a security risk because the dynamic password is nonreplayable.

**Shared tokens with memorized passwords**

There may be times when end users may have both a memorized password and a dynamic synchronous password authenticator. This occurs when several people share one token, but each has their own memorized password. When authenticating to RADIUS, special handling of these passwords is necessary to correctly authenticate.

The following two examples show how to correctly enter passwords in this situation:

**Example 1:** Enter the dynamic after the username in the format:
Username: “<name>,<dynamicPW>”
Password: “<fixed>”

Username: **Fred,23E4A7**
Password: **merchantmarine**

**Example 2:** Enter the dynamic and the memorized in the password field:
Username: “<name>”
Password: “<dynamic>,<fixed>”

Username: **Fred**
Password: **23E4A7,merchantmarine**

*Note: Passwords in the Password field are obscured.*
Asynchronous dynamic password authenticators

A user who has an asynchronous challenge/response authenticator is unable to determine the proper dynamic password until after they have received a SAM Express “challenge”. Their RADIUS dialog always has two phases, as in the example below.

- **Username:** Fred
- **Password:**
- **Challenge:** 1251
- **Response:** 2ap9

In the first phase, a user named Fred types his username and presses the **Enter** button at the Password prompt. A challenge is displayed almost immediately, which he types into his authenticator. Fred receives a new password response from his authenticator, and types the password at the response prompt.

CHAP-encoded encapsulated dynamic passwords

Some RADIUS clients (e.g., Microsoft's Windows NT RAS) always insist on CHAP-encoding the RADIUS password field, which renders the data inside that field useless in dynamic password situations such as those generally desired by customers. (The CHAP authentication algorithm encodes the data as one-way, which cannot be decoded.)

In order to compensate, a user may type his or her dynamic password adjacent to their username in the RADIUS username field, separated by a comma. For example, if Fred’s synchronous dynamic password is 1316, the RADIUS sign on dialog will look like this:

- **Username:** fred,1316
- **Password:**

If Fred were using an asynchronous, challenge-response dynamic password authenticator, the dialog would look like this:

- **Username:** fred
- **Password:**
- **Challenge:** 2155
- **Username:** 2900

In the above example, the first comma after “fred” informs the RADIUS Server that the username field will be used to communicate the dynamic password after the challenge is displayed.

If the RADIUS Server receives a RADIUS access-request packet containing only a RADIUS-encapsulated, CHAP-encoded memorized password, which is
evaluated as correct, it always responds with an access-accept packet, as RADIUS-oriented customers would expect. Therefore, if administrators want to confirm identity with a stronger authenticator, they should register ONLY that stronger authenticator (e.g., a SAM Express hardware authenticator) in the SAM Express database, and not allow the option of entry with a memorized password at all. Alternatively, administrators may set the minimum authenticator strength in the ACL to be higher than the value of a fixed password.

References

- RFC 2138
- Sample files (see below)

Sample Dictionary file

The example below shows a sample Dictionary file that is known to be compatible with the current version of the RADIUS Server. Lines that begin with a pound sign (#) are comments that are not interpreted by the RADIUS Server as it scans for dictionary information. Those lines contain information intended to help administrators understand the meaning, context, and format of the Dictionary file.

ATTRIBUTE User-Name 1string
ATTRIBUTE Password2string
ATTRIBUTE CHAP-Password3string
ATTRIBUTE Client-Id4ipaddr
ATTRIBUTE Client-Port-Id5integer
ATTRIBUTE User-Service-Type6integer
ATTRIBUTE Framed-Protocol7integer
ATTRIBUTE Framed-Address8ipaddr
ATTRIBUTE Framed-Netmask9ipaddr
ATTRIBUTE Framed-Routing10 integer
ATTRIBUTE Filter-Id11 string
ATTRIBUTE Framed-MTU12 integer
ATTRIBUTE Framed-Compression13 integer
ATTRIBUTE Login-Host14 ipaddr
ATTRIBUTE Login-Service 15 integer
ATTRIBUTE Login-TCP-Port 16 integer
ATTRIBUTE Old-Password 17 string
ATTRIBUTE Port-Message 18 string
ATTRIBUTE Dialback-No 19 string
ATTRIBUTE Dialback-Name 20 string
ATTRIBUTE Expiration 21 date
ATTRIBUTE Framed-Route 22 string
ATTRIBUTE Framed-IPX-Network 23 ipaddr
ATTRIBUTE Challenge-State 24 string
ATTRIBUTE Vendor-Specific 26 string
ATTRIBUTE Called-Station-Id 30 string
ATTRIBUTE Calling-Station-ID 31 string
ATTRIBUTE Acct-Status-Type 40 integer
ATTRIBUTE Acct-Delay-Time 41 integer
ATTRIBUTE Acct-Session-Id 44 string
ATTRIBUTE Acct-Authentic 45 integer
ATTRIBUTE Acct-Session-Time 46 integer
ATTRIBUTE NAS-Port-Type 61 integer

VENDORATTR 9cisco-avpair1 string

#
#       Integer Translations
#
#
#       User Types
#
VALUE User-Service-TypeLogin-User 1
VALUE User-Service-TypeFramed-User 2
VALUE User-Service-TypeDialback Login-User 3
VALUE User-Service-TypeDialback-Framed-User 4
VALUE User-Service-TypeOutbound-User 5
VALUE User-Service-TypeShell-User 6
VALUE User-Service-TypeAuthenticate-Only 8
VALUE User-Service-TypeCallback-NAS-Prompt 9

#
#       Framed Protocols
#
VALUE Framed-ProtocolPPP 1
VALUE Framed-ProtocolSLIP 2

#
#       Framed Routing Values
#
VALUE Framed-RoutingNone 0
VALUE Framed-RoutingBroadcast 1
VALUE Framed-RoutingListen 2
VALUE Framed-RoutingBroadcastListen 3

