SafeNet Authentication Service

Configuration Guide

Shibboleth Agent

SafeNet
THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012422-002, Rev. B
Release Date	April 2015

Trademarks

Disclaimer

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 or organization of any such revisions or changes.

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.

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 or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Applicability

The information in this document applies to:

- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)**—The software used to build a SafeNet authentication service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)**—A term used to describe an on-premises implementation of SAS-SPE.

> **NOTE:** References to BlackShield and CRYPTOCard reflect CRYPTOCard branding prior to acquisition by SafeNet. Over time, these references will change to reflect SafeNet branding, including program installation locations.

Environment

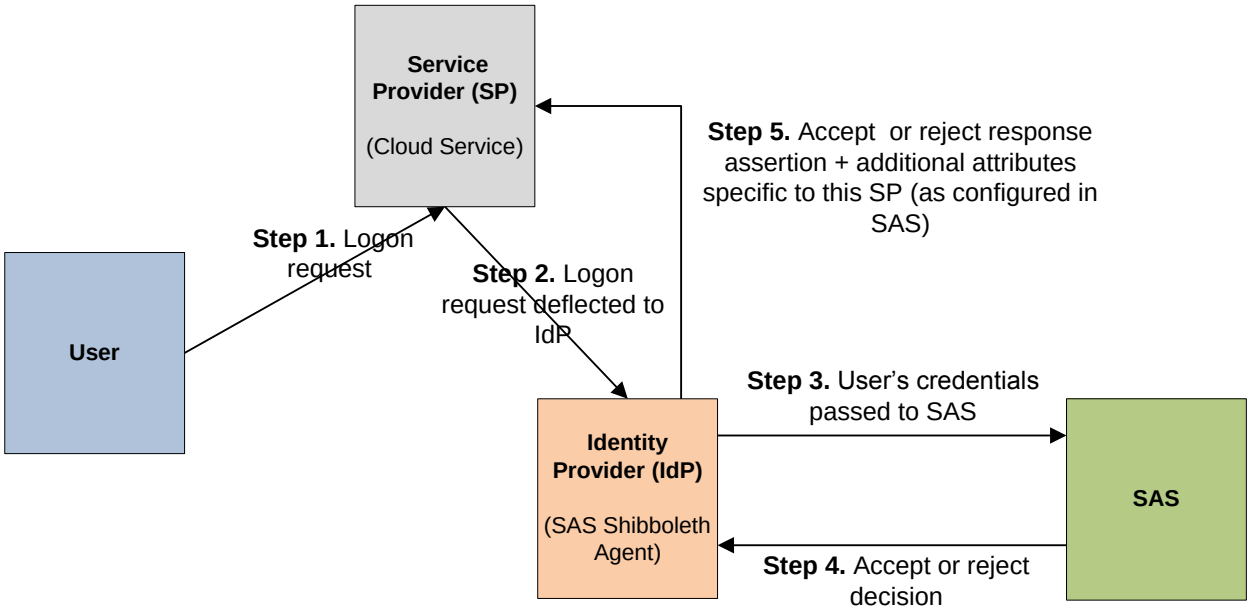
Supported Windows Versions	• Windows 2003 SP2 Server • Windows 2003 SP2 Terminal Server • Windows 2008 SP2 and Windows 2008 R2 • Windows 2008 SP2 and Windows 2008 R2 Terminal Server • Windows Server 2012 and above
Supported Architecture	• 32-bit • 64-bit
Additional Software Components	• Apache Tomcat v 7.xx http://tomcat.apache.org/download-70.cgi • Shibboleth 2.3.2 Identity Provider (SAML 2.0) http://www.shibboleth.net/downloads/identity-provider/latest/ • JRE 7 or JDK 7

Overview

The SafeNet Authentication Service (SAS) Shibboleth Agent enhances security to a Shibboleth-protected resource by enforcing two-factor authentication.

When a user tries to access a protected Service Provider (SP), the SP intercepts the request and redirects the user to the SAS Shibboleth Agent, which acts as the identity provider (IdP). The IdP collects the user's credentials and passes them on for authentication by SAS. SAS evaluates the credentials and returns an "accept" or "reject" decision to the IdP. The IdP then creates an "accept" or "reject" response assertion for the SP. The returned "accept" response assertion also carries with it some of the attributes that SAS has been configured with for this SP.

The list of all attributes that the IdP can release is included in the IdP's metadata, but what to release is controlled by SAS.



Prerequisites

Before installing the SAS Shibboleth Agent, the following applications must be installed:

- **Java Runtime Environment (JRE)** or **Java**
- **Apache Tomcat** – It is strongly recommended to install Apache Tomcat to **C:\opt\Tomcat**. The SAS Shibboleth Agent's INI file is preconfigured for this location. The location can be changed later using the Shibboleth Agent Manager.
- **Shibboleth Identity Provider (IdP)** – It is strongly recommended to install the Shibboleth Identity Provider (IdP) to **\opt\shibboleth-idp**. The SAS Shibboleth Agent's INI file is preconfigured for this location (which simplifies agent configuration).

