Blue Coat ProxySG Authentication Guide

Broadcom, the pulse logo, Connecting everything, and Symantec are among the trademarks of Broadcom. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries.

Copyright © 2020 Broadcom. All Rights Reserved.

The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, please visit www.broadcom.com.

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

Document Revision: 05/28/2020, SGOS 6.5.x and later
# Table of Contents

## About Authentication and Authorization

- About Authentication Modes ................................................................. 7
- About Authentication Challenge Types ............................................... 9
- About Surrogate Credentials ............................................................... 10
- About Active Directory Integration ...................................................... 12
  - About IWA ....................................................................................... 13
  - About LDAP ................................................................................... 15
  - About Windows SSO ......................................................................... 16
- About SAML .......................................................................................... 18
- Checklist: Prepare the IDP ....................................................................... 21

## Integrate ProxySG Authentication with Active Directory Using IWA

- Configure IWA Direct ............................................................................. 23
  - Integrate the ProxySG Appliance With Your Windows Domain .......... 24
  - Enable Kerberos in an IWA Direct Deployment ............................... 27
  - Create an IWA Direct Realm ............................................................. 28
  - Validate the IWA Realm Configuration ........................................... 33
  - Create a DNS Entry for the Authentication Domain .......................... 34
  - Configure the Web Browser for IWA ............................................... 35
  - Create an IWA Authentication Policy .............................................. 42
  - Verify Kerberos Authentication ....................................................... 49
  - Enable IWA Authentication for SSL Traffic in a Transparent Deployment ........................................................................... 51
  - Using IWA Direct in an Explicit Kerberos Load Balancing/Failover Scenario ........................................................................... 54
  - Preparing for a Kerberos Deployment ............................................ 56

- Configure IWA BCAAA ........................................................................... 57
  - Enable Kerberos in an IWA BCAAA Deployment ............................. 58
  - Create an IWA BCAAA Realm ......................................................... 60
  - Enable SSL Between BCAAA and the ProxySG Appliance .............. 64
  - Validate the IWA Realm Configuration .......................................... 70
  - Create a DNS Entry for the Authentication Domain ........................ 71
  - Configure the Web Browser for IWA .............................................. 72
  - Create an IWA Authentication Policy .............................................. 74
  - Verify Kerberos Authentication ....................................................... 81
  - Enable IWA Authentication for SSL Traffic in a Transparent Deployment ........................................................................... 83

## Integrating ProxySG Authentication with Active Directory Using Windows SSO

- Configure the Windows SSO Agent on the BCAAA Server .................. 87
- Configure the Windows SSO Agent for Domain Controller Query ........ 88
- Configure the Windows SSO Agent for Client Query ............................ 89
SAML Reference ......................................................................................................................... 152
Federation and Metadata ........................................................................................................... 152
Assertions ................................................................................................................................. 152
Profiles and Bindings .................................................................................................................. 152
Backing up the ProxySG Appliance ............................................................................................ 154
About Authentication and Authorization

**Authentication** is the process of verifying the identity of a user so that the user becomes known by the system. You can deny access to users who fail to authenticate successfully, thereby eliminating the threat of malicious clients posing as legitimate network users. For users who authenticate successfully, you can define policies that enforce your corporate usage rules and standards. You can also leverage your existing user groups to enforce policy. For example, you might want to allow your HR department access to social networking sites so that they can research potential candidates, but deny access to other user groups. This process of determining which resources a user or group can access — called **authorization** — can only occur after successful authentication.

You can also configure the appliance to log the activities of authenticated users so that you can monitor user activity in logs and reports. This allows you to assess how well your policies are working or track down users who are misusing resources or exposing your network to potential threats.

To verify the identity of the user sending a request, you must employ an authentication scheme that either challenges the user for credentials or gets those credentials from the browser (or other user agent) automatically without prompting the user (this is known as **single sign-on**). The ProxySG provides a flexible authentication facility that enables you to integrate with your existing authentication services, such as Active Directory, LDAP, RADIUS, and many more.

Integrating the ProxySG with your authentication systems is just the first step in configuring authentication. The next step is to create rules that instruct the ProxySG how to authenticate users and exactly which resources they can, and cannot, access. You define these rules by creating policy using the Visual Policy Manager (VPM) or the Content Policy Language (CPL). Because the policy engine on the ProxySG is so flexible, you can define rules that are as strict or as lenient as necessary to meet your corporate usage goals. For example:

- You could define a simple rule that allows all authenticated users access to all resources and denies all access to users who fail to authenticate successfully.

- You could allow some error tolerance in your policy or create policy that allows limited access to guest users.

- You can also define very specific rules that grant access to some resources to some users, but not all, or that limit access to resources based on the time of day or up to certain bandwidth limits.
About Authentication and Authorization

About Authentication Modes

Before the ProxySG appliance can authenticate intercepted connections, you must create the authentication policy that tells the appliance when and how to authenticate client requests. One of the policy settings you must define is the authentication mode. The authentication mode specifies the type of authentication challenge to use to obtain the client credentials and the type of surrogate credential to use, if any. You define the authentication mode when you create your policy. When creating policy using Content Policy Language (CPL), you set the authentication mode using the authenticate.mode() statement. When creating policy using the Visual Policy Manager (VPM), you set the authentication mode when creating the Authenticate object.

The appliance will automatically override the configured mode if the client cannot support the requested mode. For example, if you set the authentication mode to Origin-Cookie-Redirect, but the client does not support cookies, the appliance will automatically downgrade to Origin-IP-Redirect mode.

If you do not set an authentication mode, the appliance uses the default mode, Auto. In Auto mode the appliance will automatically determine which mode to use. However, in most cases it is best to explicitly set the mode.

The following table lists the authentication modes and when to use them.

<table>
<thead>
<tr>
<th>Authentication Mode</th>
<th>Challenge Type</th>
<th>Surrogate Credential</th>
<th>Use With</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy</td>
<td>The ProxySG appliance issues a proxy challenge (HTTP 407) for every new connection.</td>
<td>None</td>
<td>Explicit proxy</td>
</tr>
<tr>
<td>Proxy IP</td>
<td>The ProxySG appliance issues a proxy challenge (HTTP 407) for the first connection request from an unauthenticated client. It only reissues the challenge when the IP surrogate expires.</td>
<td>IP address</td>
<td>Explicit proxy, Windows SSO, or Novell SSO</td>
</tr>
<tr>
<td>Origin</td>
<td>The ProxySG appliance issues an OCS-style challenge (HTTP 401) for every new connection.</td>
<td>None</td>
<td>Reverse proxy</td>
</tr>
<tr>
<td>Origin IP</td>
<td>The ProxySG appliance issues an OCS-style challenge (HTTP 401) for the first connection request from an unauthenticated client. It only reissues the challenge when the IP surrogate expires.</td>
<td>IP address</td>
<td>Reverse proxy</td>
</tr>
<tr>
<td>Authentication Mode</td>
<td>Challenge Type</td>
<td>Surrogate Credential</td>
<td>Use With</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------</td>
<td>----------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Origin IP Redirect</td>
<td>Redirects the client to the virtual URL and then issues an OCS-style challenge (HTTP 401). It only reissues the challenge when the client's IP surrogate expires.</td>
<td>IP address</td>
<td>Transparent proxy</td>
</tr>
<tr>
<td>Origin Cookie</td>
<td>The ProxySG appliance issues an OCS-style challenge (HTTP 401) for the first connection request for each new OCS domain per client. It only reissues the challenge when the client’s cookie surrogate for the domain expires.</td>
<td>cookie</td>
<td>Reverse proxy</td>
</tr>
<tr>
<td>Origin Cookie Redirect</td>
<td>Redirects the client to the virtual URL and then issues an OCS-style challenge (HTTP 401) for the first connection request for each new OCS domain per client. It only reissues the challenge when the client’s cookie surrogate for the domain expires.</td>
<td>cookie</td>
<td>Transparent proxy</td>
</tr>
<tr>
<td>Form IP</td>
<td>The ProxySG appliance returns a form to the client to request credentials. It only reissues the challenge form when the client’s IP surrogate expires.</td>
<td>IP address</td>
<td>Reverse proxy</td>
</tr>
<tr>
<td>Form IP Redirect</td>
<td>Redirects the client to the virtual URL and then returns a form to the client to request credentials. It only reissues the challenge when the client’s IP surrogate expires.</td>
<td>IP address</td>
<td>Transparent proxy</td>
</tr>
<tr>
<td>Form Cookie</td>
<td>The ProxySG appliance returns a form to the client to request credentials for the first connection for each new OCS domain requested. After the client successfully authenticates to a domain, the ProxySG appliance will only present the form when the client’s cookie surrogate for that domain expires.</td>
<td>Cookie</td>
<td>Reverse proxy</td>
</tr>
<tr>
<td>Form Cookie Redirect</td>
<td>Redirects the client to the virtual URL and then returns a form to the client to request credentials for the first connection for each new OCS domain requested. After the client successfully authenticates to a domain, the ProxySG appliance will only present the form when the client’s cookie surrogate for that domain expires.</td>
<td>Cookie</td>
<td>Transparent proxy</td>
</tr>
</tbody>
</table>
About Authentication Challenge Types

To verify the identify of the user sending a request, you must employ an authentication scheme that either challenges the user for credentials or gets those credentials from the browser (or other user agent) automatically without prompting the user (this is known as single sign-on). The type of challenges the ProxySG presents depends on the type of authentication (that is, what realm is in use), the authentication mode, the proxy type (explicit or transparent) and the protocol of the client request.

There are three types of challenge supported by the ProxySG:

- **Proxy**—The proxy issues a challenge direct to the client (using an HTTP 407 request for HTTP and HTTPS requests). For this type of challenge, the client browser or other user agent must know that it is being proxied (that is, it is configured for explicit proxy). This challenge type is used with the Proxy and Proxy-IP authentication modes.

- **Origin**—This challenge type is used in transparent proxy deployments in which the client does not know it is being proxied. In this type of challenge, the proxy impersonates the origin content server (OCS) and returns an unauthorized response to the request (using an HTTP 401 request for HTTP and HTTPS requests). This challenge type is used with the Origin, Origin-Cookie, Origin-IP, Origin-Cookie-Redirect, and Origin-IP-Redirect authentication modes.

- **Form**—The ProxySG returns a form or redirects the client to a form that prompts for the required credentials, such as a user name and password. This challenge type is used with the Form-IP, Form-Cookie, Form-IP-Redirect, or Form-Cookie-Redirect authentication modes.
About Authentication and Authorization

About Surrogate Credentials

Most Web pages are composed of multiple objects, such as text, images, scripts, and data feeds. Therefore, when downloading a single Web page, your browser may require multiple connections in order to download all the content on the page. When authentication is enabled, each connection must be authenticated, which can result in a large volume of authentication requests and a huge load on your authentication systems. To reduce the load on your authentication systems, the ProxySG appliance can be configured to cache a token after it successfully authenticates a client request. It can then use this token—called a surrogate credential—to authenticate subsequent requests from the same user, eliminating the need to consult the authentication server each time.

The ProxySG appliance supports two types of surrogates:

- **Cookie surrogates**—After the ProxySG appliance successfully authenticates the first connection from the client it sets a cookie, which it uses to authenticate subsequent connections from the same user to any host in the same origin content server (OCS) domain. The ProxySG appliance uses a Hash-based Message Authentication Code (HMAC) to ensure that the cookie is not tampered with or copied. For added security, you can optionally configure the authentication realm to verify that the IP address in the request matches the IP address in the cookie. When configuring the realm you can also define whether to use persistent cookies, which are stored on the client system and persist across sessions, or session cookies (the default), which are only good for the browser session. Cookie surrogates only work with HTTP- and HTTPS-based connections. If the realm is configured to use cookie surrogates, it will automatically downgrade to an IP surrogate for user agents that do not support cookies.

- **IP surrogates**—After the ProxySG appliance successfully authenticates the first connection from an IP address, it keeps the IP address as a token in its surrogate cache. It then uses this surrogate to authenticate subsequent requests from the same IP address. IP surrogates are less secure than cookie surrogates because IP addresses can be spoofed. In addition, they should not be used in environments with multi-user systems (such as Citrix) or with clients behind NAT devices.