#       Framed Compression Types
Sample Users file

The example below shows a sample Users file known to be compatible with the current version of the RADIUS Server. All lines beginning with a pound sign (#) are comment lines. The RADIUS Server ignores them. They are intended to provide guidance for RADIUS Server administrators.
# Group of PPP users

```plaintext
ppp
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-Netmask = 255.255.255.255,
Framed-Routing = None,
Framed-Compression = Van-Jacobsen-TCP-IP,
Framed-Filter-Id = "std.ppp.in"
Framed-MTU = 1500
```

# Group of SLIP users

```plaintext
slip
User-Service-Type = Framed-User,
Framed-Protocol = SLIP,
Framed-Netmask = 255.255.255.255,
Framed-Routing = None,
Framed-Compression = None,
Framed-MTU = 1006
```

# Group of cslip users

```plaintext
cslip
User-Service-Type = Framed-User,
Framed-Protocol = SLIP
Framed-Netmask = 255.255.255.255,
Framed-Routing = None,
Framed-Compression = Van-Jacobsen-TCP-IP,
Framed-MTU = 1006
```

# Example Group of Developers using Dialup connections, whose privileges are limited

```plaintext
Develop
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-Netmask = 255.255.255.128,
Framed-Routing = None,
Framed-Compression = Van-Jacobsen-TCP-IP,
```
Framed-MTU = 1500,
Filter-Id = Developers,
Filter-Id = Dialin

# By default, use SAM Express for authentication and SAM
Express will assign users to one of the Group Records
defined above. (SAM Express should also generally be set
up to assign any static IP addresses.)
#
DEFAULT Password = "SAM Express"

Sample authfile

The example below shows a sample authfile configured to demand RADIUS
authentication for the DEFAULT domain through a server which is known as
"last.samplecompany.com."

# This file contains a list of separate "realms" that use the
RADIUS protocol to authenticate users requesting access,
together with the DNS name or IP address of a RADIUS server
to which RADIUS requests should be forwarded for that
domain. This allows several RADIUS servers to share the
burden of authenticating a large population of users, with
each RADIUS server handling a separate, named group or
"domain" of authorized users.
#
The first field of each line is a realm name. All realm
names must be unique within a separate IP network, and all
must be referenced with the exact same name in all authfiles
of all cooperating RADIUS servers.
#
The second field identifies the type of authentication
required by the associated realm. For this version of the
SAM Express RADIUS server, the only authentication allowed
is "RADIUS".
#
The third field contains the DNS name or IP address of the
RADIUS server that is equipped to provide further
authentication services for this domain. In a chain of
forwarding RADIUS servers, it points at the next RADIUS
server in the chain. For the last server in the chain, this
field will contain the DNS name or IP address of the host
containing this file. (The last server in the chain will use
this field to point to itself.) Each of the DNS names or IP
addresses referenced in this file must match an entry in the
“clients” file so that a corresponding cryptographic key can be located. A DEFAULT entry may be included in this file which indicates how to handle authentication requests specifying realm names not explicitly included in this file. It will specify an available RADIUS server to which this request should be relayed.

# Here are some sample entries for realms called “first”, “middle”, and “last” respectively, to illustrate how to configure a chain of RADIUS servers. In these examples, the three RADIUS servers belong to a company called “samplecompany.com”.

```
first           RADIUS          middle.samplecompany.com
middle          RADIUS          last.samplecompany.com
last            RADIUS          last.samplecompany.com
```

Finally, this “DEFAULT” entry says to pass requests with authentication realm names which didn't appear in this file along to another RADIUS server called “last.samplecompany.com”:

```
DEFAULT                            RADIUS
last.samplecompany.com
```

The RFC 2139 describes a protocol for carrying accounting information between a Network Access Server (NAS) and a shared accounting server. The NAS operates as a client of the RADIUS Accounting Server. The client is responsible for passing user accounting information to a designated RADIUS Accounting Server. The RADIUS Accounting Server then receives the accounting request and returns a response to the client indicating that it has successfully received the request.

The received information from the client(s) by the RADIUS Accounting Server includes:

- The time the session started for the user
- The time the session ended for the user
- System events

The received information is usually used for billing purposes.
How the server works

The SAM Express RADIUS Accounting Server listens for RADIUS accounting packets formatted according to the guidelines found in Internet RFC 2139. Whenever this server receives a properly formatted RADIUS accounting-request packet, it writes the contents of that packet to a disk file and then responds with a RADIUS accounting-response packet.

- The RADIUS accounting information is stored in a plain text file on the same machine where the RADIUS Accounting servlet is located.
- The SAM Express RADIUS Accounting Server software is a standalone service that does not interface with SAM Express, so it does not use the Authentication SDK.

Configuring the server

The RADIUS Accounting Server contains two configuration files: clients and dictionary (it does not need a users file). You must edit the clients file and provide the IP addresses and "RADIUS secrets" used by your RADIUS clients.

The RADIUS Accounting Server daemon listens to RADIUS accounting requests on port 1813 UDP, the /etc/services file must contain a line, such as:

```
radacct 1813/udp
```

The RADIUS accounting must be enabled in the client(s) (comm server(s)).

Starting the server

To start or stop the RADIUS Accounting Server service, use the Services function available in the Administration Tools, select the Accounting RADIUS Server and click on Start or Stop.

You can also start the RADIUS Accounting Server in debug mode from the command line, where you can specify different levels of diagnostics.