See the following for more information on installing Shibboleth:
https://wiki.shibboleth.net/confluence/display/SHIB2/IdPInstall

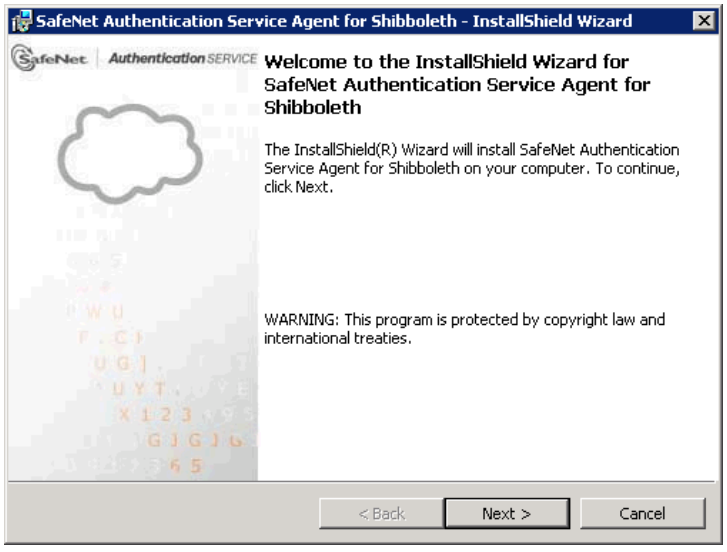
To test that Shibboleth Identity Provider (IdP) is properly installed and running, access the following URL:
http(s)://HOSTNAME:PORT/idp/profile/Status

If everything is working correctly, an "OK" message is displayed.

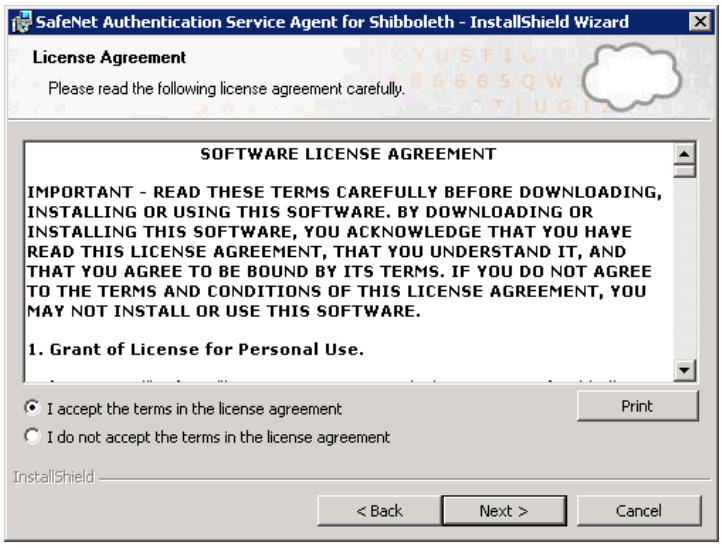
For detailed information on installing these applications, see "Installing and Configuring the Shibboleth Identity Provider" on page 14. For supported versions, see "Environment" on page 4.

Installing the SAS Shibboleth Agent

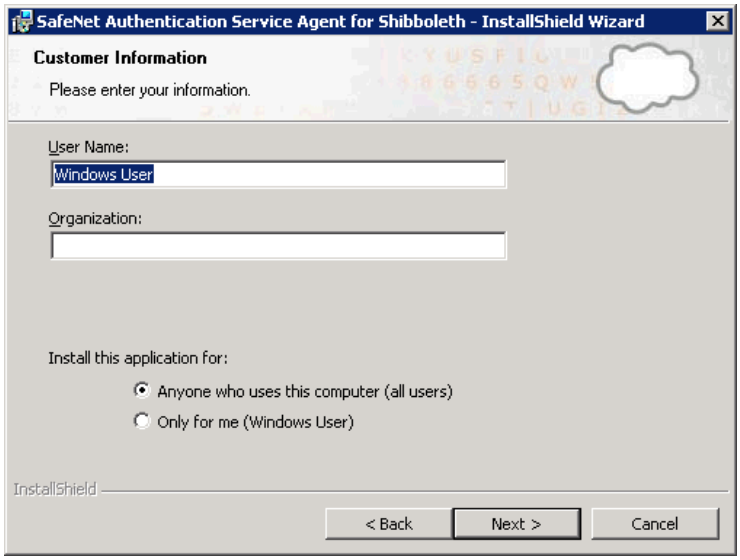
1. Locate and run one of the SAS installers:
   - SAS Agent for Shibboleth.exe (32-bit servers)
   - SAS Agent for Shibboleth x64.exe (64-bit servers)
2. On the **Welcome** window, click **Next**.



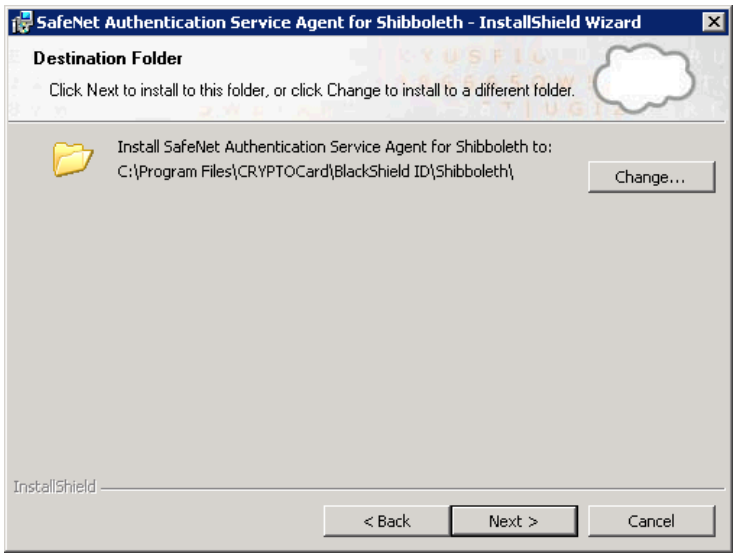
3. On the **License Agreement** window, select **I accept the terms in the license agreement** and then click **Next**.



