SafeNet Authentication Manager

Integration Guide

Using SAM as an Identity Provider for Blue Coat ProxySG

security to be free

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 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: 007-013300-001, Rev. A

Release Date: October 2015

Contents

Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as Blue Coat ProxySG.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

The Blue Coat ProxySG appliances provide complete control over all of your web traffic, delivering world-class threat protection. Robust features include user authentication, web filtering, data loss prevention, inspection, and visibility of SSL-encrypted traffic (including the ability to stream decrypted content to an external server with an Encrypted Tap license), content caching, bandwidth management, stream-splitting, and more.

The Blue Coat Secure Web Gateway Virtual Appliance (SWG VA) combines the market-leading security capabilities of Blue Coat ProxySG with the flexibility of virtualization to provide a cost-effective enterprise branch office solution. With the Blue Coat SWG VA, businesses can support web security and other critical remote office infrastructure on a common platform, reducing costs and IT resource requirements.

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Blue Coat ProxySG using SafeNet one-time password (OTP) tokens managed by SafeNet Authentication Manager.
- Configure SAML authentication in Blue Coat ProxySG using SafeNet Authentication Manager as an identity provider.

It is assumed that the Blue Coat ProxySG environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

Blue Coat ProxySG can be configured to support multi-factor authentication in several modes. The SAML authentication will be used for the purpose of working with SafeNet Authentication Manager.

Applicability

The information in this document applies to:

- **SafeNet Authentication Manager**—A server version of SAM that is used to deploy the solution on-premises in the organization.

Environment

The integration environment that was used in this document is based on the following software versions:

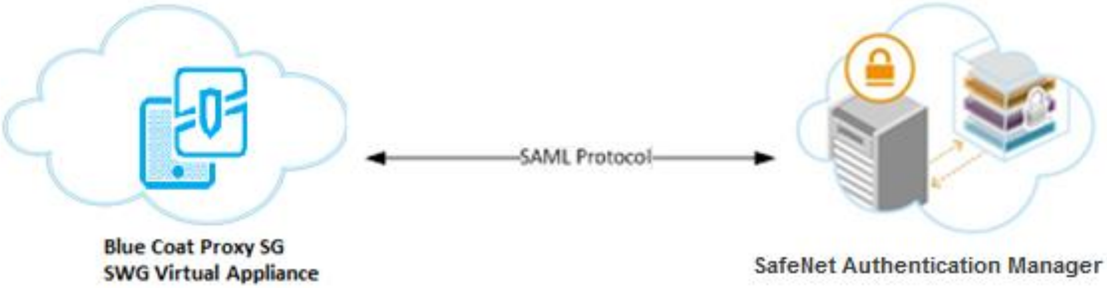
- **SafeNet Authentication Manager**—Version 8.2 (Hotfix 721)
- **Blue Coat ProxySG** (Virtual Appliance)—Model No. VA-100
- **Blue Coat ProxySG** (Software)—Version SGOS 6.5.6.4 SWG Edition

Audience

This document is targeted to system administrators who are familiar with Blue Coat ProxySG, and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Manager.

SAML Authentication using SAM

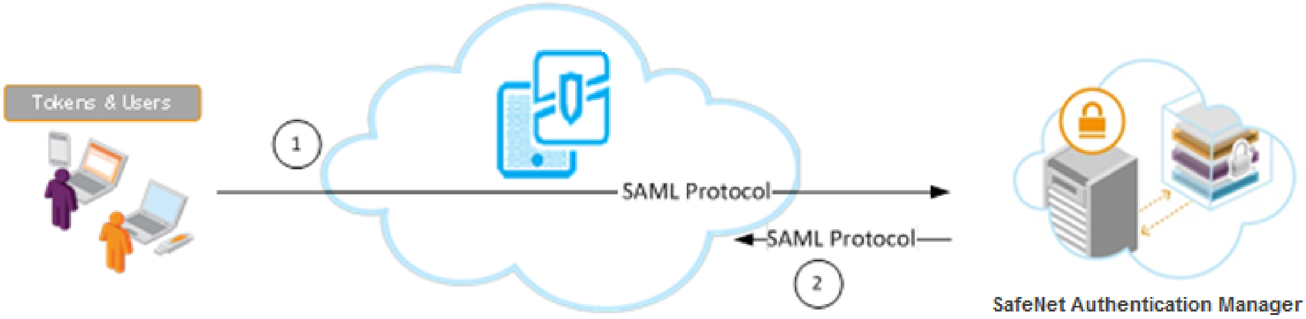
SAM provides a SAML authentication option that is already implemented in the SAM environment and can be used without any installation.



Authentication Flow using SAM

SafeNet Authentication Manager communicates with a large number of service providers and cloud-based services solutions using the SAML protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Blue Coat ProxySG.



1. A user attempts to log on to Blue Coat ProxySG. The user is redirected to SAM. SAM collects and evaluates the user's credentials.
2. SAM returns a response to Blue Coat ProxySG, accepting or rejecting the user`s authentication request.

SAML Prerequisites

To enable SafeNet Authentication Manager to receive SAML authentication requests from Blue Coat ProxySG, ensure the following:

- End users can authenticate from the Blue Coat ProxySG environment with a static password.
- The Blue Coat ProxySG virtual appliance should be configured as a reverse proxy with HTTPS services.

Configuring SafeNet Authentication Manager

Using SAM as an identity provider for Blue Coat ProxySG requires the following:

- Synchronizing User Stores to SAM, page 6
- Assigning a Token in SAM, page 6
- Configuring SAM as an Identity Provider, page 7
- Exporting the SAM Certificate, page 9
- Downloading the Blue Coat ProxySG Metadata, page 10
- Configuring SAM for SAML-based User Federation, page 10

Synchronizing User Stores to SAM

SAM manages and maintains tokens information in its data store, including the token status and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Microsoft Active Directory 2003, 2008, 2008 R2, 2012, and 2012 R2
- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

Assigning a Token in SAM

SAM supports a number of token methods that can be used as a second authentication factor for users authenticating through Blue Coat ProxySG.

The following tokens are supported:

- eToken PASS
- SafeNet GOLD
- SafeNet eToken 3400
- SafeNet eToken 3500
- eToken NG-OTP
- MobilePASS
- SafeNet eToken Virtual products

- MobilePASS Messaging
- SafeNet Mobile Authentication (iOS)

Tokens can be assigned to users as follows:

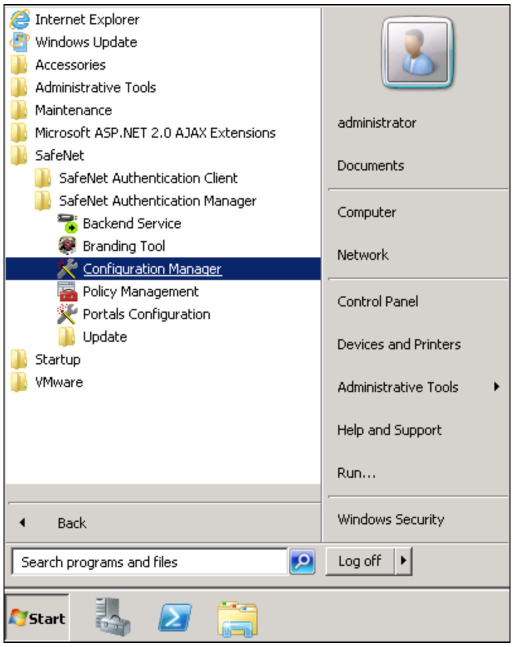
- **SAM Management Center**—Management site used by SAM administrators and helpdesk personnel for token enrollment and lifecycle management.
- **SAM Self-Service Center**—Self-service site used by end users for managing their tokens.
- **SAM Remote Service**—Self-service site used by employees not on the organization's premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet's tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator's Guide*.

Configuring SAM as an Identity Provider

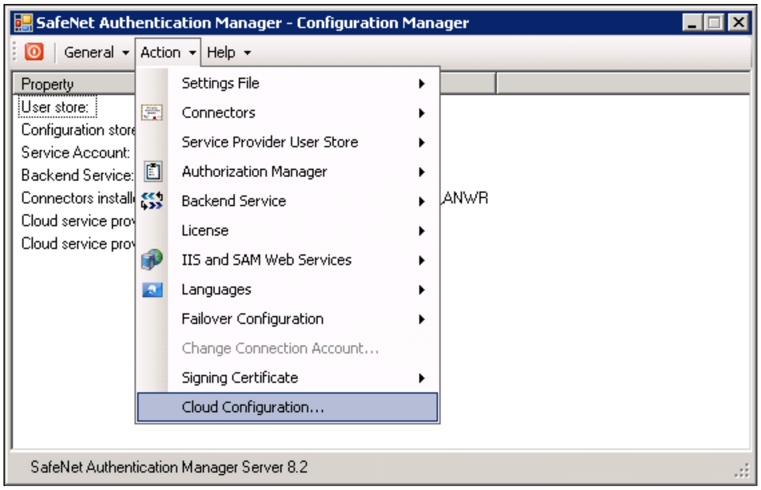
To use Blue Coat ProxySG as a service provider and SAM as an identity provider, SAM must be configured as an identity provider.

