SafeNet Authentication Service Agent for IBM Security Access Manager for Web

Installation and Configuration Guide

security to be free

All information herein is either public information or is the property of and owned solely by Gemalto NV. and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto's information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in the case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

Document Part Number: 007-012474-002

Release Date: August 2016

Contents

Preface

This document describes how to install and configure the SafeNet Authentication Service Agent for IBM Security Access Manager for Web.

Customer Release Notes

The Customer Release Notes (CRN) document provides important information about this release that is not included in other customer documentation. It is strongly recommended that you read the CRN to fully understand the capabilities, limitations, new features and known issues for this release.

Audience

This document is intended for personnel responsible for maintaining your organization's security infrastructure. This includes SafeNet Authentication Service (SAS) users and security officers, key manager administrators, and network administrators. It is assumed that the users of this document are proficient with security concepts.

All products manufactured and distributed by Gemalto are designed to be installed, operated, and maintained by personnel who have the knowledge, training, and qualifications required to safely perform the tasks assigned to them. The information, processes, and procedures contained in this document are intended for use by trained and qualified personnel only.

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 Gemalto Customer Support. Gemalto 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 Gemalto and your organization. Please consult the support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto 4690 Millennium Drive Belcamp, Maryland 21017, USA	
Phone	US	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 login to manage incidents, get latest software upgrades, and access the Gemalto Knowledge Base.	

1 Introduction

IBM® Security Access Manager

Authentication is the process of proving that a user is who he or she claims to be. An Access System enables you to configure authentication rules in the policy domains and policies that protect your resources. Authentication rules, in turn, contain authentication schemes, which provide the methods for performing verification of the user's identity.

The IBM® Security Access Manager (ISAM) is an IBM security product that helps in granting authorized users the right to use a service while preventing access to unauthorized users. This process is known as Access or Rights or Identity Management.

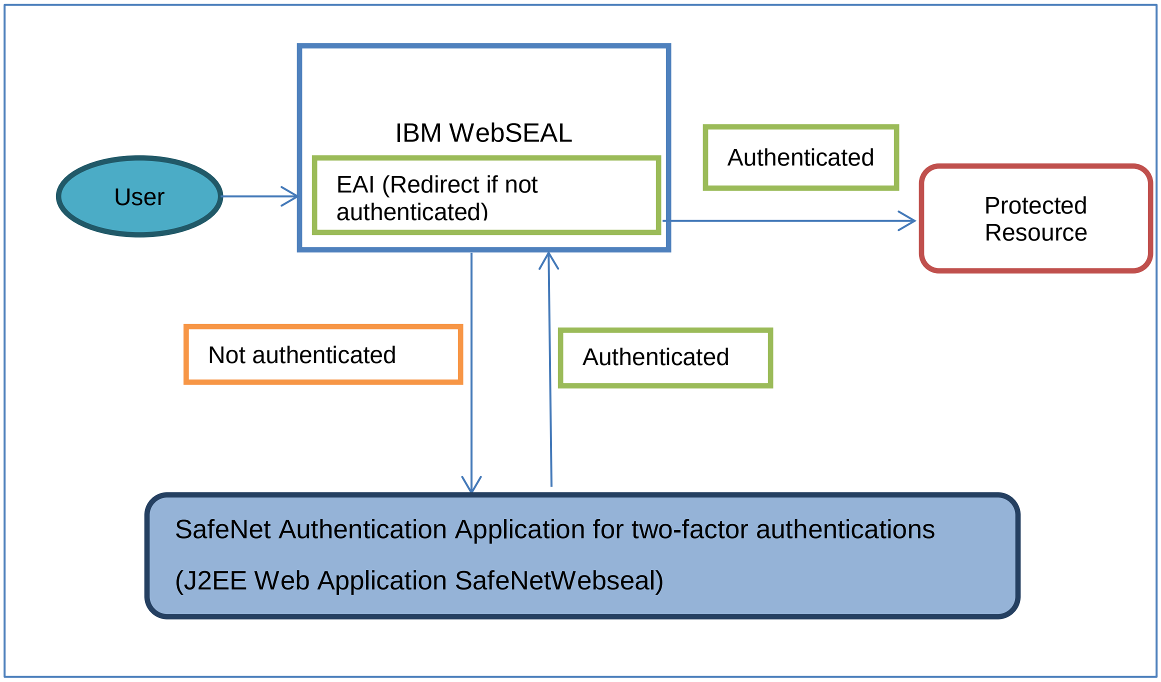
The ISAM for Web provides an integrated security management platform for authentication services, access control, authorization services, identity mapping, single sign-on, entitlements, and audit services across the enterprise resources. It also provides policy-based security management for the extended enterprise that enables customers, business partners, employees, suppliers, and distributors to securely access enterprise resources in a trusted manner.

Organizations using the ISAM for Web can implement the SafeNet Authentication Service (SAS) solution for a powerful two-factor authentication (2FA).

The SAS Agent for ISAM (for Web) utilizes IBM WebSEAL's External Authentication Interface (EAI) for two-factor authentications. When a user tries to access a protected application, the WebSEAL intercepts the request based on a defined set of rules and redirects the login request to an appropriate authentication destination. In this case, it's a custom J2EE application (for example, SafeNetWebSeal) deployed on the same physical server or an external J2EE server (Apache Tomcat 8xx).

The application receives the request, then collects the user's Lightweight Directory Access Protocol (LDAP) credentials and verifies them on a configured LDAP server (LDAP and 2FA credentials verification can be split into two stages via configuration). It then sends the collected credentials to the cloud/on-premises SAS using a highly encrypted (1024-bit) payload over SOAP protocol. The SAS then sends back an encrypted authenticated response. Upon successful authentication, the response is returned to the WebSEAL with some special response headers, which WebSEAL translates into a successful authentication. The WebSEAL adds an authentication header to the ongoing request and forwards the request to the protected resource.

The following diagram shows the environment required to implement an ISAM for Web solution using the SAS:


IBM WebSEAL
User
EAI (Redirect if not authenticated)
Authenticated
Protected Resource
Not authenticated
Authenticated
SafeNet Authentication Application for two-factor authentications
(J2EE Web Application SafeNetWebseal)

In the above example, the user wants to connect to the WebSEAL server. The following are the steps that help illustrate solution flow using the EAI mechanism:

1. User tries to access the protected resource.
2. WebSEAL EAI redirects the user to SafeNet Authentication Application (SAA).
3. SAA collects LDAP credentials from the user.
4. SAA validates the LDAP credentials against the configured LDAP server.
5. User is prompted for a one-time password (OTP).
6. User generates and provides the OTP.
7. Upon successful OTP validation, WebSEAL's required EAI headers are added to the response.
8. WebSEAL detects the headers in the response and forwards the request to the protected resource.

General Prerequisites

Ensure that the following prerequisites for installing the ISAM components are met:

- Install the following:
  - ISAM for Web 7.0, 8.0, or 9.0 (depending on the solution)
  - SAS Agent for ISAM 2.0
- Create an account in SAS Cloud or SAS PCE 3.4.
  For more information, visit: http://www.safenet-inc.com/request-information/
- Ensure that the users in the SAS are also available in the ISAM.
- Ensure administrative rights for installation and configuration of the SAS Agent for ISAM.

- Ensure that the Apache Tomcat server is up, and running on the machine we plan to host the Agent on.
    - Firewall should allow incoming connection on Apache Tomcat secure port.
    - Recommended Setting: Apache Tomcat should be configured to use SSL.

Administrator Prerequisites

To successfully configure and implement the SAS Agent for ISAM (for Web) solution, the administrator must be familiar with:

- ISAM for Web 7.0, 8.0, or 9.0
- SAS Cloud or Service Providers Edition (SPE) / Private Cloud Edition (PCE)
  Note: This guide uses SAS Cloud as an example, but the solution can also be implemented on SAS SPE / PCE.

Configuration Components

The environment components are:

- ISAM for Web 7.0, 8.0, or 9.0
- SAS Agent for ISAM, running on Apache Tomcat.

2
Installation and Configuration

Overview

The SAS Agent for ISAM can be installed on either Linux or Windows.

The following Linux versions are supported:	The following Windows versions are supported:
• RHEL 7 • SLES 12 The procedures must run on a 64-bit Operating System.	• Windows 2008 R2 • Windows 2012 R2

Installing SAS Agent on Linux

To install the SAS Agent for ISAM on Linux, follow the steps:

1. Install latest available Java SDK by following the steps in the below link
   http://tecadmin.net/install-java-8-on-centos-rhel-and-fedora/

2. Install Apache Tomcat (version 8.0.33)
   Example Commands to install Apache Tomcat (version 8.0.33):

   a. Installing Tomcat

      ```
      ➔ gunzip apache-tomcat-8.0.33.tar.gz
      ➔ tar –xvf apache-tomcat-8.0.33.tar
      ➔ cd ./apache-tomcat-8.0.33/bin
      ➔ ./startup.sh
      ```

      Verify if Tomcat is running

      ```
      ➔ ps –ef | grep –i java
      ```

      (JAVA process must be running)

   b. Configure Tomcat

      ➔ *../conf/* (move to conf folder under tomcat root)
      ➔ *vi tomcat-users.xml* (open the file in editor)

      Place the following two lines just above the last line.

      ```
      <role rolename="manager-gui"/>
      ```

<user username="tomcat" password="tomcat" roles="manager-gui"/>

Save file.

➔ Go to Tomcat bin directory, restart catalina, and check if tomcat is running.

```
./catalina.sh stop
ps –ef | grep –i java (no Java process should be running)
./catalina.sh start
ps –ef | grep –i java (Java process should be running)
```

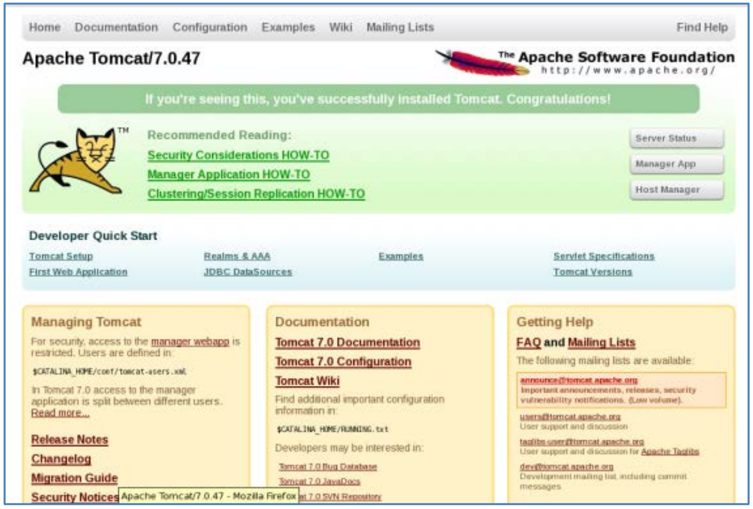
3. Install the agent using the **rpm** command: *rpm –ivh <file_name>*

The agent is installed at the **/usr/local/safenet/webseal** path.
The folder structure is as follows:

```
/webseal/bin
/webseal/bsidkey
/webseal/defaults
/webseal/ini
/webseal/log
/webseal/Open Source Licenses
/webseal/war
```

Deploying WAR File

1. Go to the Apache management console.
2. On the right side, click **Manager App** button.



If you're seeing this, you've successfully installed Tomcat. Congratulations!

For security, access to the manager webapp is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 7.0 access to the manager application is split between different users. Read more...

Find additional important configuration information in:

`$CATALINA_HOME/RUNNING.txt`

Developers may be interested in:

The following mailing lists are available:

announce@tomcat.apache.org
Important announcements, releases, security vulnerability notifications. (Low volume).

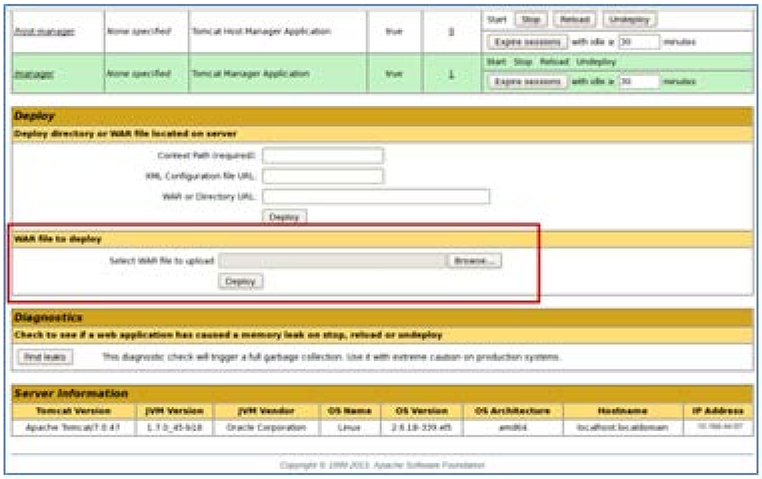
users@tomcat.apache.org
User support and discussion

taglibs-user@tomcat.apache.org
User support and discussion for Apache Taglibs

dev@tomcat.apache.org
Development mailing list, including commit messages

3. Under **WAR file to deploy**, click **Browse** and select the following file:

/usr/local/safenet/webseal/war/SafenetWebseal.war



/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

WAR file to deploy

Select WAR file to upload

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

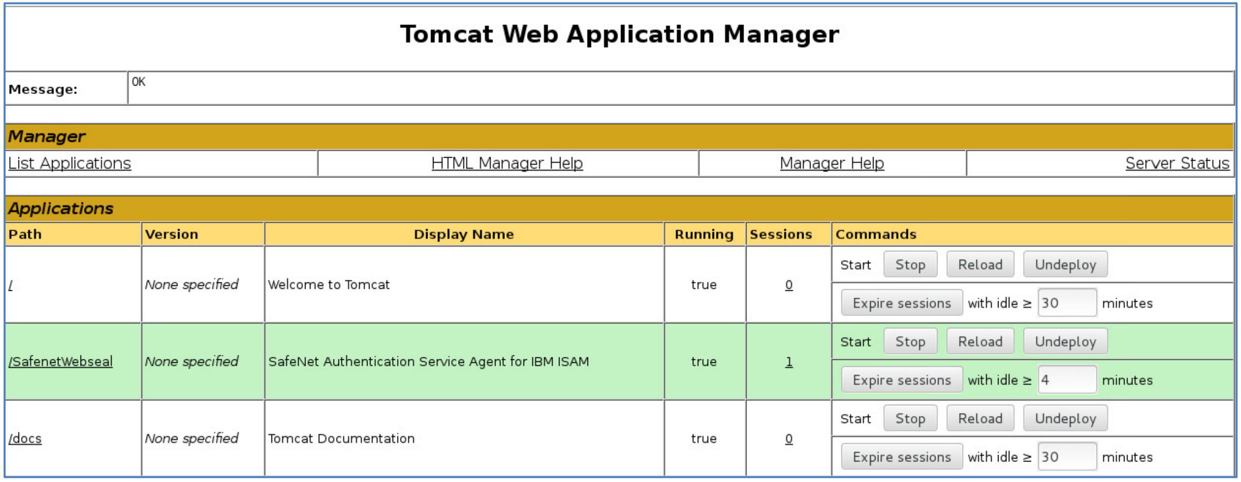
This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/7.0.47	1.7.0_45-b18	Oracle Corporation	Linux	2.6.18-339.el5	amd64	localhost.localdomain	[illegible]

Copyright © 1999-2013, Apache Software Foundation

4. Click **Deploy**.
5. After deployment, open the Application Manager and ensure that the **/SafenetWebseal** application has the value **true** in the **Running** column.