The following is an example of a typical command to start the RADIUS Accounting Server:

```
./radacctd -a . -d . -x 1 &
```

where

- `-a` specifies the directory to store accounting file detail
- `-d` specifies the location of clients and dictionary files
- `-x` specifies the level of debug (up to 8191)
Example: Enabling accounting on Cisco router

```
> radius-server host 192.168.24.42
For Windows: auth-port 1812 acct-port 1813
  • aaa accounting system start-stop radius
  • aaa accounting network start-stop radius
  • aaa accounting connection start-stop radius
  • aaa accounting exec stop-only radius
  • aaa accounting command 1 stop-only radius
  • aaa accounting command 15 wait-start radius
```

Sample accounting data

This sample shows an administrator telnetting to the router.

```
Fri Jan 1 03:38:35 1999
  • NAS-IP-Address = 192.168.24.115
  • NAS-Port = 11
  • NAS-Port-Type = Virtual
  • User-Name = “super”
  • Calling-Station-Id = “192.168.24.76”
  • Acct-Status-Type = Stop
  • Acct-Authentic = RADIUS
  • Service-Type = NAS-Prompt
  • Acct-Session-Id = “00000026”
  • Acct-Session-Time = 3
  • Acct-Delay-Time = 0

Fri Jan 1 03:38:40 1999
  • NAS-IP-Address = 192.168.24.115
  • NAS-Port = 11
  • NAS-Port-Type = Virtual
  • User-Name = “super”
  • Calling-Station-Id = “192.168.24.76”
  • Acct-Status-Type = Stop
  • Acct-Authentic = RADIUS
  • Service-Type = NAS-Prompt
  • Acct-Session-Id = “00000026”
  • Acct-Session-Time = 3
  • Acct-Delay-Time = 5
```

Troubleshooting

Troubleshooting steps for the RADIUS server are found in “Troubleshooting the RADIUS server” on page 318.
In this chapter...

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>General troubleshooting</td>
<td>306</td>
</tr>
<tr>
<td>Troubleshooting AD lockout support</td>
<td>310</td>
</tr>
<tr>
<td>Troubleshooting Replication</td>
<td>311</td>
</tr>
<tr>
<td>Troubleshooting the RADIUS server</td>
<td>318</td>
</tr>
<tr>
<td>Uninstalling SAM Express</td>
<td>321</td>
</tr>
</tbody>
</table>
This section contains general troubleshooting information you may use if you encounter issues during installation, activation, configuration, or management of SAM Express.

For additional information, visit the SafeNet Knowledge Base at www.safenet-inc.com/technical-support.

**Table 18: Troubleshooting SAM Express**

<table>
<thead>
<tr>
<th>Subject</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Installation | Installation aborts | • Does target system meet all prerequisites/requirements?  
• Check the install.log found in *(32 bit OS) Program Files\SafeNet\SAM Express\Installs*, or *(64 bit OS) Program Files (x86)\SafeNet\SAM Express\Installs* for obvious errors. |
<table>
<thead>
<tr>
<th>Subject</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Activation</strong></td>
<td>Activation fails</td>
<td>• Confirm that only the name <code>key.html</code> is being used (any variations on this name will result in activation failure).&lt;br&gt;• Contact Technical Support at 800-545-6608; provide activation key and error message.</td>
</tr>
<tr>
<td></td>
<td>Initial evaluation period has expired, but evaluation has not been completed.</td>
<td>Contact Technical Support at 800-545-6608.</td>
</tr>
<tr>
<td></td>
<td>Initial evaluation period has expired, but you would like to evaluate ESP.</td>
<td>Contact Technical Support at 800-545-6608.</td>
</tr>
<tr>
<td></td>
<td>You just renewed support, but the ADUC Snap-in support expiration date has not changed.</td>
<td>Re-activate SAM Express:&lt;br&gt;• Right-click the SAM Express node (in ADUC) and select Activate Product, or&lt;br&gt;• Go to the Portal, login, and provide your SAM Express serial number. Download the <code>key.html license key</code>. You will need to confirm that this key is named <code>key.html</code>. Place it in your SAM Express activation folder, and then restart the SAM Express Administration Server service. Upon successful activation, this license will be renamed to <code>key.activated.html</code>.</td>
</tr>
<tr>
<td><strong>Auto Updater</strong></td>
<td>Auto Updater fails.</td>
<td>• Run existing Auto Updater (which will fail).&lt;br&gt;• Go to Program Files <code>\SafeNet\SAMx\Patches</code>, launch <code>SccUpdateAgent.exe</code> (manually patches AUA to newest version).</td>
</tr>
</tbody>
</table>

*More...*
<table>
<thead>
<tr>
<th>Subject</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuration</strong></td>
<td>Error messages occur during configuration</td>
<td>Use the Configuration Utility to turn on logging for the component you are trying to configure. (See “Logging server diagnostics” on page 253.)</td>
</tr>
<tr>
<td></td>
<td>Configuration was changed, but change was not reflected</td>
<td>Verify the appropriate server(s) or service was restarted after the configuration was changed.</td>
</tr>
<tr>
<td></td>
<td>Error message when attempting to access the SAM Express tab from a user’s Properties window</td>
<td>Confirm the status of the user’s client certificate, and/or get a new certificate for a user. See “Reinstalling a server or ADUC” on page 87.</td>
</tr>
<tr>
<td></td>
<td>Successful authentication, but access is denied</td>
<td>View your event logs to verify what is occurring. (See “Viewing event logs” on page 83.)</td>
</tr>
<tr>
<td></td>
<td>Clicking on the SAM Express node in ADUC gives the error “You must be an administrator to use the ADUC snap-in.”</td>
<td>Caused by attempting to log in as parent domain admin to a server installed in a child domain. Add the parent domain admin to the local server’s “administrators” group.</td>
</tr>
</tbody>
</table>

*More...*
<table>
<thead>
<tr>
<th>Subject</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
</table>
| Authentication           | Authentication fails                         | • Verify proper entry of token password.  
• Has token been imported?  
• Verify match between token serial number and serial number of token assigned in user record.  
• Verify user properly entered their user name at login.  
• Confirm the IP address of the SAM Express server is correctly entered on the proper Authentication Settings field of the Administration window. |
| Successful authentication, but access is denied | Check user access.  
• View audit logs (refer to “Viewing a specific user's authentication activity” on page 229).  
• Verify user name is correct.  
• Check user status (account expired / locked, etc.).  
• Is user role correct?  
• Does user’s role point to the correct ACL?  
• Does ACL entry restrict access to the requested resource? | |
| Importing authenticators | All import records rejected                   | Check to see if the authenticators had been previously imported (use audit log in the SAM Express 2008 Management Console or the Event Viewer in ADUC, check by event type). |
|                          | Some import records rejected                  | Check to see if the authenticators had been previously imported (use audit log in the SAM Express Management Console or the Event Viewer in ADUC, check by event type). |
| Ports                    | How to determine if a port is active?         | For Windows, use the `netstat -an`, then search the output manually for active ports.                                                    |
### Troubleshooting AD lockout support