Even if you choose an authentication mode that does not use surrogate credentials, after a transaction has been authenticated, transactions on the same persistent connection are also considered authenticated.

You define how and if surrogate credentials are used when you configure authentication. When you define the authentication policy, you set the authentication mode, which specifies the type of challenge and the type of surrogate, if any, to use when authenticating requests. You set the length of time for which the surrogate credentials are valid—called the surrogate refresh time—when you configure the realm. By default, surrogate credentials are good for 15 minutes, which means that if the ProxySG appliance receives a request that requires authentication from the same client during this time period, it uses the surrogate credential to authenticate the request; if the surrogate credential has expired, it must reauthenticate the user and then reset the surrogate. You can also override the setting in the realm configuration by setting the surrogate refresh time in policy, for example if you want to allow a longer or shorter surrogate refresh time for different users,
subnets, destinations, or user agents. Any setting you define in policy overrides settings you define in the realm configuration.
About Active Directory Integration

If you are using Windows Active Directory (AD) in your network, you can configure the ProxySG appliance to authenticate users against your AD. There are three ways to integrate ProxySG appliance with your AD deployment:

- Integrated Windows Authentication (IWA)
- Windows Single Sign-On (Windows SSO)
- Lightweight Directory Access Protocol (LDAP)
About IWA

Integrated Windows Authentication (IWA) is an authentication scheme that allows you to authenticate and authorize users against your Windows Active Directory (AD). One of the main benefits of IWA is that it can provide a single sign-on experience for your users. When configured properly, the user agent or browser will automatically provide the users’ domain credentials to the ProxySG appliance when challenged without prompting the user.

When the ProxySG appliance receives a request that requires authentication, it consults the IWA configuration settings you have defined to determine what type of challenge to return to the client. It will try to use the strongest challenge protocol that is configured and, if the browser cannot use that protocol or if it is not configured properly, the appliance will downgrade to the next protocol. For example, if you configure the IWA realm to allow Kerberos and NTLM, but the user agent/browser does not support Kerberos, the ProxySG appliance will automatically downgrade to NTLM.

Another benefit of IWA is that it provides authorization without any additional configuration because a successful authentication response automatically includes information about the groups to which the user belongs. The ProxySG appliance can then use this group membership information to enforce its authorization policies.

When integrating the ProxySG appliance with AD using IWA, you can either connect the appliance directly to your AD domain (using IWA Direct) or you can connect via an authentication agent running on a Windows server in your domain (using IWA BCAA).
About Authentication and Authorization

About IWA Challenge Protocols

The ProxySG appliance determines which of the following protocols to use to obtain Windows domain login credentials each time it receives a client request that requires IWA authentication:

- **Kerberos**—This is the most secure protocol because it establishes mutual authentication between the client and the server using an encrypted shared key. This protocol requires additional configuration and the ProxySG appliance will silently downgrade to NTLM if Kerberos is not set up properly or if the client cannot do Kerberos. For more information, see "Preparing for a Kerberos Deployment" on page 56.

- **NTLM**—Uses an encrypted challenge/response that includes a hash of the password. NTLM requires two trips between the workstation and the ProxySG appliance, and one trip between the appliance and the Domain Controller. It therefore puts more load on the network than Kerberos, which only requires one trip between the workstation and the ProxySG appliance and doesn't require a trip between the appliance and the Domain Controller.

- **Basic**—Prompts the user for a username and password to authenticate the user against the Windows Active Directory.

When the ProxySG appliance receives a request that requires authentication, it consults the IWA configuration settings you have defined to determine what type of challenge protocol to return to the client. It will try to use the strongest protocol that is configured and, if the browser cannot use that protocol or if it is not configured properly, the appliance will downgrade to the next strongest protocol. For example, if you configure the IWA realm to allow Kerberos and NTLM authentication, but the user agent/browser does not support Kerberos, the ProxySG appliance will automatically downgrade to NTLM.
About LDAP

LDAP (lightweight directory access protocol) is a communication protocol used to access directory information over your network. Typically an LDAP directory, such as Microsoft Active Directory or OpenLDAP, stores information about your end users and network resources into various entries, which can be referenced by various LDAP-aware client applications, such as email client. A benefit of using LDAP is you can take advantage of your existing LDAP solution and apply it to your ProxySG deployment. As a result, all applications using LDAP resources can be managed from a single source, simplifying administration tasks. The ProxySG appliance can be configured to use any LDAP-compatible directory service to provide user information to authenticate users in your deployment.

When the ProxySG appliance receives an authentication request, it attempts to establish a session with the LDAP directory by authenticating (or binding) to the server. A client can then perform various LDAP operations on the directory data, like searching for a user, to make decisions based on authentication and authorization policy. Keep in mind, you'll need to create authentication and authorization policies using the VPM or CPL before network access controls are put into effect.

When users attempt to access network resources (such as the Internet), they are prompted to enter their user credentials. As these credentials are not retained upon application shutdown, users are generally required to submit their credentials more frequently. This repeated sign on is one of the disadvantages of LDAP authentication. If you are looking for a true single sign on solution, consider using Integrated Windows Authentication (IWA) or Windows SSO authentication.

Alternatively, if you need something that provides additional security, you can use Kerberos authentication via IWA.
About Windows SSO

With Windows SSO authentication, client IP addresses are mapped to usernames based on Windows Active Directory logins. Therefore, this type of authentication will only work if your clients are running in a Windows domain environment. In addition, because usernames are derived from IP address mappings, Windows SSO authentication only works well in environments where one IP address maps to one user. Environments with multi-user systems (such as Citrix) or with clients behind NAT devices are not suitable for Windows SSO authentication.

One of the benefits of Windows SSO authentication is that users are never prompted for credentials. Instead, there are two ways that the BC AAA Windows SSO agent can obtain the users IP address-user name mapping:

- **Domain Controller Query**—Whenever a user logs in to the Windows domain, the client system establishes a NetBIOS session with the Windows Domain Controller (DC). When you configure the BC AAAA Windows SSO agent to use DC query (DCQ), the agent immediately begins querying the DC(s) for the user name associated with each current NetBIOS session (that is, it does not wait until it receives an authentication request from the appliance). The agent then uses this information to create a IP-to-user mapping table and stores in the RAM. When the appliance sends an authentication request to the BC AAAA Windows SSO agent, the agent checks to see if it has the IP address contained in the authentication request in its mapping table. If it has the mapping and the mapping is still valid (based on the freshness of the entry), authentication succeeds and it returns the username to the appliance.

  If it does not have the IP address, one of two things will happen:

  - If the authentication realm is configured to perform client query (CQ) in addition to DC query, at this point it will perform CQ.
  - If CQ is not enabled, the agent will return an authentication failed response to the appliance. In this case, report entries detailing network behavior for this user will contain IP addresses instead of user names until the next successful authentication.

  To use DCQ, you must explicitly enable it both in the Windows SSO agent configuration on the BC AAA server and in the Windows SSO realm settings on the appliance. When you configure the agent, you also specify settings such as which DCs to query (by default, it queries all of them) and how long an IP-to-user mapping is valid.

- **Client Query**—With CQ, the BC AAAA Windows SSO agent obtains login information for a user by directly querying the client system. To do this, it opens a Server Message Block (SMB) connection with the client to determine the user name of the logged in user. If the agent finds one logged in user, authentication succeeds; if it does not find a logged in user, or if it finds more than one logged in user, authentication fails. In this case, report entries detailing network behavior for this user will contain IP addresses instead of user names until the next successful authentication request.
For CQ to work, the Windows SSO agent must be able to open an SMB connection to the client systems over port 445. The Windows firewall on many Windows client operating systems block this port by default. In this case, you must modify the Windows firewall settings to allow remote access to client systems through port 445.
About SAML

SAML 2.0 was developed by the OASIS Security Services Technical Committee. It is an industry standard for retrieving authorization and identity information in XML documents to facilitate single sign-on (SSO) applications or services on the Internet. In SAML authentication, the following entities exchange information:

- **Identity providers (IDPs)**, which are identity stores. For example, an IDP may have a back-end directory of users. The IDP authenticates the users. See "Checklist: Prepare the IDP" on page 21 for supported IDPs.

- **Service providers (SPs)**, which provide access to applications or services to users. It is the entity that creates an authenticated session for the user. In SGOS 6.5.x, the ProxySG appliance acts as the service provider.

> SAML realms are not compatible with administrative authentication to the Management Console.

After you have defined and configured a SAML realm, and both the IDP and SP have federated and exchanged metadata, authentication can occur.

See "SAML Reference" on page 152 for descriptions of key concepts in SAML.

The following is an overview of what happens when a user goes to a website that requires authentication.

**Step 1- Initial user request**
The ProxySG appliance intercepts the user’s request and redirects the web browser to the IDP. The redirect URL includes the SAML authentication request that should be submitted to the IDP’s SSO service.

If the Disable Client Redirect option is enabled, the appliance does not redirect the client to the IDP. See “Configure the SAML Realm” on page 125 for information.

**Step 2 - Authentication request and response**

1. The IDP requests valid credentials or checks for stored credentials.
2. The appliance responds with credentials.
3. The IDP signs an authentication response with its private signing key. If the IDP has been configured to send encrypted assertions, the IDP encrypts the assertion before sending it to the appliance.
4. The IDP sends assertions to the appliance and signs the response with its private key.
5. The IDP sends the authentication response to the appliance. The response contains the user’s username, which is not exposed to the appliance.

**Step 3 - Assertion decryption and validation**

The appliance decrypts (if necessary) and validates the assertions.

The IDP requests user credentials from the appliance, such as requesting a valid login/password or checking valid session cookies for stored credentials.

If the appliance responds with valid credentials, the IDP:

- Signs an authentication response with its private signing key. If the IDP has been configured to send encrypted assertions, the IDP encrypts the assertion before sending it to the appliance.
- Sends the authentication response to the appliance. The response contains the user’s username, which is not exposed to the appliance.
About Authentication and Authorization

The appliance:

- Decrypts encrypted assertions and rejects any unsigned assertions.
- Validates the assertions and uses the private key to retrieve the user’s name and group memberships (as specified in assertion attributes) from the assertion.

**Step 4 - User request validation**

1. The appliance uses the public key to validate the user request.
2. The appliance redirects the user to the website.

The appliance:

- Uses the corresponding public key, which is embedded in the IDP’s signing certificate, to validate the user request.
- Redirects the user to the website and creates an authenticated session for the user.
SAML Requirements

Setting up a SAML realm for the ProxySG appliance requires one of the following IDPs:

- Microsoft® Active Directory Federation Services (AD FS) 2.0
  
  AD FS 1.0 ships with Windows Server 2008. If you want to use the SAML realm with AD FS, you must download AD FS 2.0 from the Microsoft website and install it.

- CA SiteMinder® Federation Partnership R12

- Oracle® Identity Federation 11g

- (Available in SGOS 6.5.2 and later) Shibboleth 2.3.5

Checklist: Prepare the IDP

Before you set up a SAML realm, make sure that you have done the following for your IDP:

- Installed and configured the administration software

- Set up the identity store for authentication

- Identified the default user attribute to be passed in SAML assertions, for example, the User Principal Name attribute in LDAP

- Identified any additional attributes that you want to be passed in assertions, for example, the memberOf attribute, which identifies the groups of which a user is a direct member in LDAP

- Determined the location (URL) of the IDP’s metadata file. You require this to complete the steps in "Configure the SAML Realm" on page 125. If you import metadata, the realm uses its preconfigured settings. See "Export the IDP Metadata File" on page 119 for instructions on locating the metadata file for the IDP.

- To import SiteMinder, Oracle, or Shibboleth metadata, use the following CLI command:

  
  # (config saml <realm-name>) inline idp-metadata <XML>

To avoid errors, Blue Coat recommends that you import metadata through the CLI instead of entering the information manually in the Management Console.
Integrate ProxySG Authentication with Active Directory Using IWA

With Integrated Windows Authentication (IWA), users are authenticated based on their Windows Active Directory domain logins. There are two ways you can integrate the ProxySG appliance with your Active Directory using IWA:

- **IWA Direct**—The ProxySG appliance will communicate directly with your Domain Controllers (DCs) to obtain authentication information. This option requires that you join the ProxySG appliance to your Windows domain. See "Configure IWA Direct" on the facing page.