1. From the Windows **Start** menu, click **Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.



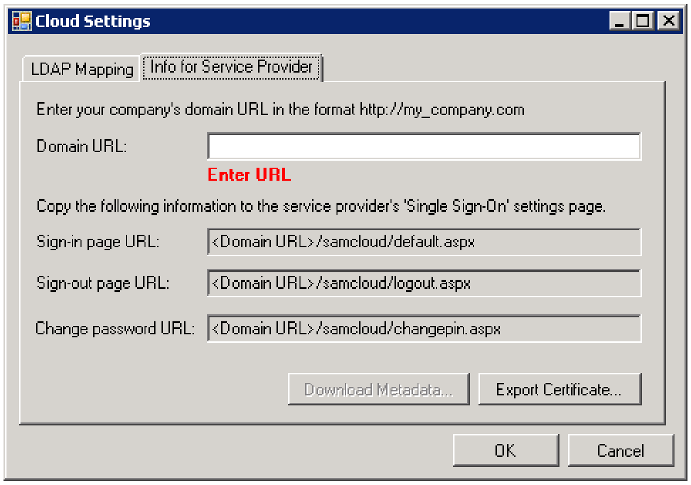
(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

2. Click the **Action** tab, and then select **Cloud Configuration**.



3. Click the **Info for Service Provider** tab.

4. Type the web address of the SAM portal server in the **Domain URL** field.



Enter your company's domain URL in the format http://my_company.com

Domain URL:

Enter URL

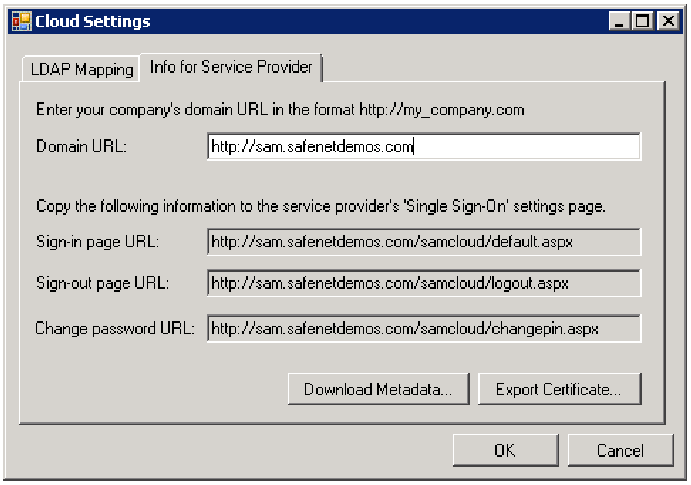
Copy the following information to the service provider's 'Single Sign-On' settings page.

Sign-in page URL: <Domain URL>/samcloud/default.aspx

Sign-out page URL: <Domain URL>/samcloud/logout.aspx

Change password URL: <Domain URL>/samcloud/changepin.aspx

The remaining fields are generated according to the Domain URL that was entered.



Enter your company's domain URL in the format http://my_company.com

Domain URL: http://sam.safenetdemos.com

Copy the following information to the service provider's 'Single Sign-On' settings page.

Sign-in page URL: http://sam.safenetdemos.com/samcloud/default.aspx

Sign-out page URL: http://sam.safenetdemos.com/samcloud/logout.aspx

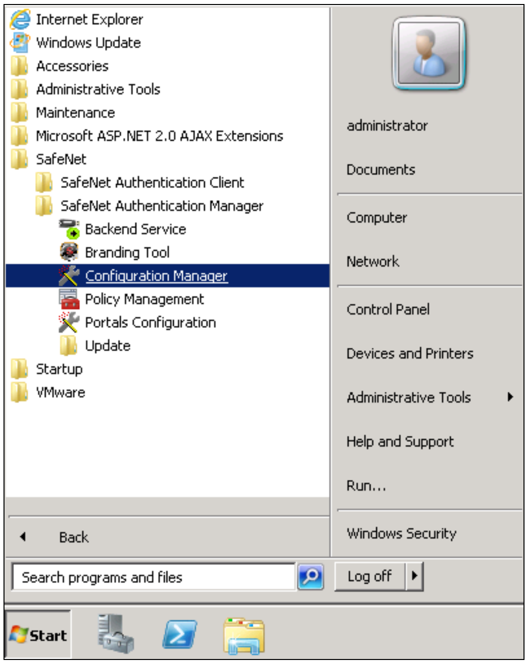
Change password URL: http://sam.safenetdemos.com/samcloud/changepin.aspx

5. Click **OK**.

Exporting the SAM Certificate

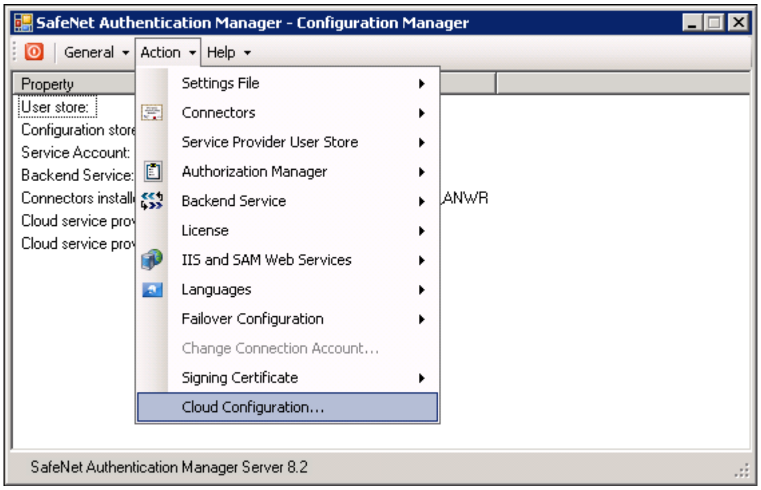
SAM`s certificate is shared between SAM and Blue Coat ProxySG. The certificate will be used to sign the authentication requests.

1. From the Windows **Start** menu, click **Programs > SafeNet > SafeNet Authentication Manager > Configuration Manager**.



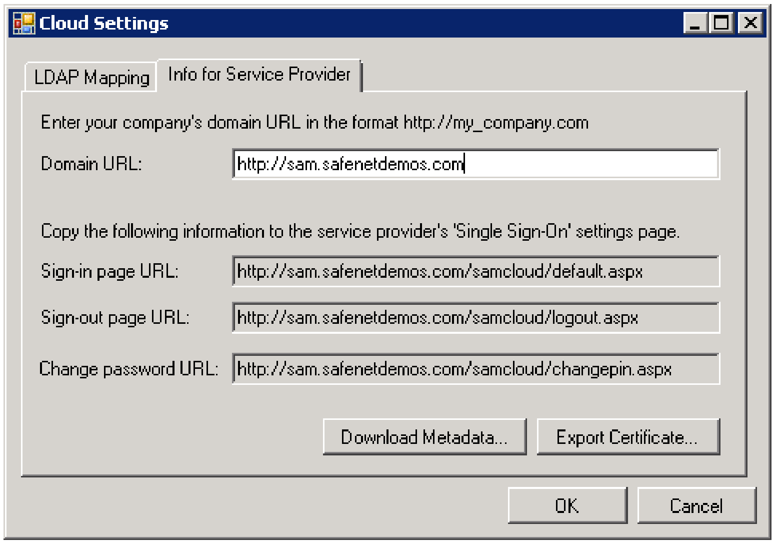
(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

2. Click the **Action** tab, and then select **Cloud Configuration**.



3. On the **Info for Service Provider** tab.

4. Click **Export Certificate**, and then save the certificate file. This certificate file will be imported later into Blue Coat ProxySG.



Enter your company's domain URL in the format http://my_company.com

Domain URL: http://sam.safenetdemos.com

Copy the following information to the service provider's 'Single Sign-On' settings page.

Sign-in page URL: http://sam.safenetdemos.com/samcloud/default.aspx

Sign-out page URL: http://sam.safenetdemos.com/samcloud/logout.aspx

Change password URL: http://sam.safenetdemos.com/samcloud/changepin.aspx

5. Copy the values of the **Sign-in page URL**, **Sign-out page URL**, and **Change password URL** fields, and save them in a text file. These URLs will be required while configuring Blue Coat ProxySG.
6. Click **OK**.

Downloading the Blue Coat ProxySG Metadata

You can export the ProxySG metadata using the following link:

https://<IP-address of ProxySG>:8082/saml/metadata/<realm-name>/sp

For **realm-name**, see “Creating a SAML Realm” on page 13.

Configuring SAM for SAML-based User Federation

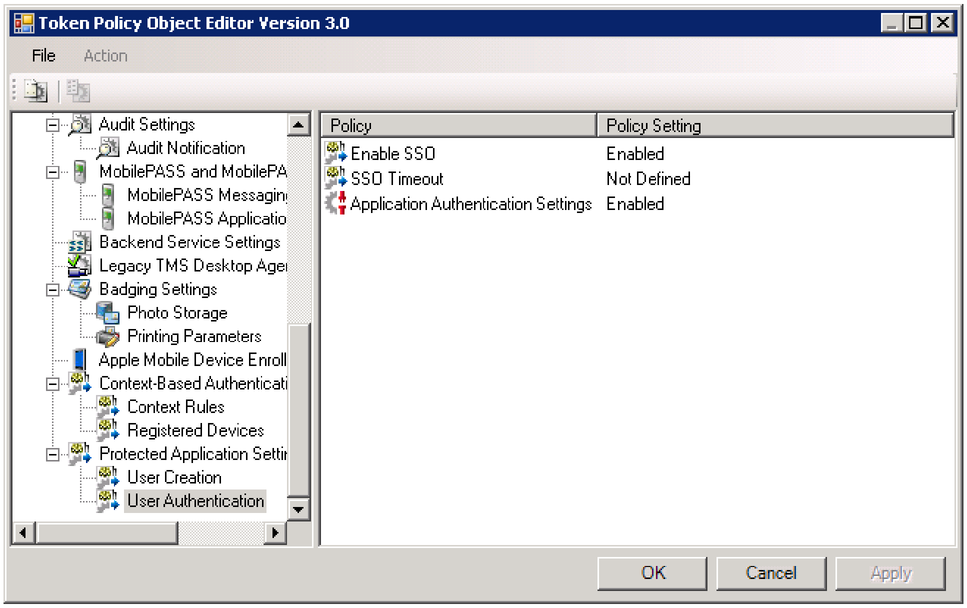
SAM’s Token Policy Object (TPO) policies include application authentication settings for SAML service providers. These settings are used by SAM’s portal to communicate with service providers.