Troubleshooting the AD lockout feature can be done by setting the following three parameters (which control logging of the SccADHelper module):

<table>
<thead>
<tr>
<th>Subject</th>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>Server(s) not responding</td>
<td>1 Use installation and management utility to determine if servers are running.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 Restart server(s).</td>
</tr>
<tr>
<td></td>
<td>Need to restart server(s)</td>
<td>See “Stopping and starting servers” on page 252.</td>
</tr>
<tr>
<td>Uninstalling</td>
<td>After uninstalling and reinstalling SAM Express, access to the SAM Express folder is denied</td>
<td>Uninstalling SAM Express may not completely remove all files related to the software. Ensure that all directory and registry content has been removed, then reinstall the software.</td>
</tr>
</tbody>
</table>

**Parameter: LogFile**  
Value Type: REG_SZ  
Default: none  
Description: Specifies the fully qualified path to the log file for SccADHelper.

**Parameter: LogFileFlags**  
Value Type: REG_DWORD  
Valid Range: 0, 1, 2, 3  
Default: 0  
Description: Controls the default level:

0 - None  
1 - Errors, Info, Debug  
2 - Errors, Info  
3 - Errors

**Parameter: MaxFileSize**  
Value Type: REG_DWORD  
Default: 100  
Description: The maximum size, in KB, of the log file before rolling over to a new file.
Table 19 contains a series of troubleshooting symptoms and their possible causes that can help in locating and correcting technical issues.

If you need to contact SafeNet’s Technical Support, it would be helpful to have on-hand the `sccservers.ini` file from each SAM Express server, and make sure its filename contains the server’s IP address and/or name.

**Important:** If any of the resolutions listed here involve changing the `sccservers.ini` file, the Admin server will need to be restarted for the change(s) to take effect.

Table 19: Troubleshooting replication

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Poss. cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>When attempting to connect to MySQL, the message below appears. <strong>ERROR 2003: Can't connect to MySQL server on 'localhost' (10061)</strong></td>
<td>Terminal Services is running in execute mode.</td>
<td>Switch Terminal Services to install mode so MySQL is executed using local workstation paths. Use one of the following 2 methods: 1 Run the following command first ‘change user /install’. 2 Run the scripts listed to the left using the <code>tsexec.exe</code>. Examples: <code>tsexec.exe AddReplPeer.bat &lt;IPaddress&gt;</code> <code>tsexec.exe QueryChangeLog.bat</code> <code>tsexec.exe mysql –u root -ppassword</code></td>
</tr>
<tr>
<td>Replication is not working. • QueryChangeLog.bat never shows entries in the ChangeLog. (Empty Set) • No errors found in SccAdSrvcLog.txt or SAM Express EV log.</td>
<td>Replication is not enabled in the <code>sccservers.ini</code> file.</td>
<td>Verify #DBActionListenerClass line in <code>sccservers.ini</code> file is uncommented. This line must be uncommented in order to turn replication ON and for DB changes to be propagated to the ChangeLog.</td>
</tr>
</tbody>
</table>

More...
## Troubleshooting Replication

### Replication is not working

1. **QueryChangeLog.bat** shows the # of entries is growing in the ChangeLog.
2. No errors found in *SccAdSrvrlog.txt* or SAM Express EV log.

### Symptom Poss. cause Resolution

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Poss. cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication is not working</td>
<td>Replication peers are not enabled in the <em>sccservers.ini</em> file.</td>
<td>Verify the appropriate ReplNext and/or ReplPrev lines are uncommented and properly configured.</td>
</tr>
<tr>
<td>Replication is not working</td>
<td>Replication peer(s) not configured to point to localhost.</td>
<td>Verify the appropriate ReplNext and/or ReplPrev lines are properly configured for the IP/host name of the replication peers and are not configured for the <em>localhost</em> address.</td>
</tr>
<tr>
<td>Replication is not working</td>
<td>Replication peers are not time-synced</td>
<td>In the message to the left, the local server appears to fail to replicate to its ReplNext because the ReplNext contains a newer entry. The symptoms listed to the left may indicate that the local server's date/time settings are behind the ReplNext.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In the message to the left, the local server appears to fail to replicate to its ReplNext because the ReplNext contains a newer entry. The symptoms listed to the left may indicate that the local server's date/time settings are behind the ReplNext.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Check the date and time settings on the local server to make sure it matches that of the ReplNext.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Configure all SAM Express replication peers to use NTP for time syncing.</td>
</tr>
</tbody>
</table>

---

*More...*
<table>
<thead>
<tr>
<th>Symptom</th>
<th>Poss. cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| Replication is not working. QueryChangeLog.bat shows entries are queued-up in the ChangeLog and the following error occurs in either SccAdSrvrlog.txt or SAM Express EV: | AddReplPeer script wasn’t properly executed | - Review the error message to determine which server isn’t properly configured. In the error to the left, the server cannot connect to its ReplNext peer.  
- Go to the ReplNext peer and run AddReplPeer script specifying the IP/name of the server that logged the error message. |
| Error: (JdbcDBProvider ReplNext ERROR 2008/02/26 14:50:10.365 (CST)) Failed processing <SQL not available> | | |
| SQL State: 08001 Error Code: 0 Message: | Replication is misconfigured to point to its own IP or hostname. | Verify the appropriate ReplNext and/or ReplPrev lines are properly configured for the IP/hostname of the replication peers and are not configured for the IP/hostname of itself. |
| Server configuration denies access to data source.                     | | |

**More...**
<table>
<thead>
<tr>
<th>Symptom</th>
<th>Poss. cause</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication is not working. QueryChangeLog.bat shows entries are queued-up in the ChangeLog and the following error occurs in either SccAdSrvrlog.txt or SAM Express EV: (JdbcDBProvider ReplNext ERROR 2008/02/26 16:34:18.544 (CST)) Failed processing &lt;SQL not available&gt; SQL State: 08S01 Error Code: 0 Message: Cannot connect to MySQL server on 10.10.90.57:5010. Is there a MySQL server running on the machine/port you are trying to connect to? (java.net.ConnectException)</td>
<td>Port 5010 isn't LISTENING</td>
<td>Review the error message to determine which server generated the error. In the error to the left, the server cannot connect to its ReplNext peer. Go to the ReplNext peer and verify: 1 The SAM Express Database service is started. 2 Port 5010 is in the LISTENING state using ‘netstat –na</td>
</tr>
</tbody>
</table>