- **IWA BCAA**—The ProxySG appliance will contact the BCAA server when it needs to authenticate a user. This option requires that you install the Blue Coat Authentication and Authorization Agent (BCAAA) on a dedicated server in your Windows domain and configure it to communicate with both the DC and with the appliance as an authentication agent. Use this option if you do not want to allow the ProxySG appliance to join your Windows domain. See "Configure IWA BCAA" on page 57.
Configure IWA Direct

To configure IWA Direct authentication, you must complete the following tasks:

1. Join the ProxySG appliance to the Windows domain. See "Integrate the ProxySG Appliance With Your Windows Domain" on the next page.

2. (Kerberos only) If you plan to use Kerberos authentication, you must make sure that authentication requests are directed to the DNS name of the appliance’s Active Directory machine account name. See "Enable Kerberos in an IWA Direct Deployment" on page 27.


4. Verify that the appliance can successfully authenticate an Active Directory user using the IWA realm you created. See "Validate the IWA Realm Configuration" on page 70.

5. Create a DNS entry for the ProxySG authentication URL. See "Create a DNS Entry for the Authentication Domain" on page 71.

6. Configure the client browsers for single sign-on. See "Configure the Web Browser for IWA" on page 72.

7. Create the policy rules that will enforce authentication and, optionally, authorization. See "Create an IWA Authentication Policy" on page 74.

8. (Kerberos only) Verify that Kerberos is configured properly. See "Verify Kerberos Authentication" on page 81.

9. (optional) Enable authentication for HTTPS traffic. This step is only required if you want to authenticate HTTPS traffic in a transparent deployment. Explicit deployments can authenticate HTTPS traffic without any additional configuration provided that you have a valid SSL license installed. See "Enable IWA Authentication for SSL Traffic in a Transparent Deployment" on page 83.

For details on optimizing your IWA-Direct or BCAA configuration, see Optimize IWA Authentication.
Integrate the ProxySG Appliance With Your Windows Domain

To integrate the ProxySG appliance into your Windows domain, you must complete the following tasks:

Step 1 - Synchronize the ProxySG appliances and DC Clocks

The ProxySG cannot join a Windows domain unless its internal clock is in sync with the Domain Controller. To ensure that the ProxySG clocks are synchronized with the Domain Controller clock, use either of the following techniques:

- Specify the same NTP servers for the ProxySG appliances and the Domain Controller.
- Configure the ProxySG appliances to use the Domain Controller as the NTP source server.

The ProxySG NTP configuration options are located on the Configuration > General > Clock tab.

Step 2 - Join the ProxySG appliance to the Windows Domain

After you have synchronized the ProxySG appliance’s internal clock with the Domain Controller, you can join the appliance to the Windows Domain as follows:

1. From the ProxySG Management Console, select Configuration > Authentication > Windows Domain > Windows Domain.
2. Click New; the Add Windows Domain dialog displays.
3. Enter a Domain name alias and then click OK.
4. Click Apply and then click OK.
5. Select the domain Name you created. When you select it, the Details fields become active.
6. In the **DNS domain name** field, enter the DNS name for the Windows Active Directory domain. This is not the fully qualified domain name of the ProxySG.

   The ProxySG appliance must be able to resolve the DNS domain name you supply for the Active Directory domain or the appliance will not be able to join the domain. If DNS resolution fails, check your DNS configuration.

7. In the **SG host name** field, enter the hostname to use for this ProxySG appliance. Blue Coat recommends the appliance name or any name helpful for your recognition. The name you enter must be unique in your Active Directory.

8. Click **Join Domain**; the Join domain dialog displays.

9. Enter the primary domain access **Username** and **Password** in the format: username@dnsname. For example: administrator@blue9.acme.com. This account must have administrator privileges.
10. Click **OK**. The appliance displays a message indicating that the domain was successfully joined.

11. Click **OK** to close the dialog. The value in the **Joined** field changes to **Yes**.
Enable Kerberos in an IWA Direct Deployment

In an IWA Direct realm, Kerberos configuration is minimal because the appliance has its own machine account in Active Directory and it uses its account password to decrypt service tickets from clients. Therefore, there is no need for you to create a privileged Active Directory account or generate a service principal name (SPN) for the appliance (as is required with an IWA BCAAA realm).

To ensure that IWA uses the Kerberos protocol rather than downgrading to NTLM, you need to make sure that authentication requests are directed to the DNS name of the appliance’s Active Directory machine account name as follows:

1. Create a DNS “A” record for the ProxySG that resolves to the DNS name of the appliance’s Active Directory machine account name. For example, if you have an appliance named ProxySG1 with IP address 1.2.3.4 in the blue9 Active Directory domain at acme.com, you would create the following DNS record: ProxySG1.blue9.acme.com Host(A) 1.2.3.4

2. Ensure that client requests are directed to the DNS name for the ProxySG appliance’s Active Directory machine account:
   - **Explicit deployments**—Configure the explicit proxy settings on the client browser to point to this DNS name.
   - **Transparent deployments**—Set the Virtual URL in the realm configuration (on the IWA General tab) to this DNS name. In addition, make sure that the DNS name for the ProxySG appliance’s Active Directory domain is either included in the workstation’s list of imputing DNS suffixes or explicitly specified as part of IE’s local intranet zone. For example, if your AD domain DNS name is blue9.acme.com, then you would add *.blue9.acme.com to IE’s local intranet zone. See "Create an IWA Direct Realm" on the next page for details.
Create an IWA Direct Realm

The IWA realm contains the configuration settings that the ProxySG appliance needs to be able to perform IWA authentication, including how to connect to the Active Directory, which authentication protocols to support, how long to wait before timing out, and where to redirect transparent requests, if applicable. After you join the ProxySG appliance to the Windows domain, you can create the IWA Direct realm as follows:

1. Create the realm.
   a. Select Configuration > Authentication > IWA > IWA Realms.
   b. Click New.
   c. Enter a Realm name. The name can be 32 characters long and composed of alphanumeric characters and underscores. The name must start with a letter.
   d. In the Active Directory Connection field, select Direct.

   ![Info](This option will be grayed out if you have not yet joined the appliance to a Windows domain.)

   e. Click OK to close the dialog.
   f. To save your settings, click Apply.

2. Select the IWA Servers tab.
3. From the **Realm name** drop-down list, select the IWA realm you want to configure.

4. Specify the type of credentials to accept from the browser/user agent.

   By default, all credential types are allowed and the ProxySG appliance will try to use Kerberos (the default authentication method for Windows clients), but will automatically downgrade to a different challenge type depending on the browser/user agent capabilities.

   - **Allow Basic credentials**—Prompts the user for a username and password to authenticate the user against the Windows Active Directory.
   
   - **Allow NTLM credentials**—Uses an encrypted challenge/response that includes a hash of the password.
   
   - **Allow Kerberos credentials**—Uses a ticket containing an encrypted session key in place of a user name and password. If you select this option, NTLM is automatically selected as well; in the event that the browser/user agent and/or the ProxySG are not configured properly for Kerberos, the appliance will automatically downgrade to NTLM.

5. (Optional) If you are sharing a service principal name (SPN) across multiple ProxySG appliances in a load balancing configuration, click **Set credentials**, enter the **User name** and **Password** for an Active Directory account, and then click **OK**. For details, see "Using IWA Direct in an Explicit Kerberos Load..."
Integrate ProxySG Authentication with Active Directory Using IWA

Balancing/Failover Scenario* on page 54.

6. (Optional) To change the amount of time the appliance will wait for an authentication response before timing out, enter a new value in the **Timeout request after x seconds** field (default 60 seconds).

7. Click **Apply**.

8. Verify that you have configured the realm successfully.
   
   a. Click **Test Configuration**.
   
   b. When prompted, enter the username and password of a user in the Windows domain and then click **OK**.
   
   c. The appliance sends an authentication request to the configured server and then displays a message indicating whether the authentication succeeded or failed. If the test failed, go back and make sure you have configured the realm properly. If the test succeeds, the message also displays a list of groups to which the user belongs.
9. Select the **IWA General** tab.

10. Select the **Realm name**.

11. (Optional) By default, the ProxySG appliance displays the authentication realm name when prompting the user for authentication credentials. To change the name that is displayed when the ProxySG appliance challenges the user for credentials from the default realm name, enter a new value in the Display name field, up to a maximum of 128 characters. This field cannot be left empty.

12. (Optional) If you want to change how often the appliance reauthenticates a client, modify the refresh and timeout values.

   - **Credential refresh time**—(Basic credentials only) Specifies the amount of time the appliance will cache Basic credentials (username and password) and use these cached credentials to authenticate the user rather than sending another request to the authentication server. By default, basic credentials are good for 900 seconds (15 minutes).

   - **Surrogate refresh time**—After the appliance successfully authenticates a client, it caches the client’s IP address or a cookie (depending on the authentication mode that is in use) in its surrogate cache. If it receives subsequent requests from the same client during the surrogate refresh time, it uses the IP address or cookie in its cache to authenticate the user instead of sending a request to the authentication server. By default, the surrogate credential is good for 900 seconds (15 minutes).

   - **Inactivity timeout**—When a client request is successfully authenticated, the appliance establishes an active session with the client and as long as that session stays active, the appliance will not attempt to reauthenticate requests from that client. This setting specifies how long the client session can be inactive before the appliance terminates the session; subsequent requests from that client will require authentication. By default, the client can be inactive for 900 seconds (15 minutes).

     If the **Challenge user after logout** option is selected, the appliance will automatically challenge the client for credentials when the session becomes inactive. If you are using a challenge method that prompts the user for credentials, you may want to deselect this option.

   - **Rejected credentials time**—(Basic credentials only) Specifies whether to cache failed authentication attempts (bad password, expired account, disabled account, old password, or server down). If the client attempts to connect again during the rejected credentials time, the appliance will automatically reject the request for the specified period of time. Enter a value from 1 second (the default) to 10 seconds. Or, to disable this option, enter 0.

13. (Optional) Modify how the appliance uses cookie surrogates by modifying the Cookies settings. These settings are only applicable if you plan to use an authentication mode that uses cookie surrogates.

   - **Use persistent cookies**—By default, this option is deselected, which means that the appliance
will use session cookies when creating a cookie surrogate for a client. Session cookies are only valid during the current browser session and are deleted when the user closes the browser. Therefore, the ProxySG appliance must reauthenticate the client each time the user starts a new browser session. If you select this option, the appliance will use persistent cookies instead of session cookies. Persistent cookies are stored on the client system and are therefore not deleted at the end of the browser session. When using persistent cookies, the appliance will only need to reauthenticate a client when the cookie in its surrogate credential database expires.

- **Verify the IP address in the cookie**—By default, this option is selected, which means that the appliance will only accept a cookie from a client if the client IP matches the IP address in the surrogate cookie. To enable the appliance to accept cookies from IP addresses that do not match the address in the cookie—for example if you use DHCP—deselect this option.

14. **(Transparent proxy only) Specify the URL to which to redirect client requests that require authentication in the Virtual URL field.**

The way you configure the Virtual URL depends on what authentication method you are using:

- **NTLM**—The Virtual URL must contain a simple hostname that does not contain any dots (for example, use http://myproxy rather than http://myproxy.acme.com. This allows IE to recognize the URL as part of the Intranet zone rather than the Internet zone so that the browser will automatically return credentials when challenged rather than prompting the user.

  In addition, the Virtual URL must resolve to the IP address of the ProxySG appliance. To accomplish this, you must add an "A" record to your internal DNS server that associates the Virtual URL with the IP address of the ProxySG appliance.

- **Kerberos**—If you’re using Kerberos in a non-load balancing IWA Direct realm, the Virtual URL must be the DNS name of the ProxySG appliance in the Active Directory domain. Typically this will be the DNS name of the Active Directory domain prefixed with the ProxySG appliance machine account name. For example, sg.b1ue9.local1. If you do not use the Active Directory DNS name of the ProxySG as the Virtual URL, all authentication transactions will be downgraded to NTLM.