For general portal configuration, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

To edit the TPO for SAM’s portal configuration:

1. Open the **Token Policy Object Editor** for the appropriate group. See the *SafeNet Authentication Manager 8.2 Administrator’s Guide* for more information.

2. In the left pane, click **Protected Application Settings > User Authentication**.



Policy	Policy Setting
Enable SSO	Enabled
SSO Timeout	Not Defined
Application Authentication Settings	Enabled

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

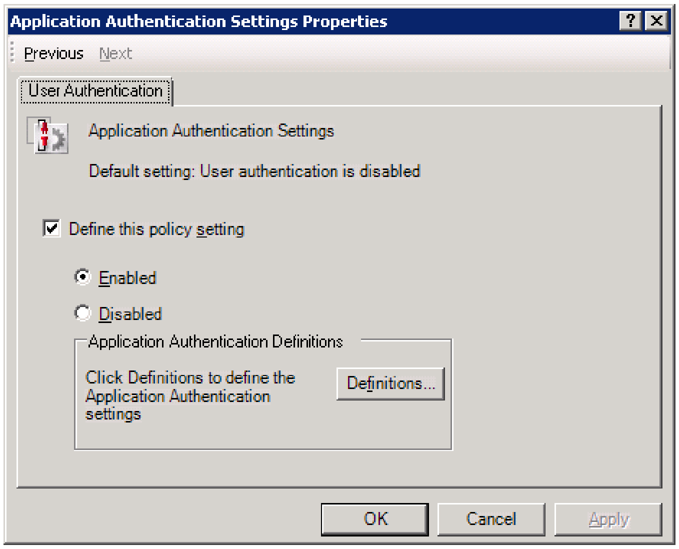
3. In the right pane, double-click **Application Authentication Settings**.

4. On the **Application Authentication Settings Properties** window, perform the following steps:

   a. Select **Define this policy setting**.

   a. Select **Enabled**.

   b. Click **Definitions**.



Application Authentication Settings

Default setting: User authentication is disabled

☑ Define this policy setting

● Enabled

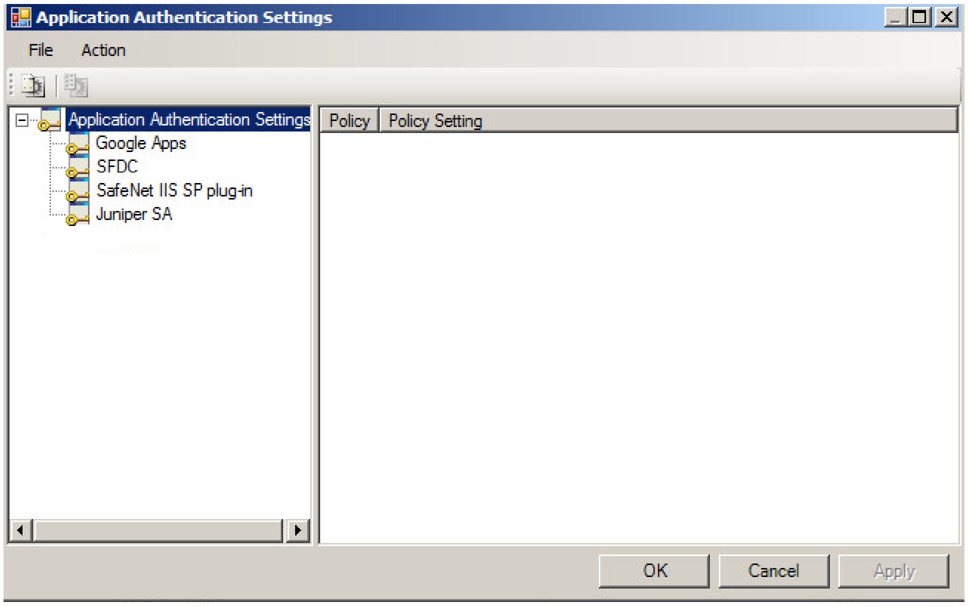
○ Disabled

Application Authentication Definitions

Click Definitions to define the Application Authentication settings

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

5. On the **Application Authentication Settings** window, right-click **Application Authentication Settings**, and then click **Create a new profile**.



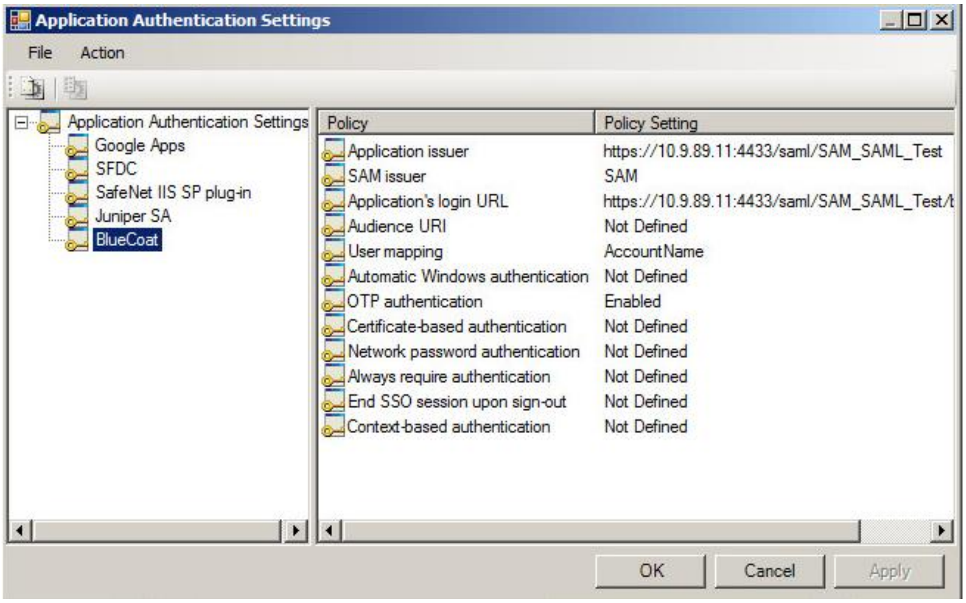
(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

6. In the left pane, right-click the new profile, and then rename it to a user-friendly name.
7. In the left pane, click the new profile.
8. In the right pane, double-click on the following policies, and enter the appropriate information:

Application Issuer	Enter the Entity ID of Blue Coat ProxySG (for example, **https://<Virtual IP of ProxySG>:4433/saml/SAM_SAML**).
SAM issuer	Enter a unique SAM ID to be identified in SAML authentication. This entity ID should match the entity ID of the SAM metadata file.
Application's login URL	Enter the ACS URL of Blue Coat ProxySG (for example, **https://<Virtual IP of ProxySG >:4433/saml/SAM_SAML/bcsamlpost**).
User mapping	Select **AccountName**.

9. Enable the appropriate authentication methods for your organization. See the *SafeNet Authentication Manager Version 8.2 Administrator's Guide* for detailed information about authentication methods.

   The following is an example of the completed policy fields in the **Application Authentication Settings** window:



Policy	Policy Setting
Application issuer	https://10.9.89.11:4433/saml/SAM_SAML_Test
SAM issuer	SAM
Application's login URL	https://10.9.89.11:4433/saml/SAM_SAML_Test/t
Audience URI	Not Defined
User mapping	AccountName
Automatic Windows authentication	Not Defined
OTP authentication	Enabled
Certificate-based authentication	Not Defined
Network password authentication	Not Defined
Always require authentication	Not Defined
End SSO session upon sign-out	Not Defined
Context-based authentication	Not Defined

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

10. Click **OK** until all of the **Token Policy Object Editor** windows are closed.\

Configuring Blue Coat ProxySG

Adding SafeNet Authentication Manager as an identity provider in Blue Coat ProxySG requires the following:

- Creating a SAML Realm, page 13
- Configuring the CA Certificate List, page 17
- Configuring an Authentication Policy, page 19

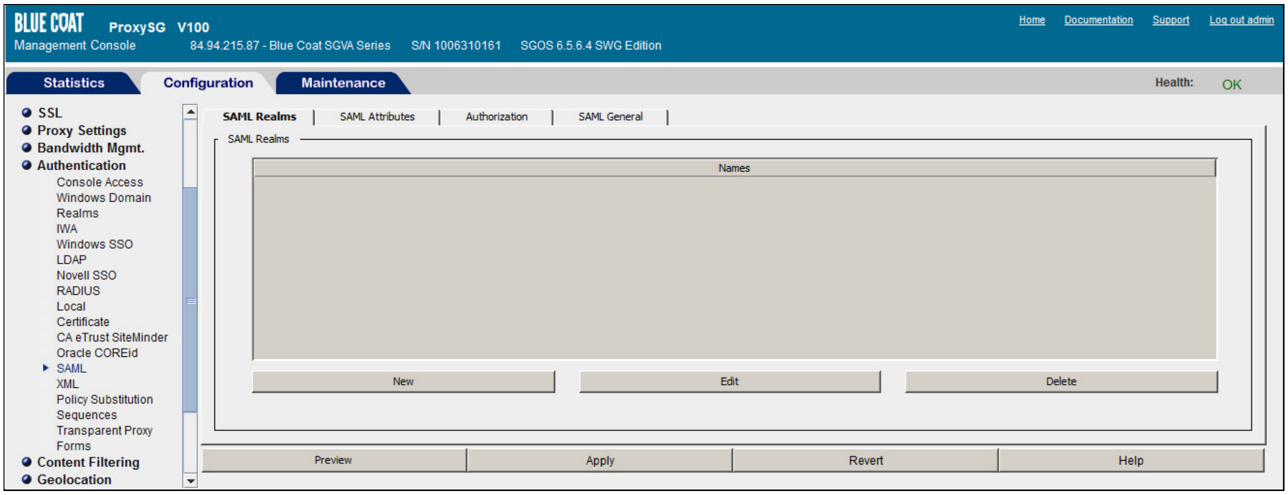
Creating a SAML Realm

1. In a web browser, open the following URL and log in as an administrator:

   https://<ProxySG_IP_Address>:8082

   where **ProxySG_IP_Address** is the IP address of the ProxySG virtual appliance, and **8082** is the default management port.