Tomcat Web Application Manager

Message: OK

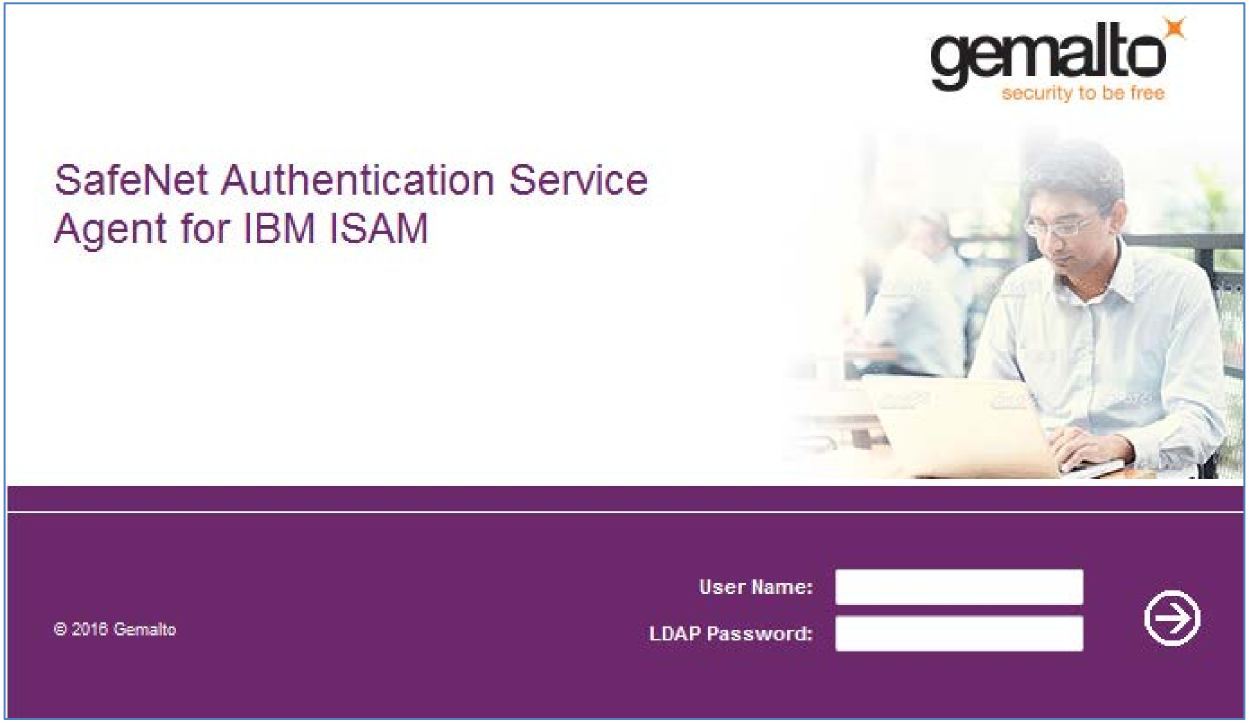
Manager

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/SafenetWebseal	None specified	SafeNet Authentication Service Agent for IBM ISAM	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 4 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

6. Restart Tomcat.
7. To test the app, click the **/SafenetWebseal** hyperlink.

The Agent login screen appears.



Viewing SAS Agent Version

1. Run the following command to view the name of the installed RPM package:

   rpm -qa | grep ISAM

2. Run the following command, and in the output, search for **Version**:

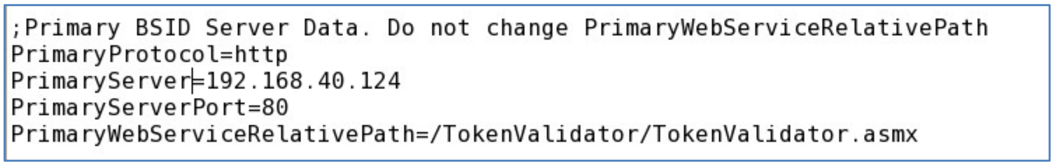
   rpm -qi <name of the package>

Configuring SAS Agent on Linux

The SAS Agent for ISAM configuration file can be found at the following path: **/usr/local/safenet/webseal/ini**.

JCryptoWrapper.ini is the configuration file that contains all the relevant configurations for the agent. The following describes some of the main configuration keys:

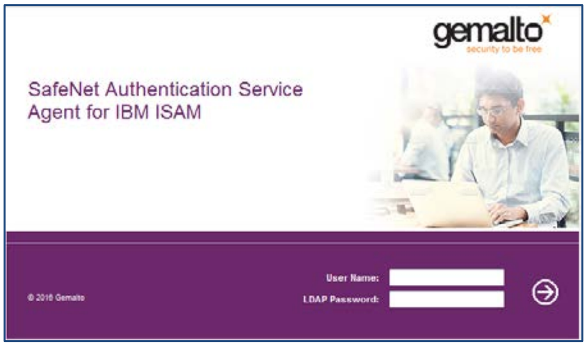
- **PrimaryServer** is the IP of the primary BSID server.



```
;Primary BSID Server Data. Do not change PrimaryWebServiceRelativePath
PrimaryProtocol=http
PrimaryServer=192.168.40.124
PrimaryServerPort=80
PrimaryWebServiceRelativePath=/TokenValidator/TokenValidator.asmx
```

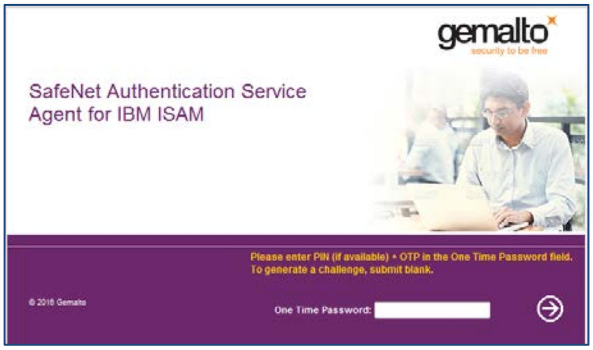
- If you want the user to provide a One Time Password (OTP) on the first authentication screen, set the value of **USE_SPLIT_AUTH** to **0**.

  Example 1:
  USE_SPLIT_AUTH=1



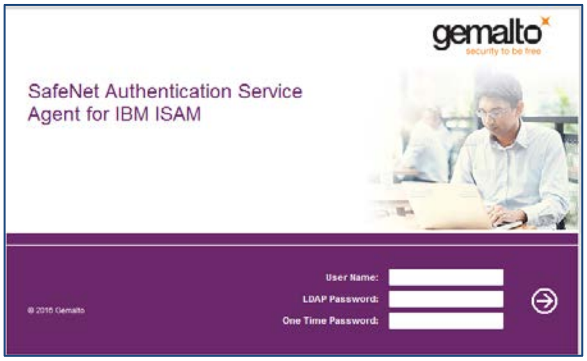
Enter a valid **User Name** and **LDAP Password**, click the forward arrow button**.**

The following One Time Password screen appears:



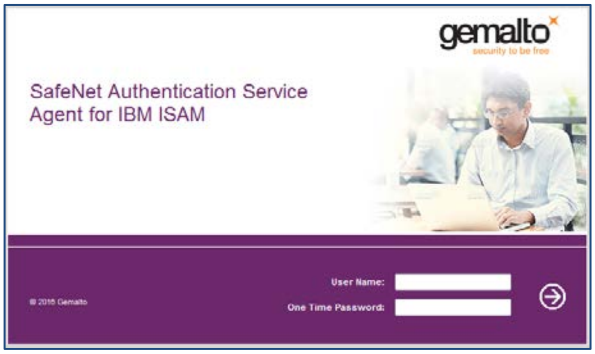
Please enter PIN (if available) + OTP in the One Time Password field.
To generate a challenge, submit blank.

Example 2: **USE_SPLIT_AUTH=0**

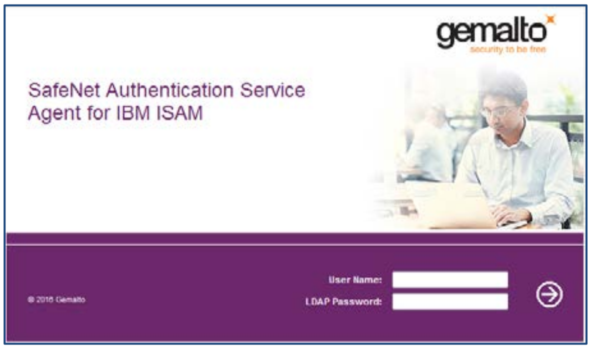


- To disable LDAP authentication, set the value of **LDAP_AUTH** to **0**.

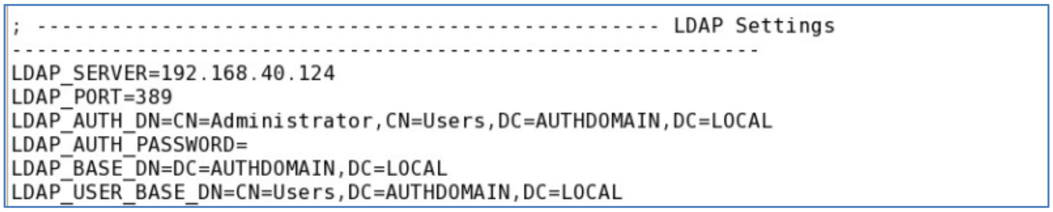
Example 1: **LDAP_AUTH=0**



Example 2: **LDAP_AUTH=1**



- LDAP bind credentials are configured in the ini file.



```
; --------------------------------------------------- LDAP Settings
---------------------------------------------------------
LDAP_SERVER=192.168.40.124
LDAP_PORT=389
LDAP_AUTH_DN=CN=Administrator,CN=Users,DC=AUTHDOMAIN,DC=LOCAL
LDAP_AUTH_PASSWORD=
LDAP_BASE_DN=DC=AUTHDOMAIN,DC=LOCAL
LDAP_USER_BASE_DN=CN=Users,DC=AUTHDOMAIN,DC=LOCAL
```

Update the default LDAP credentials to those required by your Active Directory.

Note: **CN=Administrator** is just an example. Any user with LDAP read rights can be configured.

Customizing Login Page

In the **/usr/local/safenet/webseal/defaults** folder, the following language specific folders for login page branding and customization must be present:

- **en** (for English)
- **ar** (for Arabic)
- **fr** (for French)

Installing SAS Agent on Windows

To install the SAS Agent for ISAM on Windows, follow the steps:

1. Install JRE (Java Runtime Environment) — version 1.8.0_71.
   For more information, click here.
2. Install Apache Tomcat — version 8.0.30.
   For more information, click here.
3. From the installation package, copy the **SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0.zip** file on the server and extract in the **<System Root Dir>**. The destination path is **<System Root Dir>\SafeNet- Authentication-Service-Agent-For-IBM-ISAM-2-0**.

   For example, if your **<System Root Dir>** is C, the destination path will be **C:\SafeNet- Authentication-Service-Agent-For-IBM-ISAM-2-0**.

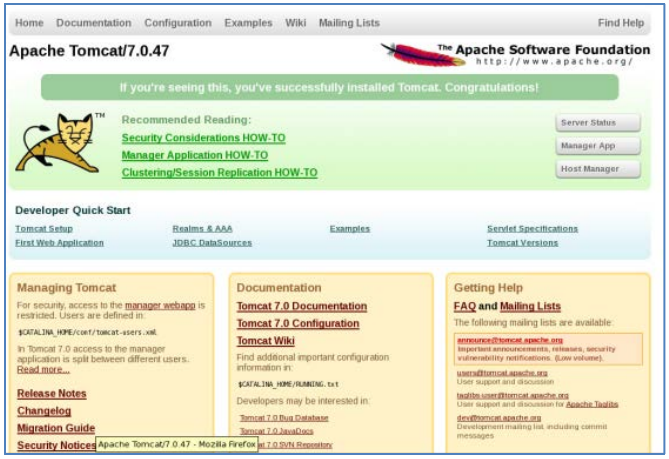
The folder structure is as follows:

\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0\bin
\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0\bsidkey

\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0\defaults
\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0l\ini
\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0\log
\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0\war

Deploying WAR File

1. Go to the Apache management console.
2. On the right side, click **Manager App** button.



Apache Tomcat/7.0.47

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:
Security Considerations HOW-TO
Manager Application HOW-TO
Clustering/Session Replication HOW-TO

Developer Quick Start

Tomcat Setup	Realms & AAA	Examples	Servlet Specifications
First Web Application	JDBC DataSources		Tomcat Versions

Managing Tomcat

For security, access to the manager webapp is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 7.0 access to the manager application is split between different users. Read more...

Release Notes
Changelog
Migration Guide
Security Notices

Apache Tomcat/7.0.47 - Mozilla Firefox

Documentation

Tomcat 7.0 Documentation
Tomcat 7.0 Configuration
Tomcat Wiki

Find additional important configuration information in:

`$CATALINA_HOME/RUNNING.txt`

Developers may be interested in:

Tomcat 7.0 Bug Database
Tomcat 7.0 JavaDocs
Tomcat 7.0 SVN Repository

Getting Help

FAQ and Mailing Lists

The following mailing lists are available:

announce@tomcat.apache.org
Important announcements, releases, security vulnerability notifications. (Low volume).

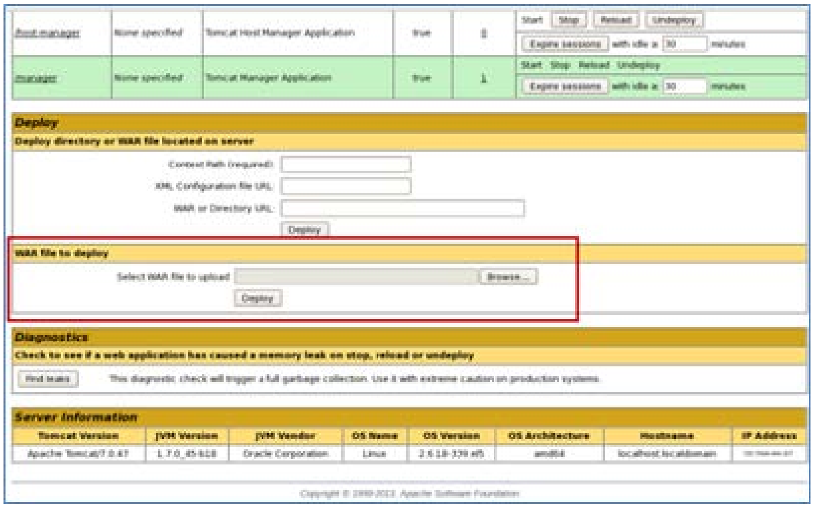
users@tomcat.apache.org
User support and discussion

taglibs-user@tomcat.apache.org
User support and discussion for Apache Taglibs

dev@tomcat.apache.org
Development mailing list, including commit messages

3. Under **WAR file to deploy**, click **Browse** and select the following file:

   <System Root Dir>\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0\war\SafenetWebseal.war



/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

Deploy

Deploy directory or WAR file located on server

Context Path (required):
XML Configuration file URL:
WAR or Directory URL:

Deploy

WAR file to deploy

Select WAR file to upload Browse...

Deploy

Diagnostics

Check to see if a web application has caused a memory leak on stop, reload or undeploy

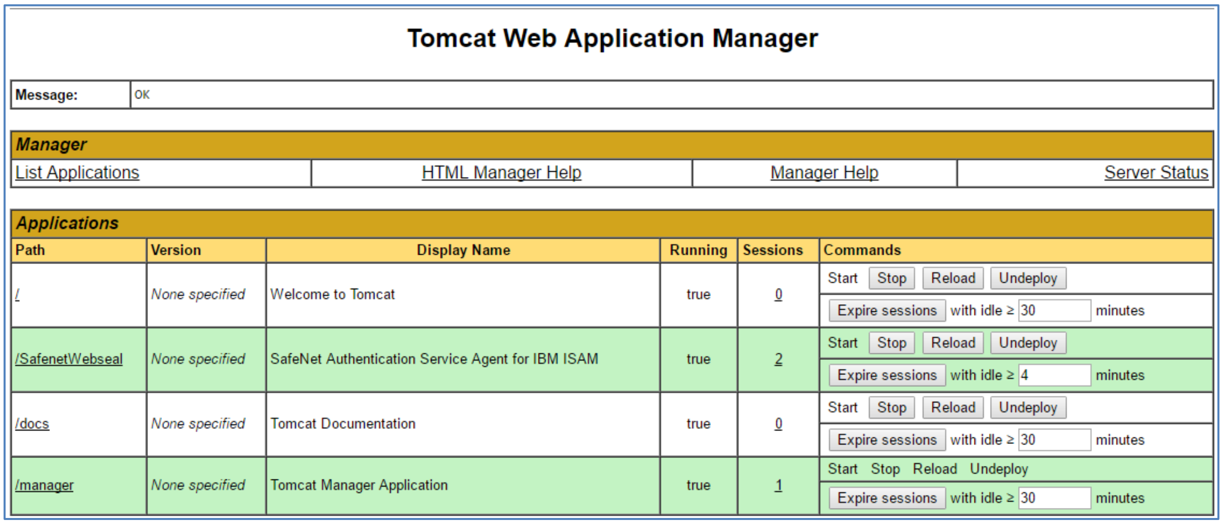
Find leaks This diagnostic check will trigger a full garbage collection. Use it with extreme caution on production systems.

Server Information

Tomcat Version	JVM Version	JVM Vendor	OS Name	OS Version	OS Architecture	Hostname	IP Address
Apache Tomcat/7.0.47	1.7.0_45-b18	Oracle Corporation	Linux	2.6.18-339.el5	amd64	localhost.localdomain	[illegible]

Copyright © 1999-2013, Apache Software Foundation

4. Click **Deploy**.
5. After deployment, open the Application Manager and ensure that the ***/SafenetWebseal*** application has the value **true** in the **Running** column.