15. **(Optional) If you want to prompt the client for authentication credentials whenever the inactivity timeout expires, select the Challenge user after logout check box.**

16. **To save the realm configuration, click Apply.**
Validate the IWA Realm Configuration

After you configure an authentication realm on the ProxySG, you must verify that the ProxySG appliance can successfully connect to the authentication server and successfully authenticate a user as follows:

1. In the Management Console, select Configuration > Authentication > IWA > IWA Servers.
2. Click Test Configuration.
3. When prompted, enter the username and password of a user in the Windows domain and then click OK.
4. The appliance sends an authentication request to the configured server and then displays a message indicating whether the authentication succeeded or failed.
   - If the test fails, go back and make sure you have configured the realm properly.
   - If the test succeeds, the message also displays a list of groups to which the user belongs (IWA Direct) or a list of groups of interest to which the user belongs (IWA BCAA). A group of interest is a group that is referenced in ProxySG policy.

![Test Configuration](image)
Create a DNS Entry for the Authentication Domain

For IWA authentication to be successful, your clients must be able to resolve the fully qualified domain name of the ProxySG authentication URL to the IP address of the ProxySG appliance.

1. Create a DNS "A" record that associates the ProxySG authentication domain with the IP address of the ProxySG appliance. The fully qualified domain name (FQDN) that you use depends on whether you are using an explicit or transparent deployment:
   - **Explicit deployments**—Set the hostname in the DNS A record to match the ProxySG domain name specified in the browser's explicit proxy configuration.
   - **Transparent deployments**—Set the hostname in the DNS A record to match the Virtual URL in the IWA configuration.

2. Configure the client systems to use the DNS server where you created the "A" records for the ProxySG appliance.

3. From a client system, ping the hostname specified in the A record to ensure that it resolves to the IP address of the ProxySG appliance.
Configure the Web Browser for IWA

One of the main benefits of IWA is that it can provide a single sign-on experience for users because it uses the workstation login to authenticate users. When configured properly, the browser will provide the credentials to the ProxySG appliance transparently when challenged for NTLM or Kerberos credentials (the user will always be prompted for Basic authentication credentials).

IWA only works with Windows domain credentials. If users log in to the workstation using local credentials instead of domain credentials, they will be always be prompted whenever the ProxySG returns an authentication challenge.

Both Internet Explorer (IE) and Firefox can be configured to provide authentication credentials to the ProxySG appliance transparently:

- By default, IE will automatically provide authentication credentials to any site in the local Intranet zone. If the URL for your ProxySG appliance (explicit deployments) or virtual URL (for transparent deployments) contains a single hostname (that is, http://myproxy instead of http://myproxy.acme.com) you will not have to configure IE for IWA. If your ProxySG URL (virtual or explicit) does not fall within the Intranet zone, you will need to configure the IE to trust the URL. Keep in mind, however, that Kerberos deployments will require you to use the full URL for the Active Directory machine account (either the BCAA machine account for IWA BCAA or the ProxySG machine account for IWA direct). In these cases, you will need to add the full URL to the local Intranet zone.

- Firefox does not provide support for IWA by default and will therefore always need to be configured if you want to provide a single sign-on experience for your users.

For explicit proxy deployments, you must also make sure the browser is configured to send requests to the ProxySG appliance. See "Configure Client Web Browsers for Explicit Proxy" on page 37.

The procedure for configuring the browser to automatically provide login credentials to the ProxySG appliance is browser-specific:

- **Internet Explorer**
  1. Select **Tools > Internet Options**.
  2. Select the **Security** tab.
  3. Select the **Local Intranet** zone and click **Sites > Advanced**.
  4. Enter the fully qualified domain name of the ProxySG appliance (for explicit deployments) or the virtual URL (for transparent deployments) in the **Add this website to the zone** field and then click **Add > Close > OK**.
Integrate ProxySG Authentication with Active Directory Using IWA

5. Select the **Advanced** tab and make sure the **Security > Enable Integrated Windows Authentication** option is selected.

6. Click **OK** to save your changes and close the Internet Options dialog.

Firefox

1. In the browser's **Location** field, enter `about:config`.

2. Click **I'll be careful, I promise!** to continue to the `about:config` page.

3. To get the browser to trust the ProxySG appliance and negotiate authentication with it, you must set values for the following options: `network.automatic-ntlm-auth.trusted-uris`, `network.negotiate-auth.delegation-uris`, `network.negotiate-auth.trusted-uris`. For each option, complete the following steps:

   a. Locate the option you want to set by scrolling or entering the option name in the **Filter** field.

   b. Double-click the option to open the Enter string value dialog.

   c. Enter the fully-qualified domain name of the ProxySG appliance (for explicit deployments) or the virtual URL (for transparent deployments). If you have more than one ProxySG appliance that will challenge users for authentication credentials, separate the entries with commas.

   d. Click **OK**.
Configure Client Web Browsers for Explicit Proxy

When you deploy the ProxySG appliance explicitly, the appliance is not in the direct path of network traffic. To ensure that all Web requests are managed by the appliance, you must configure the Web browsers for all network users to point to the appliance.

There are two ways to configure client browsers for explicit proxy:

- Manually configure the Web browsers to send Web requests to the ProxySG appliance
- Automatically configure the Web browsers using PAC files
Configure the Web Browser to Use the Explicit Proxy

If you do not use PAC files to automatically configure network access information for clients in your network, you must manually configure the Web browser to send Web requests to the ProxySG appliance.

Typically, the browser proxy configuration requires the IP address or hostname of the ProxySG appliance and the port on which the ProxySG appliance will listen for traffic. The default port is 8080. The required hostname format (that is, whether you must provide a fully qualified DNS hostname or a short hostname) depends on the DNS configuration on your client systems.

The procedure for manual configuration varies by your Web browser version. Select the appropriate set of instructions from the list below:

- **Internet Explorer**
  1. Select Tools > Internet Options.
  2. Select the Connections tab.
  3. If you are using a LAN, click LAN Settings. If you are using a Dial-up or Virtual Private Network connection, click Add to set up the connection wizard.
  4. Make sure the Automatically detect proxy settings and Use automatic configuration script options are not checked.
  5. Select Use a proxy server for your LAN.
  7. For HTTP, enter the IP address of the ProxySG appliance, and add the port number; 8080 is the default.
  8. Select Use the same proxy server for all protocols.
  9. (Optional for non-administrative users, best practice, recommended when setting up the Web browser for ProxySG appliance administrators) Enter the ProxySG appliance IP address for Do not use the proxy server for addresses beginning with:

      This setting ensures that administrators are never locked out from access to the Management Console; requests that match the entries above are not intercepted by the ProxySG appliance.
  10. (Optional) If you do not want to intercept your local or internal Web servers, enable Bypass proxy server for local addresses and enter the IP addresses.
  11. Click OK to save your settings and close all open dialogs.

- **Firefox**
  1. Select Tools > Options.
  2. Select Advanced icon.
  3. Select the Network tab.
4. Click **Settings** under the Connection panel.

5. Select **Manual proxy configuration**.

6. In the **HTTP Proxy** field, enter the ProxySG appliance’s IP address and port number; 8080 by default.

7. Select **Use this proxy server for all protocols**.

8. (Optional for non-administrative users, Best practice, recommended when setting up the Web browser for ProxySG appliance administrators) Enter the IP address of the ProxySG or the subnet to exclude in the **No proxy for** field.

9. Click **OK** to save your settings and close all open dialogs.
Set Up the Explicit Proxy to Use a PAC File

The Proxy Auto Configuration (PAC) file is a means of controlling user access to the Internet or the intranet. A PAC file is a JavaScript file with a .pac extension that contains instructions on when and whether the Web browser should use the ProxySG appliance for retrieving requested content. Network administrators like to use PAC files because they are centrally administered, and easy to update.

If you already have a PAC file on a Web server in your network, add the URL for this file to the Web browser configuration for all clients in your network. Defining the location of the PAC file enables the Web browser to discover and download the proxy configuration instructions for handling Web requests.

To define the location of the PAC file on the Web browser and test the configuration:

1. Launch the Web browser.
2. Add the URL for the PAC file in the Web browser. Follow the instructions for your Web browser:

   **Internet Explorer**
   a. Select **Tools > Internet Options > Connections > LAN Settings**.
      
      If you are using a Dial-up or Virtual Private Network connection, select the necessary connection and click the **Settings** button.
   b. Select the **Use automatic configuration script** option and add the URL in the **Address** field.
   c. Click **OK** to save your changes.

   **Firefox**
   a. Select **Tools > Options > Advanced > Network > Connection Settings**.
   b. Select **Automatic proxy configuration URL** and add the URL in the corresponding input field.
   c. Click **OK** to save your changes.

Web browsers typically cache the PAC file. To test modifications to your PAC file settings, you must:

- **Reload** the PAC file in Firefox.
- Close all browser sessions and clear the cache in IE.

**Safari on Macintosh**

a. Select **Apple menu > System Preferences**.
b. Select **Internet & Wireless > Network**.
c. Select Advanced > Proxies.

d. Select Automatic Proxy Configuration and add the URL for the location of the PAC file in the input field.

e. Click Apply Now.

3. Verify that your Web requests are being intercepted by the ProxySG.

a. Enter a URL and click through a few links on the Web page. For example, go to www.bluecoat.com and navigate through the website.

b. Launch the ProxySG Management Console.

c. Select Statistics > Summary > Efficiency.

d. Verify that the ProxySG appliance displays **Explicit HTTP** traffic in the Savings panel.

<table>
<thead>
<tr>
<th>Service</th>
<th>Bytes Saved Last Hour</th>
<th>Percent Savings</th>
</tr>
</thead>
<tbody>
<tr>
<td>FF-Mgmt</td>
<td>1.05 KB</td>
<td>0.99% (1.01x)</td>
</tr>
<tr>
<td>Explicit HTTP</td>
<td>563 B</td>
<td>n/a</td>
</tr>
</tbody>
</table>
Create an IWA Authentication Policy

After you verify that BCAAA and the ProxySG appliance can successfully authenticate users against your Active Directory (AD), you must create the policy that enables authentication on the appliance. You can create a basic authentication policy that simply requires all requests to be authenticated and allows or denies access upon successful authentication. Or you can define more complex policies with rules that apply to a specific source address, subnet, port, user agent, or request header. Or, you can define different rules for different destinations. You can also create policies that allow access to guest users.

You can additionally create authorization policies that restrict access by user or group membership.

This topic shows how to create a policy using the Visual Policy Manager (VPM). You can also create policy using the Content Policy Language (CPL). Refer to the Content Policy Language Reference for details.

Note that you must create an IWA realm before you can define the corresponding authentication policy.

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.

2. Create the policy rule that enables the ProxySG appliance to authenticate client requests.
   b. Enter a Layer Name or accept the default name and then click OK. The first policy rule displays with default settings.

3. Configure the authentication policy settings.
   a. In the Action column of the first row, right-click and then select Set. The Set Action Object dialog displays.
   b. Click New and then select one of the following authentication objects:
      - **Authenticate**—Use this option if you do not need to log user IDs for denied requests. With this option, if policy causes a request to be denied before the user is authenticated, the user ID associated with the request will not be available for access logging.
      - **Force Authenticate**—Use this option to force the appliance to authenticate requests even if they are denied before authentication would normally occur. This ensures that user IDs are available for access logging.
If you plan to create a guest authentication policy, create a combined object that contains the Authenticate object and a Permit Authentication Error object (be sure to select All Except User Credentials Required).

c. (optional) Specify a Name for the authentication object.

d. Select the IWA Realm from the drop-down list.

e. Select the authentication mode from the Mode drop-down list. Although you can select Auto to have the ProxySG appliance automatically choose an authentication mode, it is usually better to make a selection that is appropriate for your deployment as follows:

- **Explicit deployments**—Select Proxy or Proxy IP. The Proxy IP mode reduces the load on the network because it uses an IP surrogate to reauthenticate clients that have already successfully authenticated.

- **Transparent deployments**—Select Origin Cookie Redirect. This mode redirects the client to the virtual URL for authentication and uses a cookie surrogate to reauthenticate clients that have already successfully authenticated. The appliance will automatically downgrade to the Origin IP Redirect mode for user agents that do not support cookies.

f. Click OK to close the Add Authenticate Object or Add Force Authenticate object dialog.

g. Click OK to close the Set Action Object dialog.