2. On the **Blue Coat Management Console** window, click the **Configuration** tab, and then in the left pane, click **Authentication > SAML**.

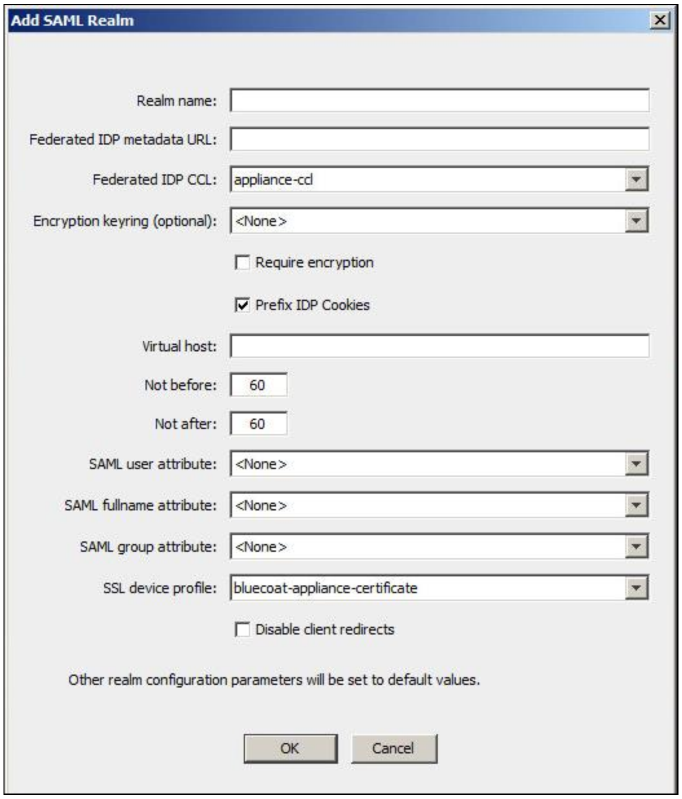


(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

3. In the right pane, on the **SAML Realms** tab, click **New**.

4. On the **Add SAML Realm** window, complete the following fields, and then click **OK**.

Realm name	Enter a valid name for the new SAML realm (for example, **SAM_SAML**).
Federated IDP CCL	Select the browser-trusted CCL.
Virtual host	Specify the hostname for the SAML endpoint.



Realm name:

Federated IDP metadata URL:

Federated IDP CCL: appliance-ccl

Encryption keyring (optional): <None>

□ Require encryption

☑ Prefix IDP Cookies

Virtual host:

Not before: 60

Not after: 60

SAML user attribute: <None>

SAML fullname attribute: <None>

SAML group attribute: <None>

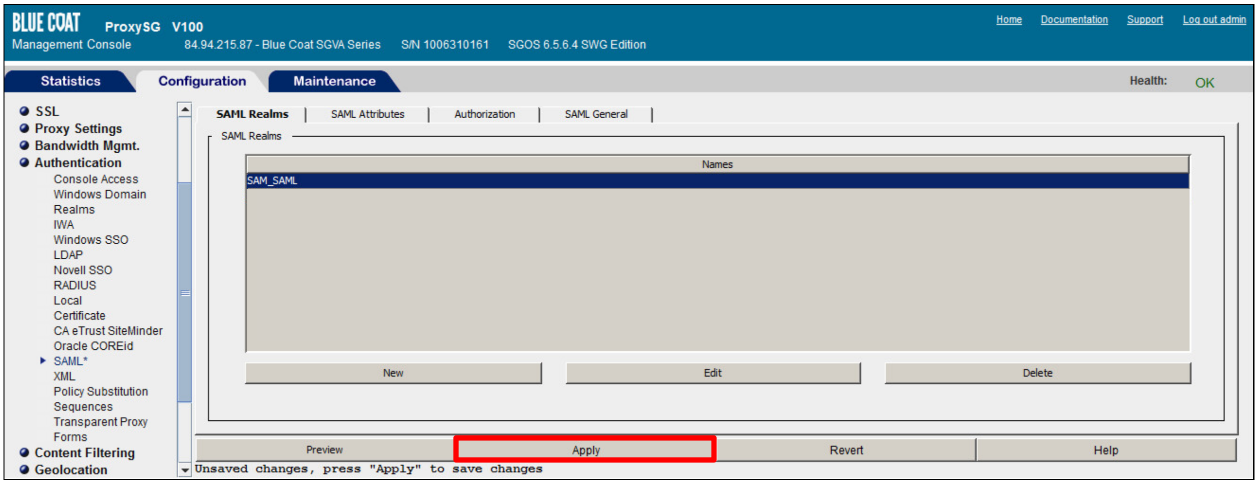
SSL device profile: bluecoat-appliance-certificate

□ Disable client redirects

Other realm configuration parameters will be set to default values.

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

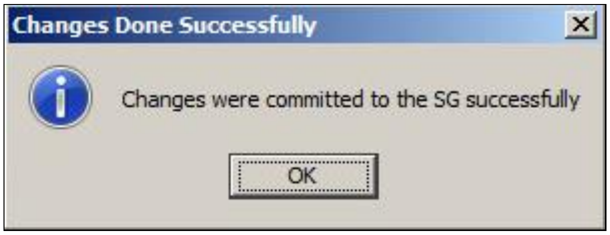
5. Click **Apply**.



```
Unsaved changes, press "Apply" to save changes
```

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

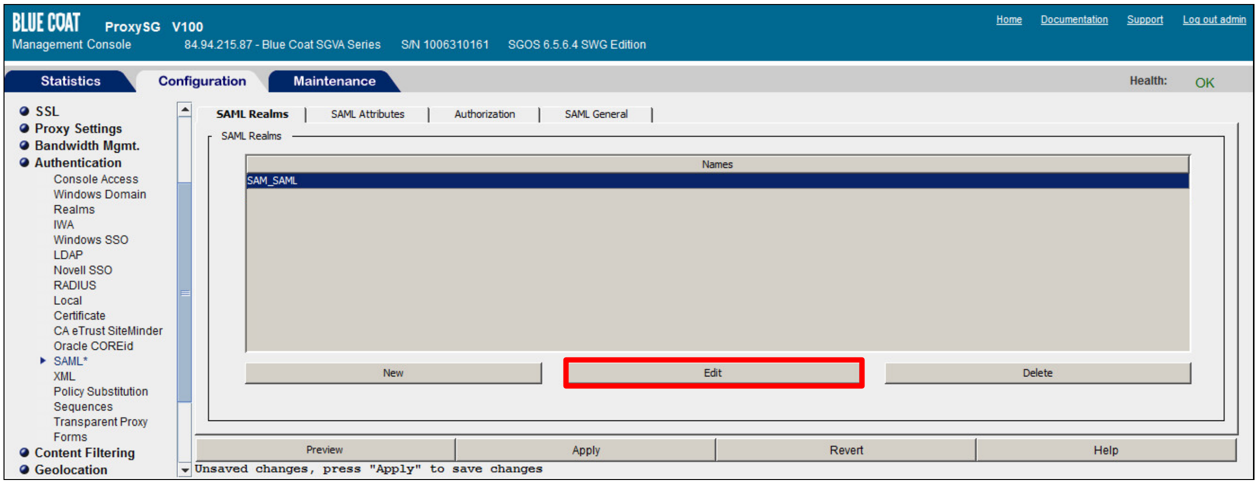
6. Click **OK**.



Changes were committed to the SG successfully

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

7. Select the newly created SAML realm (for example, **SAM_SAML**), and then click **Edit**.

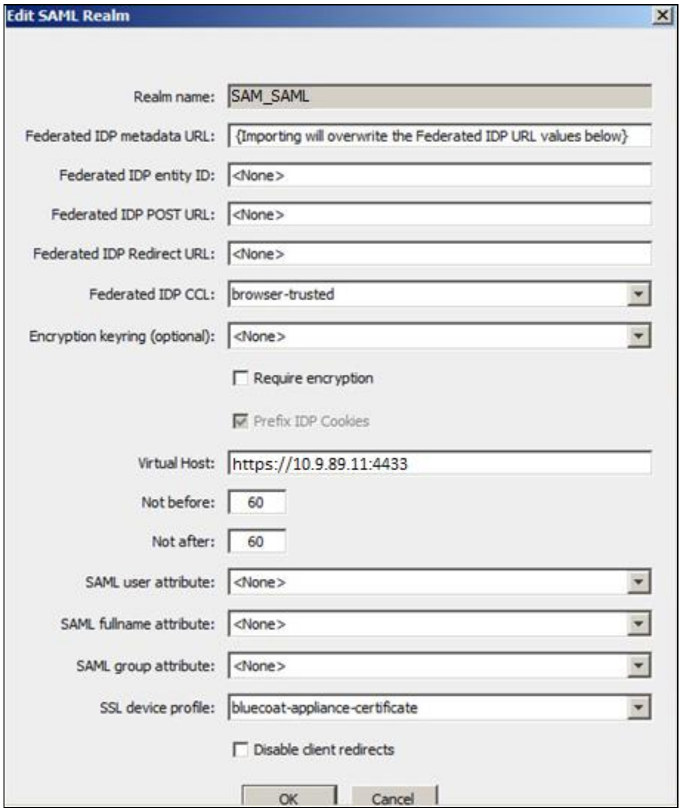


```
Unsaved changes, press "Apply" to save changes
```

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

8. On the **Edit SAML Realm** window, complete the following fields, and then click **OK**.

Federated IDP entity ID	Enter the entity ID of SAM.
Federated IDP POST URL	Enter **http://<IP Address of SAM Server>/samcloud/default.aspx**.
Federated IDP Redirect URL	Enter **http://<IP Address of SAM Server>/samcloud/default.aspx**.