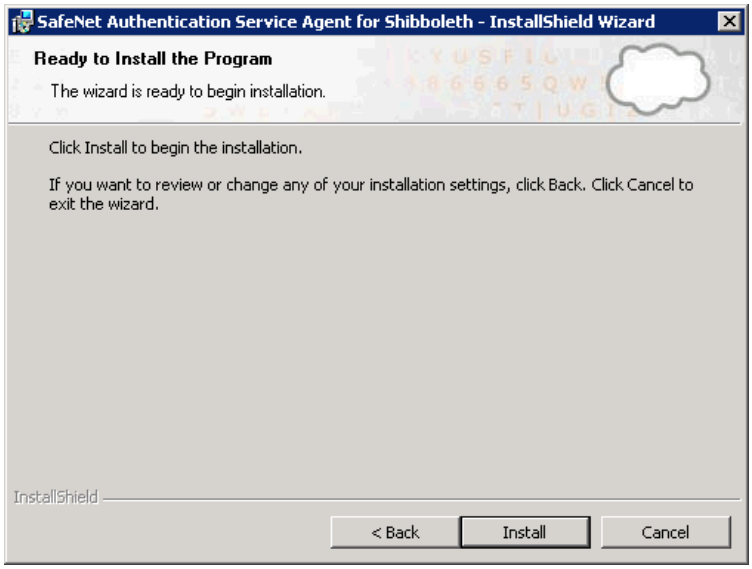
4. On the **Customer Information** window, enter the **User Name** and **Organization**, and then click **Next**.



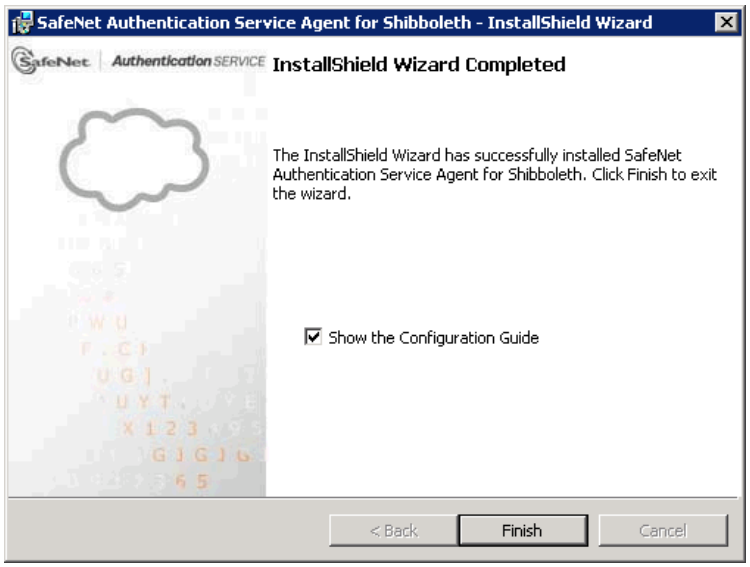
5. On the **Destination Folder** window, click **Next** to select the default installation destination folder, or click **Change** to browse to and select a different folder. Click **Next** to continue.



6. On the **Ready to Install the Program** window, click **Install**.



7. When the installation process is finished, the **Installshield Wizard Completed** window is displayed. Click **Finish** to exit the wizard.



Configuring the Agent Key File

This agent uses an encrypted key file to communicate with the authentication web service. This ensures all communication attempts made against the web service are from valid, recognized agents. To accomplish this, a key file is loaded and registered with SAS agents, and then a matching key file is installed and registered with the web service.

A sample key file (Agent.bsidkey) has been installed for evaluation purposes; however, it is strongly recommended to generate your own key file for a production environment, as the sample file is publicly distributed.

To load the key file:

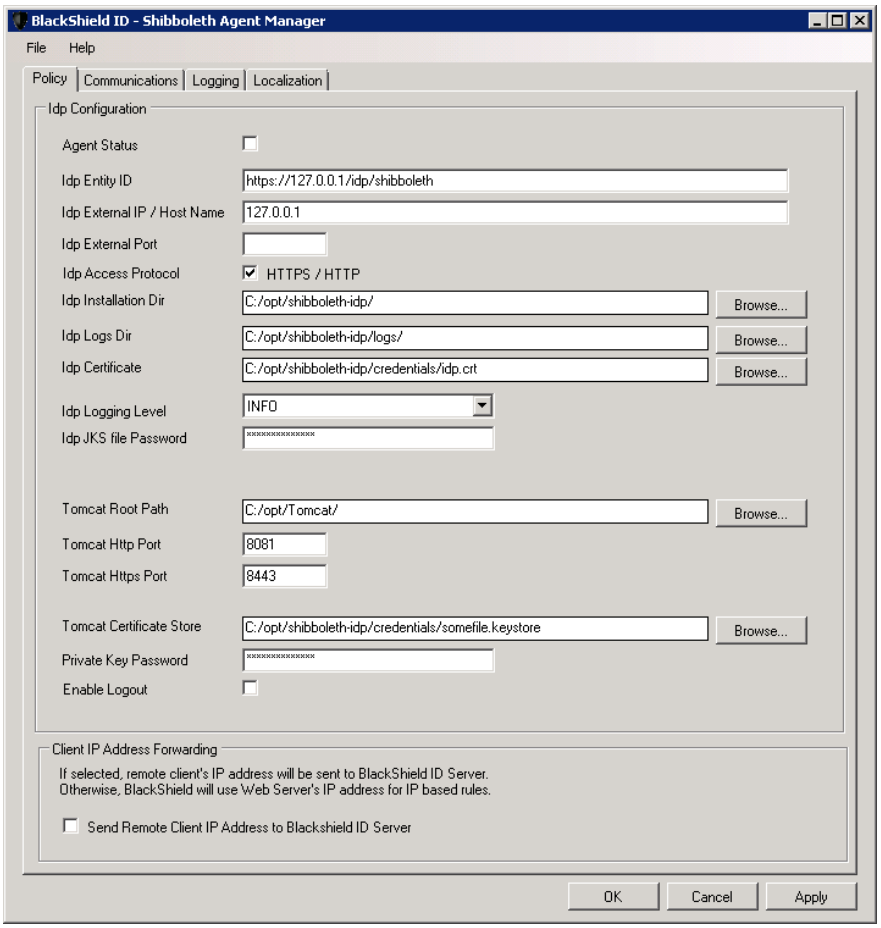
1. In SAS, select the **COMMs** tab and download an agent key file from the **Authentication Agent Settings** section.
2. To open the Shibboleth Agent Manager, click **Start > All Programs > SafeNet > Agents > Shibboleth Agent**.
3. Click the **Communications** tab (see “Configuring the SAS Shibboleth Agent” on page 10).
4. Click the Agent Encryption Key File **Browse** button and navigate to the agent key file.
5. Click **Apply**.

Configuring the SAS Shibboleth Agent

The Shibboleth agent can be configured for both **http** and **https** regardless of SAS configuration; however, it is recommended that the agent be configured to match the security mode of the SAS server, preferably **https** only.

To configure the agent:

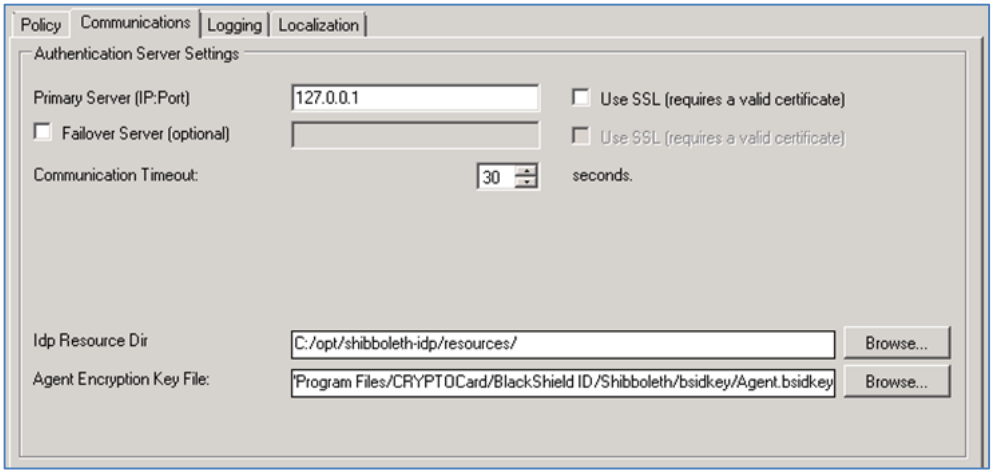
1. To open the Shibboleth Agent Manager, click **Start > All Programs > SafeNet > Agents > Shibboleth Agent Configuration Tool**.
2. Click the **Policy** tab.



3. Complete the following fields:

Agent Status	Select this option to enable the Shibboleth Agent.
Idp Entity ID	This is a globally unique URL-based identifier that cannot match with another IdP or SP. Typically, it is a URL by which the IdP or SP is publically accessible.
Idp External IP/Host Name	This is the public Host/IP on which the IdP will be visible to the outside world. For example, if the IdP is inside the firewall and is listening on IP 192.168.1.10 and port 8081 as HTTP service, you must redirect your external port 80 to 192.168.1.10's internal port 8081. Similarly, if the IdP is running as HTTPS service on port 8443, you must redirect external 443 to the respective IdP's internal port (by default: 8443).
Idp External Port	This is the external port that you will redirect to the internal port as described above. As explained earlier, Entity ID is a globally unique identifier; the combination of Schema, Host, Port and Path creates a unique identifier for IdP and SP. The Host is usually a fully qualified domain name, such as FQDN.
Idp Access Protocol	Enable for HTTPS. Disable for HTTP.
Idp Installation Dir	Path to the IdP installation directory.
Idp Logs Dir	Path to the logs directory.
Idp Logging level	Select the required logging level.
Idp – Certificate	Enter the path to the certificate file. This certificate will be embedded in the IdP metadata and is used to sign the response assertions.
Tomcat Root Path	Path to Tomcat.
Tomcat HTTP port	Tomcat HTTP port.
Tomcat HTTPS port	Tomcat HTTPS port.
Tomcat Certificate Store	Enter the path to the Tomcat certificate store. This is mandatory if using HTTPS. This certificate is a server identification certificate and must be according to your server's name or FQDN.
Private Key Password	Enter the private key password.
Enable Logout	Select to enable logout. Typically, IdPs do not support logout functionality. SAML standards have no support for logout and it is considered against the spirit of true single sign-on (SSO). However, this agent does support logout functionality and is controlled by this setting. The IdP metadata has a node indicating the URL to which the user should be redirected by the SP if they want to terminate an existing authenticated session. This logout URL is visible, along with other IdP URLs in SAS.
Send Remote Client IP address to SAS Server	Typically, for SAS to enforce IP-related rules, it detects the IP using the request origin. However, if there is a proxy between the SP and the IdP, this may not be the intended IP. If there is proxy, and if this setting is enabled, the IdP will send the SP's IP to SAS as opposed to SAS detecting the IdP's IP to force any custom rules. Under normal circumstances, this setting should be disabled.

