



THE  
DATA  
PROTECTION  
COMPANY

# SafeNet Authentication Manager Express

## CUSTOMER RELEASE NOTES

**Version:** 8.2  
**Build:** 6.1.10b124  
**Issue Date:** 23 March 2015  
**Document Part Number:** 007-012833-001, Rev. B

### Contents

Product Description .....	2
Release Description.....	2
New Features and Enhancements.....	2
SafeNet RADIUS Server Enhancements .....	2
Turning off the Accounting Server.....	2
Customized Message Return for Authentication Pass and Fail.....	2
Support for MS Exchange 2013 in the SAMx OWA Agent.....	3
MySQL Upgraded to 5.6.20.....	3
DSKPP Enrollment of Mobile PASS Authenticators .....	3
Support for SafeNet Mobile PASS v8.4.....	3
Pooled Software Authenticator Count Visible in ADUC Snap-in.....	3
Support for Citrix Web Interface v5.4 .....	3
Disabling SSL 3.0 in AAA Server and Admin Server.....	3
Components Upgrade .....	4
Released Components .....	4
Component Versions .....	4
Advisory Notes.....	5
Supported Platforms .....	5
Installation Pre-requisites.....	5
Known Issues .....	6
Product Documentation .....	6
Support Contacts.....	7

## Product Description

---

SafeNet Authentication Manager Express (SAMx) by SafeNet is a multi-factor authentication solution for Microsoft Windows platforms. SAMx enables management of the complete user authentication lifecycle, making it easy to protect your most important assets and applications. It links users with easy-to-use tokens (including hardware, software, and SMS-based tokens), and it seamlessly integrates with your existing Microsoft Windows management tools.

## Release Description

---

SAMx 8.2 is the next maintenance release for SAMx. This release includes new features and enhancements, and several third-party components update to address specific security vulnerabilities inherent to those components. The third-party components include JRE, MySQL, and Apache Tomcat.

## New Features and Enhancements

---

### SafeNet RADIUS Server Enhancements

#### Turning off the Accounting Server

With this release, it is possible to run the SafeNet RADIUS server while the Accounting server is turned off. In order to run the RADIUS server without accounting, set the value of the attribute **UserAccountingServer** to **False** in the **settings.cfg** file.

#### Customized Message Return for Authentication Pass and Fail

It is now possible to define the configurable messages with every successful or failed authentication request to the SafeNet RADIUS server. This can be achieved by setting the appropriate values of the attributes **AuthenticationSuccessfulMessage** and **AuthenticationFailureMessage** in the **settings.cfg** file.

It is important to note that, in the absence of these attributes in the **settings.cfg** file, the SafeNet RADIUS server will not append any custom message with a “pass” or “fail” message. The sample content of the **settings.cfg** file is shown below.

*# Set the appropriate text that will be sent back by SafeNet Radius server on successful authentication.*

*# When this attribute is not present or left blank, no message is sent.*

*# Restart the SafeNet Radius Service, if the value is changed or the attribute is removed.*

**AuthenticationSuccessfulMessage = SafeWord Authentication successful**

*# Set the appropriate text that will be sent back by SafeNet Radius server on failed authentication.*

*# When this attribute is not present or left blank, no message is sent.*

*# Restart the SafeNet Radius Service, if the value is changed or the attribute is removed.*

**AuthenticationFailureMessage = Authentication failed**

## Support for MS Exchange 2013 in the SAMx OWA Agent

The SAMx OWA Agent has been updated to support strong authentication for Outlook Web Application under Microsoft Exchange 2013. It can also provide strong authentication to Exchange Admin Center (EAC). For usage and configuration details, refer to the SAMx Administrator's Guide or the SAMx Agents Administration Guide.

## MySQL Upgraded to 5.6.20

The database server has been upgraded to 5.6.20-enterprise-commercial. The database upgrade is automatically handled during the SAMx update installation.

## DSKPP Enrollment of Mobile PASS Authenticators

The previous release of SAMx had intermittent issues with auto enrollment of Mobile PASS tokens. The implementation of DSKPP has been revamped in this release and all the issues have been addressed.

## Support for SafeNet Mobile PASS v8.4

This release supports the seamless usage with SafeNet Mobile PASS v8.4.

## Pooled Software Authenticator Count Visible in ADUC Snap-in

The ADUC snap-in now supports the reporting of pooled software authenticator license count. The SafeWord administrator is now able to view the activation support information for pooled software authenticators.

## Support for Citrix Web Interface v5.4

The Citrix Web Agent now supports extending the SafeWord strong authentication to the Citrix Web Interface v5.4. For information on how to use the Citrix Web Agent, refer to the SAMx Agents Administration Guide.