Tomcat Web Application Manager

Message:	OK

Manager

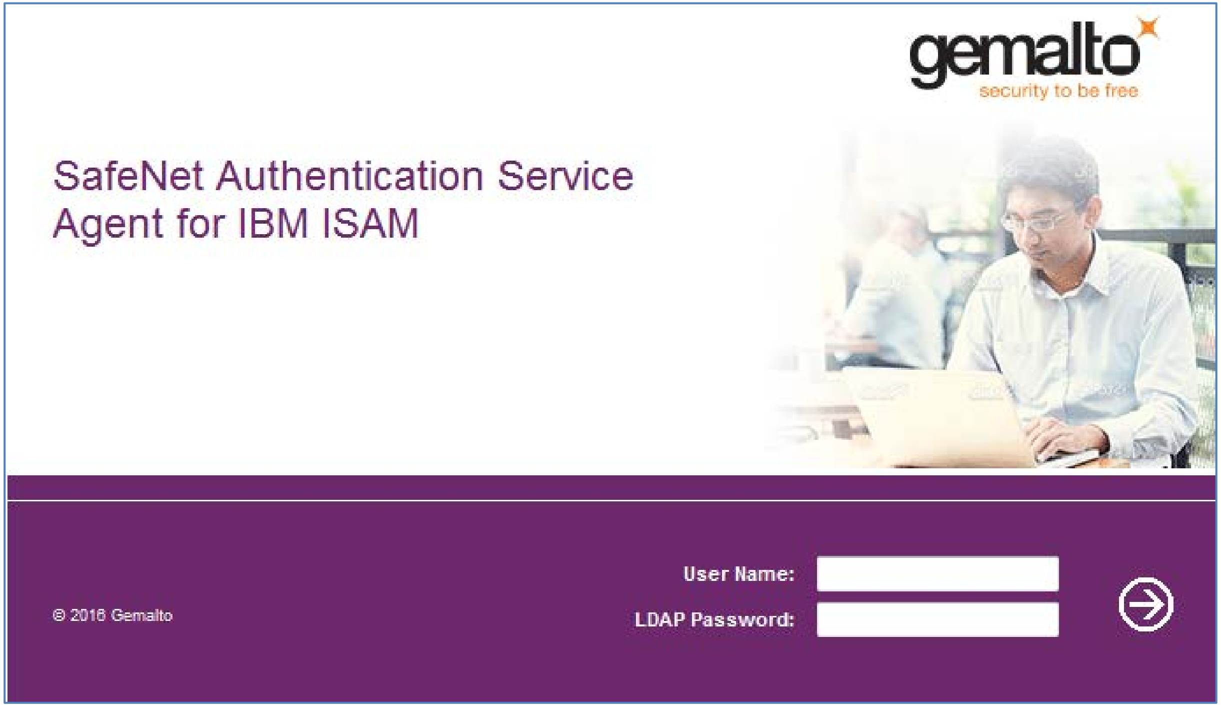
List Applications	HTML Manager Help	Manager Help	Server Status

Applications

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/SafenetWebseal	None specified	SafeNet Authentication Service Agent for IBM ISAM	true	2	Start Stop Reload Undeploy Expire sessions with idle ≥ 4 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	1	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

6. Restart Tomcat.
7. To test the app, click the **/SafenetWebseal** hyperlink.

   The Agent login screen appears.



Configuring SAS Agent on Windows

The SAS Agent for ISAM configuration file is located at the following path:
<System Root Dir>\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0\ini.

JCryptoWrapperWin.ini contains all the relevant configurations for the agent. The following describes some of the tested configuration keys:

- Set the value of **PrimaryServiceURL** to the URL of the primary SAS server.
  Example: **PrimaryServiceURL=https://agent1.safenet-inc.com/TokenValidator/TokenValidator.asmx**

- If you want the user to provide a One-Time Password (OTP) on the first authentication screen, set the value of **USE_SPLIT_AUTH** to **0**.
  Example: **USE_SPLIT_AUTH=0**

- To disable LDAP authentication, set the value of **LDAP_AUTH** to **0**.
  Example: **LDAP_AUTH=0**

- Depending on your **<System Root Dir>**, set the value for **EncryptionKeyFile**, **CryptoCOMPath**, and **TEMPLATE_DIR**.
  Example:
  EncryptionKeyFile=C:/SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0/bsidkey/Agent.bsidkey
  CryptoCOMPath=C:/SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0/bin/x64/CryptoCOM.dll
  TEMPLATE_DIR=C:/SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0/defaults/

  Note: Though Windows generally uses backslash (\), the above path mentions forward slash (/). The use of forward slash is correct, and the backslash must not be used to mention the above paths.

- LDAP bind credentials are configured in the file.

  Example:

  LDAP_SERVER=192.168.40.120

  LDAP_PORT=389

  LDAP_AUTH_DN=CN=Administrator, CN=Users, DC=ISAM, DC=com

  LDAP_AUTH_PASSWORD=

  LDAP_BASE_DN=DC=ISAM, DC=com

  LDAP_USER_BASE_DN=CN=Users, DC=ISAM, DC=com

  Update the LDAP credentials to those required by your LDAP Directory.

  Note: **CN=Administrator** is just an example. It can be any user that is present in the Users group.

After setting parameters in the **JCryptoWrapperWin.ini** file, restart the Apache Tomcat server.
To restart, follow the steps:

1. From the **Start** menu, open the **Configure Tomcat** window.
2. On the **General** tab, click **Stop**. Then click **Start**.
3. Click **OK**.

Or, restart the Apache Tomcat server using *services.msc*.

Customizing Login Page

In the **<System Root Dir>\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0\defaults\** folder, the following language specific folders for login page branding and customization must be present:

- **en** (for English)
- **ar** (for Arabic)
- **fr** (for French)

3 ISAM Basic Configuration

This chapter explains the steps needed to do basic configuration of ISAM for Web 7.0, 8.0, and 9.0. This will enable the user to authenticate the protected web application(s) using the SAS Agent for ISAM.

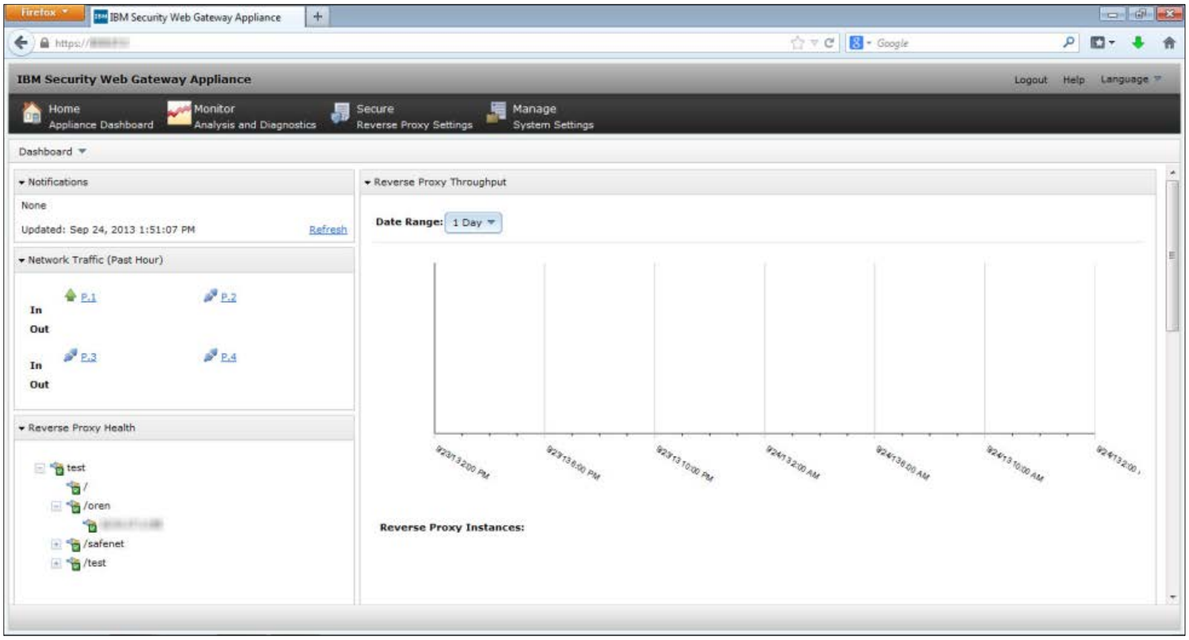
Configuring ISAM for Web 7.0

The ISAM for Web 7.0 is configured with default options.

In the following example, a reverse proxy is used with two junctions. One junction is the protected web application, and the other is the SafeNet WebSEAL external authentication agent.
Ensure that the reverse proxy is already configured for the protected web application.

To configure the ISAM for Web 7.0, follow the steps:

1. Login to the **IBM Security Web Gateway Appliance** console.



https://[redacted]

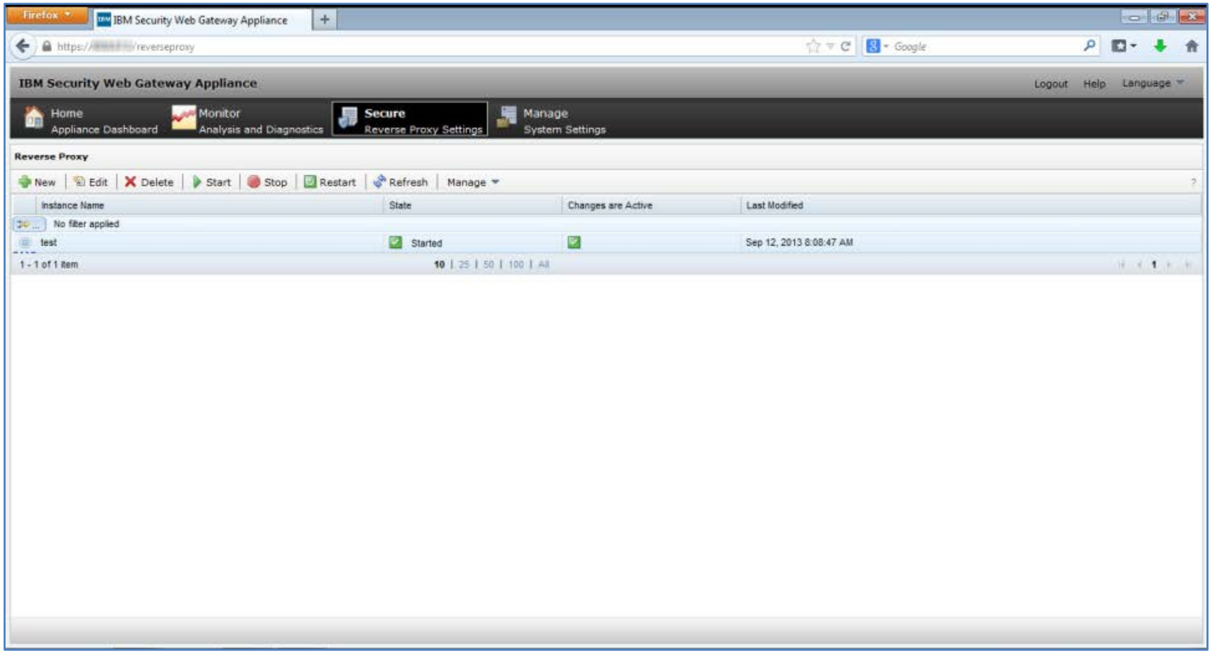
Notifications: None

Updated: Sep 24, 2013 1:51:07 PM

Date Range: 1 Day

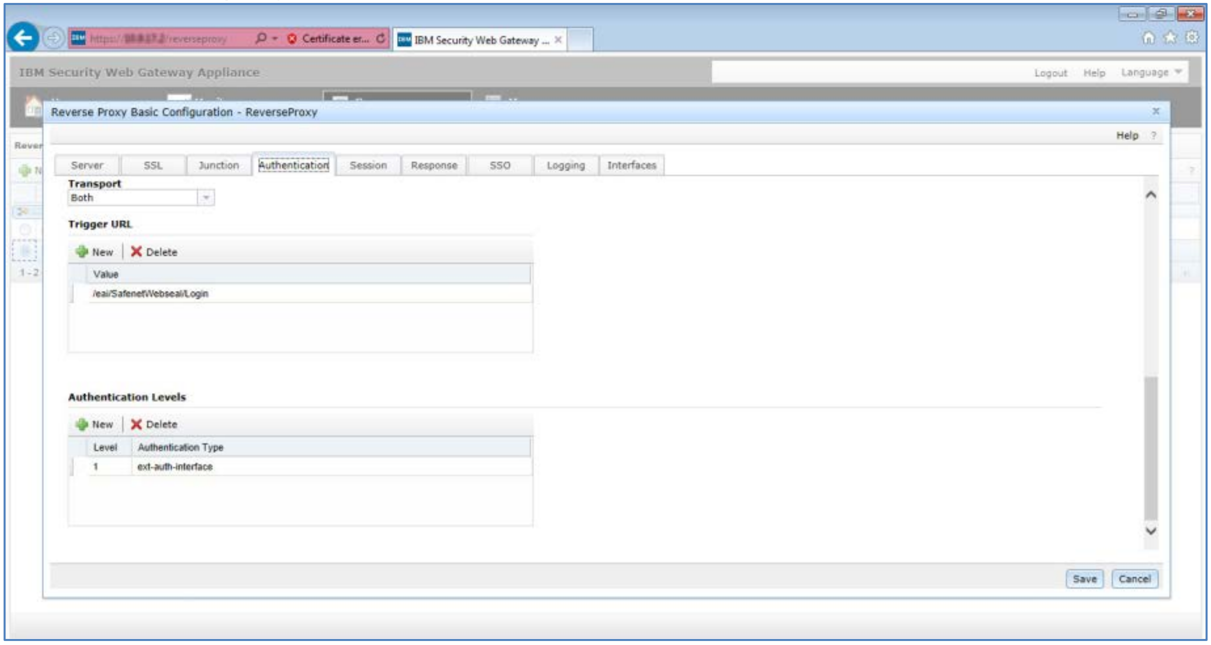
Reverse Proxy Instances:

2. Click **Secure > Reverse Proxy**.



Instance Name	State	Changes are Active	Last Modified
test	✓ Started	✓	Sep 12, 2013 8:08:47 AM

3. Select the reverse proxy and, click **Edit**.


https://[redacted]/reverseproxy
Certificate er...
IBM Security Web Gateway ...
IBM Security Web Gateway Appliance
Logout
Help
Language
Reverse Proxy Basic Configuration - ReverseProxy
Help
Server
SSL
Junction
Authentication
Session
Response
SSO
Logging
Interfaces
New
Delete
New
Delete
Save
Cancel

Transport: Both

Trigger URL

Value
/eai/SafenetWebseal/Login

Authentication Levels

Level	Authentication Type
1	ext-auth-interface

4. On the **Authentication** tab, add a new **Trigger URL**: /eai/SafenetWebseal/Login

5. Add a new **Authentication Level** called **ext-auth-interface**.

6. Login to the ISAM from the web Command Line Interface (CLI) and create the following Access Control List (ACL) for unauthenticated users:

```
pdadmin sec_master> acl create unauth

pdadmin sec_master> acl modify unauth set group iv-admin TcmdbsvaBRrxl

pdadmin sec_master> acl modify unauth set group webseal-servers Tgmdbsrxl
pdadmin sec_master> acl modify unauth set user sec_master TcmdbsvaBRrxl

pdadmin sec_master> acl modify unauth set any-other Trx

pdadmin sec_master> acl modify unauth set unauthenticated Trxc
```

Attach the ACL you created to the **eai** application (object).
For example: **pdadmin sec_master> acl attach <object name/reverse proxy>/eai unauth**

7. For running the solution on the Firefox web browser, create and attach the ACL using the following commands:

Create an ACL:

```
pdadmin sec_master> create webseal-favicon

pdadmin sec_master> modify webseal-favicon description “favicon access”
```

Provide the permissions:

```
pdadmin sec_master> modify webseal-favicon set unauthenticated Tr
```

(There might be warnings after the above command, ignore them)

```
pdadmin sec_master> modify webseal-favicon set any-other Tr
```

(There might be warnings after the above command, ignore them)

Check ACL details:

```
pdadmin sec_master> acl show webseal-favicon
```

Output:

```
_ACL name: webseal-favicon

Description: favicon access

Entries:

Any-other Tr

Unauthenticated Tr

User sec_master TcmdbsvaBRrl_
```

List down objects:

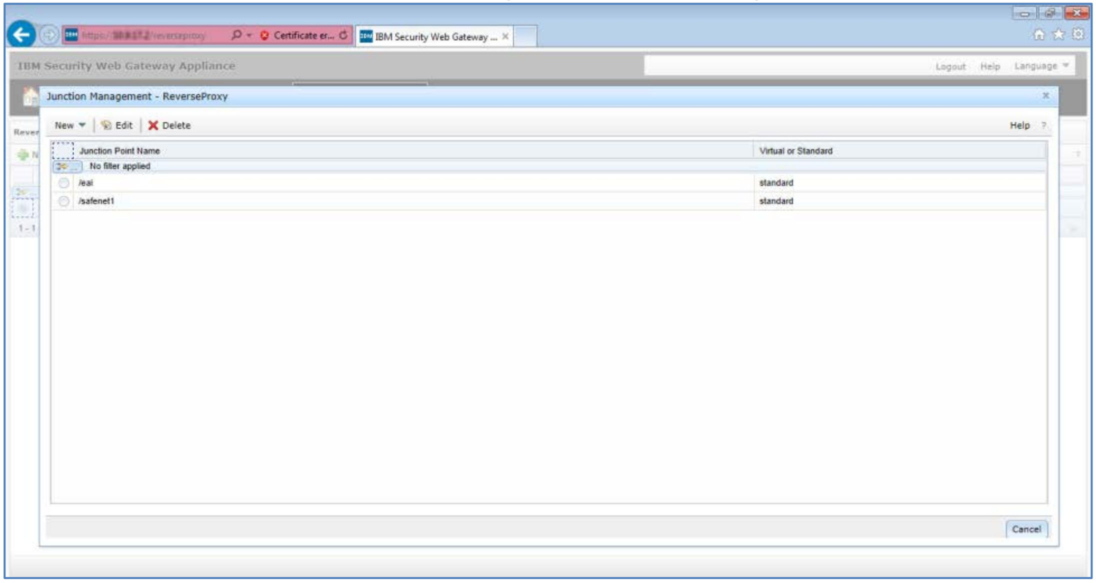
```
pdadmin sec_master>Object list /WebSEAL

/WebSEAL/webseal-ReverseProxy
```