More...
### Chapter 12: Troubleshooting

#### Troubleshooting Replication

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Poss. cause</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| Replication is not working. QueryChangeLog.bat shows entries are queued-up in the ChangeLog and the following error occurs in either SccAdSrvrlog.txt or SAM Express EV:  
(ReplLogProcessor ReplJanitor ERROR 2007/10/18 18:29:50.765 (EST)) Replication thread 'ReplNext' has been inactive since Thu Oct 18 18:14:29 EST 2007. Please check database status on the peer and network connectivity. | The SAM Express Server has lost connection to the replication peer. | Review the error message to determine which server generated the error. In the error to the left, the SAM Express server has lost its thread connection to the ReplNext peer. |
| Port 5010 isn't LISTENING | Go to the ReplNext peer and verify:  
1. The SAM Express Database service is started.  
2. Port 5010 is in the LISTENING state using netstat -na | | more command. |
| Replication seems to be working, however, the SccAdSrvrlog.txt and SAM Express Event Viewer log messages similar to the following sample: | | Open a command window (on ReplNext) and perform a telnet test to localhost over port 5010 (telnet localhost 5010) to verify port 5010 is accepting connections.  
- If local connectivity works but the remote MySQL server cannot connect, investigate the possibility that some 3rd party device is blocking the connection or that network connectivity intermittently fails. |

**More...**
### Symptom

(JdbcDBProvider **ReplNext-T0**
ERROR 2007/12/21
14:18:26.703 (PST))

**commitChanges failed because no rows matched**

**update criteria:** UPDATE
SccUser SET
sccComment='Carnell Tolbert - m21763 -
cman',sccModifiedBy='EasspServer on 198.149.32.75:5030
Preferences:
STANDARD',sccModificationDateTime='2007/12/21 16:26:04.250
(GMT)'.....

<snip>

WHERE sccEntryId='SccUser-
cman-2007/12/19 21:32:38.762
(GMT) (on 198.149.32.75:5040)-4490'

Another example:

(JdbcDBProvider **ReplNext-T0**
ERROR 2007/12/20
13:20:49.875 (PST))

**commitChanges failed because no rows matched**

**update criteria:** UPDATE
SccDesAuthenticator SET
sccModifiedBy='cmoser',sccModificationDateTime='2007/12/17
21:21:21.593 (GMT) (on
198.149.32.75:5040)'

4258'

---

### Poss. cause

SAM Express databases are out of sync or contain unique sccEntryId entries.

### Resolution

Review the error message to determine which server generated the error. In the sample errors shown in the Symptoms column (left), the SAM Express server fails to update the user ‘cman’ and token ‘K60998’ on the ReplNext peer. The error messages indicate that the entries the SAM Express server was trying to replicate do not exist on the ReplNext peer. SAM Express uses the sccEntryId field to ‘find’ the entry in the replication peer DB. In this case, the user ‘cman’ and token ‘K60998’ may exist on both servers but the sccEntryId assigned to the user ‘cman’ and token ‘K60998’ on each server is different. In order for replication to work, both servers must contain the same sccEntryId for user ‘cman’ and token ‘K60998’. One common reason for having unique sccEntryId values for the same user or same token is that the tokens or users were created separately on each SAM Express server before replication was configured. In addition, the backup/restore procedures were not used to manually sync the DBs before replication was configured. To resolve the issue, determine which SAM Express server is most up-to-date. Perform a backup of that SAM Express server and then restore this DB to another SAM Express server using the overwrite entries option.
### Symptom

WHERE
sccEntryId='SccDesAuthenticator-K60998-2007/12/12
17:40:18.514 (GMT) (on 198.149.32.75:5040)-

Replication seems to be working, however, the SccAdSrvrlog.txt and SAM Express Event Viewer log messages similar to the following:

(ReplPeerUpdaterManager ReplNext-T0 ERROR 2007/12/21 12:21:50.593 (PST)) Unable to replicate changes for entry 'NALIKHAN' for more than 24 hour(s). Purging change log without replicating. Please check data integrity of this entry across all servers!

### Poss. cause

SAM Express databases are out of sync or contain unique sccEntryId entries.

### Resolution

With replication configured, the restore operation will replicate the DB to all SAM Express servers.

Perform a backup of that SAM Express Server and then restore this DB to another SAM Express server using the ‘overwrite entries’ option.

Review the error message to determine which server generated the error. In the sample error to the left, the SAM Express server has failed to update the ‘NALIKHAN’ entry on the ReplNext peer for 24 hours. By default, SAM Express servers are configured to purge entries from the ChangeLog if they cannot be replicated for 24 consecutive hours.

The ChangeLog purging is controlled by the following setting in the sccservers.ini file:

\textit{ReplPurgeChangeLogHours=24}

As the error message to the left indicates, purging the ChangeLog entry raises concerns about the data integrity across all replication peers. It’s likely this purge message was proceeded by several other messages indicating failed replication attempts for the entry ‘NALIKHAN’, such as the \textit{commitChanges failed because no rows matched update criteria} message above. These previous messages must be investigated and resolved in order to stop entries from being purged.
Troubleshooting the RADIUS server

This section provides assistance for specific problems you may encounter with the RADIUS Server.

General troubleshooting

The following general troubleshooting tips may cover most common problems:

- Verify that network connectivity exists between the client and the RADIUS server. Sometimes a router or firewall is added and can cause network routes to break. Try to run ping to verify that the route isn't being impeded. Try to run the server in debug mode to see if a packet is arriving from the client.