## Disabling SSL 3.0 in AAA Server and Admin Server

The two core components of SAMx communicate with various applications over a secured channel. Due to the recently reported vulnerabilities and the corresponding recommended solution, the AAA Server and Admin Server will by default negotiate a secure channel only by using TLS 1.0.

It is not recommended to use SSL 3.0. However, if there is a need to enable SSL 3.0 on the channel, it can be done by making appropriate entries in the **sccservers.ini** file. The **sccserver.ini** file can be found in the **Servers/SHARED** folder.

The following settings, which will enable both SSL 3.0 and TLS 1.0, can be added to the **sccserver.ini** file:

```
SSL_Min_Protocol=SSL3
```

```
SSL_Max_Protocol=TLS10
```

## Components Upgrade

The following components have been upgraded in this release.

Updated Component	Version
Java Runtime Environment	1.7.0_60
MySQL	5.6.20
OpenSSL	0.9.8zb
Apache Tomcat	6.0.41

## Released Components

---

### Component Versions

SAMx uses the third-party software tools, including the open source tools. The following table lists these tools and their version numbers:

Component	Version
Java Runtime Environment	1.7.0_60
BeanShell	1.3.0
MySQL	5.6.20
OpenSSL	0.9.8zb
JExcelAPI	2.3.14
Expat	2.0.0
IAIK	3.0.3
Apache Tomcat	6.0.41
Apache Velocity	1.4
Apache Commons Collections	3.2
Apache Commons Daemon	1.0.3

# Advisory Notes

---

## Supported Platforms

SAMx supports the latest 32-bit and 64-bit Microsoft Windows platforms, including:

- Vista
- Windows 7
- Windows 8
- Server 2003
- Server 2008
- Server 2008 R2 (except Server 2008 Core and Business)
- Server 2012
- Server 2012 Essentials
- Server 2012 R2
- Server 2012 R2 Essentials

SafeNet continues to expand MobilePASS device support. For a current list of supported devices, and to download the latest clients, visit: <http://www.safenet-inc.com/GetMP>.

## Installation Pre-requisites

Before installing SAMx, VC++ 2008 Runtime should be installed. To download the VC++ 2008 Runtime application, refer to the following links:

- For Windows 32-bit environment: <http://www.microsoft.com/en-in/download/details.aspx?id=29>
- For Windows 64-bit environment: <http://www.microsoft.com/en-in/download/details.aspx?id=15336>

**Note:** If you are uninstalling the old version of SAMx, clean the Windows Registry before proceeding with the installation of SAMx 6.1.10 b124.

## Known Issues

---

Issue	Description
Windows Server 2003 operating systems	<p>There is an intermittent behavior during SAMx installation on the Server 2003 platform where the error message “Could not open key” is returned and the installation is failed. This issue is related to security privilege elevation for Registry Key settings. It is a known bug in Windows XP, Windows Vista, and Windows Server 2003 platforms. The KB article can be found <a href="#">here</a>.</p> <p>To resolve this problem, start the Windows Command Prompt as an administrator, and then run the following command:</p> <p><b>secedit /configure /cfg %windir%\repair\secsetup.inf /db secsetup.sdb /verbose</b></p>
Windows 2012 operating systems	<p>The following are the important points for the correct operation in Windows 2012 environments:</p> <ul style="list-style-type: none"><li>• Even if logged in as an administrator, most of the SAMx features require to right-click a shortcut and click “Run as Administrator” in order to work properly.</li><li>• Shortcuts that open webpages, such as those for agent configuration, do not work in the Metro version of Internet Explorer.</li><li>• The Internet Zone, typically Local Intranet, must have the option <b>Enable Protected Mode</b> disabled.</li><li>• The user account running Admin Console must be granted the <b>write</b> permission for the directory ...\<b>AdminConsole\certificates</b>.</li></ul>

## Product Documentation

---

The latest product documentation is stored on the web. It is available either from the **View Documentation** button during installation, or on the SAMx product documentation download webpage at <http://www.safenet-inc.com/support/SAMx-documentation/>. To view the documents, you must have Internet access.

The following new and/or updated documents are available for download:

- *SAM Express Upgrade Instructions*
- *SAM Express Version 8.2 Administration Guide*
- *SAM Express RADIUS Integration Guide*
- *SAM Express UWA/WLS Integration Guide*
- *SAM Express Version 8.2 Customer Release Notes*
- *SAM Express Agents Administration Guide*

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 Contacts

---

If you have questions or need additional assistance, contact SafeNet Customer Support through the listings below:

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	<a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a> Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	