4. (optional) Restrict authentication to a subset of client requests, based on source or destination request attributes.

The default settings in the policy rule will cause the ProxySG appliance to authenticate all client requests. You can set the Source and/or Destination columns to restrict authentication to a specified subset of requests. For example,

a. In the Source or Destination column of the first row, right-click and then select Set. The Set Source Object or Set Destination object dialog displays.

b. Click New and then select an object that represents the subset of requests you want to authenticate. After you select an object, you will be prompted to provide details. For example, if you choose the Client IP Address/Subnet object, you will be prompted for an IP address and subnet mask/prefix to which this rule will apply.

When you first deploy your authentication policy, you may want to limit authentication to the source address of a test workstation or subnet. This allows you to identify and troubleshoot any configuration issues before rolling the policy out into production.

5. (optional) Add additional policy rules to refine your authentication policy.

A single Web Authentication Layer rule with the authenticate action is all you need to enable
Integrate ProxySG Authentication with Active Directory Using IWA

authentication. However, there may be some cases where you want to bypass authentication for certain requests and enable it for others. For example, you may have a certain client, subnet, or URL on which you do not require authentication or you may have some custom applications that do not know how to handle authentication requests. In this case, you would add an additional rule to your Web Authentication Layer policy to instruct the ProxySG appliance how to handle the exceptions.


b. Specify which client requests this rule applies to by setting the Source or Destination columns.

c. Specify what the ProxySG appliance should do with requests that match the source and/or destination setting you have defined by right-clicking in the Action column of the row, and selecting Set.

   ■ If you want to authenticate requests that match the specified source and/or destination request settings you have defined, click New and select Authenticate and click OK.

   ■ If you want to bypass authentication for the matching requests, select Do Not Authenticate and click OK.

d. Prioritize the order in which you want the ProxySG appliance to enforce the rules by selecting the rule you want to move and clicking Move up or Move down. The ProxySG appliance evaluates the rules in the order in which they appear in the policy layer. As soon as it finds a rule that matches the request, it will enforce the specified action (in this case, either to authenticate or not authenticate the request). Therefore, you should put more specific rules above general rules. For example, if you have a two rules in your policy—one that is set to authenticate requests from any source or destination and one that is set to not authenticate requests from a specific subnet—you would put the one that bypasses authentication in front of the general rule that matches all requests.

6. Install the authentication policy.

   a. Click Install policy.

   b. Click OK to acknowledge that the policy was successfully installed.
Create an IWA Guest Authentication Policy

A guest authentication policy enables users who do not have a Windows domain account on your network to access Internet resources.

To create an IWA guest authentication policy:

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.

2. Create a Web Authentication Layer for authenticating client requests for your domain users.
   See "Create an IWA Authentication Policy" on page 74 for instructions.

3. Create a second Web Authentication Layer to provide guest access.
   b. Enter a Layer Name to distinguish this layer from the previous layer (for example, Guest Authentication) and then click OK. The first policy rule displays with default settings.

4. Configure the source.
   a. In the Source column of the first row, right-click and then select Set. The Set Source Object dialog displays.
   b. Click New and then select User Authentication Error. The Add User Authentication Error Object dialog displays.
   c. Select Any errors and click OK twice to save the source object and close the dialogs.

5. Configure the action.
   a. Right-click the Action column and then select Set. The Set Action Object dialog displays.
   b. Click New and then select the Authenticate Guest object. The Add Authenticate Guest object dialog displays.
   c. Select Use realm and then select your IWA realm from the drop-down list.
   d. Enter a Guest Username. This will be the name that appears in your access log whenever guest access is granted; it does not correlate to an Active Directory user account.
   e. Click OK twice to save the Action object and close the dialogs.

6. Make sure that the Web Authentication Layer for your guest policy is positioned after the your main Web Authentication Layer.
Integrate ProxySG Authentication with Active Directory Using IWA

To re-order the layers, select Edit > Reorder Layers.

7. Install the authentication policy.
   a. Click Install policy.
   b. Click OK to acknowledge that the policy was successfully installed.
Create an IWA Authorization Policy

One of the benefits of IWA is that it automatically returns authorization information for a user in response to an authentication request. You do not have to perform any additional configuration to get authorization to work. After successfully authenticating a user, the appliance receives a list of all groups (IWA Direct) or groups of interest (IWA BCAAA) to which the user belongs.

This topic shows how to create a policy using the Visual Policy Manager (VPM). You can also create policy using the Content Policy Language (CPL). Refer to the Content Policy Language Reference for details.

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.

2. Create a Web Access Layer.
   b. Enter a Layer Name or accept the default name and then click OK.

3. Specify the user or group to authorize (the source).
   a. In the Source column of the first row, right-click and then select Set. The Set Source Object dialog displays.
   b. Click New and then select the type of Active Directory object this rule will authorize:
      - To create a rule for authorizing a group, select Group. The Add Group Object dialog displays.
      - To create rule for authorizing a user, select User. The Add User Object dialog displays.
   c. Select the IWA realm from the Authentication Realm drop-down list.
   d. Specify the name of the Active Directory user or group that rule will authorize:
      - If you know the name of the Active Directory user or group, enter it in the Group or User field.
      - If you don't know the Active Directory name of the user or group, click Browse and select the group from the IWA Browser.
   e. Click OK to close the Add Group Object or Add User Object dialog.
   f. Click OK to close the Set Source Object dialog.

4. Specify whether to allow or deny requests from the specified user or group.
Integrate ProxySG Authentication with Active Directory Using IWA

a. Right-click the **Action** column.

b. Select one of the following options:

   - **Allow**—Select this option if the default proxy policy for the appliance is set to deny proxy access through the ProxySG appliance. This is the default in a secure web gateway deployment.

   - **Deny**—Select this option if the default proxy policy for the appliance is set to allow proxy transactions.

   If you aren't sure what the default proxy policy is set to on your appliance, go to **Configuration > Policy > Policy Options**.

5. (Optional) Define any additional parameters that you want this rule to enforce.

6. To create additional authorization rules, repeat Steps 3 through 5.

7. Install the policy.

   a. Click **Install policy**.

   b. Click **OK** to acknowledge that the policy was successfully installed.
Verify Kerberos Authentication

Even if you configure IWA to allow Kerberos, Kerberos will only be used if configured properly. If the ProxySG appliance cannot successfully negotiate Kerberos with a client, it will silently downgrade to use NTLM authentication. Because this happens behind the scenes, you may not know whether you are using Kerberos or NTLM.

1. To verify that the ProxySG appliance is attempting to negotiate Kerberos authentication, take a packet capture on the client and look for the NEGOTIATE message. The client uses the NEGOTIATE message to communicate the type of authentication it supports to the ProxySG appliance. This will show up as either a WWW-Authenticate: NEGOTIATE (transparent) or Proxy-Authenticate: NEGOTIATE message. Note that this message alone does not indicate that Kerberos will be used.

2. To verify that the client is using Kerberos, take a packet capture from the client and use the display filter to view Kerberos requests. If Kerberos authentication is in use you will see Kerberos requests and responses between the client and the Domain Controller as well as the Kerberos ticket in the GET
Integrate ProxySG Authentication with Active Directory Using IWA request.
Enable IWA Authentication for SSL Traffic in a Transparent Deployment

After you configure IWA, you must complete the following additional tasks if you are using a transparent proxy deployment and you want to authenticate SSL traffic:

1. Make sure you have an SSL license.

   Although some ProxySG appliance models include an SSL license, other models require that you purchase and install an add-on license. To see whether you have a valid SSL license, launch the ProxySG Management Console and select Maintenance > Licensing > View. You should check that SSL displays in the list of licensed components.

2. Create an HTTPS Reverse Proxy service to listen for authentication requests.
   a. Select Configuration > Services > Proxy Services.
   b. Click New Service.
   c. Enter a unique Name for the service to identify it as your IWA authentication service.
   d. Select HTTPS Reverse Proxy from the Proxy drop-down list.
   e. Select the Keyring that you want to use to establish SSL sessions for this service.
Integrate ProxySG Authentication with Active Directory Using IWA

To configure the listening port, click New and then configure the service as follows:

- Set **Destination Address** to **Explicit**.
- Set the **Port range** to the port number on which you want this service to listen for incoming authentication requests. Note that you will need to use this same port number in the Virtual URL you define for the realm.
- Set the **Action** to **Intercept**.
- Click **OK** to save the listener settings.

If necessary, configure your firewall to allow traffic between the client workstations and the ProxySG appliance on the port you just configured.

3. Create an IWA realm for authenticating your HTTPS traffic.

You create the realm the same way that you created the IWA realm for your HTTP traffic, with the difference being the URL to which authentication requests are directed:

- Create the IWA realm as described in "Create an IWA Direct Realm" on page 28 or "Create an IWA BCAA Realm" on page 60.

- On the **IWA General** tab, set the **Virtual URL** to a URL that points to the HTTPS Reverse Proxy Service you created for IWA authentication. For example, if you configured your HTTPS Reverse Proxy service to listen on port 4433, you would enter a URL such as `https://myproxy:4433`.

- Make sure your **DNS server** is set up to resolve the hostname to the IP address of the ProxySG appliance.

4. Create the policy rule to enable the appliance to intercept HTTPS traffic.

- Launch the Visual Policy Manager (VPM) by selecting **Configuration > Policy > Visual Policy Manager > Launch**.

- Select **Policy > Add SSL Intercept Layer**.

- Enter a **Layer Name** or accept the default name and then click **OK**. The first policy rule displays with default settings.

- Right-click the **Action** column and select **Set**.

- Click **New** and select **Enable HTTPS Interception**.

- Check the **Issuer Keyring** check box and select the keyring you specified in the HTTPS Reverse Proxy service settings.

- Click **OK**.
5. Create the policy rule that enables the ProxySG appliance to authenticate client HTTPS requests.
   b. Enter a Layer Name or accept the default name and then click OK. The first policy rule displays with default settings.
   c. In the Action column of the first row, right-click and then select Set. The Set Action Object dialog displays.
   d. Click New and then select Authenticate.
   e. Select the IWA Realm from the drop-down list. Make sure you select the realm you created for your HTTPS traffic.
   f. Select the authentication mode from the Mode drop-down list. For transparent authentication, you will usually want to select Origin Cookie Redirect. This mode redirects the client to the virtual URL for authentication and uses a cookie surrogate to reauthenticate clients that have already successfully authenticated. The appliance will automatically downgrade to the Origin IP Redirect mode for user agents that do not support cookies.
   g. Click OK to close the Add Authenticate Object or Add Force Authenticate object dialog.
   h. Click OK to close the Set Action Object dialog.

6. Install the policy rules you created.
   a. Click Install policy.
   b. Click OK to acknowledge that the policy was successfully installed.
Integrate ProxySG Authentication with Active Directory Using IWA

Using IWA Direct in an Explicit Kerberos Load Balancing/Failover Scenario

In a standard IWA Direct Kerberos deployment, the Kerberos service principal name (SPN) of the appliance is the appliance’s own Active Directory machine account name. However, in a load balancing configuration, multiple ProxySG appliances must be able to decrypt the service tickets from the clients. For this reason, all ProxySG appliances in a load balancing group must share the same SPN. This will not work if each appliance uses its own machine account to process Kerberos authentication requests. In this case, you must create a new Active Directory account and use it to create a SPN that can be used by all appliances in the group. To deploy Kerberos in this configuration you must:

1. Set up a load balancing device in front of your appliances and designate a virtual IP address to use for all explicit proxy request. The load balancing device will then forward the requests to the ProxySG appliances in the group based on the load balancing rules you have defined.

2. Create a DNS entry for the device that resolves to this IP address. Note that the DNS name that you use must not map to an existing machine account name in Active Directory or the ProxySG appliance will not be able to authenticate Kerberos service tickets and authentication will fail.

3. Create an Active Directory account for the Kerberos load balancing user. This account does not need any special privileges. You will create the SPN using this account and the ProxySG appliances will use the account credentials to decrypt the service tickets from clients.