Attach ACL (created above) with the Object listed:

```
pdadmin sec_master> acl attach /WebSEALwebseal-ReverseProxy/favicon.ico webseal-favicon
```

8. Select the reverse proxy, and select **Manage > Junction Management**.


https://[redacted]/reverseproxy
Certificate er...
IBM Security Web Gateway ...
IBM Security Web Gateway Appliance
Logout
Help
Language
Junction Management - ReverseProxy
New
Edit
Delete
Help
Cancel

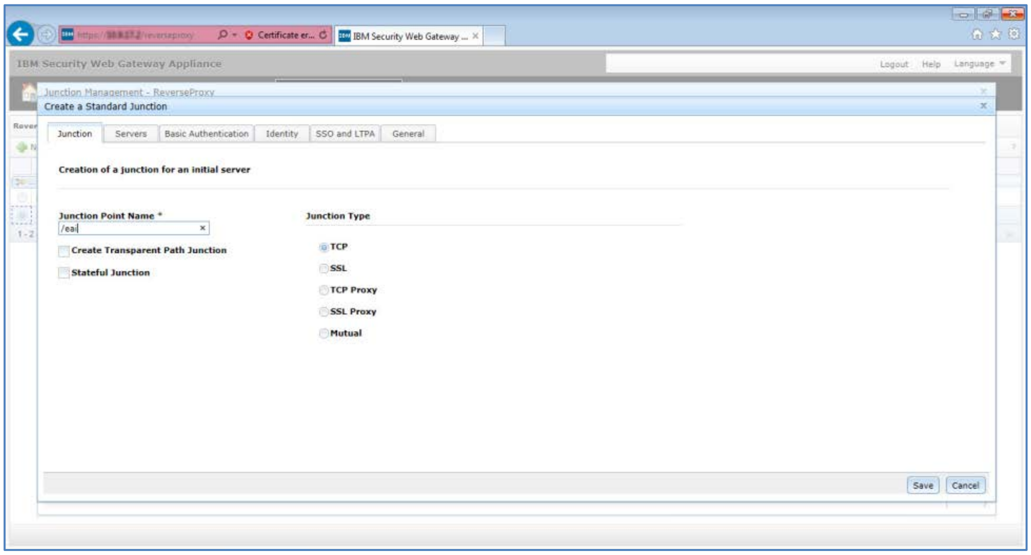
Junction Point Name	Virtual or Standard
No filter applied	
/eai	standard
/safenet1	standard

Creating Junction

A WebSEAL junction is an HTTP (or HTTPS) connection between a front-end WebSEAL server and a back-end Web application server. Junctions logically combine the Web space of the back-end server with the Web space of the WebSEAL server, resulting in a unified view of the entire Web object space.

Perform the following steps to create a new junction in which the SAS EAI server is the junction server:

I. Select **New > Standard Junction**.


https://[redacted]/reverseproxy
Certificate er...
IBM Security Web Gateway ...
IBM Security Web Gateway Appliance
Logout
Help
Language
Junction Management - ReverseProxy
Create a Standard Junction
Junction
Servers
Basic Authentication
Identity
SSO and LTPA
General
Save
Cancel

Creation of a junction for an initial server

Junction Point Name *
/eai

□ Create Transparent Path Junction

□ Stateful Junction

Junction Type

● TCP
○ SSL
○ TCP Proxy
○ SSL Proxy
○ Mutual

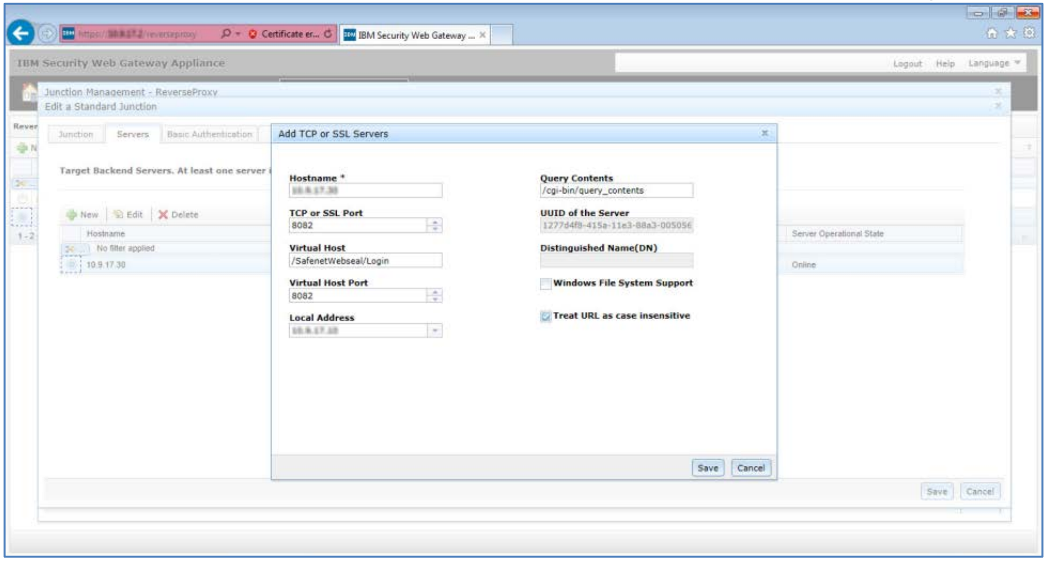
II. On **Junction** tab, add a **Junction Point Name**.

III. Under **Junction Type**, select **TCP**.

IV. Click **Servers** tab, and click **New**.

V. In the **Hostname** field, enter the SAS EAI agent server information.

VI. In the **Virtual Host** field, add the path to the login folder: **/SafenetWebseal/Login**



Add TCP or SSL Servers

Hostname *: [redacted]

TCP or SSL Port: 8082

Virtual Host: /SafenetWebseal/Login

Virtual Host Port: 8082

Local Address: [redacted]

Query Contents: /cgi-bin/query_contents

UUID of the Server: 1277d4f8-415a-11e3-88a3-005056

Distinguished Name(DN):

□ Windows File System Support

☑ Treat URL as case insensitive

VII. Enter other fields as required, and click **Save**. You will be returned to the **Reverse Proxy** page.

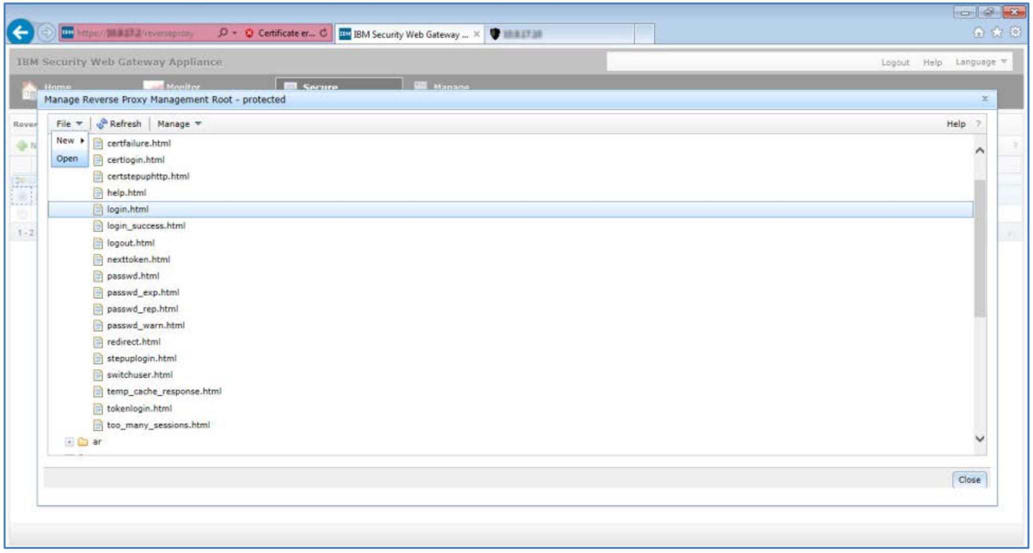
Configuring Redirection to EAI Agent

Complete the following steps to configure redirection to the EAI Agent:

I. Select **Secure > Reverse Proxy**.

II. Click the reverse proxy, and select **Manage > Management Root**.

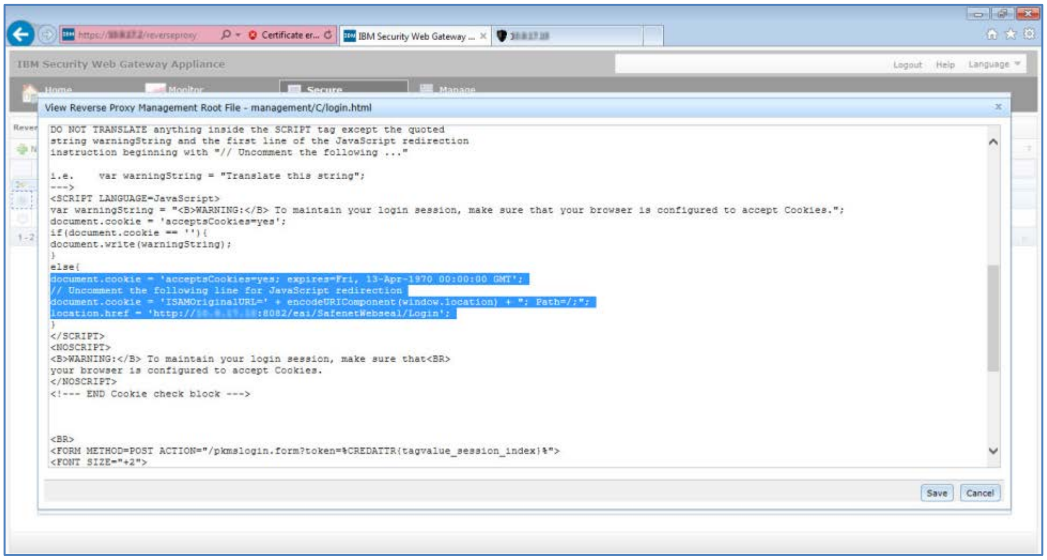
III. In the **Management Root list** (under the language specific folder), click **login.html**.
Note that the supported languages are only English, French, and Arabic.



IV. Click **File > Open.**

V. In the first **<script>** tag, add the following script to redirect to the reverse proxy that holds the SAS Agent for ISAM:

document.cookie = 'ISAMOriginalURL=' + encodeURIComponent(window.location) + "; Path=/;"; location.href = /eai/SafenetWebseal/Login'


https://[redacted]/reverseproxy
Certificate er...
IBM Security Web Gateway ...
IBM Security Web Gateway Appliance
Logout
Help
Language
Home
Monitor
Secure
Manage
View Reverse Proxy Management Root File - management/C/login.html
Save
Cancel

```
DO NOT TRANSLATE anything inside the SCRIPT tag except the quoted
string warningString and the first line of the JavaScript redirection
instruction beginning with "// Uncomment the following ..."

i.e.    var warningString = "Translate this string";
--->
<SCRIPT LANGUAGE=JavaScript>
var warningString = "<B>WARNING:</B> To maintain your login session, make sure that your browser is configured to accept Cookies.";
document.cookie = 'acceptsCookies=yes';
if(document.cookie == ''){
document.write(warningString);
}
else{
document.cookie = 'acceptsCookies=yes; expires=Fri, 13-Apr-1970 00:00:00 GMT';
// Uncomment the following line for JavaScript redirection
document.cookie = 'ISAMOriginalURL=' + encodeURIComponent(window.location) + "; Path=/;";
location.href = 'http://[redacted]:8082/eai/SafenetWebseal/Login';
}
</SCRIPT>
<NOSCRIPT>
<B>WARNING:</B> To maintain your login session, make sure that<BR>
your browser is configured to accept Cookies.
</NOSCRIPT>
<!--- END Cookie check block --->



<BR>
<FORM METHOD=POST ACTION="/pkmslogin.form?token=%CREDATTR{tagvalue_session_index}%">
<FONT SIZE="+2">
```

VI. Click **Save**.

VII. Deploy and restart the reverse proxy.

Configuring ISAM for Web 8.0 or 9.0

The users can authenticate protected web application(s) using the SAS EAI Agent by configuring ISAM for Web 8.0 / 9.0. To configure the ISAM for Web 8.0 / 9.0, complete the following:

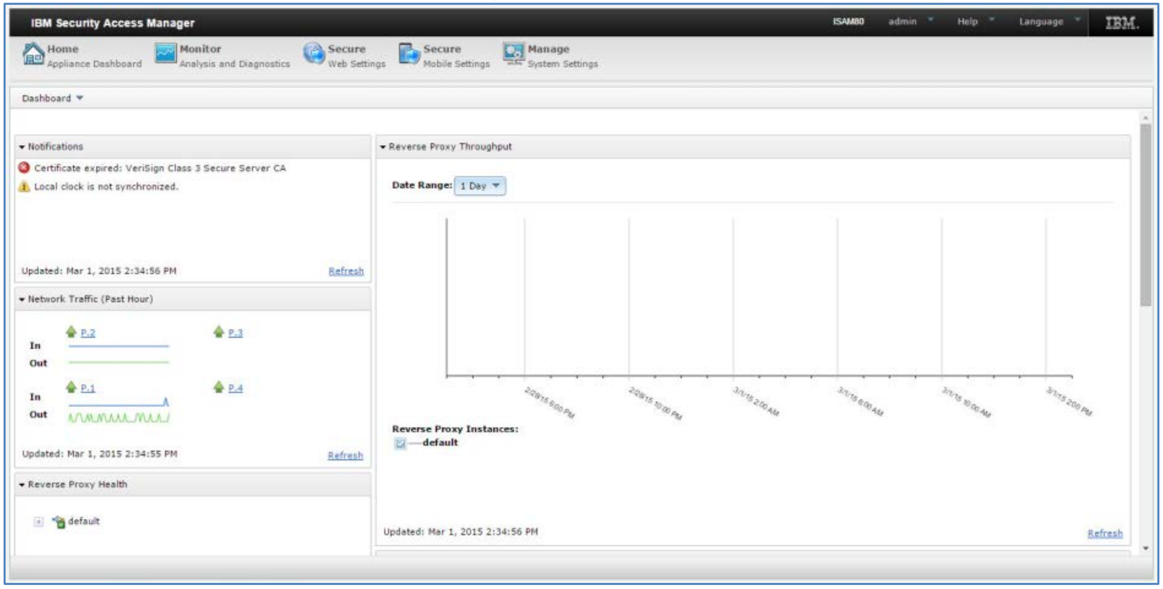
- **Creating EAI Junction**
- **Configuring Reverse Proxy**
- **Configuring Authentication Policy**
- **Configuring Secure Policy**
- **Assigning Policy to Protected Resource**
- **Configuring to Enable HTTP Redirect (for ISAM 9 only)**

Creating EAI Junction

The ISAM for Web 8 / 9 is configured with default options.

In the following example, a reverse proxy with junctions is used. One junction is the protected web application, and the other is the SafeNet WebSEAL external authentication agent.
Ensure that the reverse proxy is already configured for the protected web application.

1. Login to the **IBM Security Access Manager** console.



Certificate expired: VeriSign Class 3 Secure Server CA

Local clock is not synchronized.