Realm name: SAM_SAML

Federated IDP metadata URL: {Importing will overwrite the Federated IDP URL values below}

Federated IDP entity ID: <None>

Federated IDP POST URL: <None>

Federated IDP Redirect URL: <None>

Federated IDP CCL: browser-trusted

Encryption keyring (optional): <None>

☐ Require encryption

☑ Prefix IDP Cookies

Virtual Host: https://10.9.89.11:4433

Not before: 60

Not after: 60

SAML user attribute: <None>

SAML fullname attribute: <None>

SAML group attribute: <None>

SSL device profile: bluecoat-appliance-certificate

☐ Disable client redirects

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

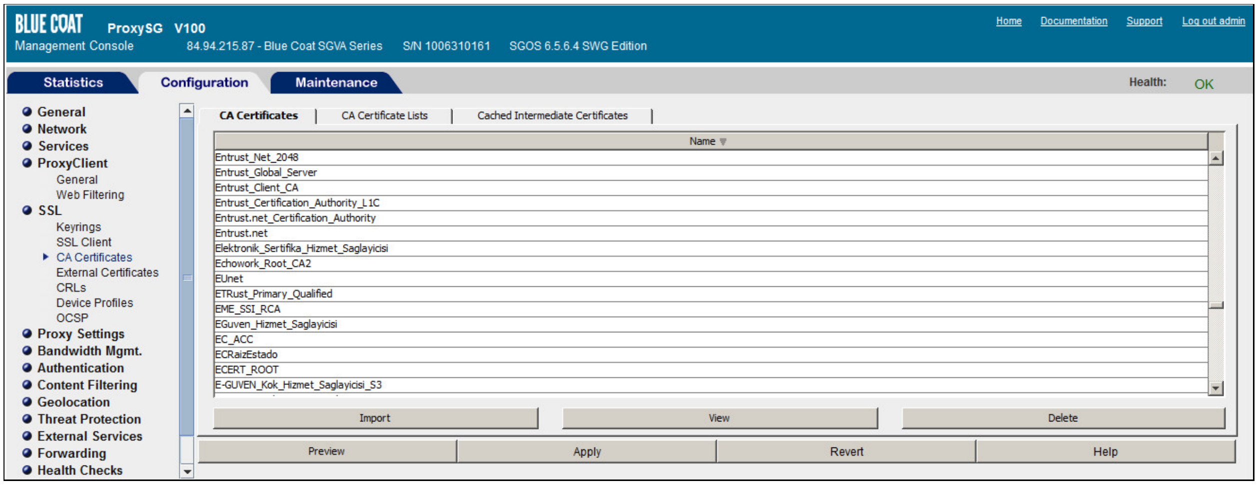
9. Click **Apply**, and then click **OK**.

Configuring the CA Certificate List

The ProxySG appliance CA certificate list (CCL) must contain the IDP's signing certificates.

Importing the IDP Certificate

1. On the **Blue Coat Management Console** window, click the **Configuration** tab, and then in the left pane, click **SSL > CA Certificates**.



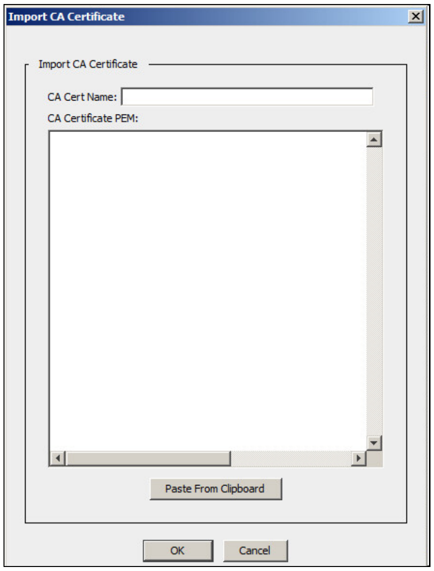
Name
Entrust_Net_2048
Entrust_Global_Server
Entrust_Client_CA
Entrust_Certification_Authority_L1C
Entrust.net_Certification_Authority
Entrust.net
Elektronik_Sertifika_Hizmet_Saglayicisi
Echowork_Root_CA2
EUnet
ETRust_Primary_Qualified
EME_SSI_RCA
EGuven_Hizmet_Saglayicisi
EC_ACC
ECRaizEstado
ECERT_ROOT
E-GUVEN_Kok_Hizmet_Saglayicisi_S3

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

2. In the right pane, on the **CA Certificates** tab, click **Import**.

3. On the **Import CA Certificate** window, complete the following fields, and then click **OK**.

CA Cert Name	Enter the name of the certificate.
CA Certificate PEM	Paste the identity provider certificate you download in "Exporting the SAM Certificate" on page 9.

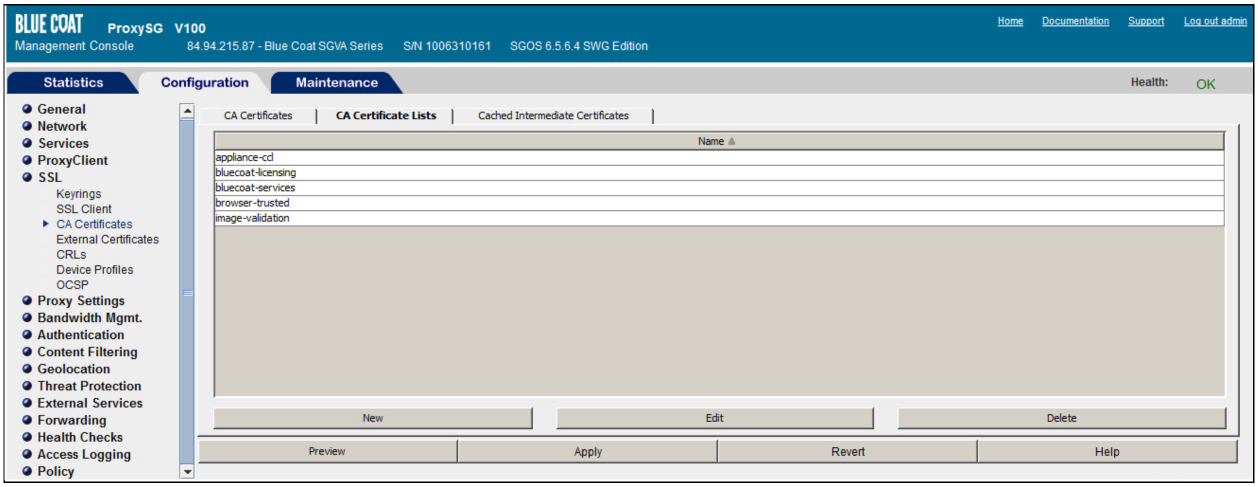


(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

4. Click **Apply**, and then click **OK**.

Creating a CA Certificate Lists

1. On the **Blue Coat Management Console** window, click the **Configuration** tab, and then in the left pane, click **SSL > CA Certificates**.



Name
appliance-ccl
bluecoat-licensing
bluecoat-services
browser-trusted
image-validation

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

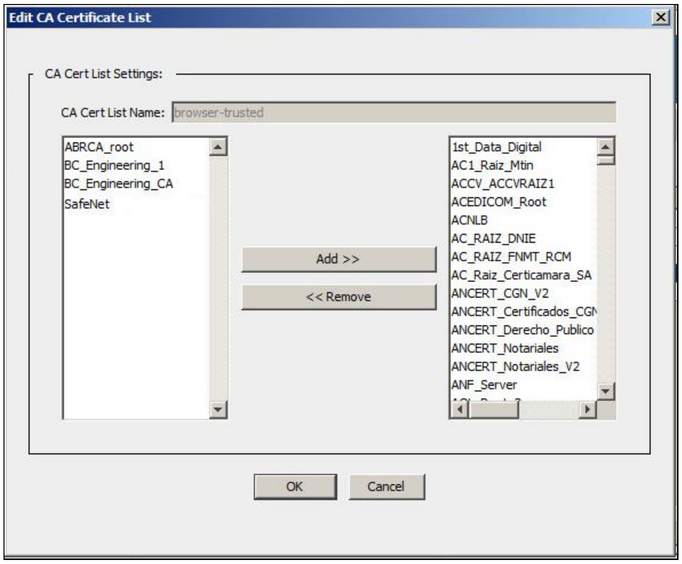
2. In the right pane, on the **CA Certificate Lists** tab, select **browser-trusted**, and then click **Edit**.

3. On the **Edit CA Certificate List** window, perform the following steps:

   a. In the list box on the left, select the imported identity provider certificate (for example, **SafeNet**).

   b. Click **Add >>** to move the selected certificate to the list box on the right.

   c. Click **OK**.