4. Use the Active Directory account you just created to create an SPN for the load balancing group as follows:

   a. Open a command prompt as administrator on the Domain Controller.

   b. Enter the following command:

   ```
   setspn -A HTTP/<LoadBalancer_FQDN> <AD_Account_Name>
   ```

   where `<LoadBalancer_FQDN>` is the fully qualified domain name (FQDN) of the load balancing device and `<AD_Account_Name>` is the name of the Active Directory user you created for the load balancing group. Note that this command is case-sensitive.

   For example, if the FQDN of the load balancing device is `lb.acme.com` and the Active Directory account name you created is `KerberosLBUser`, you would enter the following command:

   ```
   setspn -A HTTP/lb.acme.com KerberosLBUser
   ```

   Do not assign the same SPN to multiple Active Directory accounts or the browser will fall back to NTLM without providing any warning or explanation. To list all SPNs that are currently registered on an account, use the `setspn -L <AD_Account_Name>` command. If you find a duplicate, remove the extraneous SPN using the `setspn -D <SPN>` command.
5. On each ProxySG, create an IWA Direct realm. When configuring the realm on each appliance, you must provide the credentials for the AD Kerberos load balancing user you created. On the IWA Servers tab click Set credentials, enter the AD account User name and Password, and then click Update. Note that the user name you provide must be in the User Principal Name (UPN) format, for example admin@acme.com.

6. Configure the client browser explicit proxy settings to point to the FQDN of the load balancing device.
Preparing for a Kerberos Deployment

Kerberos is the recommended challenge protocol for IWA because it is more secure than NTLM or Basic and it puts the least load on your network.

To ensure that IWA uses the Kerberos protocol rather than downgrading to NTLM, you must make sure that authentication requests are directed to the Kerberos service associated with the ProxySG appliance. The way you configure this depends on how your IWA realm is connecting to the Active Directory as follows:

- "Enable Kerberos in an IWA Direct Deployment" on page 27
- "Enable Kerberos in an IWA BCAA Deployment" on page 58
Configure IWA BCAAA

To configure IWA BCAAA authentication, you must complete the following tasks:

1. Install BCAAA on a Windows server that is a member of the Windows domain. Refer to the [BCAAA Service Requirements](#) document for more information about installing BCAAA.

2. (Kerberos only) If you plan to use Kerberos authentication, register BCAAA as a Kerberos service. See "Enable Kerberos in an IWA BCAAA Deployment" on the next page.

3. Configure the ProxySG appliance for IWA. See "Create an IWA BCAAA Realm" on page 60.

4. (optional) Set up secure communication between the ProxySG appliance and BCAAA. See "Enable SSL Between BCAAA and the ProxySG Appliance" on page 64.

5. Verify that the appliance can successfully authenticate an Active Directory user using the IWA realm you created. See "Validate the IWA Realm Configuration" on page 70.

6. Create a DNS entry for the ProxySG authentication URL. See "Create a DNS Entry for the Authentication Domain" on page 71.

7. Configure the client browsers for single sign-on. See "Configure the Web Browser for IWA" on page 72.

8. Create the policy rules that will enforce authentication and, optionally, authorization. See "Create an IWA Authentication Policy" on page 74.

9. (Kerberos only) Verify that Kerberos is configured properly. See "Verify Kerberos Authentication" on page 81.

10. (optional) Enable authentication for HTTPS traffic. This step is only required if you want to authenticate HTTPS traffic in a transparent deployment. Explicit deployments can authenticate HTTPS traffic without any additional configuration provided that you have a valid SSL license installed. See "Enable IWA Authentication for SSL Traffic in a Transparent Deployment" on page 83.
Enable Kerberos in an IWA BCAAAA Deployment

For the BCAAAA service to participate in an IWA Kerberos authentication exchange, it must share a secret with the Kerberos server (called a KDC) and have registered an appropriate Service Principal Name (SPN).

To prepare for a BCAAAA Kerberos deployment:

1. On your DNS server, create a DNS “A” record for the ProxySG that resolves to the appliance’s Fully Qualified Domain Name (FQDN). Keep in mind that the DNS name you choose must not match the Active Directory machine account name for the appliance. For example, rather than using the machine name, you might create a DNS entry for the appliance using a name such as bcaaaUser1. Supposing the appliance is in the acme.com domain and has an IP address of 1.2.3.4, you would create the following DNS record:

   bcaaaUser1.acme.com Host(A) 1.2.3.4

2. Create a domain user account for the BCAAAA service in the Windows Active Directory (AD).

3. Install BCAAAA. Refer to the BCAAAA Service Requirements document for more information about installing BCAAAA.

4. Configure the BCAAAA Windows service on the system where you installed BCAAAA to log on using the domain user account you created for it in Step 2 rather than using the local system account.

5. In the Local Security Policy of the server on which BCAAAA is running, modify the user rights assignment for the BCAAAA domain user to have the following rights:

   - Full access to the directory where you installed BCAAAA
   - Act as part of the operating system
   - Log on as a service

6. Register the Kerberos Service Principal Name (SPN) for the ProxySG appliance:

   a. Log in to the Domain Controller using an account with administrative access and open a command prompt.

   b. Enter the following case-sensitive command:

      ```
      setspn -A HTTP/<FQDN_of_ProxySG> <AD_Account_Name>
      ```

      Where `<FQDN_of_ProxySG>` is the FQDN of the ProxySG appliance as specified in the browser’s explicit proxy configuration (explicit deployments) or in the Virtual URL setting in the IWA realm configuration (transparent deployments) and `<AD_Account_Name>` is the name of the BCAAAA domain service account.
Integrate ProxySG Authentication with Active Directory Using IWA

For example:

```
setspn -A HTTP/bcaaaUser1.acme.com AcmeDomain\BCAAAuser
```

Do not assign the same SPN to multiple Active Directory accounts or the browser will fall back to NTLM without providing any warning or explanation. To list all SPNs that are currently registered on an account, use the `setspn -L <AD Account Name>` command. If you find a duplicate, use the `setspn -D <SPN>` command to remove the duplicate SPN.
Create an IWA BCAA Realm

After you install BCAA, you must configure the appliance to communicate with it. On the ProxySG appliance, the settings required for the appliance to communicate with BCAA are contained in a realm. To enable IWA BCAA authentication, you must create an IWA realm and configure it to work with your BCAA server.

1. Create the IWA realm and configure it to communicate with the BCAA server(s).
   a. In the ProxySG Management Console, select **Configuration > Authentication > IWA > IWA Realms**.
   b. To add a new IWA realm, click **New**.
   c. When prompted, enter a **Realm name**.
   d. In the **Primary server host** field, enter the hostname or IP address of the server where you installed BCAA. In addition, if you configured BCAA to use a port other than the default (16101), change the value in the **Port** field to match what you configured on BCAA.
      
      If you plan to secure communication between the appliance and BCAA, use a host name rather than an IP address. The DNS server that the appliance is configured to use must be able to resolve the hostname.
   e. Click **OK**. The realm you just created is added to the **IWA Realms** tab.
   f. Select the **IWA Servers** tab and then select the **Realm name** to configure.
   g. (Optional) If you have installed and configured a second BCAA server for failover, enter the **Alternate server host** and **Port** values in the **Servers** section.
   h. (Optional) To change the amount of time the appliance will wait for an authentication response from BCAA before timing out, enter a new value in the **Timeout request after x seconds** field (default 60 seconds).

2. Specify the type of credentials to accept from the browser/user agent.

   By default, all credential types are allowed and the ProxySG appliance will try to use Kerberos (the default authentication method for Windows clients), but will automatically downgrade to a different challenge type depending on the browser/user agent capabilities.

   - **Allow Basic credentials**—Prompts the user for a username and password to authenticate the user against the Windows Active Directory. Because the username and password are sent in plaintext, it is important to enable SSL between BCAA and the ProxySG appliance if you allow Basic authentication.
Integrate ProxySG Authentication with Active Directory Using IWA

- **Allow NTLM credentials**—Uses an encrypted challenge/response that includes a hash of the password. Because the plaintext username and password are not sent across the wire, this method is more secure than Basic authentication.

- **Allow Kerberos credentials**—Uses a ticket containing an encrypted session key in place of a user name and password. This is the most secure method because it establishes mutual authentication between the client and the server using an encrypted shared key. However, if you select this option, NTLM is automatically selected as well; in the event that the browser/user agent and/or the BCAA server are not configured properly for Kerberos, the ProxySG appliance will downgrade to NTLM.

3. Verify that you have configured the realm successfully.
   a. Click **Test Configuration**.
   b. When prompted, enter the username and password of a user in the Windows domain and then click **OK**.
   c. The appliance sends an authentication request to the configured server and then displays a message indicating whether the authentication succeeded or failed. If the test failed, go back and make sure you have configured the realm properly. If the test succeeds, the message also displays a list of groups to which the user belongs.

4. (Optional) Modify the refresh and timeout values on the **IWA General** tab if you want to change how often the ProxySG appliance reauthenticates a client.
   - **Credential refresh time**—(Basic credentials only) Specifies the amount of time the ProxySG appliance will cache Basic credentials (username and password) and use these cached credentials to authenticate the user rather than sending another request to BCAA. By default, basic credentials are good for 900 seconds (15 minutes).
   - **Surrogate refresh time**—After the ProxySG appliance successfully authenticates a client, it caches the client’s IP address or a cookie (depending on the authentication mode that is in use) in its surrogate cache. If it receives subsequent requests from the same client during the
Integrate ProxySG Authentication with Active Directory Using IWA

Surrogate refresh time, it uses the IP address or cookie in its cache to authenticate the user instead of sending a request to BCAA. By default, the surrogate credential is good for 900 seconds (15 minutes).

- **Inactivity timeout**—When a client request is successfully authenticated, the ProxySG appliance establishes an active session with the client and as long as that session stays active, the ProxySG appliance will not attempt to reauthenticate requests from that client. This setting specifies how long the client session can be inactive before the ProxySG appliance terminates the session; subsequent requests from that client will require authentication. By default, the client can be inactive for 900 seconds (15 minutes).

  If the **Challenge user after logout** option is selected, the ProxySG appliance will automatically challenge the client for credentials when the session becomes inactive. If you are using a challenge method that prompts the user for credentials, you may want to deselect this option.

- **Rejected credentials time**—(Basic credentials only) Specifies whether to cache failed authentication attempts (bad password, expired account, disabled account, old password, or server down). If the client attempts to connect again during the rejected credentials time, the ProxySG appliance will automatically reject the request for the specified period of time. Enter a value from 1 second (the default) to 10 seconds. Or, to disable this option, enter 0.

5. (Optional) Modify how the appliance uses cookie surrogates by modifying the **Cookies** settings on the **IWA General** tab. The cookie settings are only applicable if you plan to use an authentication mode that uses cookie surrogates.

- **Use persistent cookies**—By default, this option is deselected, which means that the ProxySG appliance will use session cookies when creating a cookie surrogate for a client. Session cookies are only valid during the current browser session and are deleted when the user closes the browser. Therefore, the ProxySG must reauthenticate the client each time the user starts a new browser session. If you select this option, the appliance will use persistent cookies instead of session cookies. Persistent cookies are stored on the client system and are therefore not deleted at the end of the browser session. When using persistent cookies, the ProxySG appliance will only need to reauthenticate a client when the cookie in its surrogate credential database expires.

- **Verify the IP address in the cookie**—By default, this option is selected, which means that the ProxySG appliance will only accept a cookie from a client if the client IP matches the IP address in the surrogate cookie. To enable the appliance to accept cookies from IP addresses that do not match the address in the cookie—for example if you use DHCP—deselect this option.

6. (Transparent proxy only) Specify the URL to which to redirect client requests that require authentication in the **Virtual URL** field.

  For best results, the virtual URL you specify must:
- Contain a simple hostname that does not contain any dots (for example, use http://myproxy rather than http://myproxy.acme.com. This allows IE to recognize the URL as part of the Intranet zone rather than the Internet zone so that the browser will automatically return credentials when challenged rather than prompting the user.

-Resolve to the IP address of the ProxySG appliance. To accomplish this, you must add an "A" record to your internal DNS server that associates the virtual URL with the IP address of the ProxySG appliance.