Updated: Mar 1, 2015 2:34:56 PM

Updated: Mar 1, 2015 2:34:55 PM

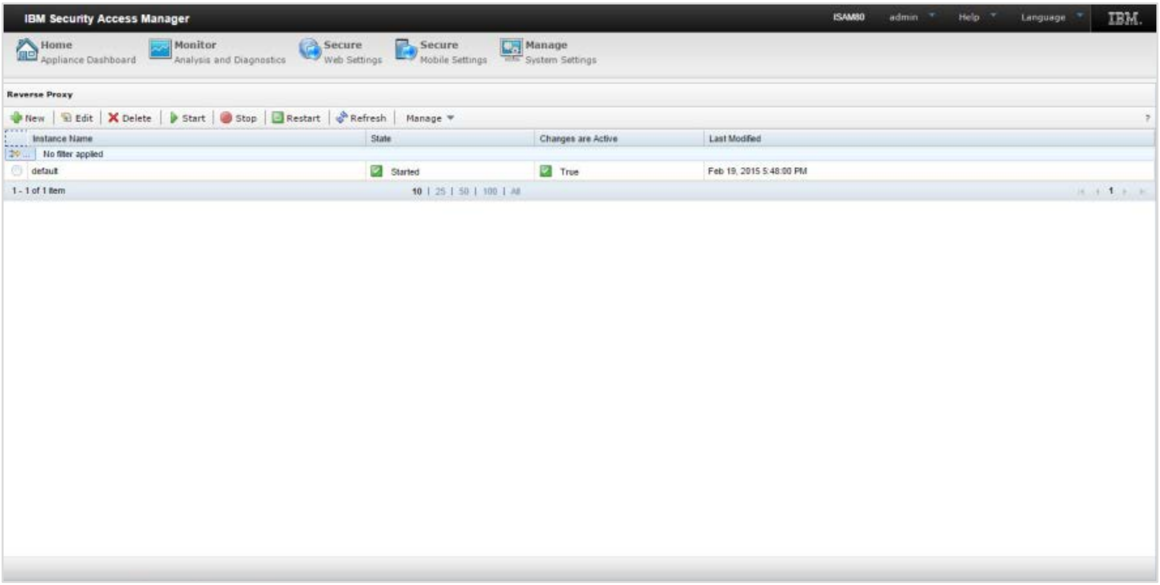
Date Range: 1 Day

Reverse Proxy Instances: ☑ default

Updated: Mar 1, 2015 2:34:56 PM

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

2. Select **Secure Web Settings > Manage > Reverse Proxy**.



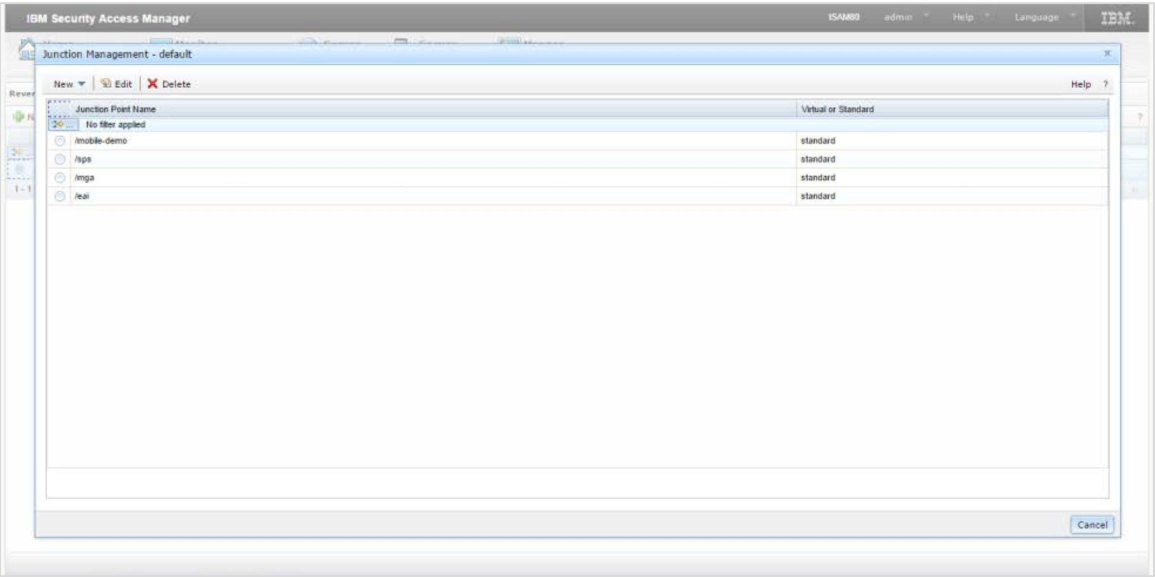
Reverse Proxy

Instance Name	State	Changes are Active	Last Modified
No filter applied			
○ default	☑ Started	☑ True	Feb 19, 2015 5:48:00 PM

1 - 1 of 1 item   10 | 25 | 50 | 100 | All   1

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

3. Select the reverse proxy, and click **Manage > Junction Management**.

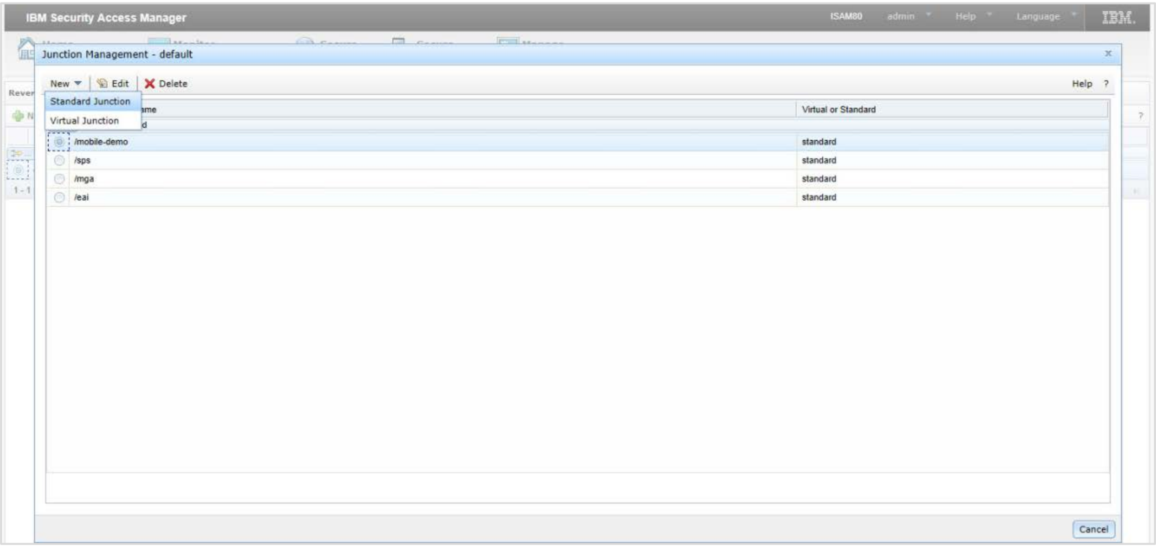


Junction Management - default

Junction Point Name	Virtual or Standard
No filter applied	
○ /mobile-demo	standard
○ /sps	standard
○ /mga	standard
○ /eai	standard

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

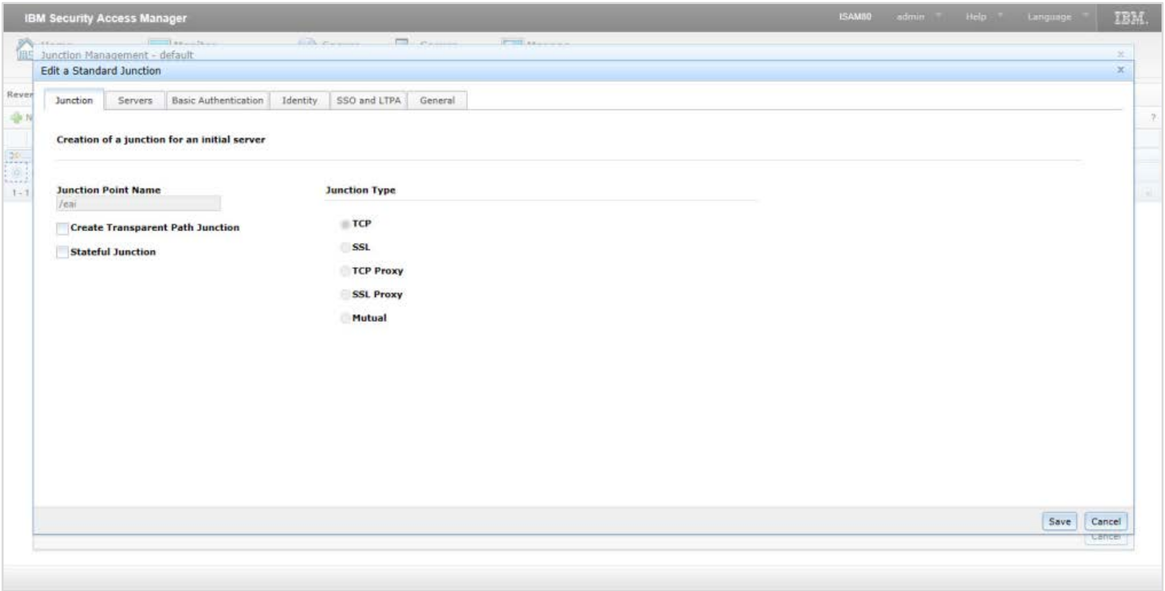
4. Click **New > Standard Junction**.



ame	Virtual or Standard
/mobile-demo	standard
/sps	standard
/mga	standard
/eai	standard

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

5. Under **Junction Point Name**, specify a name for the junction, and under **Junction Type**, select **TCP**.



Creation of a junction for an initial server

Junction Point Name: /eai

□ Create Transparent Path Junction

□ Stateful Junction

Junction Type

● TCP

○ SSL

○ TCP Proxy

○ SSL Proxy

○ Mutual

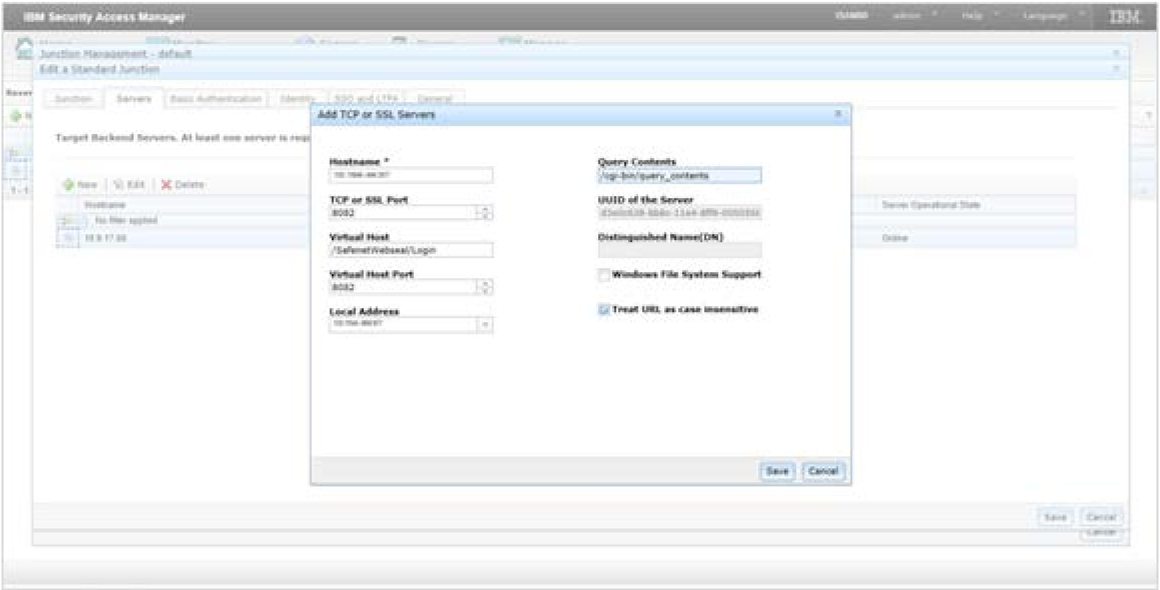
(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

6. Click **Servers** tab, and click **New**. The **Add TCP or SSL Servers** window is displayed.

7. Complete the following fields, and click **Save**.

Hostname	Enter the IP address of the EAI server.
TCP or SSL Port	Select the port that the ISAM will use to access the EAI server.
Virtual Host	Enter **/SafenetWebseal/Login**.
Virtual Host Port	Select the port that the ISAM will use to access the EAI server.
Local Address	Select the reverse proxy IP address.

Query Contents	Enter **/cgi-bin/query_contents**.
Treat URL as case insensitive	Select this check box.



Add TCP or SSL Servers

Hostname *

TCP or SSL Port: 8082

Virtual Host: /SafenetWebseal/Logon

Virtual Host Port: 8082

Local Address

Query Contents: /cgi-bin/query_contents

UUID of the Server

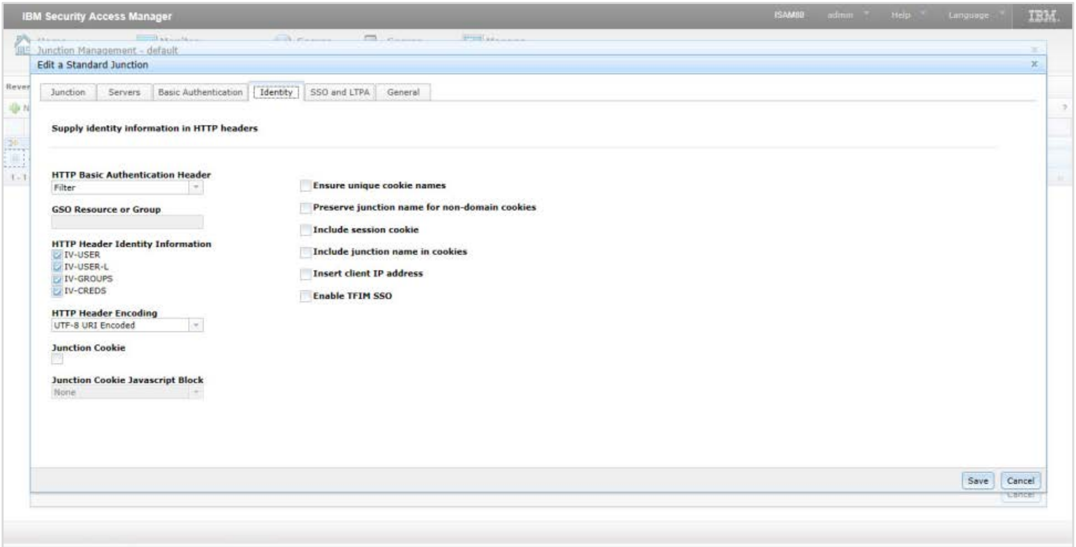
Distinguished Name(DN)

☐ Windows File System Support

☑ Treat URL as case insensitive

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

8. Click **Identity** tab, and verify if all of the check boxes under **HTTP Header Identity Information** are selected.



Supply identity information in HTTP headers

HTTP Basic Authentication Header: Filter

GSO Resource or Group

HTTP Header Identity Information
☑ IV-USER
☑ IV-USER-L
☑ IV-GROUPS
☑ IV-CREDS

HTTP Header Encoding: UTF-8 URI Encoded

Junction Cookie ☐

Junction Cookie Javascript Block: None

☐ Ensure unique cookie names
☐ Preserve junction name for non-domain cookies
☐ Include session cookie
☐ Include junction name in cookies
☐ Insert client IP address
☐ Enable TFIM SSO

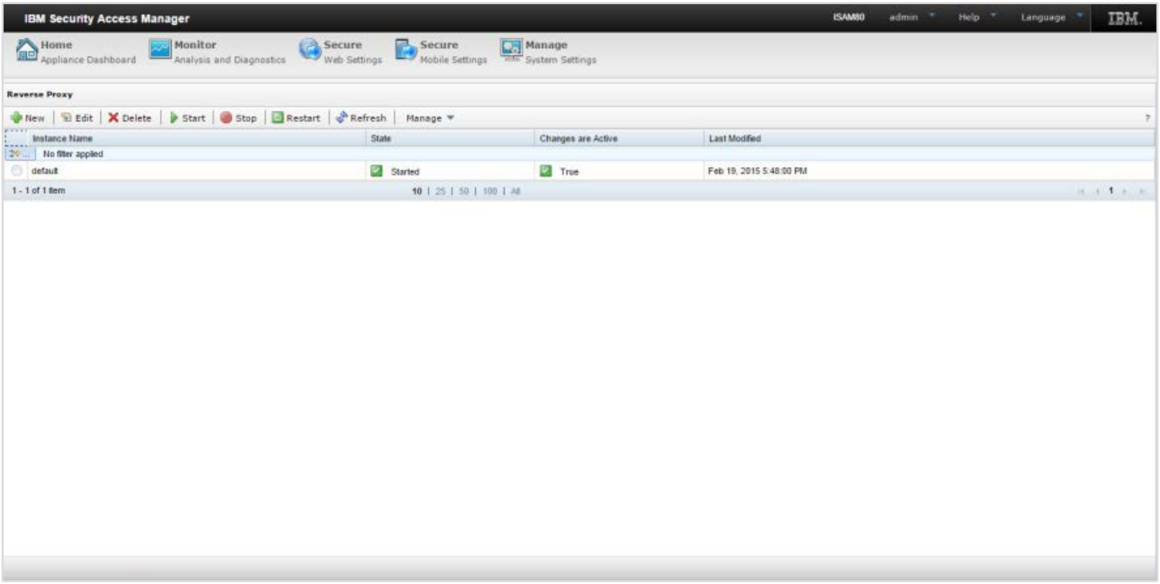
(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

9. Click **Save**.

Configuring Reverse Proxy

Configure the triggering URL and the external authentication for the reverse proxy, by following the steps:

1. In the **IBM Security Access Manager** console, select **Secure Web Settings > Manage > Reverse Proxy**.

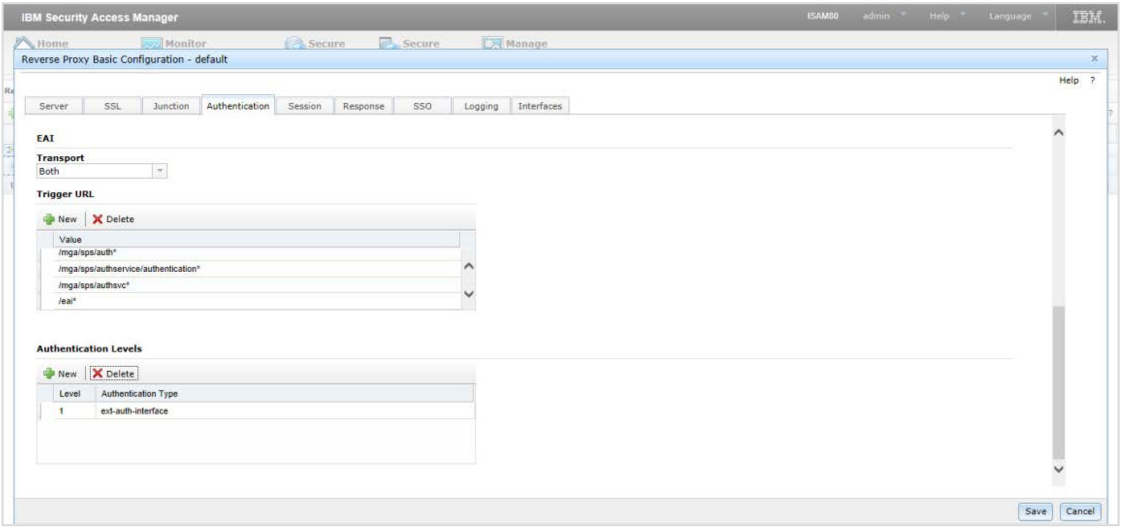


Instance Name	State	Changes are Active	Last Modified
default	☑ Started	☑ True	Feb 19, 2015 5:48:00 PM

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

2. Select the reverse proxy, and click **Edit**.
3. Click **Authentication** tab.
4. Complete the following, and click **Save**:

Trigger URL	Click **New**, and add the EAI junction URL that you created in the previous procedure (for example, **/eai***). The ISAM supports regular expressions.
Authentication Levels	Click **New**, and add **ext-auth-interface**.