- If you see “unrecognized host” in the output log file then the client wasn't matched with an entry in the clients file. If you have a NAT router in between the client and the server then you need to make sure the correct IP address is used. Add the corresponding client IP address and secret key into the clients file.

- If authentication between the RADIUS and Authentication Engine appears to not be working, verify that the host and port of the authentication server is present in the `radius.cfg` file in the 02 entry. A valid entry looks like “02 SAM Express Authen. Server Name: 192.168.13.54 0 0 5031”. Check the protocol being used in the “55 Eassp Version:202” entry. Typically 202 protocol goes to port 5031. See the `radius.cfg` file for more details.

- If the user appears to be passing SAM Express authentication in the audit logs but the RADIUS server is sending an Access-Reject:
  - Verify that if a group is being used, that it exists within the users file and is properly configured. See the users file for more information.
  - This can also be due to a `swec.md5` issue if using 202 protocol. Stop the RADIUS server, locate a file named `swec.md5` and delete it. The server will recreate this file and it may fix some problems.

Check the radius.cfg configuration files

Verify that the `radius.cfg` file exists in the directory and make sure the contents are correctly formatted. The RADIUS Server’s Authentication SDK interface is configured via the `radius.cfg` file. Sample settings for the `radius.cfg` file are shown below.

```
02 SAM Express Authen. Server Name: 192.168.13.54 0 0 5031
16 Send Status Messages to Console:ERROR
17 Send Status Messages to Log File:ALL
18 Status Message Log Filename:radius.log
20 Max log file length in KB:64K
```
Chapter 12: Troubleshooting

Troubleshooting the RADIUS server

23 Status Message Label:radius
27 Client Type:RADIUS
55 Eassp Version:202
57 SSL Enable:ON
58 SSL Cipher:DEFAULT

The most common problem area in the radius.cfg file is Line 02. Ensure that you have the correct hostname or IP address of the authentication server. Additionally, verify the port and the EASSP version match each other.

**Tip:** For EASSP 202, use port 5031.

---

**The clients file**

The clients file is usually located in the RADIUSServer directory. The most common problem in the clients file is a wrong or missing RADIUS-encryption key. RADIUS packets will be dropped if a client is not listed.

---

**The users file**

The most common problem in the users file (typically located in the RADIUSServer directory), is an incorrect or missing DEFAULT profile entry.

---

**The dictionary file**

The dictionary file is usually located in the RADIUSServer directory.

---

**Conflicts with other RADIUS servers**

Windows installs a service on many installations named Internet Authentication Service (IAS), which contains a RADIUS component. If this service is running, it will conflict with the default port for the RADIUS Server. To resolve this conflict, you can stop IAS, and set the startup to Manual. As an alternative, you can reconfigure the RADIUS Server to start on a different port. The port configuration is located in the .\system32\drivers\etc\services file.

In this file there are entries labeled "radius 1812/udp" and "radacct 1813/udp" which are consulted to determine the port that the RADIUS Server will use. Additionally, the RADIUS Server will consult the registry for the command line parameters used by RADIUS while running as a service. You may alter the named entry so that the RADIUS Server will look for it in the Services file by adding a "-S name" to the RADIUS service command line in the key named CL found at HKLM\System\CurrentControlSet\Services\SccRADIUSServer.
Launch the SAM Express RADIUS server in debug mode

For examples and help with the server's daemon syntax, use the command:

```
./radiusd -h or radiusd /?
```

The response you will see will appear similar to the example below:

```
Usage:./radiusd [ -a acct_dir ] [ -s ] [ -S name ] [ -x [debuglevel]] [ -d db_dir ] [-l [logdir]] [-A AccountingPort]
```

- **-a acct_dir** specifies an alternate directory for RADIUS accounting.
- **-s** runs RADIUS in single-threaded mode without spawning a child process to handle each authentication request.
- **-S name** allows two or more RADIUS Servers to run simultaneously on the same computer, each one uniquely named and accessing a separate port through the `/etc/services` database.
- **-A <port>** specifies the port on which the Accounting Server listens for accounting packets. For example if you assign a port number 0 to `<port>`, the accounting server will start on the port number specified in the services file. If the `-A` option is not specified, the accounting process will not start, but authorization packets will still be authenticated.
- **-r <char>** overrides the proxy site char.
- **-w** to run as windows service.
- **-x [debuglevel]** displays a verbose log of diagnostic messages. The optional `debuglevel` is a decimal number from 1 to 32767, bit-coded as follows:

  Bit 15 displays advanced timestamp information
  Bit 14 displays information during CSP device authentication
  Bit 13 displays information during RADIUS proxying
  Bit12= Display audit information for accounting purposes
  Bit11= Display debug messages in Vendor-Specific areas
  Bit10= Display debug messages in user exits areas
  Bit 9= Display timestamps as RADIUS request packets arrive
  Bit 8= Display important trace info. in Authorization areas
  Bit 7= Display incoming RADIUS packet summary
  Bit 6= Display outgoing RADIUS packet summary
  Bit 5= Display incoming SAM Express Parameter Blocks
  Bit 4= Display outgoing SAM Express Parameter Blocks
  Bit 3= Display messages on entry to each function call
  Bit 2= Display important trace info in SAM Express areas
  Bit 1= Display important trace info in nonSAM Express areas
  Bit 0= Attach RADIUS packet details to summaries
Uninstalling SAM Express

To uninstall SAM Express, run the Windows Start > Settings > Control Panel > Add/Remove Programs tool. When the Add/Remove Programs window appears, select SAM Express and continue following the prompts to remove the software.

Note: Uninstalling in Windows 2008 and later uses the Programs and Features utility found in Settings > Control Panel.

Diagnostic traces during correct operation

Start the RADIUS Server in debug mode using the debug level of 999, as shown below.

```
./radiusd -x 999 -d .
```

To uninstall SAM Express, run the Windows Start > Settings > Control Panel > Add/Remove Programs tool. When the Add/Remove Programs window appears, select SAM Express and continue following the prompts to remove the software.

Note: Uninstalling in Windows 2008 and later uses the Programs and Features utility found in Settings > Control Panel.