7. (Optional) If you want to prompt the client for authentication credentials whenever the inactivity timeout expires, select the **Challenge user after logout** check box.

8. Click **Apply**.
Enable SSL Between BCAAAA and the ProxySG Appliance

By default, transactions between BCAAAA and the ProxySG appliance are not encrypted. You can secure the transactions between BCAAAA and the ProxySG by enabling SSL on this connection as follows:

1. Configure the BCAAAA server for SSL.

   You can do this either during the BCAAAA installation process, if you haven't yet installed it, or after installation by editing the bcaaa.ini file, which is by default installed to the C:\Program Files\BlueCoat Systems\BCAAA.

   The following table shows the configuration settings for both methods of configuring BCAAAA:

<table>
<thead>
<tr>
<th>BCAAAA Installation SSL Settings</th>
<th>bcaaa.ini SSL Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL Requirements—Select Permitted or Required.</td>
<td>UseSSL=1</td>
</tr>
<tr>
<td>Certificate Subject—Enter the hostname of the server where you are installing BCAAAA; do not use the IP address. Your DNS server must be able to resolve the hostname you supply.</td>
<td>CertificateSubject=&lt;BCAAA_server_hostname&gt;</td>
</tr>
<tr>
<td>Save the automatically generated certificate in the certificate store?—Select Yes. Note that this option only appears if the BCAAAA installation generated a new self-signed certificate.</td>
<td>If you did not generate a certificate during the BCAAAA installation process, you must obtain one for the server and add it to the certificate store before you can configure SSL. Or, re-run the BCAAAA setup and allow it to create a certificate and store it in the local certificate store.</td>
</tr>
<tr>
<td>Require the ProxySG to provide a valid certificate in order to connect?—Select No.</td>
<td>VerifySG=0</td>
</tr>
</tbody>
</table>

2. Export the BCAAAA CA server certificate.

   a. From the BCAAAA server, click Start > Run. The Run dialog opens.

   b. To launch the Microsoft Management Console (MMC), enter MMC in the Open field and then click OK.

   c. Select File > Add/Remove Snap-in. The Add/Remove Snap-in dialog displays.

   d. Click Add. The Add Standalone Snap-in dialog displays.

   e. Select Certificates from the Snap-in list and click Add. The Certificates snap-in wizard starts.

   f. Select Service Account and then click Next.
g. Select Local computer and then click Next.

h. From the Service account list, select the account you created for BCAA and then click Finish and then click Close.

i. Click OK to save your changes and close the Add/Remove Snap-in dialog.

j. In the list of certificate elements, select BCAA > Personal > Certificates and then double-click to open the certificate that corresponds to the hostname that you specified during the BCAA installation.

k. Select Details > Copy to File. The Certificate Export Wizard starts.

l. For the export file format, select Base-64 encoded X.509 (.CER) and then click Next.

m. On the Files to Export screen, Browse to a location that is accessible from the system from which you administer the ProxySG appliance, enter a File name to save the certificate as, click Save, and then click Next.

n. Click Finish and then click OK.

o. Close the MMC console.

p. Restart the BCAA services.

3. Import the BCAA CA certificate into the ProxySG appliance.

a. From the system from which you administer the ProxySG appliance, browse to the file that contains the certificate you extracted from the BCAA server in Step 2m. Open the file using a text editor (such as Notepad) and copy the contents to your Windows clipboard.

b. From the ProxySG Management Console, select Configuration > SSL > CA Certificates.

c. Click Import.

d. Enter a name for the new certificate (for example, BCAA) in the CA Cert Name field.

e. Paste the certificate you extracted from the BCAA server into the CA Certificate PEM field, making sure to include the BEGIN CERTIFICATE and END CERTIFICATE.

f. Click OK. The BCAA CA certificate gets added to the bottom of the list of CA certificates.

g. Click Apply.

4. Add the CA certificate to the CA Certificate List (CCL) that is associated with the device profile you want the ProxySG appliance to use when connecting to BCAA.

When you create an authentication realm and enable SSL, the default device profile is selected by default. This device profile uses the browser-trusted CCL by default. Therefore, the easiest way to associate the BCAA CA certificate with the browser-trusted CCL and use the default device profile as follows:
Integrate ProxySG Authentication with Active Directory Using IWA

a. In the Management Console, select **Configure > SSL > CA Certificate List**.

b. Select the **browser-trusted** CA Certificate List and click **Edit**. The Edit CA Certificate List dialog displays.

c. Select the BCAAA CA certificate you just imported from the list on the left and then click **Add**. The certificate entry moves to the bottom of the list on the right.

d. Click **OK** and then click **Apply**.

5. Configure the ProxySG appliance to connect to BCAAA using SSL.

a. Make sure the field that specifies the BCAAA host is set to the DNS name of the server and that it matches the CN name of the certificate you specified when you installed BCAAA.
   
   ○ For IWA realms, you configure the BCAAA server name in the **Servers** section of the **IWA Servers** tab.
   
   ○ For Windows SSO and Novell SSO realms, you set the BCAAA server name in the **Host** field on the **Agents** tab.

b. Select the **Enable SSL** check box.

c. Select the **SSL device profile** to use when connecting to BCAAA over SSL. Make sure the device profile you select has been configured to trust the BCAAA CA as described in Step 4.

   The **Enable SSL** and **SSL device profile** fields are located on the **IWA Servers** tab for IWA realms and on the **Agents** tab for other realms.

d. Click **Apply**.
Configure Mutual SSL Between BCAAAA and the ProxySG

With mutual authentication, both the client (the ProxySG appliance in this case) and the server (BCAAA) must provide a valid certificate before the secure channel can be established. Therefore, to set up mutual authentication, both the client and the server must have a valid certificate and each must have the CA certificate for the other. In addition, you must enable mutual authentication on the BCAAAA server.

1. Configure the BCAAAA server for SSL.

   You can do this either during the BCAAAA installation, if you haven’t yet installed it, or after installation by editing the bcaaa.ini file, which is by default installed to the C:\Program Files\Blue Coat Systems\BCAAA.

   The following table shows the configuration settings for both methods of configuring BCAAAA:

<table>
<thead>
<tr>
<th>BCAAAA Installation SSL Settings</th>
<th>bcaaa.ini SSL Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSL Requirements</strong>—Select Permitted or Required.</td>
<td>UseSSL=1</td>
</tr>
<tr>
<td><strong>Certificate Subject</strong>—Enter the hostname of the server where you are installing BCAAAA; do not use the IP address. Your DNS server must be able to resolve the hostname you supply.</td>
<td>CertificateSubject=&lt;BCAAA_server_hostname&gt;</td>
</tr>
<tr>
<td><strong>Save the automatically generated certificate in the certificate store?</strong>—Select Yes. Note that this option only appears if the BCAAAA installation generated a new self-signed certificate.</td>
<td>If you did not generate a certificate during the BCAAAA installation, you must obtain one for the server and add it to the certificate store before you can configure SSL. Or, re-run the BCAAAA setup and allow it to create a certificate and store it in the local certificate store.</td>
</tr>
<tr>
<td><strong>Require the ProxySG to provide a valid certificate in order to connect?</strong>—Select Yes.</td>
<td>VerifySG=1</td>
</tr>
</tbody>
</table>

2. Export the BCAAAA CA server certificate.

   a. From the BCAAAA server, click **Start > Run**. The Run dialog opens.
   b. To launch the Microsoft Management Console (MMC), enter MMC in the **Open** field and then click **OK**.
   c. Select **File > Add/Remove Snap-in**. The Add/Remove Snap-in dialog displays.
   d. Click **Add**. The Add Standalone Snap-in dialog displays.
   e. Select **Certificates** from the Snap-in list and click **Add**. The Certificates snap-in wizard starts.
f. Select **Service Account** and then click **Next**.

g. Select **Local computer** and then click **Next**.

h. From the **Service account** list, select the account you created for BCAA and then click **Finish** and then click **Close**.

i. Click **OK** to save your changes and close the Add/Remove Snap-in dialog.

j. In the list of certificate elements, select **BCAAA > Personal > Certificates** and then double-click to open the certificate that corresponds to the hostname that you specified during the BCAA installation.

k. Select **Details > Copy to File**. The Certificate Export Wizard starts.

l. For the export file format, select **Base-64 encoded X.509 (.CER)** and then click **Next**.

m. On the Files to Export screen, **Browse** to a location that is accessible from the system from which you administer the ProxySG appliance, enter a **File name** to save the certificate as, click **Save**, and then click **Next**.

n. Click **Finish** and then click **OK**.

o. Close the MMC console.

p. Restart the BCAA services.

3. Import the BCAA CA certificate into the ProxySG appliance.

   a. From the system from which you administer the ProxySG appliance, browse to the file that contains the certificate you extracted from the BCAA server in Step 2m. Open the file using a text editor (such as Notepad) and copy the contents to your Windows clipboard.

   b. From the ProxySG Management Console, select **Configuration > SSL > CA Certificates**.

   c. Click **Import**.

   d. Enter a name for the new certificate (for example, BCAA) in the **CA Cert Name** field.

   e. Paste the certificate you extracted from the BCAA server into the **CA Certificate PEM** field, making sure to include the BEGIN CERTIFICATE and END CERTIFICATE.

   f. Click **OK**. The BCAA CA certificate gets added to the bottom of the list of CA certificates.

   g. Click **Apply**.

4. Add the CA certificate to the CA Certificate List (CCL) that is associated with the device profile you want the ProxySG appliance to use when connecting to BCAA.

   When you create an authentication realm and enable SSL, the default device profile is selected by default. This device profile uses the browser-trusted CCL by default. Therefore, the easiest way to
associate the BCAA CA certificate with the browser-trusted CCL and use the default device profile as follows:

a. In the Management Console, select **Configure > SSL > CA Certificate List.**

b. Select the **browser-trusted** CA Certificate List and click **Edit.** The Edit CA Certificate List dialog displays.

c. Select the BCAA CA certificate you just imported from the list on the left and then click **Add.** The certificate entry moves to the bottom of the list on the right.

d. Click **OK** and then click **Apply.**

5. Configure the ProxySG to appliance to connect to BCAA using SSL.

a. Make sure the field that specifies the BCAA host is set to the DNS name of the server and that it matches the CN name of the certificate you specified when you installed BCAA.
   
   o For IWA realms, you configure the BCAA server name in the **Servers** section of the IWA Servers tab.
   
   o For Windows SSO and Novell SSO realms, you set the BCAA server name in the **Host** field on the Agents tab.

b. Select the **Enable SSL** check box.

c. Select the **SSL device profile** to use when connecting to BCAA over SSL. Make sure the device profile you select has been configured to trust the BCAA CA as described in Step 4.

   ![](image)

   The **Enable SSL** and **SSL device profile** fields are located on the IWA Servers tab for IWA realms and on the Agents tab for other realms.

d. Click **Apply.**
Validate the IWA Realm Configuration

After you configure an authentication realm on the ProxySG, you must verify that the ProxySG appliance can successfully connect to the authentication server and successfully authenticate a user as follows:

1. In the Management Console, select Configuration > Authentication > IWA > IWA Servers.
2. Click Test Configuration.
3. When prompted, enter the username and password of a user in the Windows domain and then click OK.
4. The appliance sends an authentication request to the configured server and then displays a message indicating whether the authentication succeeded or failed.
   - If the test fails, go back and make sure you have configured the realm properly.
   - If the test succeeds, the message also displays a list of groups to which the user belongs (IWA Direct) or a list of groups of interest to which the user belongs (IWA BCAAA). A group of interest is a group that is referenced in ProxySG policy.

![Test Configuration successful message](image)
Create a DNS Entry for the Authentication Domain

For IWA authentication to be successful, your clients must be able to resolve the fully qualified domain name of the ProxySG authentication URL to the IP address of the ProxySG appliance.

1. Create a DNS "A" record that associates the ProxySG authentication domain with the IP address of the ProxySG appliance. The fully qualified domain name (FQDN) that you use depends on whether you are using an explicit or transparent deployment:
   - **Explicit deployments**—Set the hostname in the DNS A record to match the ProxySG domain name specified in the browser’s explicit proxy configuration.
   - **Transparent deployments**—Set the hostname in the DNS A record to match the Virtual URL in the IWA configuration.