EAI

Transport: Both

Trigger URL

Value
/mga/sps/auth*
/mga/sps/authservice/authentication*
/mga/sps/authsvc*
/eai*

Authentication Levels

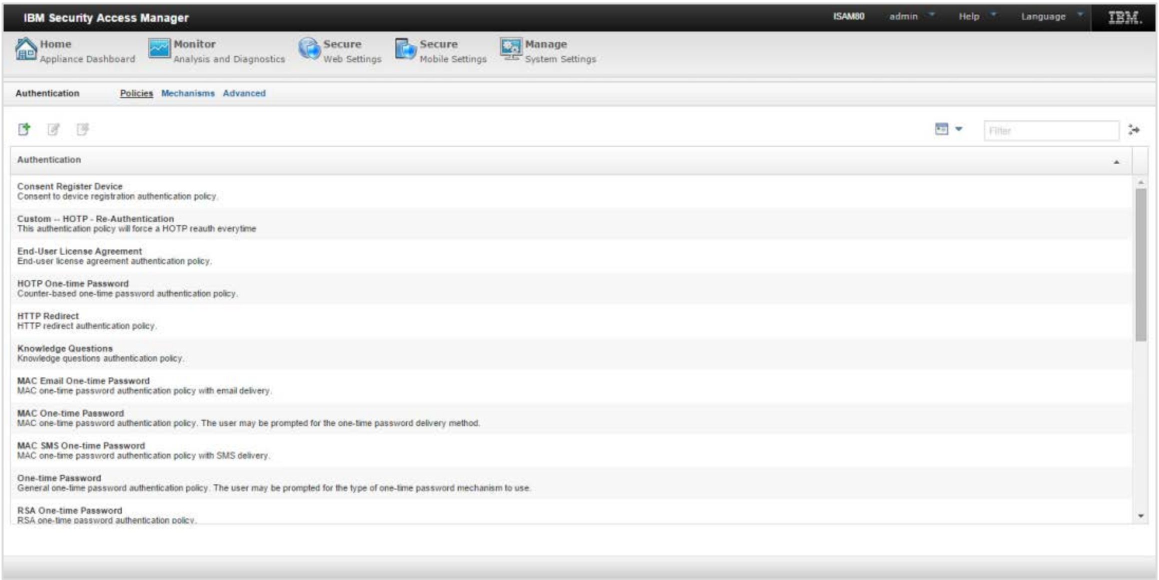
Level	Authentication Type
1	ext-auth-interface

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

Configuring Authentication Policy

Configure the HTTP redirect mechanism by following the steps:

1. In the **IBM Security Access Manager** console, select **Secure Mobile Settings > Policy > Authentication**.



Authentication

Consent Register Device
Consent to device registration authentication policy.

Custom -- HOTP - Re-Authentication
This authentication policy will force a HOTP reauth everytime

End-User License Agreement
End-user license agreement authentication policy.

HOTP One-time Password
Counter-based one-time password authentication policy.

HTTP Redirect
HTTP redirect authentication policy.

Knowledge Questions
Knowledge questions authentication policy.

MAC Email One-time Password
MAC one-time password authentication policy with email delivery.

MAC One-time Password
MAC one-time password authentication policy. The user may be prompted for the one-time password delivery method.

MAC SMS One-time Password
MAC one-time password authentication policy with SMS delivery.

One-time Password
General one-time password authentication policy. The user may be prompted for the type of one-time password mechanism to use.

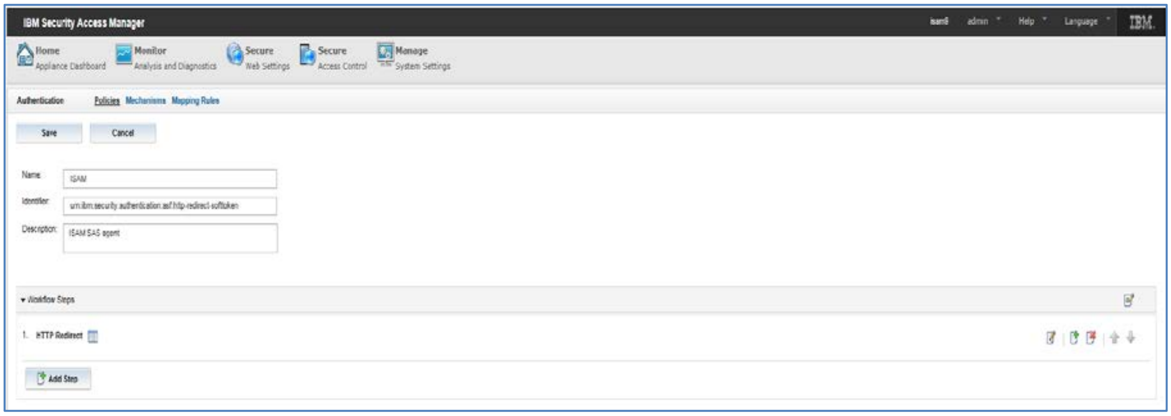
RSA One-time Password
RSA one-time password authentication policy.

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

2. Click to create a new authentication policy.

3. Complete the following fields, and click **Save**.

Name	Enter the policy name.
Identifier	Enter the urn identifier: **urn:ibm:security:authentication:asf:http-redirect-softtoken**
Workflow Steps	Click **Add Step**, and select **HTTP Redirect**.



Name: ISAM

Identifier: urn:ibm:security:authentication:asf:http-redirect-softtoken

Description: ISAM SAS agent

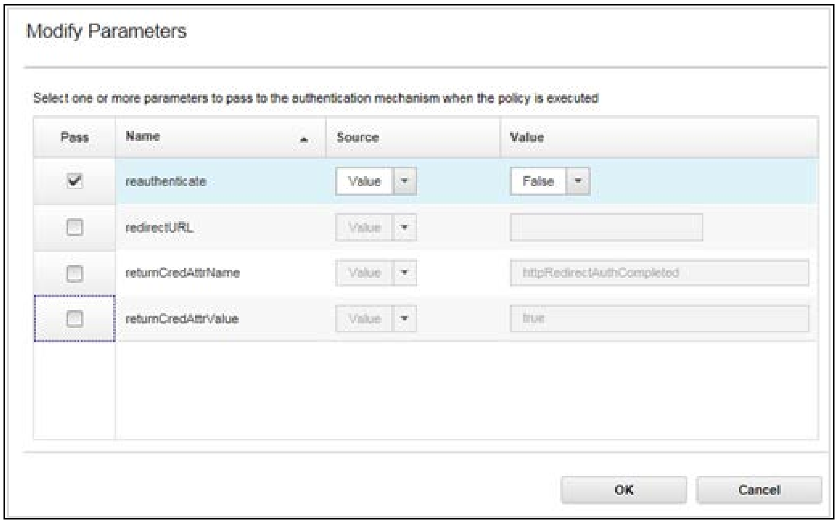
Workflow Steps

1. HTTP Redirect

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

4. Click the icon next to **HTTP Redirect**.

5. In **Pass** column, select the check box for the row containing **reauthenticate**.
For this row, in the **Source** column select **Value**, and in the **Value** column, select **False**.
Click **OK**.



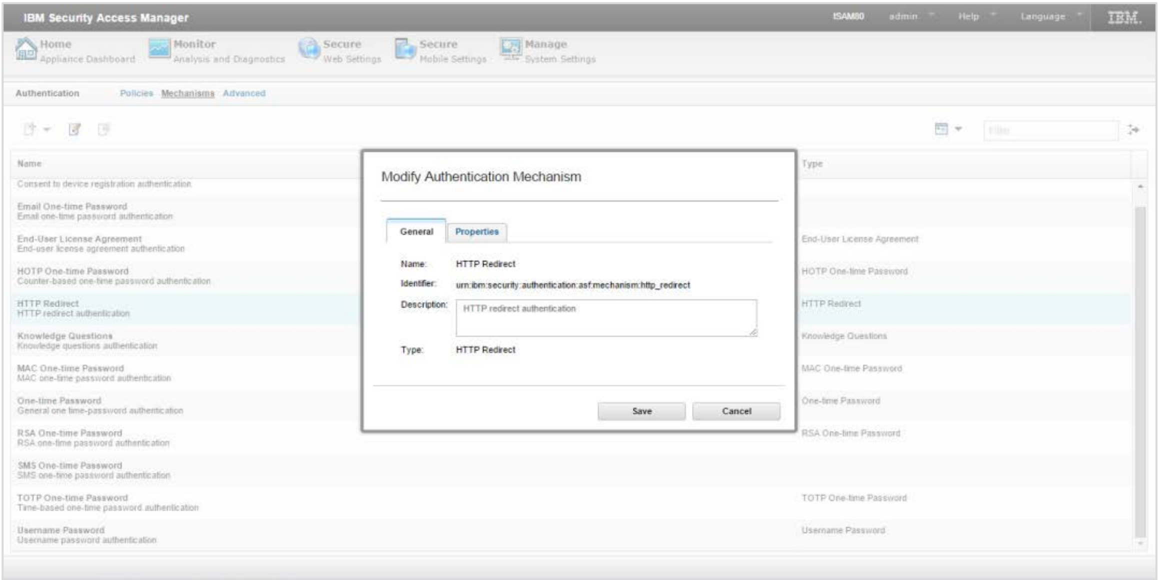
Modify Parameters

Select one or more parameters to pass to the authentication mechanism when the policy is executed

Pass	Name	Source	Value
☑	reauthenticate	Value	False
□	redirectURL	Value	
□	returnCredAttrName	Value	httpRedirectAuthCompleted
□	returnCredAttrValue	Value	true

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

6. Click **Mechanisms**, and select **HTTP Redirect**.
7. Click **Modify Authentication Mechanism**.



Name	Type
Consent to device registration authentication	
Email One-time Password Email one-time password authentication	
End-User License Agreement End-user license agreement authentication	End-User License Agreement
HOTP One-time Password Counter-based one-time password authentication	HOTP One-time Password
HTTP Redirect HTTP redirect authentication	HTTP Redirect
Knowledge Questions Knowledge questions authentication	Knowledge Questions
MAC One-time Password MAC one-time password authentication	MAC One-time Password
One-time Password General one time-password authentication	One-time Password
RSA One-time Password RSA one-time password authentication	RSA One-time Password
SMS One-time Password SMS one-time password authentication	
TOTP One-time Password Time-based one-time password authentication	TOTP One-time Password
Username Password Username password authentication	Username Password

Modify Authentication Mechanism

General | Properties

Name: HTTP Redirect

Identifier: urn:ibm:security:authentication:asf:mechanism:http_redirect

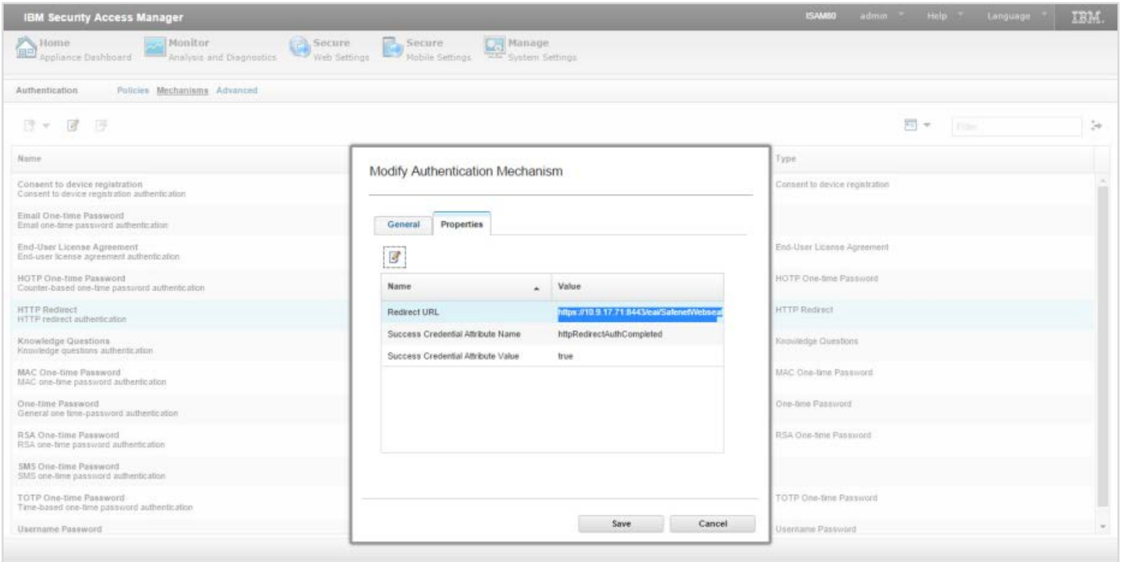
Description: HTTP redirect authentication

Type: HTTP Redirect

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

8. Click **Properties** tab.
9. Complete the following details, and click **Save**.

Redirect URL	Enter the URL in the following format: **https://<Application Interface IP>:port/eai/SafenetWebseal/Login**. Example: **https://10.0.0.1:8443/eai/SafenetWebseal/Login**
Success Credential Attribute Name	Enter **httpRedirectAuthCompleted**.
Success Credential Attribute Value	Set this value to **true**.



Name	Type
Consent to device registration Consent to device registration authentication	Consent to device registration
Email One-time Password Email one-time password authentication	
End-User License Agreement End-user license agreement authentication	End-User License Agreement
HOTP One-time Password Counter-based one-time password authentication	HOTP One-time Password
HTTP Redirect HTTP redirect authentication	HTTP Redirect
Knowledge Questions Knowledge questions authentication	Knowledge Questions
MAC One-time Password MAC one-time password authentication	MAC One-time Password
One-time Password General one time-password authentication	One-time Password
RSA One-time Password RSA one-time password authentication	RSA One-time Password
SMS One-time Password SMS one-time password authentication	
TOTP One-time Password Time-based one-time password authentication	TOTP One-time Password
Username Password	Username Password

Modify Authentication Mechanism

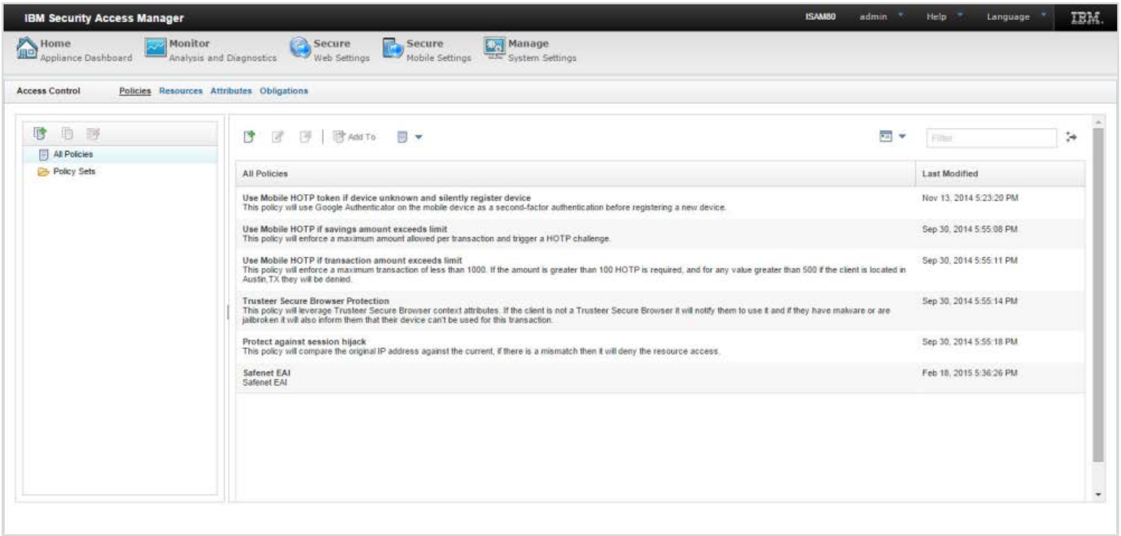
Name	Value
Redirect URL	https://10.9.17.71:8443/eai/SafenetWebseal
Success Credential Attribute Name	httpRedirectAuthCompleted
Success Credential Attribute Value	true

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

Configuring Secure Policy

To use the redirect mechanism, create an access control policy and assign it to the relevant resource. The access control policy will create a grade based on a predefined context vector, and will be used to define the access policy.