CA Cert List Name: browser-trusted

ABRCA_root
BC_Engineering_1
BC_Engineering_CA
SafeNet

1st_Data_Digital
AC1_Raiz_Mtin
ACCV_ACCVRAIZ1
ACEDICOM_Root
ACNLB
AC_RAIZ_DNIE
AC_RAIZ_FNMT_RCM
AC_Raiz_Certicamara_SA
ANCERT_CGN_V2
ANCERT_Certificados_CGN
ANCERT_Derecho_Publico
ANCERT_Notariales
ANCERT_Notariales_V2
ANF_Server

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

4. Click **Apply**, and then click **OK**.

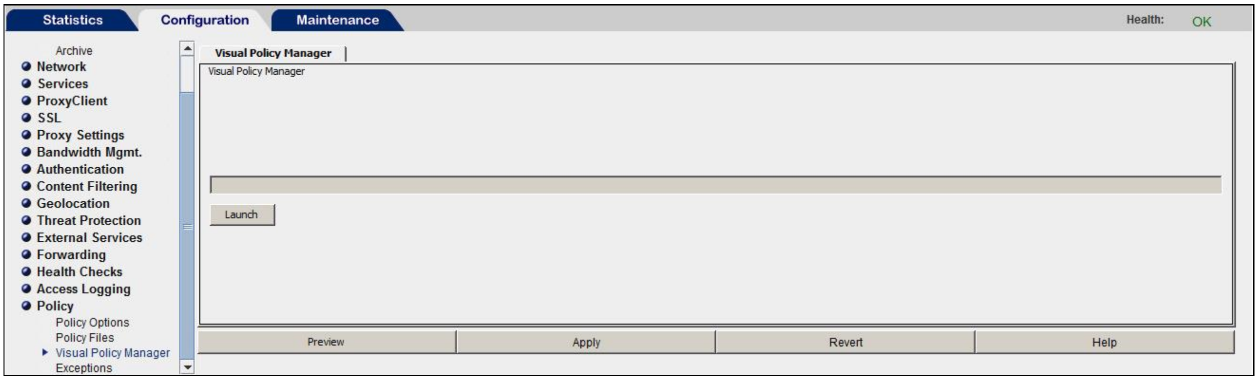
Configuring an Authentication Policy

With an authentication realm configured, now configure a policy on the ProxySG appliance to authenticate, log, and control user access to the web server.

The sections below explain setting up rules to authenticate users, restrict access for specific users and groups, and deny all other access to the web server.

Creating the Web Authentication Layer

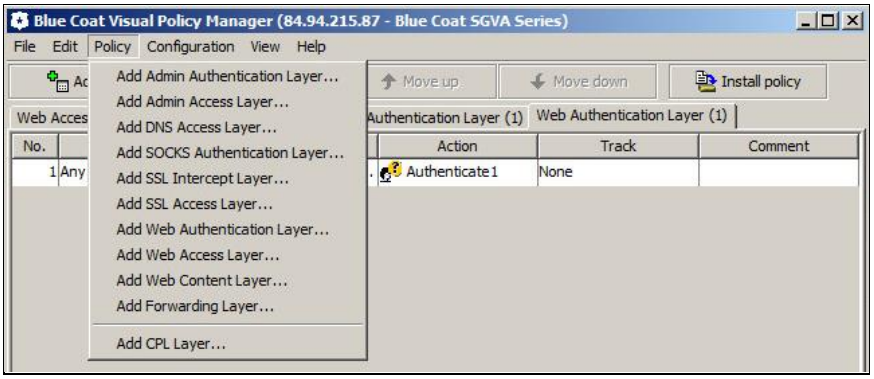
1. On the **Blue Coat Management Console** window, click the **Configuration** tab, and in the left pane, click **Policy > Visual Policy Manager**.



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

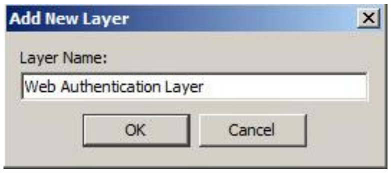
2. In the right pane, click **Launch**.

3. On the **Visual Policy Manager** window, click **Policy**, and then select **Add Web Authentication Layer**.



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

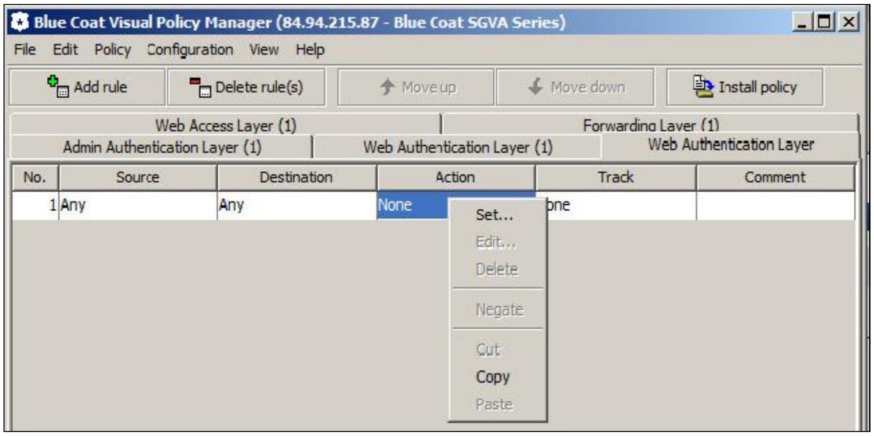
4. On the **Add New Layer** window, enter a descriptive name for the Web Authentication Layer, and then click **OK**.



Layer Name: Web Authentication Layer

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

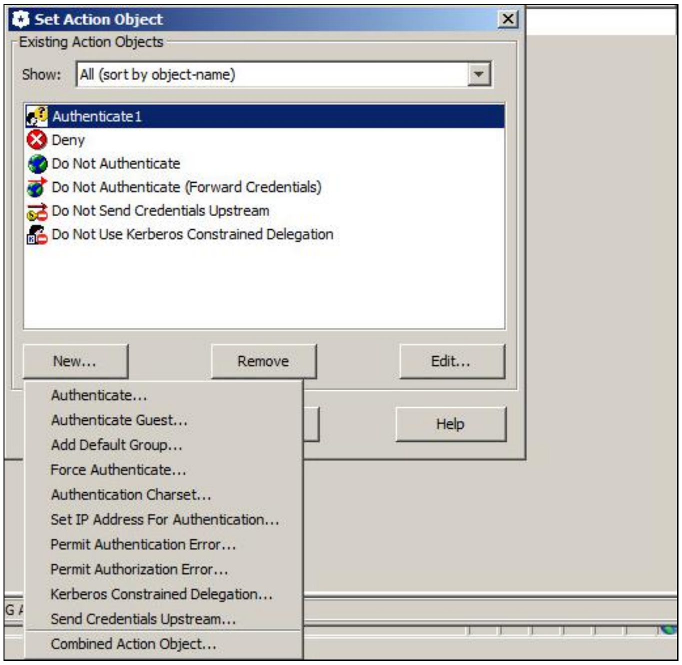
5. Right-click on the **Action** column of the default rule, and then select **Set**.



No.	Source	Destination	Action	Track	Comment
1	Any	Any	None	bne	

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

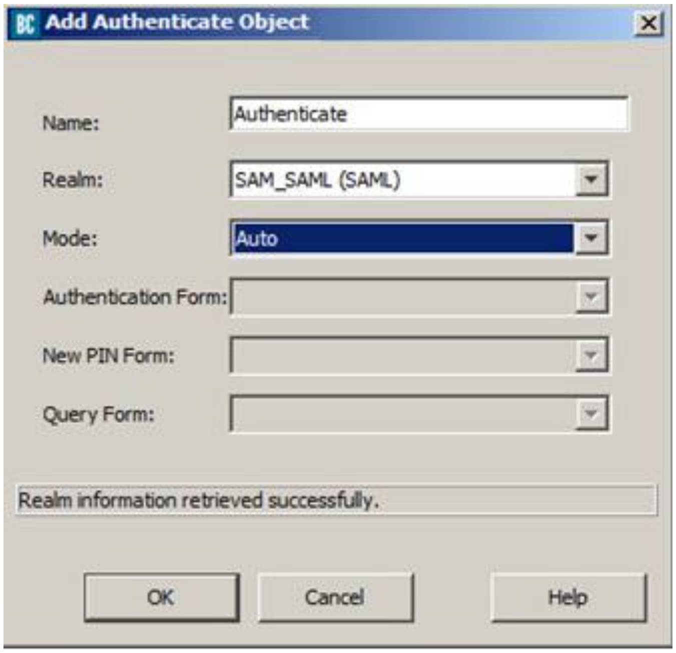
6. On the **Set Action Object** window, click **New**, and then select **Authenticate**.


Set Action Object
Existing Action Objects
Show: All (sort by object-name)
Authenticate1
Deny
Do Not Authenticate
Do Not Authenticate (Forward Credentials)
Do Not Send Credentials Upstream
Do Not Use Kerberos Constrained Delegation
New...
Remove
Edit...
Help
Authenticate...
Authenticate Guest...
Add Default Group...
Force Authenticate...
Authentication Charset...
Set IP Address For Authentication...
Permit Authentication Error...
Permit Authorization Error...
Kerberos Constrained Delegation...
Send Credentials Upstream...
Combined Action Object...

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

7. On the **Add Authenticate Object** window, complete the following fields, and then click **OK**.

Name	Enter the name of the Authenticate Object (for example, **Authenticate**).
Realm	Select the SAML realm that you created in “Creating a SAML Realm” on page 13 (for example, **SAM_SAML**).
Mode	Select **Auto**. The appliance will automatically determine which mode to use.