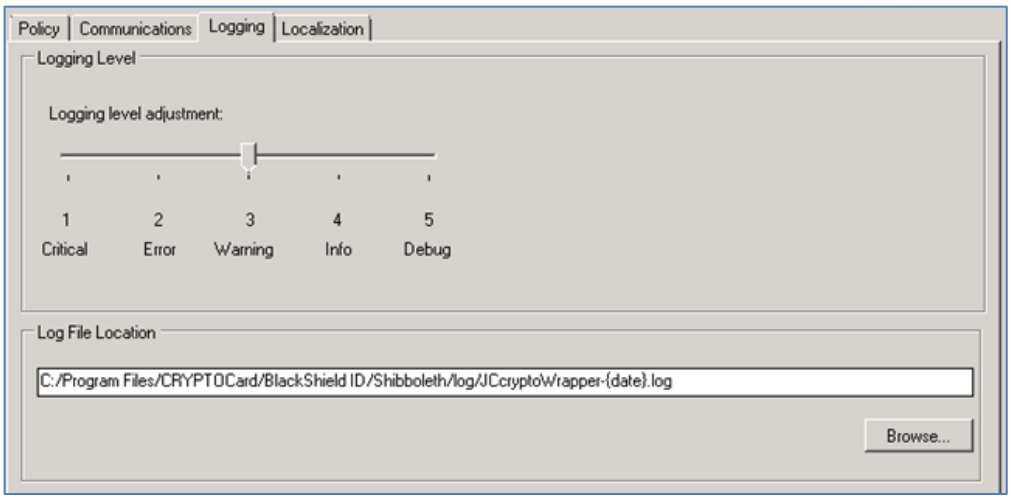
4. Click the **Policy** tab.



Complete the fields as follows:

Primary Server (IP:Port)	Enter the IP address of the SAS server.
Communication Timeout	Enter the required timeout period.
IdP Resource Dir	Enter the path to the IdP resource directory.
Agent Encryption File Key	For details, see “Configuring the Agent Key File” on page 9.

5. Select the **Logging** tab.

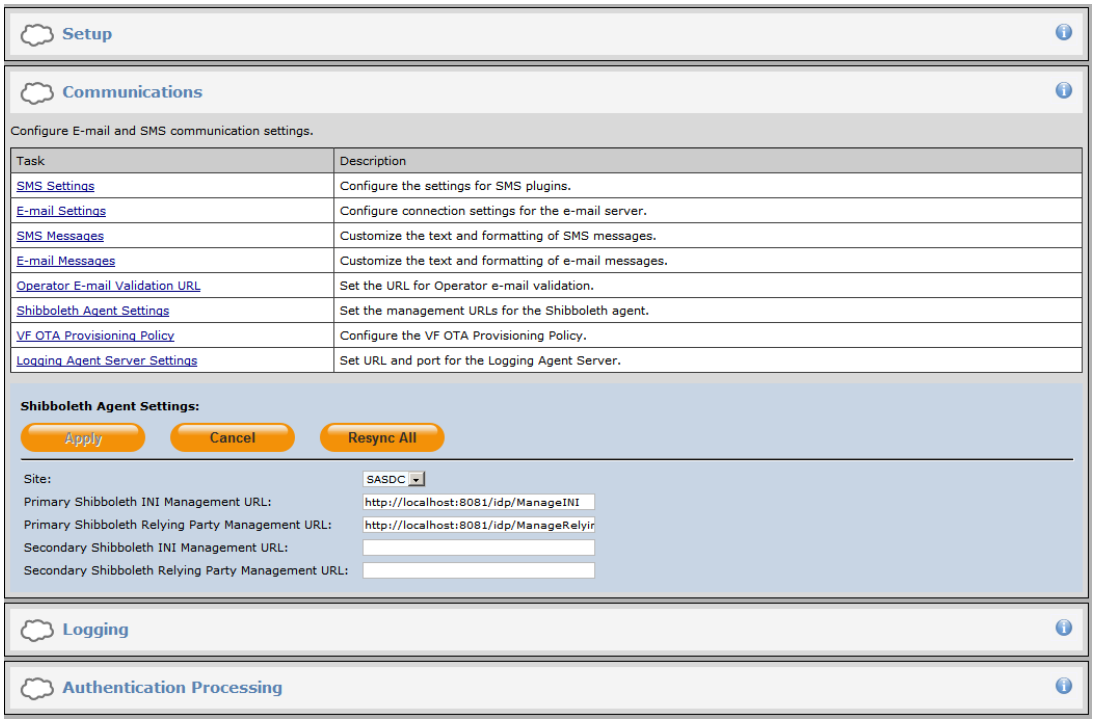


6. Select the required logging level and log file location.

Configuring Shibboleth Agent in SAS Manager

The settings in the SAS Management Console determine how Shibboleth and SAS communicate.