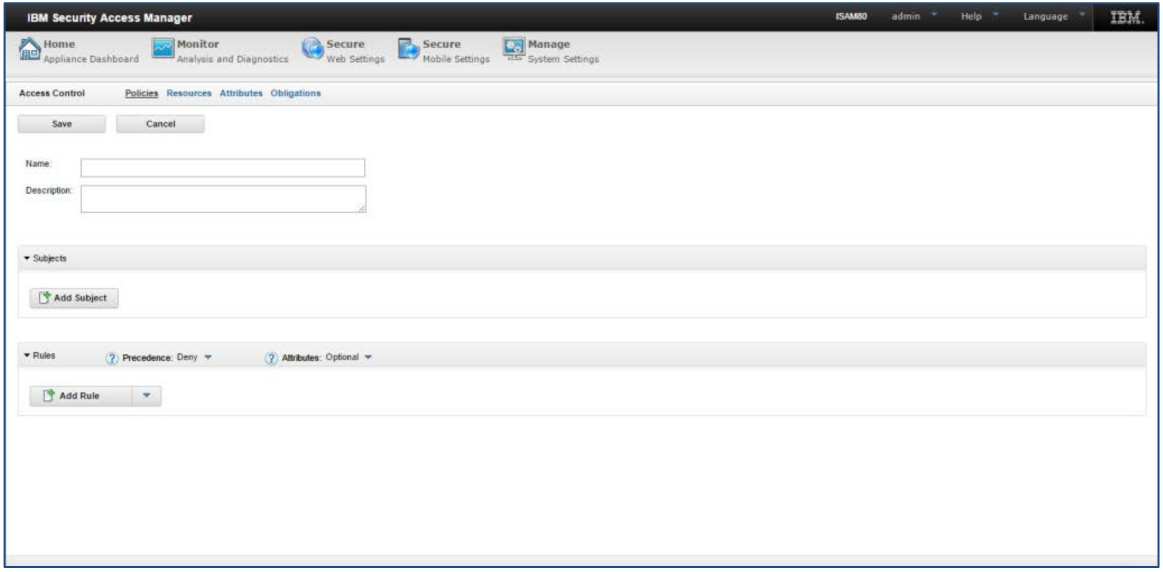
1. In the **IBM Security Access Manager** console, select **Secure Mobile Settings > Policy > Access Control**.



All Policies	Last Modified
Use Mobile HOTP token if device unknown and silently register device This policy will use Google Authenticator on the mobile device as a second-factor authentication before registering a new device.	Nov 13, 2014 5:23:20 PM
Use Mobile HOTP if savings amount exceeds limit This policy will enforce a maximum amount allowed per transaction and trigger a HOTP challenge.	Sep 30, 2014 5:55:08 PM
Use Mobile HOTP if transaction amount exceeds limit This policy will enforce a maximum transaction of less than 1000. If the amount is greater than 100 HOTP is required, and for any value greater than 500 if the client is located in Austin,TX they will be denied.	Sep 30, 2014 5:55:11 PM
Trusteer Secure Browser Protection This policy will leverage Trusteer Secure Browser context attributes. If the client is not a Trusteer Secure Browser it will notify them to use it and if they have malware or are jailbroken it will also inform them that their device can't be used for this transaction.	Sep 30, 2014 5:55:14 PM
Protect against session hijack This policy will compare the original IP address against the current, if there is a mismatch then it will deny the resource access.	Sep 30, 2014 5:55:18 PM
Safenet EAI Safenet EAI	Feb 18, 2015 5:36:26 PM

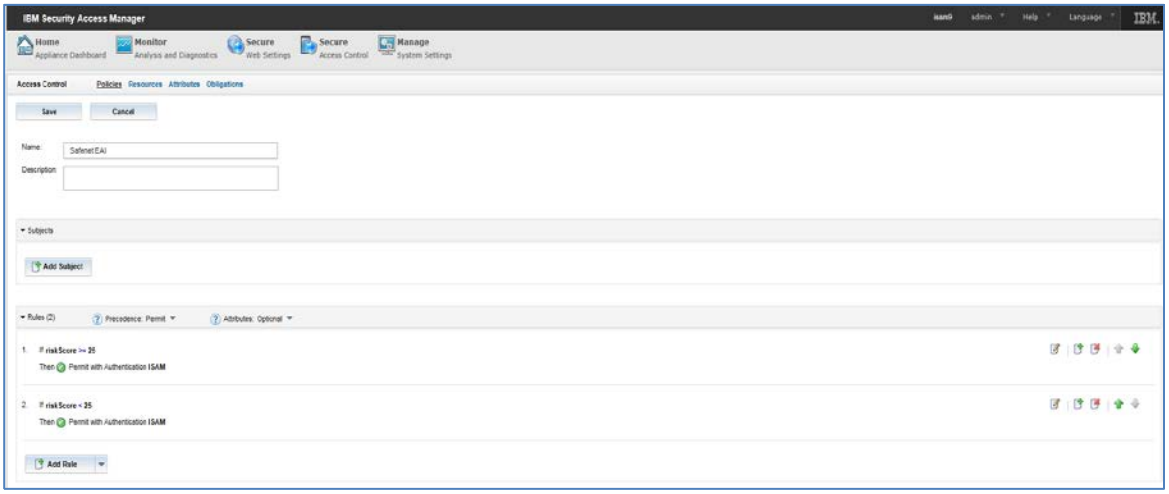
(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

2. Click the create policy icon . The create policy window is displayed.



(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

3. Configure the access control policy. Use the required URN for the HTTP redirect authentication mechanism.



Name: SafenetEAI

Description:

Rules (2) Precedence: Permit Attributes: Optional

1. If riskScore >= 25
Then Permit with Authentication ISAM

2. If riskScore < 25
Then Permit with Authentication ISAM

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

For example, we have configured the following settings in our test lab.

a. If **riskScore** >=25,
Permit with Authentication ISAM

b. If **riskScore** < 25,
Permit with Authentication ISAM

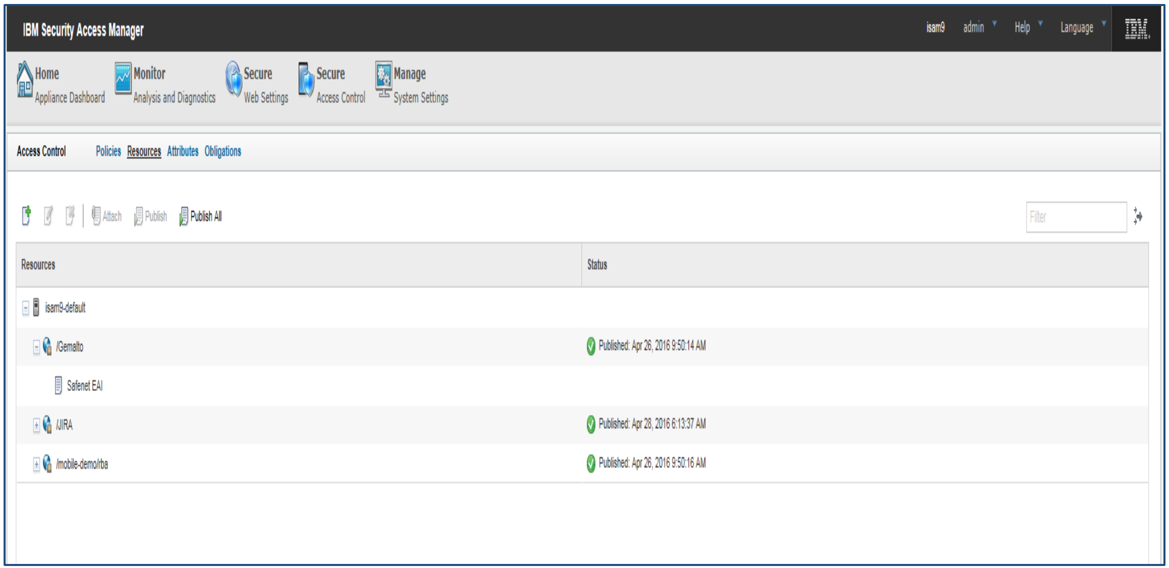
Note: It is only a test setting, and the actual settings may differ based on requirements of your organization's access policy.

4. Click **Save**.

Assigning Policy to Protected Resource

Now you can assign the access control policy that you created in “Configuring Secure Policy” to the protected resource.

1. In the **IBM Security Access Manager** console, select **Secure Mobile Settings > Access Control > Resources**.



Resources	Status
isam9-default	
/Gemalto	Published: Apr 26, 2016 9:50:14 AM
Safenet EAI	
/JIRA	Published: Apr 28, 2016 6:13:37 AM
/mobile-demo/rba	Published: Apr 26, 2016 9:50:16 AM

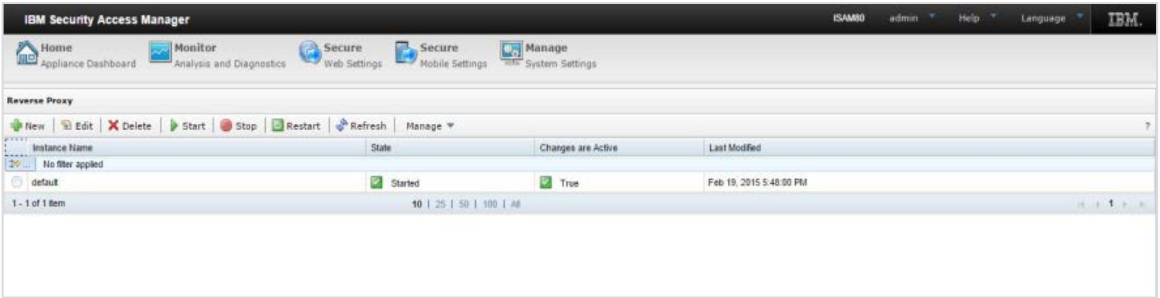
(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

2. Select the protected resource, and click **Attach**.
3. Click **Publish All**.

Configuring to Enable HTTP Redirect (for ISAM 9 only)

To enable HTTP redirect in ISAM 9.0, complete the following steps:

1. In the **IBM Security Access Manager** console, select **Secure Web Settings > Manage > Reverse Proxy**.

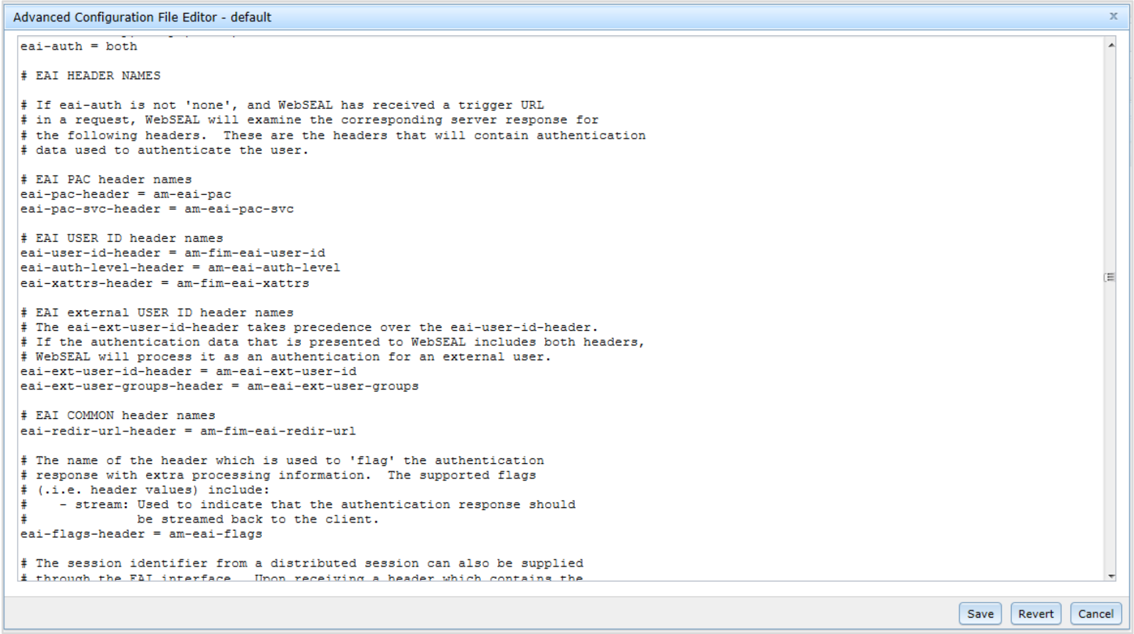


Instance Name	State	Changes are Active	Last Modified
default	✓ Started	✓ True	Feb 19, 2015 5:48:00 PM

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

2. Select the reverse proxy, and click **Manage > Configuration > Edit Configuration File**.
3. In **Advanced Configuration File Editor**, complete the following:
   a. Replace am-eai-user-id with am-fim-eai-user-id.
   b. Replace **am-eai-xattrs** with **am-fim-eai-xattrs**.
   c. Replace **am-eai-redir-url** with **am-fim-eai-redir-url**.

Click **Save**.



```
eai-auth = both

# EAI HEADER NAMES

# If eai-auth is not 'none', and WebSEAL has received a trigger URL
# in a request, WebSEAL will examine the corresponding server response for
# the following headers.  These are the headers that will contain authentication
# data used to authenticate the user.

# EAI PAC header names
eai-pac-header = am-eai-pac
eai-pac-svc-header = am-eai-pac-svc

# EAI USER ID header names
eai-user-id-header = am-fim-eai-user-id
eai-auth-level-header = am-eai-auth-level
eai-xattrs-header = am-fim-eai-xattrs

# EAI external USER ID header names
# The eai-ext-user-id-header takes precedence over the eai-user-id-header.
# If the authentication data that is presented to WebSEAL includes both headers,
# WebSEAL will process it as an authentication for an external user.
eai-ext-user-id-header = am-eai-ext-user-id
eai-ext-user-groups-header = am-eai-ext-user-groups

# EAI COMMON header names
eai-redir-url-header = am-fim-eai-redir-url

# The name of the header which is used to 'flag' the authentication
# response with extra processing information.  The supported flags
# (.i.e. header values) include:
#    - stream: Used to indicate that the authentication response should
#              be streamed back to the client.
eai-flags-header = am-eai-flags

# The session identifier from a distributed session can also be supplied
# through the EAI interface.  Upon receiving a header which contains the
```

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

4. Restart the reverse proxy.

4 SAS Configuration

This chapter explains how to use the SAS console to configure an Auth Node for the Agent.

Configuring SAS

After the SAS Agent for ISAM has been configured as a junction server, the agent's IP address must be added as an Auth Node to your organization.

To configure the SAS Agent Auth Node, follow the steps:

1. Login to the SAS Console.
2. Click **Virtual Server > Comms**.
3. Under **Auth Nodes**, select **Auth Node** and click **Add.**
4. Enter the following information:
   - Agent Description: Description of the Agent.
   - Low IP Address In Range: The IP Address of the SAS Agent for ISAM

   Ensure that the **FreeRADIUS Synchronization** is not selected since this is a web service agent.
5. Click **Save**.