Add Authenticate Object

Name: Authenticate

Realm: SAM_SAML (SAML)

Mode: Auto

Authentication Form:

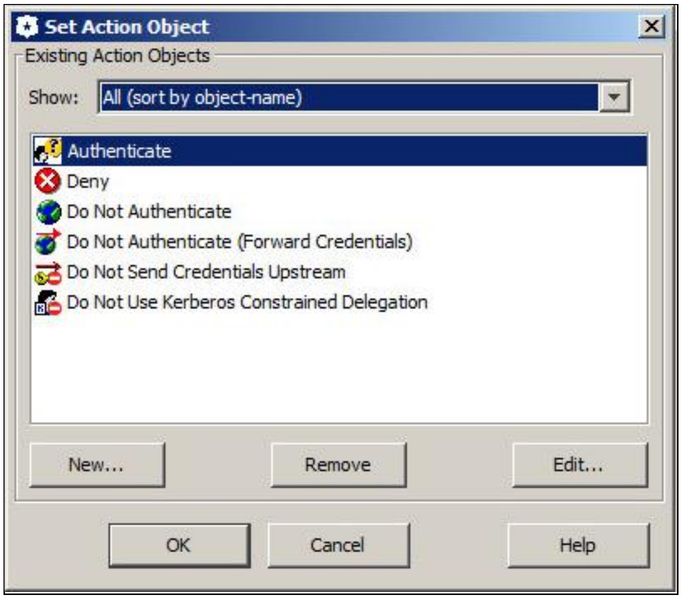
New PIN Form:

Query Form:

Realm information retrieved successfully.

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

8. On the **Set Action Object** window, click **OK**.



Set Action Object

Existing Action Objects

Show: All (sort by object-name)

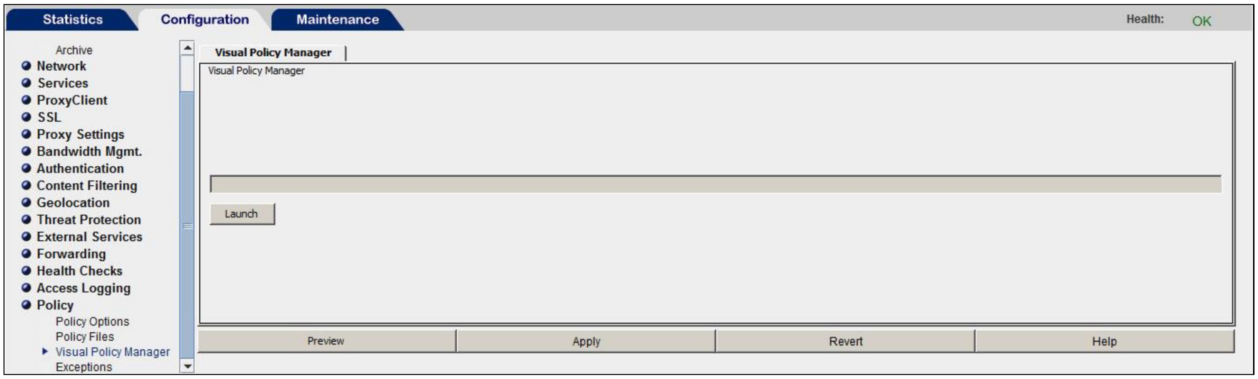
- Authenticate
- Deny
- Do Not Authenticate
- Do Not Authenticate (Forward Credentials)
- Do Not Send Credentials Upstream
- Do Not Use Kerberos Constrained Delegation

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

Creating a Web Access Rule

Create a policy rule that enables the ProxySG appliance to grant users access to the network.

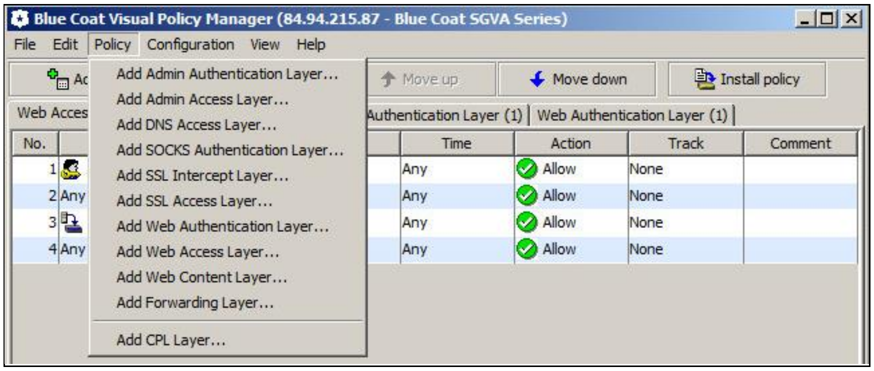
1. On the **Blue Coat Management Console** window, click the **Configuration** tab, and in the left pane, click **Policy > Visual Policy Manager**.



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

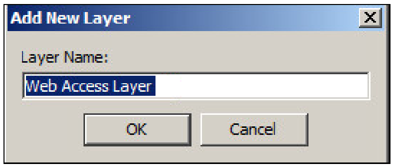
2. In the right pane, click **Launch**.

3. On the **Visual Policy Manager** window, click **Policy**, and then select **Add Web Access Layer**.



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

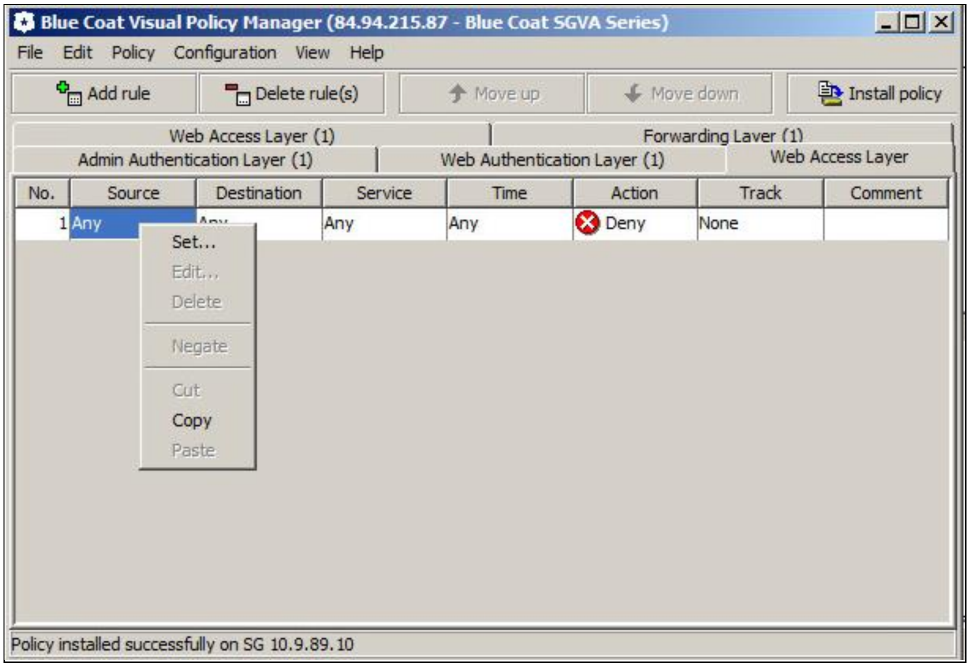
4. On the **Add New Layer** window, enter a descriptive name for the Web Access Layer, and then click **OK**.



Layer Name: Web Access Layer

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

5. Right-click on the **Source** column of the default rule, and then select **Set**.

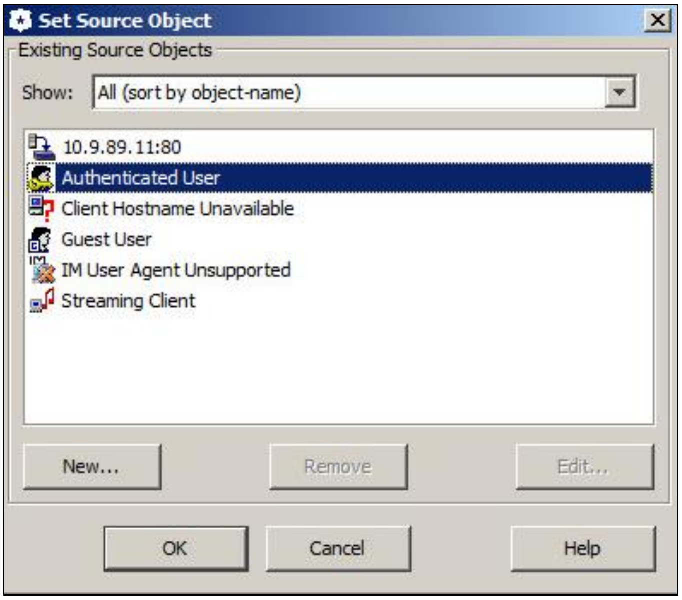


No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	Any	Any	Any	Deny	None	

Policy installed successfully on SG 10.9.89.10

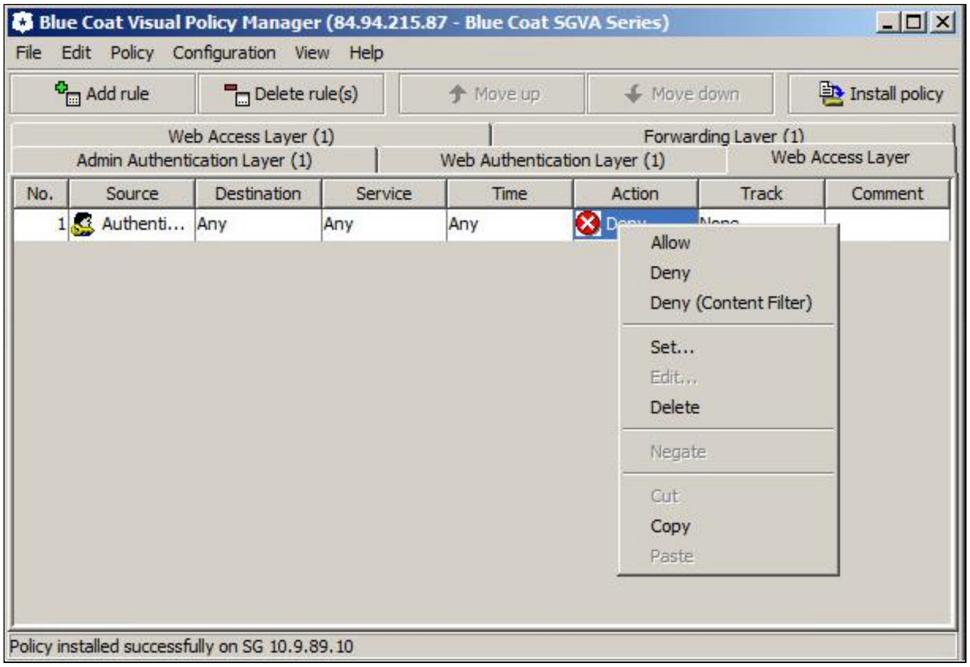
(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)

6. On the **Set Source Object** window, select **Authenticated User**, and then click **OK**.



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

7. Right-click on the **Action** column of the default rule, and then select **Allow**. The icon in the **Action** column changes from red to green.