1. In the SAS Management Console, click **Systems > Communications > Shibboleth Agent Settings**.



2. Complete the fields as follows:

Site	Indicates the computer, if more than one computer is being used for SAS.
Primary Shibboleth INI Management URL	The URL that SAS uses to communicate SP-related customizations to the primary Shibboleth server.
Primary Shibboleth Relying Party Management URL	The URL that the primary Shibboleth agent uses to communicate with SAS regarding any changes related to the addition or removal of an SP.
Secondary Shibboleth INI Management URL	The URL that SAS uses to communicate SP-related customizations to a secondary Shibboleth server.
Secondary Shibboleth Relying Party Management URL	The URL that the secondary Shibboleth agent uses to communicate with SAS regarding any changes related to the addition or removal of an SP.

Resynchronizing the Shibboleth Agent Settings in SAS Manager

If something has been changed in the identity provider (IdP) configurations that changed the EntityID of the IdP (normally the Scheme, Port, Domain Name - FQDN) and Path, the IdP loses all SP-related configurations.

The configurations related to SPs still exist in SAS and they must be resynchronized with the IdP. The **Resynch** function collects the information from SAS and sends it in encrypted format to the Primary (and if required, Secondary) Shibboleth agent.

To resynchronize the Shibboleth agent with SAS:

1. In the SAS Service Manager, select **System > Communications > Shibboleth agent settings**.
2. Click **Resync All**. A message is displayed that the SAML 2.0 data was successfully synchronized with the remote Shibboleth agent.

Installing and Configuring the Shibboleth Identity Provider

This section describes a process for installing and configuring a Shibboleth 2.3.2 Identity Provider.

Prerequisites

The following prerequisites are required:

- Windows 2003\2008\2008 R2 server
- Java JDK 1.6 or 1.7 (http://www.java.com/en/download/index.jsp)
- Apache Tomcat 7.x (http://tomcat.apache.org/download-70.cgi
- Shibboleth 2.3.2 Identity Provider (http://shibboleth.net/downloads/identity-provider/2.3.2/)
- tomcat6-dta-ssl-1.0.0.jar (https://build.shibboleth.net/nexus/content/repositories/releases/edu/internet2/middleware/security/tomcat6/tomcat6-dta-ssl/1.0.0/tomcat6-dta-ssl-1.0.0.jar)
- SAS Agent for Shibboleth

Components

Shibboleth is dependent on several components, which must be installed in the following order:

- Java JDK 1.6 or 1.7
- Apache Tomcat 7.0
- SAML Shibboleth 2.3.2
- SAS Agent for Shibboleth

Java JDK 1.7 Installation/Configuration

1. Install Java JDK 1.7 (jdk-7u21-windows-x64.exe) on your Shibboleth server.

   (Note: Java JDK 1.6 is also supported.)
2. Run the installer and go through the default installation.
3. Go to W**indows Control Panel > System > Advanced System Settings**.
4. Click **Advanced > Environment Variables**.
5. Under **System Variables**, select **New**.
6. In **Variable Name**, enter **JAVA_HOME**.
7. In **Variable Value**, enter **C:\Program Files\Java\jdk1.7.0_21**.
8. Click **OK** three times.
9. Reboot the Shibboleth server to set PATH.

Apache Tomcat Installation and Configuration

Be certain to perform all steps in this section as described.

1. Install Apache Tomcat 7.x (apache-tomcat-7.0.40.exe) on your Shibboleth server.
2. In the **Choose Components** window:
   a. Select **Custom** from the list.
   b. Select all components except for **Examples**.

      NOTE: Do not select **Native** checkbox or else Shibboleth will not load properly after applying changes later on in the configuration.
   c. Click **Next**.
3. In the **HTTP/1.1 Connector Port**, enter **8081**. (Modify this port only.)

   NOTE: Port 8081 will be changed later.
4. In the **Tomcat Administrator Login** section:
   a. Enter a **User Name** and **Password** for Apache Tomcat access.

      NOTE: The credentials entered here will be used later to verify if Tomcat is running properly.
   b. Click **Next** to continue.
5. On the **Java Virtual Machine** window, change the **Path** to **C:\Program Files\Java\jdk1.7.0_21**.
6. On the **Choose Install Location** screen, verify that the install path is **C:\Program Files\Apache Software Foundation\Tomcat 7.0**.

7. After Apache Tomcat has been installed, clear the **Run Apache Tomcat** and **Show Readme** check boxes.
8. Click **Close**.
9. Click **Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Monitor Tomcat** to launch **Monitor Tomcat**.
10. On the **General** tab, change **Startup type** from **Manual** to **Automatic**.
11. Under **Service Status**, click the **Start** button.
12. Open Windows Explorer, go to the following location, and create the endorsed directory **C:\Program Files\Apache Software Foundation\Tomcat 7.0**.