5
Running the Solution

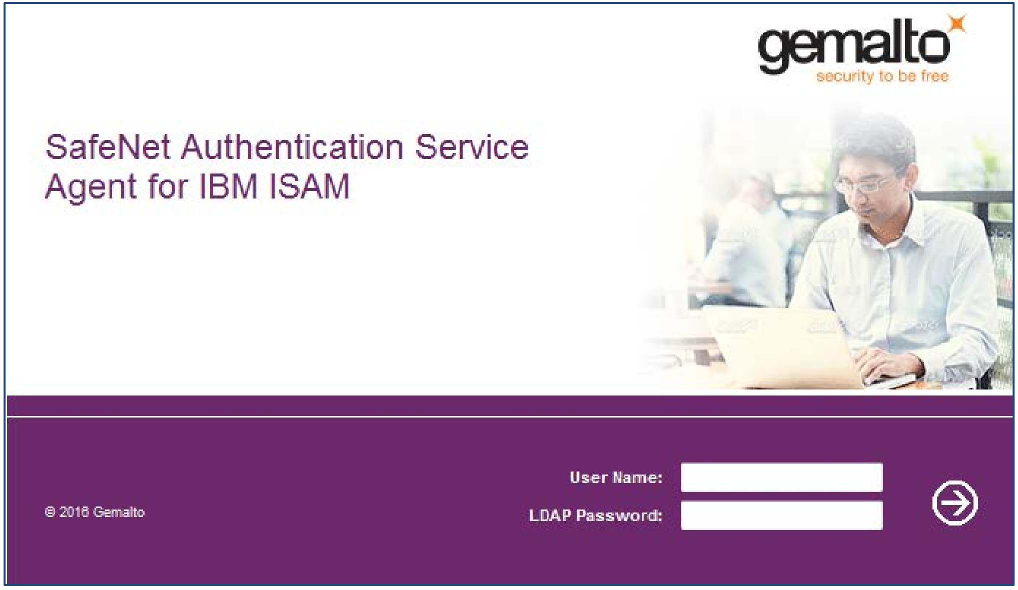
Accessing Protected Resource on ISAM 7.0

To login to the protected resource, follow the steps:

1. In a web browser, open the URL of the reverse proxy of the WebSEAL protected resource.

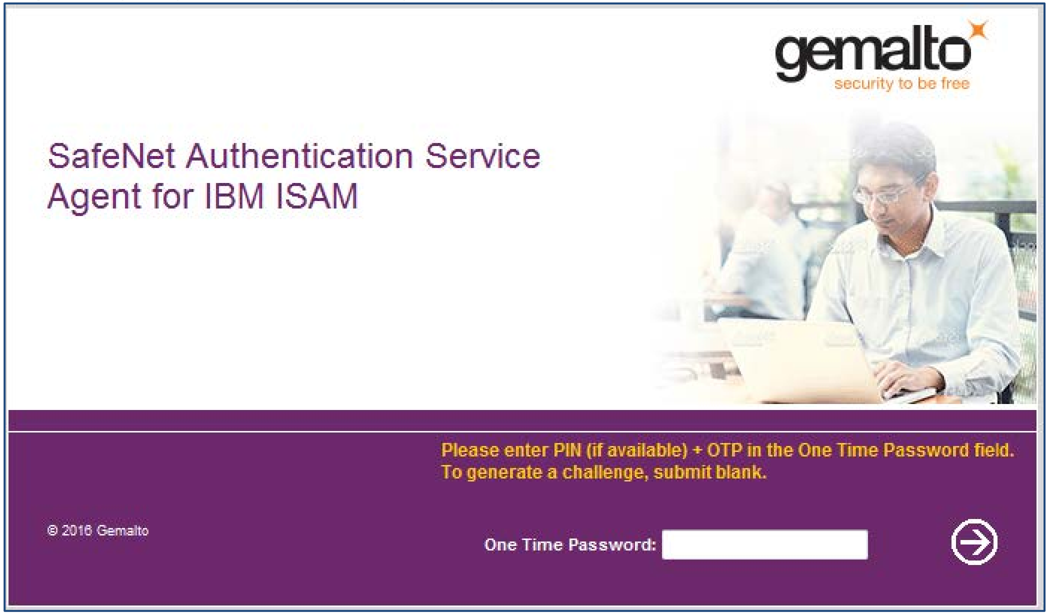
   Example: **https://<IP address of application interface> :< port number on which reverse proxy is configured>/<protected resource>**

2. You will be redirected to the Gemalto Authentication application for login.
   Enter your username and LDAP password, and click the forward arrow button.



NOTE: For this solution, Split Mode is set ON and the LDAP Authentication is enabled.

3. You are prompted to enter a One-Time Password (OTP).
   Depending on your configuration, you may need to enter a PIN together with the OTP.



Please enter PIN (if available) + OTP in the One Time Password field.
To generate a challenge, submit blank.

NOTE: Depending on your token type, you may need to generate an OTP.

4. Enter the OTP, and click the forward arrow button.
   You will be redirected to the WebSEAL protected resource.

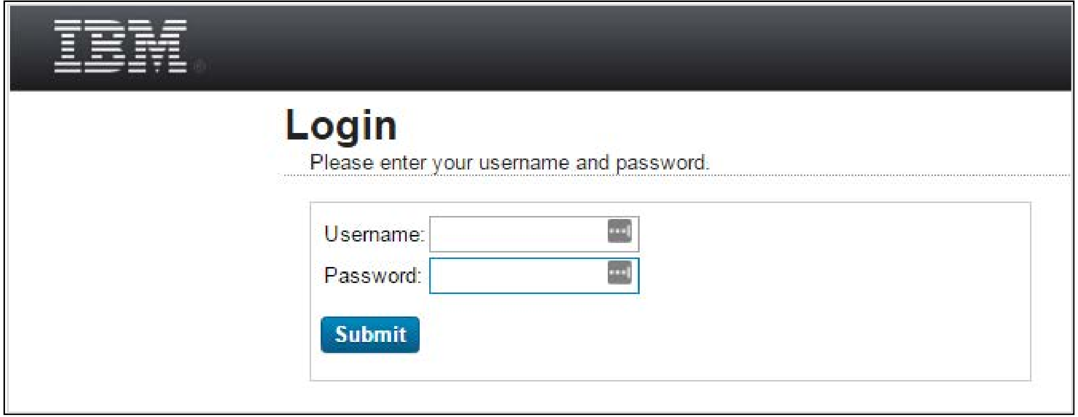
Accessing Protected Resource on ISAM 8.0 or 9.0

To login to the protected resource, follow the steps:

1. In a web browser, open the URL of the reverse proxy of the WebSEAL protected resource.

   Example: **https://<IP address of application interface> :< port number on which reverse proxy is configured>/<protected resource>**

2. You will be redirected to the ISAM application for login.
   Enter your username and password in ISAM, and click **Submit**.



Login

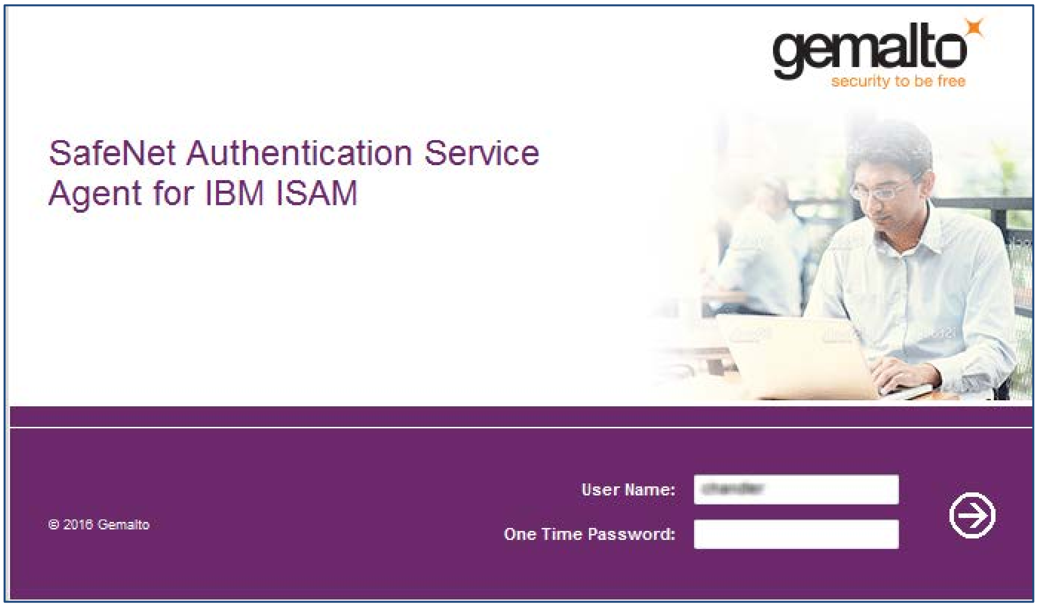
Please enter your username and password.

Username:

Password:

(The screen image above is from IBM® software. Trademarks are the property of their respective owners.)

3. You will be redirected to the Gemalto Authentication application for login.
   The **User Name** field is pre-filled with the username provided in the previous step.
   Enter the **One Time Password**, and click the forward arrow button.



SafeNet Authentication Service
Agent for IBM ISAM

© 2016 Gemalto

User Name: [redacted]

One Time Password:

NOTE: For this solution, Split Mode is set ON and the LDAP Authentication is disabled.

4. You will be redirected to the WebSEAL protected resource.

6

Troubleshooting

Logs

In the Linux system, logs for the SAS Agent for ISAM are located at:

/usr/local/safenet/webseal/log/JCryptoWrapper-<date>.log

<tomcat installed path>/logs/catalina.<date>.log

In the Windows system, logs for the SAS Agent for ISAM are located at:

<System Root Dir>\SafeNet-Authentication-Service-Agent-For-IBM-ISAM-2-0\log\JCryptoWrapper-<date>.log

<tomcat installed path>\logs\catalina.<date>.log

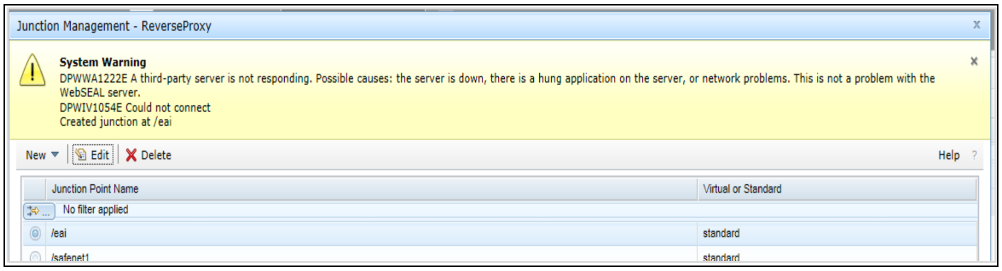
Chrome Browser Issue

When a user tries to access the protected resource on Chrome web browser for the very first time or after clearing the cache of the web browser, the protected resource is not available. Instead, a favicon icon is shown on the Chrome browser. This issue occurs because of the way ISAM 7.0 handles favicon.

Resolution: Close the Chrome browser and access the URL again. The favicon gets cached and the issue does not replicate. The protected resource now becomes available to the user.

Warning While Configuring Junctions

When the third party server is not reachable due to configuration issues, you may see the warning as shown below. Rectify and save the configuration.



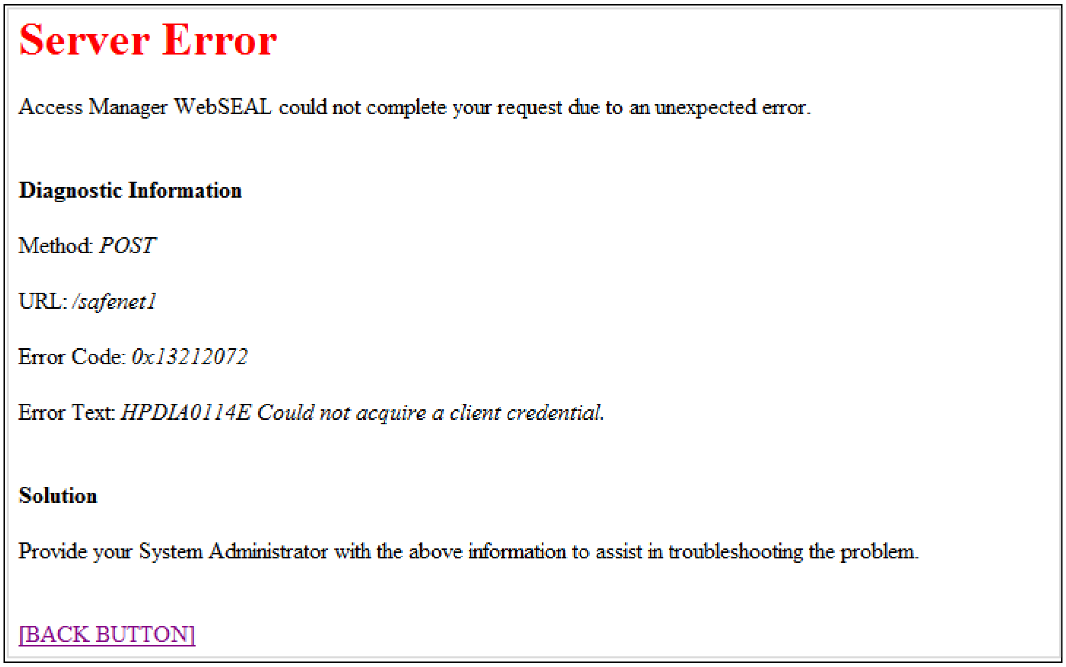
System Warning
DPWWA1222E A third-party server is not responding. Possible causes: the server is down, there is a hung application on the server, or network problems. This is not a problem with the WebSEAL server.
DPWIV1054E Could not connect
Created junction at /eai

Junction Point Name	Virtual or Standard
No filter applied	
/eai	standard
/safenet1	standard

Errors While Accessing Protected Resource

Scenario 1

When a user does not exist in ISAM but is present in SAS and LDAP (used by the Agent), the authentication is successful but the user does not reach the protected resource. In this case, the error shown below appears:



Server Error

Access Manager WebSEAL could not complete your request due to an unexpected error.

Diagnostic Information

Method: *POST*

URL: */safenet1*

Error Code: *0x13212072*

Error Text: *HPDIA0114E Could not acquire a client credential.*

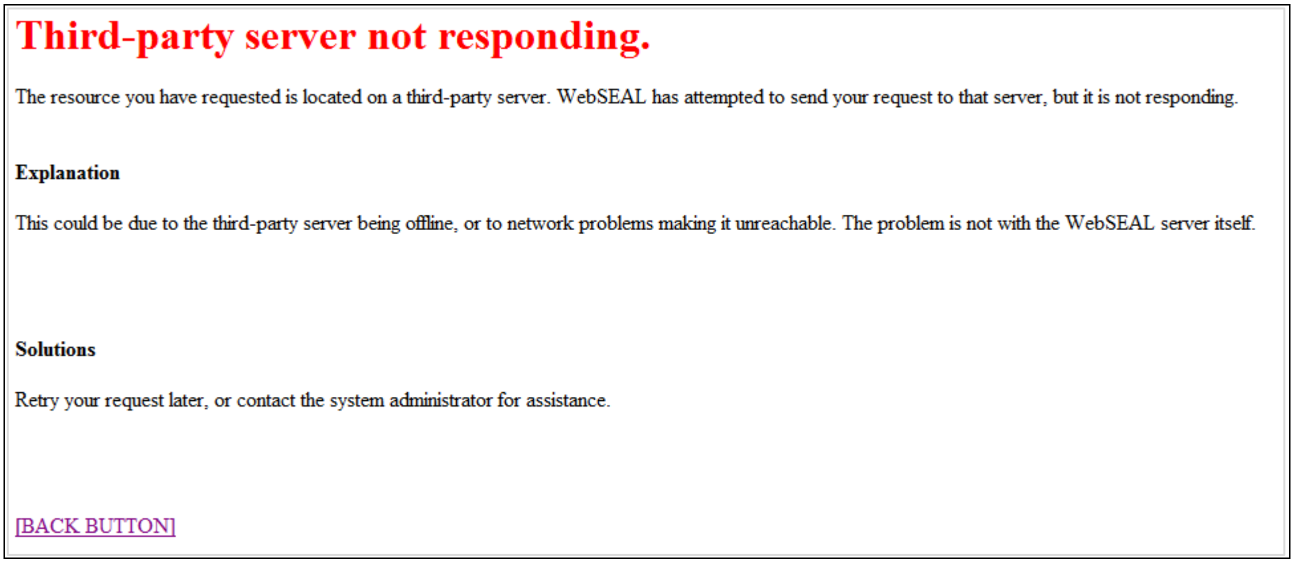
Solution

Provide your System Administrator with the above information to assist in troubleshooting the problem.

[BACK BUTTON]

Scenario 2

When the /eai junction server is responding but the protected resource is not responding, and the user tries to access the protected resource, the error shown below appears:



Third-party server not responding.

The resource you have requested is located on a third-party server. WebSEAL has attempted to send your request to that server, but it is not responding.

Explanation

This could be due to the third-party server being offline, or to network problems making it unreachable. The problem is not with the WebSEAL server itself.

Solutions

Retry your request later, or contact the system administrator for assistance.

[BACK BUTTON]

Resolution:

1. Open the **IBM Security Web gateway Appliance** console.
2. Go to **Secure > Manage > Reverse Proxy**.
3. Select the reverse proxy instance where one of the junctions had the Agent hosted.
   Open **Open Junction Management** under **Manage**.
4. Select the **/<protected resource>** junction and click **Edit**.
5. On **Servers** tab, select the backend server and click **Edit**.
6. Verify the port number to which the Transmission Control Protocol (TCP) is listening.