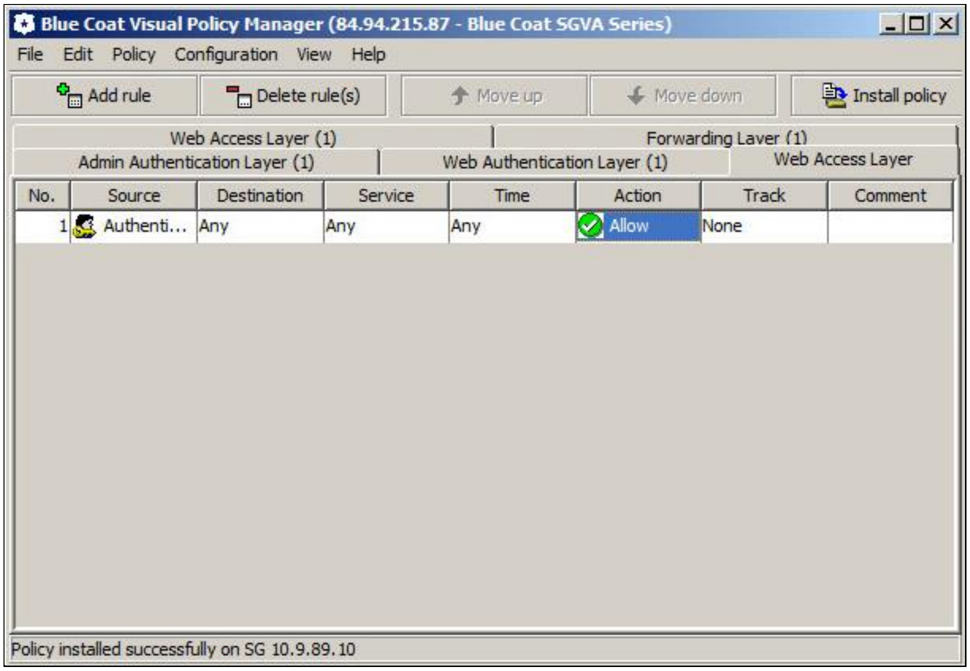


No.	Source	Destination	Service	Time	Action	Track	Comment
1	Authenti...	Any	Any	Any	Deny	None	

Policy installed successfully on SG 10.9.89.10

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

8. Click **Install policy**.



No.	Source	Destination	Service	Time	Action	Track	Comment
1	Authenti...	Any	Any	Any	Allow	None	

Policy installed successfully on SG 10.9.89.10

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

9. Click **OK**.

Running the Solution

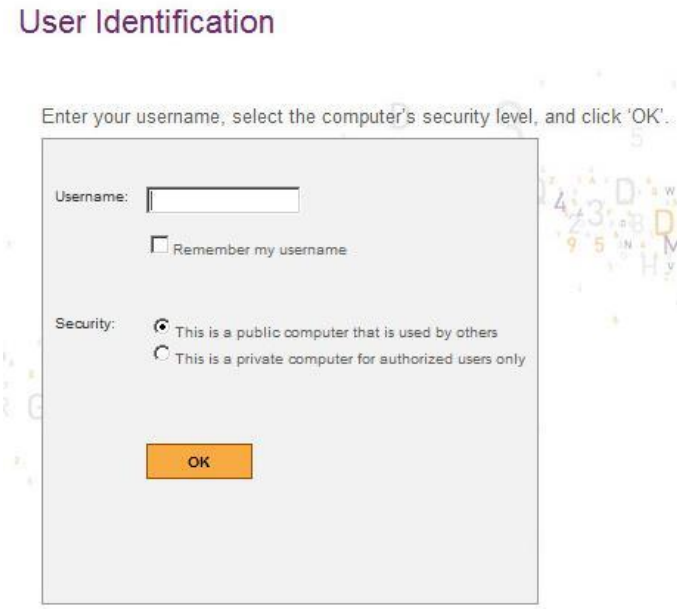
Before running the solution, ensure that the Blue Coat ProxySG virtual appliance is configured as a reverse proxy with HTTPS service.

In this solution, the SafeNet e-Token PASS is used as the enrolled token.

1. Open the following URL in a web browser: **https://<Virtual IP of Bluecoat>**

   where **Virtual IP of Bluecoat** is an IP address that is configured on the ProxySG appliance.

2. You are redirected to the SAM login page. In the **Username** field, enter your user name, and then click **OK**.



User Identification

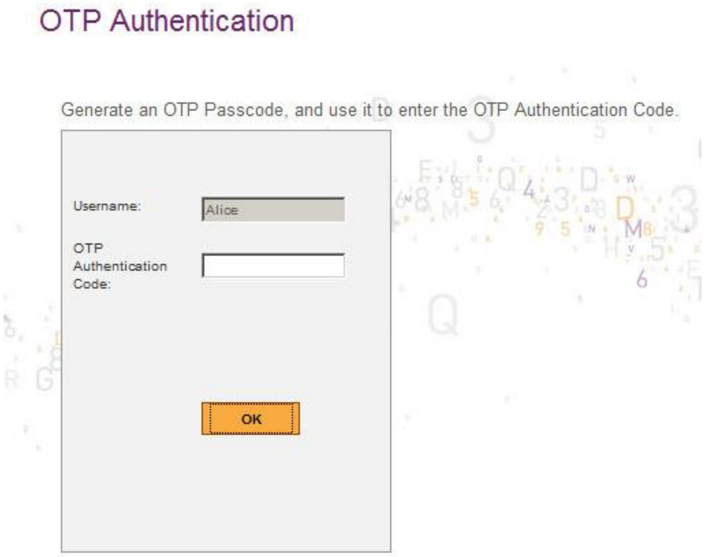
Enter your username, select the computer's security level, and click 'OK'.

Username:

□ Remember my username

Security:
● This is a public computer that is used by others
○ This is a private computer for authorized users only

3. The **OTP Authentication** page is displayed. Generate a one-time password using the SafeNet token, enter it in the **OTP Authentication Code** field, and then click **OK**.



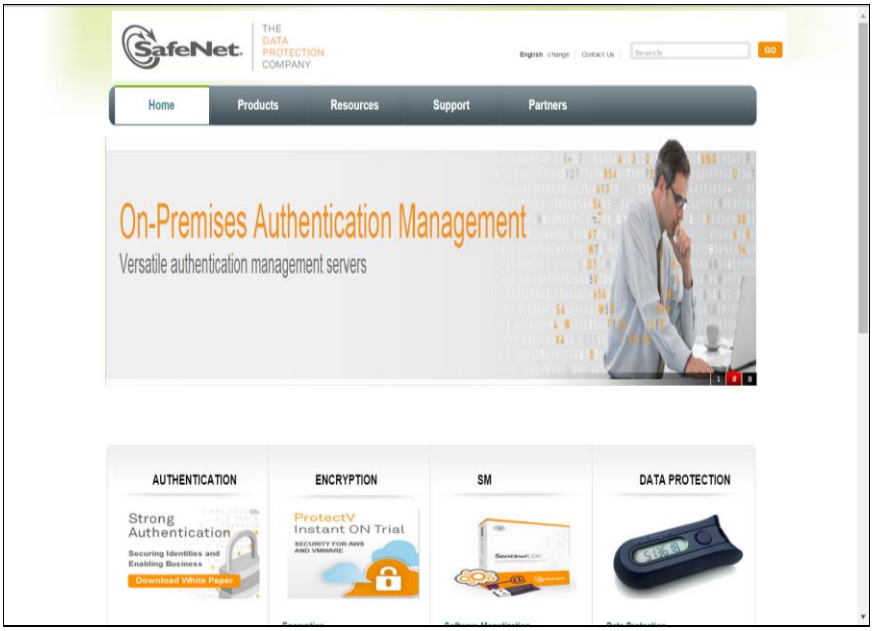
OTP Authentication

Generate an OTP Passcode, and use it to enter the OTP Authentication Code.

Username: Alice

OTP Authentication Code:

After successful authentication, you are allowed to access the requested web page.


SafeNet
THE DATA PROTECTION COMPANY
English change | Contact Us | Search GO
Home
Products
Resources
Support
Partners
On-Premises Authentication Management
Versatile authentication management servers
AUTHENTICATION
Strong Authentication
Securing Identities and Enabling Business
Download White Paper
ENCRYPTION
ProtectV Instant ON Trial
SECURITY FOR AWS AND VMWARE
SM
DATA PROTECTION

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 this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information	
Address	Gemalto, 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 Gemalto Knowledge Base.	