SAML Shibboleth Installation and Configuration

1. On your Shibboleth server, extract **shibboleth-identityprovider-2.3.2-bin.zip**.
2. Open a command prompt and browse to the directory extracted **shibboleth-identityprovider-2.3.2-bin** directory (for example, C**:\SAML (Shibboleth)\shibboleth-identityprovider-2.3.2-bin**).
3. Run the command: **install.bat**
   a. Install in the **c:\opt\shibboleth-idp** directory.
   b. Enter the fully qualified DNS name (ex.**192.168.21.xxx**).
   c. Enter a password for the keystore (used by the internal certificate).
4. Download **tomcat6-dta-ssl-1.0.0.jar** from the Shibboleth website:

   (https://build.shibboleth.net/nexus/content/repositories/releases/edu/internet2/middleware/security/tomcat6/tomcat6-dta-ssl/1.0.0/tomcat6-dta-ssl-1.0.0.jar) to the following location: **C:\opt\shibboleth-idp\lib\endorsed**
5. Copy all the contents from the endorsed directory to the following location:

   C:\Program Files\Apache Software Foundation\Tomcat 7.0\endorsed
6. Start the Apache Tomcat 7 service from Monitor Tomcat by clicking **Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Monitor Tomcat**.
7. On the **General** tab, go to the **Service Status** section and click the **Start** button.
8. To verify that it is working properly, open a browser and go to **http://127.0.0.1:8081**.
9. Stop the Apache Tomcat 7 service.

Generating a Java Keystore

This section describes how to generate a self-signed Java Keystore. It does not describe how to generate a Java Keystore to be used for publically accessible systems.

1. Open the command prompt and go to **C:\Program Files\Java\jdk1.7.0_21\bin**.
2. In the command prompt, type the following command, replacing **<IP>** with the IP address of your Shibboleth server, and then press **Enter**:

   keytool -genkey -alias server -keyalg RSA -keysize 2048 -keystore <*IP*>.jks
3. The command prompts for the keystore password. Enter the password set in under “SAML Shibboleth Installation and Configuration” on page 16. Enter the password again to confirm.
4. A series of fields is displayed:
   - First and last name
   - Organizational Unit
   - Organization

- City or Locality
- State or Province
- Two letter country code

5. Leave these fields blank and press **Enter** until it displays the following:

   CN=Unknown, OU=Unknown, O=Unknown, L=Unknown, ST=Unknown, C=Unknown correct? [no]

6. When asked if this is correct, enter **yes**.
7. Enter the key password for the server. It is the same password as the keystore password entered under “SAML Shibboleth Installation and Configuration” on page 16. Press **Enter**.
8. Copy the newly created JKS file that is located in **C:\Program Files\Java\jdk1.7.0_21\bin** to **C:/Program Files/Apache Software Foundation/Tomcat 7.0/conf/**.

SAS Agent for Shibboleth x64 Installation and Configuration

1. On the Shibboleth server, run the SAS Agent for Shibboleth as an administrator. Run through the entire installation and select all default configurations.

   The package should be installed under: **C:\Program Files\CRYPTOCard\BlackShield ID\Shibboleth**

2. To launch the SAS Shibboleth Agent Configuration Tool, click **Start > All Programs > SafeNet > Agents > Shibboleth Agent Configuration Tool**.
3. On the **Policy** tab, perform the following steps:
   a. Clear the **Agent Status** option.
   b. Enter the IP address of the server in **Idp External IP/Host Name** field.
   c. Enter in **444** in the **Idp External Port** field.
   d. Ensure the paths are as follows:
      - **Idp Installation Dir:** C:/opt/shibboleth-idp/
      - **Idp Logs Dir:** C:/opt/shibboleth-idp/logs/
      - **Idp Certificate:** C:/opt/shibboleth-idp/credentials/idp.crt
   e. In the **Idp JKS file Password** field, enter the Java Keystore Password that was set under “Generating a Java Keystore” on page 16.
   f. Ensure the **Tomcat Root Path** is as follows:

      C:/Program Files/Apache Software Foundation/Tomcat 7.0/

   g. Enter **8081** in the **Tomcat Http Port** field.
   h. Enter **8443** in the **Tomcat Https Port** field.
   i. Ensure the **Tomcat Certificate Store** is as follows:

      C:/Program Files/Apache Software Foundation/Tomcat 7.0/conf/(IP Address of Server).jks

   j. In the **Private Key Password** field, enter the Java Keystore Password that was set under “Generating a Java Keystore” on page 16.
4. Click the **Communications** tab.

5. Under **Authentication Server Settings**, do the following:
   a. Enter the IP Address of SAS into the **Primary Server (IP:Port)** field.
   b. (OPTIONAL): If there is a failover SAS server, enable the **Failover Server** option and enter the IP address of the Secondary SAS Server.
6. In the **Idp Resources Dir** section, ensure the path is as follows: **C:/opt/shibboleth-idp/resources/**
7. Click **Apply**. (Ignore any backup directory error message you might receive.)
8. Click the **Policy** tab and select **Agent status.**
9. Enter **443** in the **Idp External Port** field.
10. Click **OK**. Accept any window that may open.
11. Close the Shibboleth Agent Configuration Tool.
12. To verify that it is working properly, open a browser and go to **http://127.0.0.1:8081**.
13. Click **Manager App** in the right pane.
14. Enter the user name and password that were set in under "Apache Tomcat Installation and Configuration" on page 15. Note that these entries are case-sensitive.
15. In the **Applications** list, you should see **/idp**, where **Running** is set to **True**.
16. Stop the Apache Tomcat 7 service from Monitor Tomcat.