- **-d db_dir** sets the path of the RADIUS user database directory (db_dir) where a dictionary file is located.
- **-l** writes a log file called *audit.log* in the same directory as the binary.
- **-l <path>** writes *audit.log* to the path the user gives.
- **No -l** will not write the log file.

**Note:** The log name *audit.log* cannot be modified by users.

- **-v** displays the RADIUS Server version number.
Chapter 12: Troubleshooting

Uninstalling SAM Express
Symbols
.jad file 84

A
Access Control List (ACL)
default login ACL explained 124
entries, explained 125
entries, ordering and sorting 141
intro 124
sequential evaluation of entries 141
Activation
from website 30
new tokens 33
on a remote ADUC 32
troubleshooting 254
verifying with ADUC 32
verifying with SAM Express
   Management Console 33
with ADUC 29
Active Directory 48, 108
AD lockout
   setting 210
troubleshooting 257
adding users with the wizard 163
AddReplPeer.bat 228
Admin Server
   signing key 208
Administration Server configuration 205
Administration Service/Server 4
ADUC
   admin levels in 64
configuring Messaging providers 88
ADUC Management Console 3, 5
Agent service restarts 217
agents
   Citrix Access Gateway, introduced 9
common screens 214
   DLA 10
   IAS, introduced 9
   OWA 10
   Web Interface, introduced 9
alias 158
allowing dial-in access 18
allowing self-enrollment 83, 87
alternative group policies, configuring 74
Android 2, 7, 48, 78
archive (archiving)
   advanced features 183
   changing the default value 218
   configuring archive of audit logs 182
deleting archived audit log file 182
during minimal activity periods 218
loading archived log file 181
logs, managing 180
running without an archive log master 219
unloading archive set 181
Attack Lock 171, 193, 194
disabling per individual user 171
resetting a locked account 171
audit logs 176
   archiving 182
   finding 177
   managing archives 180
authentication
troubleshooting 256
viewing activity 178
Authentication Engine (AAA Server) 4
configuring 214
authentication policy 212
Authenticator Administration Guide 2
authenticator strengths 140
Authenticators
   RADIUS support 240
   strength of 151
   strength of fixed password 153
   strength table 140
authfile
   RADIUS sample 248
Authorization 236
Auto Updater 2
   introduction 6
   manually downloading updates 68
troubleshooting 254
   using 68
automatic enrollment parameters 84

B
BES policy 84
BlackBerry 2, 7
BlackBerry devices 48, 78

C
certificates
   SSL 73
   synchronizing 73
Index

change log 223
clients file
  RADIUS troubleshooting 266
Cloud Authentication Server 7
Cloud Portal
  configuration 35
Cloud Server 23
  installation preference 26
components
  changing ports on 200
computers in DMZ 74
configuration
  troubleshooting 255
configuring
  alternative group policies 74
  Authentication Engine 214
  common agent screens 214
  logging 215
  the Administration Server 205
creating
  personalization data attributes 168
  roles 142
credentials 23
Custom User Management
  and IdMapper.cfg file 209

D
database
  back up with command line 191
  back up/restore with ADUC 71
  back up/restore with SAM Express
    Management Console 189
debug mode
  RADIUS 267
default login ACL
  reconfiguring 195
default role
  reconfiguring 194
diagnostic file locations 202
diagnostic traces
  correct operation 268
  SAM Express RADIUS server 268
dial-in access 18
dictionary file
  RADIUS troubleshooting 266
DMZ, computers in 74

E
  editing the sccservers.ini file 228
  emergency passcodes, generating 61
  encryption keys 24, 222, 224
  Enrollment Portal 78, 84
  Enterprise Solution Pack (ESP)
    introduced 11
  ESP 23
  evaluation tokens 34
event logs
    viewing 69

F
  file types
    sccservers.ini 228
    signers.cfg 208
  fixed passwords
    expiration 154
    minimum length 154
    passwords to remember 154
    profiles 153

G
general tab settings 194
generating emergency passcodes 61
Google Apps 7, 23
groups
  admin groups 123
  and subgroups 123
  global 124
  GLOBAL DATA 124
  non-global 124
  subgroups 136

I
  Idle Timeout
    OWA Agent 217
importing authenticators
  troubleshooting 256
Importing token data files 51
increasing performance
  by archiving during minimal activity
    periods 218
  by running without an archive log master
    219
using multiple database connections 218
individual server log archiving
  enabling 219
installation
  encryption keys 24
  signing keys 24
  troubleshooting 254
installing
  multiple servers 24
iPhone/iPod touch 2, 7
iPhone/iPod touch devices 48, 78
IPv4/IPv6 addresses
  core servers and 138
  disabling temporary IPv4 addresses 138
  introduced 2
  log server 195
RADIUS/RADIUS Accounting servers
  exception 138

J

J2ME 2, 7, 48, 78

K

keys
  Admin server 208
  Authentication Engine (AAA server) 208
  changing 208
  compromised 208
  managing 208
keys (activation)
  key.activated.html 32
  key.html 31, 32, 33
keys (encryption)
  database encryption key 24
  database signing key 24, 208
keywords
  with archives 183

L

log master
  backing up 226
  designating 226
logging
  configuring 215
  configuring ADUC for 69
  reconfiguring 195
server diagnostics 201
  using ADUC 69
logging settings 215
login ACL 124
login password 222, 224

M

Messaging
  editing provider information 94
  via OWA 99
Messaging Application 97
  customizing 98
Messaging providers
  AD users 88
messaging token 78
Messaging tokens 48
Messaging tokens and SMS 7
Messaging tokens and SMTP 7
MobilePASS 7, 23, 78
  providers 88
MobilePASS Factory 78
MobilePASS Messaging 2
MobilePASS Messaging tokens 48
MobilePASS Portal 78
MobilePASS records
  generating 49
MobilePASS Software Administration Guide
  2
MobilePASS Software tokens 48
monitoring servers 203

N

Network Address Translation (NAT) 224
Network Time Protocol (NTP) 225
Next peer 222