    To launch Monitor Tomcat, click **Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Monitor Tomcat**.
17. On the **General** tab, go to the **Service Status** section and click **Stop**.

Additional Shibboleth Changes

These changes should be performed on a system that is running only Shibboleth.

1. In Windows Explorer, go to the following location:

   C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf
2. Open the **server.xml** file in Notepad.
3. Click **Edit**, and then select **Replace**. Make the following replacements:
   - Replace 8081 with 80
   - Replace 8443 with 443
4. Save and close the file.
5. To launch the Shibboleth Agent Configuration Tool, click **Start > All Programs > SafeNet > Agents > Shibboleth Agent Configuration Tool**.
   - Enter **80** in the **Tomcat Http Port** field.
   - Enter **443** in the **Tomcat Https Port** field.
6. Restart the Apache Tomcat 7 service from Monitor Tomcat.

   To launch Monitor Tomcat, click **Start > All Programs > Apache Tomcat 7.0 Tomcat7 > Monitor Tomcat**.
7. On the **General** tab, go to the **Service Status** section and click **Restart**.
8. To verify that it is working properly, open a browser and go to **https://127.0.0.1**.

Moving the Shibboleth Certificate

Primary SAS Server

Create the **cert** directory at **C:\Program Files\CRYPTOCard\BlackShield ID\BlackShield Site\Console**.

Shibboleth Server

Copy the **idp.crt** file from **C:/opt/shibboleth-idp/credentials/** to the following location on Primary SAS Server:

D:\Program Files\CRYPTOCard\BlackShield ID\BlackShield Site\Console\cert

SAS SPE Configuration

Shibboleth Integration

1. Log in to the SAS Management Console as an administrator (SYSTEM level).
2. Click **System > Communications > Shibboleth Agent Settings**.
3. Enter the IP address of the Shibboleth Server:
   - Primary Shibboleth INI Management URL (for example, http://192.168.21.xxx/...)
   - Primary Shibboleth Relying Party Management *URL* (for example, http://192.168.21.xxx/...)
4. **OPTIONAL:** If required, enter secondary configuration information.
5. Apply your changes.
6. Click the **Shibboleth Agent Settings link**, and then click **Resync All**.
7. If the configuration was successful, the following message is displayed:

   "SAML 2.0 data was successfully synchronized with the remote agent."

Adding an Auth Node

Once Shibboleth is running, it will need to be added as an Auth Node in SAS. The Auth Node will only need to be added to the Top Level Organization.

1. Log in to the SAS Management Console as an administrator (SYSTEM level).
2. Click **Virtual Server > Comms**.
3. Under **Auth Nodes**, click **Auth Node > Add.**
4. Enter the following information:
   - **Agent Description**
   - **Low IP Address In Range** – the IP address of Shibboleth
5. Clear the **FreeRADIUS Synchronization** option as this is a web service agent
6. Click **Save**.

Additional SAS Input for Shibboleth

1. Log in as an Operator for the Top Level Organization.
2. Click **Administration > Customize References > SAML Settings**.
3. Enter the following information:

SAML Version	2
Entity ID	https://IP_Address_or_DNS_of_Shibbloeth/idp/shibboleth
Identity Provider AuthRequest login URL	https://IP_Address_or_DNS_of_Shibbloeth/idp/profile/Shibboleth/SSO
Identity Provider HTTP-POST login URL	https://IP_Address_or_DNS_of_Shibbloeth/idp/profile/SAML2/POST/SSO
Identity Provider HTTP-POST-SimpleSign login URL	https://IP_Address_or_DNS_of_Shibbloeth/idp/profile/SAML2/POST-SimpleSign/SSO
Identity Provider HTTP-Redirect login URL	https://IP_Address_or_DNS_of_Shibbloeth/idp/profile/SAML2/Redirect/SSO
Identity Provider logout URL	https://IP_Address_or_DNS_of_Shibbloeth/idp/signout.jsp
Download URL for Identity Provider Certificate	https://IP_Address_or_DNS_of_SAS/console/cert/idp.crt

4. Click **Apply**.

Removal of the Apache Directory and Default Page (Optional)

This procedure is recommended for production environments.

1. Browse to the following location: **C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps**
2. Rename the following directories:
   - host-manager
   - manager
   - docs
3. Under **C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\ROOT**, perform the following steps:
   a. Rename **index.jsp** to **index.jsp.old**.
   b. Create a blank **index.jsp** file.

Troubleshooting

To test the status of Shibboleth, browse to **https://127.0.0.1/idp/profile/Status**.

Note that your TCP port may differ.

Shibboleth errors will appear in the following file: **opt\shibboleth-idp\logs\idp-process.log**

Public certificate errors or general Tomcat errors will appear in the following directory:

C:\Program Files\Apache Software Foundation\Tomcat 7.0\logs

The SAS Shibboleth agent logs can be found in the following directory:

C:\Program Files\CRYPTOCard\BlackShield ID\Shibboleth\log

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when phone support is available to you.

Table 1: Support Contacts

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com 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.	