O

objects 123
optional Agents 8
Outlook Web Access (OWA) Agent
  10
  timeouts 216
Outlook Web Access Agent 99
P

passcode timeouts 89
password
  change administrator account password 80
  user center 108
passwords
  changing ADUC administrative password 49
  ensuring security of 109
  memorized RADIUS-encrypted 240
  RADIUS usernames, memorized and appended to 241
  RADIUS, asynchronous dynamic authenticators 243
  RADIUS, CHAP encoded 243
  RADIUS, encapsulated dynamic 243
  RADIUS, synchronous dynamic appended to usernames 241
  RADIUS, synchronous dynamic, encrypted 241
  RADIUS-encrypted, memorized 240
  SAM Express Management Console, changing the default 134
  SAM Express Management Console, default 128
permissions 22
personalization data
  editing attributes 172
  removing attributes 172
  setting up 168
PINs
  adding or changing with the ADUC 59
  changing 112, 113
  deleting 62
  requiring 58, 149
  using with tokens 59
Portals Configuration tool 35
ports
  changing 200
  troubleshooting 256
pre-authentication 99
Previous peer 222
priority
  in roles 143
  valid range 143
privileged users 122
Privileges

for user types 123
Helpdesk staff 160
Local administrator 161
System administrator 162
tab 159
product serial number 22
programming files 130
properties
  user 57

Q

QueryChangeLog.bat 223

R

RADIUS
  conflicts with other servers 266
  RADIUS Accounting server 7
  RADIUS support
    IAS Agent and 9
  RADIUS/RADIUS Acct Server
    configuration files 236
    configuring 205
    creating an ACL entry and role for 236
    Default user record 238
    introduced 7
    protocol 234
    proxy configuration 238
  RADIUSdictionary file 244
  rcr.txt file 45
references
  SAM Express RADIUS server 244
reinstalling
  ADUC 73
  SAM Express Server 73
remote access policy
  allowing dial-in access 18
replication 222
  multiple peer 222
report
  creating 184
  templates 185
  worksheet generation 186
reporting
  log archival impact on 182
requesting passcodes via Messaging Application 97
Require SSL Connections 217
resetting an attack-locked account 171
restoring the database
  during replication 227
  with the SAM Express Management Console 189
restrictions, ACL entry 125
ReSync Window 152
resynchronizing tokens
  ReSync Window 152
  Sync Window 151
resynchronizing tokens with ADUC 60
resynchronizing tokens with the SAM Express Management Console 149
ring topology architecture 222
roles
  assigning to users 156
  creating 142
  priority 143
roles, ACL entry 125

S
SaaS 7
SafeNet MobilePASS 7
SAM Express
  ADUC Management Console 3, 5
core components 3
database 4
designating a log master with the Management Console 226
Management Console 3, 6
SAM Express server 4
serial number 28
uninstalling 268
User Center 4
SAM Express database 108
  and the User Center 119
  and User Center 119
SAM Express passcode field
  hide 217
SAM Express tab on User Properties window 5
SafeNet tokens
  accessing the User Center 110
  changing PINs 112, 113
  enrolling 110
  synchronizing 116
  testing 114
Salesforce.com 7, 23
sccservers.ini 207, 218
searching
for unassigned tokens 60
utility 60
self-enrolling tokens 83
servers
  AAA
    configuring 214
    hostname/port for agent auth requests 214
    introduced 4
    keys 208
    performance settings 207
    SoftPIN use 207
    user information lookup for agents 209
    user lockout status in AD 210
    adding to monitored list 203
Admin server
  configuring 205
  introduced 4
  changing ports 200
  cloning 204
  default ports 24
  diagnostic file locations 202
  encryption/signing keys during installation 24
  installing multiple 24
  monitoring status of 203
RADIUS
  prerequisites 236
  protocol 234
RADIUS/RADIUS Acct
  introduced 7
  removing from monitored list 204
SAM Express server
  installation requirements 17
  not on domain controller 23, 25
  starting and stopping 200
  tab settings 195
  troubleshooting 257
service restarts after Agent configurations 217
sessions
  viewing user 198
signers.cfg 208
signing keys 24
SoftPINs
  configuring Authenticator Engine for 207
  using 158
software serial number 28
software token 78
Software tokens 48
SSL certificates 73
subgroups 136
subjects, ACL entry 125
Support
  authenticator counts 45
  renewal 45
support data file 45
Sync Window 151

T

testing replication 232
time sync between peer machines 225
timeouts
  OWA Agent 216
timestamps on change log 223
Token Assignment Wizard 53
token data records
  deleting 63
Token group ID 28
token record replication 223
tokens
  administrator-assigned using ADUC 53
  assigning in ADUC
  assigning tokens in ADUC
  assigning with the SAM Express Management Console 149
deleting from the database 63
finding users assigned specific tokens 60
modifying token profiles 151
reassigning 62
resynchronizing with ADUC 60
resynchronizing with the SAM Express Management Console 149
search utility 60
searching for unassigned 60
testing with ADUC 59
Troubleshooting 254
  common problems 265
radius.cfg file 265
TSEEXEC 229
types of groups 124

U

unassigned tokens 60
uninstalling SAM Express 268
Universal Coordinated Time (UTC) 225
unprivileged users 123
  adding 163
unregistered user ID 194
URL redirect 99
Use scenario
  ADUC and SAM Express Management Console 13
  SAM Express Management Console 12
User Center 13
  accessing the 110
  and SAM Express Database 119
  changing PINs 112, 113
  configuring for a SAM Express database 119
  enrolling tokens 110
  features 110
  initializing 108
  overview 108
  password 108
  synchronizing tokens 116
  testing tokens 114
User Center password 222, 224
user wizard 163
users
  adding user accounts manually 156
  aliases to user accounts 158
  assigning roles to 156
  configuring groups in RADIUS 237
  deleting records 167
  properties 57
  RADIUS file troubleshooting 266
  revoking sessions 198
  sample RADIUS file 246
  session management 198
  system administrator 123
  unprivileged 123

V

Verifying replication in AD environments 232
viewing event logs 69
VPN support
  IAS Agent and 9

W

Windows Desktops 2, 7, 48, 78
Windows Time service 225