2. Configure the client systems to use the DNS server where you created the "A" records for the ProxySG appliance.

3. From a client system, ping the hostname specified in the A record to ensure that it resolves to the IP address of the ProxySG appliance.
Integrate ProxySG Authentication with Active Directory Using IWA

Configure the Web Browser for IWA

One of the main benefits of IWA is that it can provide a single sign-on experience for users because it uses the workstation login to authenticate users. When configured properly, the browser will provide the credentials to the ProxySG appliance transparently when challenged for NTLM or Kerberos credentials (the user will always be prompted for Basic authentication credentials).

IWA only works with Windows domain credentials. If users log in to the workstation using local credentials instead of domain credentials, they will be always be prompted whenever the ProxySG returns an authentication challenge.

Both Internet Explorer (IE) and Firefox can be configured to provide authentication credentials to the ProxySG appliance transparently:

- By default, IE will automatically provide authentication credentials to any site in the local Intranet zone. If the URL for your ProxySG appliance (explicit deployments) or virtual URL (for transparent deployments) contains a single hostname (that is, http://myproxy instead of http://myproxy.acme.com) you will not have to configure IE for IWA. If your ProxySG URL (virtual or explicit) does not fall within the Intranet zone, you will need to configure the IE to trust the URL. Keep in mind, however, that Kerberos deployments will require you to use the full URL for the Active Directory machine account (either the BCAA machine account for IWA BCAA or the ProxySG machine account for IWA direct). In these cases, you will need to add the full URL to the local Intranet zone.

- Firefox does not provide support for IWA by default and will therefore always need to be configured if you want to provide a single sign-on experience for your users.

For explicit proxy deployments, you must also make sure the browser is configured to send requests to the ProxySG appliance. See "Configure Client Web Browsers for Explicit Proxy" on page 37.

The procedure for configuring the browser to automatically provide login credentials to the ProxySG appliance is browser-specific:

- **Internet Explorer**
  1. Select Tools > Internet Options.
  2. Select the Security tab.
  3. Select the Local Intranet zone and click Sites > Advanced.
  4. Enter the fully qualified domain name of the ProxySG appliance (for explicit deployments) or the virtual URL (for transparent deployments) in the Add this website to the zone field and then click Add > Close > OK.
5. Select the Advanced tab and make sure the Security > Enable Integrated Windows Authentication option is selected.

6. Click OK to save your changes and close the Internet Options dialog.

**Firefox**

1. In the browser's Location field, enter about:config.

2. Click I'll be careful, I promise! to continue to the about:config page.

3. To get the browser to trust the ProxySG appliance and negotiate authentication with it, you must set values for the following options: `network.automatic-ntlm-auth.trusted-uris`, `network.negotiate-auth.delegation-uris`, `network.negotiate-auth.trusted-uris`. For each option, complete the following steps:

   a. Locate the option you want to set by scrolling or entering the option name in the Filter field.

   b. Double-click the option to open the Enter string value dialog.

   c. Enter the fully-qualified domain name of the ProxySG appliance (for explicit deployments) or the virtual URL (for transparent deployments). If you have more than one ProxySG appliance that will challenge users for authentication credentials, separate the entries with commas.

   d. Click OK.
Create an IWA Authentication Policy

After you verify that BCAA and the ProxySG appliance can successfully authenticate users against your Active Directory (AD), you must create the policy that enables authentication on the appliance. You can create a basic authentication policy that simply requires all requests to be authenticated and allows or denies access upon successful authentication. Or you can define more complex policies with rules that apply to a specific source address, subnet, port, user agent, or request header. Or, you can define different rules for different destinations. You can also create policies that allow access to guest users.

You can additionally create authorization policies that restrict access by user or group membership.

This topic shows how to create a policy using the Visual Policy Manager (VPM). You can also create policy using the Content Policy Language (CPL). Refer to the Content Policy Language Reference for details.

Note that you must create an IWA realm before you can define the corresponding authentication policy.

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.

2. Create the policy rule that enables the ProxySG appliance to authenticate client requests.
   b. Enter a Layer Name or accept the default name and then click OK. The first policy rule displays with default settings.

3. Configure the authentication policy settings.
   a. In the Action column of the first row, right-click and then select Set. The Set Action Object dialog displays.
   b. Click New and then select one of the following authentication objects:
      - **Authenticate**—Use this option if you do not need to log user IDs for denied requests. With this option, if policy causes a request to be denied before the user is authenticated, the user ID associated with the request will not be available for access logging.
      - **Force Authenticate**—Use this option to force the appliance to authenticate requests even if they are denied before authentication would normally occur. This ensures that user IDs are available for access logging.
If you plan to create a guest authentication policy, create a combined object that contains the Authenticate object and a Permit Authentication Error object (be sure to select All Except User Credentials Required).

c. (optional) Specify a Name for the authentication object.

d. Select the IWA Realm from the drop-down list.

e. Select the authentication mode from the Mode drop-down list. Although you can select Auto to have the ProxySG appliance automatically choose an authentication mode, it is usually better to make a selection that is appropriate for your deployment as follows:

- **Explicit deployments**—Select Proxy or Proxy IP. The Proxy IP mode reduces the load on the network because it uses an IP surrogate to reauthenticate clients that have already successfully authenticated.

- **Transparent deployments**—Select Origin Cookie Redirect. This mode redirects the client to the virtual URL for authentication and uses a cookie surrogate to reauthenticate clients that have already successfully authenticated. The appliance will automatically downgrade to the Origin IP Redirect mode for user agents that do not support cookies.

f. Click OK to close the Add Authenticate Object or Add Force Authenticate object dialog.

g. Click OK to close the Set Action Object dialog.

4. (optional) Restrict authentication to a subset of client requests, based on source or destination request attributes.

The default settings in the policy rule will cause the ProxySG appliance to authenticate all client requests. You can set the Source and/or Destination columns to restrict authentication to a specified subset of requests. For example,

a. In the Source or Destination column of the first row, right-click and then select Set. The Set Source Object or Set Destination object dialog displays.

b. Click New and then select an object that represents the subset of requests you want to authenticate. After you select an object, you will be prompted to provide details. For example, if you choose the Client IP Address/Subnet object, you will be prompted for an IP address and subnet mask/prefix to which this rule will apply.

When you first deploy your authentication policy, you may want to limit authentication to the source address of a test workstation or subnet. This allows you to identify and troubleshoot any configuration issues before rolling the policy out into production.

5. (optional) Add additional policy rules to refine your authentication policy.

A single Web Authentication Layer rule with the authenticate action is all you need to enable
Integrate ProxySG Authentication with Active Directory Using IWA

authentication. However, there may be some cases where you want to bypass authentication for certain requests and enable it for others. For example, you may have a certain client, subnet, or URL on which you do not require authentication or you may have some custom applications that do not know how to handle authentication requests. In this case, you would add an additional rule to your Web Authentication Layer policy to instruct the ProxySG appliance how to handle the exceptions.


b. Specify which client requests this rule applies to by setting the Source or Destination columns.

c. Specify what the ProxySG appliance should do with requests that match the source and/or destination setting you have defined by right-clicking in the Action column of the row, and selecting Set.

   - If you want to authenticate requests that match the specified source and/or destination request settings you have defined, click New and select Authenticate and click OK.

   - If you want to bypass authentication for the matching requests, select Do Not Authenticate and click OK.

d. Prioritize the order in which you want the ProxySG appliance to enforce the rules by selecting the rule you want to move and clicking Move up or Move down. The ProxySG appliance evaluates the rules in the order in which they appear in the policy layer. As soon as it finds a rule that matches the request, it will enforce the specified action (in this case, either to authenticate or not authenticate the request). Therefore, you should put more specific rules above general rules. For example, if you have two rules in your policy—one that is set to authenticate requests from any source or destination and one that is set to not authenticate requests from a specific subnet—you would put the one that bypasses authentication in front of the general rule that matches all requests.

6. Install the authentication policy.

   a. Click Install policy.

   b. Click OK to acknowledge that the policy was successfully installed.
Create an IWA Guest Authentication Policy

A guest authentication policy enables users who do not have a Windows domain account on your network to access Internet resources.

To create an IWA guest authentication policy:

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.

2. Create a Web Authentication Layer for authenticating client requests for your domain users.
   See "Create an IWA Authentication Policy" on page 74 for instructions.

3. Create a second Web Authentication Layer to provide guest access.
   b. Enter a Layer Name to distinguish this layer from the previous layer (for example, Guest Authentication) and then click OK. The first policy rule displays with default settings.

4. Configure the source.
   a. In the Source column of the first row, right-click and then select Set. The Set Source Object dialog displays.
   b. Click New and then select User Authentication Error. The Add User Authentication Error Object dialog displays.
   c. Select Any errors and click OK twice to save the source object and close the dialogs.

5. Configure the action.
   a. Right-click the Action column and then select Set. The Set Action Object dialog displays.
   b. Click New and then select the Authenticate Guest object. The Add Authenticate Guest object dialog displays.
   c. Select Use realm and then select your IWA realm from the drop-down list.
   d. Enter a Guest Username. This will be the name that appears in your access log whenever guest access is granted; it does not correlate to an Active Directory user account.
   e. Click OK twice to save the Action object and close the dialogs.

6. Make sure that the Web Authentication Layer for your guest policy is positioned after the your main Web Authentication Layer.
To re-order the layers, select **Edit > Reorder Layers**.

7. Install the authentication policy.
   a. Click **Install policy**.
   b. Click **OK** to acknowledge that the policy was successfully installed.
Create an IWA Authorization Policy

One of the benefits of IWA is that it automatically returns authorization information for a user in response to an authentication request. You do not have to perform any additional configuration to get authorization to work. After successfully authenticating a user, the appliance receives a list of all groups (IWA Direct) or groups of interest (IWA BCAAA) to which the user belongs.

This topic shows how to create a policy using the Visual Policy Manager (VPM). You can also create policy using the Content Policy Language (CPL). Refer to the Content Policy Language Reference for details.

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.

2. Create a Web Access Layer.
   b. Enter a Layer Name or accept the default name and then click OK.

3. Specify the user or group to authorize (the source).
   a. In the Source column of the first row, right-click and then select Set. The Set Source Object dialog displays.
   b. Click New and then select the type of Active Directory object this rule will authorize:
      - To create a rule for authorizing a group, select Group. The Add Group Object dialog displays.
      - To create rule for authorizing a user, select User. The Add User Object dialog displays.
   c. Select the IWA realm from the Authentication Realm drop-down list.
   d. Specify the name of the Active Directory user or group that rule will authorize:
      - If you know the name of the Active Directory user or group, enter it in the Group or User field.
      - If you don't know the Active Directory name of the user or group, click Browse and select the group from the IWA Browser.
   e. Click OK to close the Add Group Object or Add User Object dialog.
   f. Click OK to close the Set Source Object dialog.

4. Specify whether to allow or deny requests from the specified user or group.
Integrate ProxySG Authentication with Active Directory Using IWA

a. Right-click the **Action** column.

b. Select one of the following options:
   - **Allow**—Select this option if the default proxy policy for the appliance is set to deny proxy access through the ProxySG appliance. This is the default in a secure web gateway deployment.
   - **Deny**—Select this option if the default proxy policy for the appliance is set to allow proxy transactions.

   If you aren't sure what the default proxy policy is set to on your appliance, go to **Configuration > Policy > Policy Options**.

5. (Optional) Define any additional parameters that you want this rule to enforce.

6. To create additional authorization rules, repeat Steps 3 through 5.

7. Install the policy.
   a. Click **Install policy**.
   b. Click **OK** to acknowledge that the policy was successfully installed.
Integrate ProxySG Authentication with Active Directory Using IWA

**Verify Kerberos Authentication**

Even if you configure IWA to allow Kerberos, Kerberos will only be used if configured properly. If the ProxySG appliance cannot successfully negotiate Kerberos with a client, it will silently downgrade to use NTLM authentication. Because this happens behind the scenes, you may not know whether you are using Kerberos or NTLM.

1. To verify that the ProxySG appliance is attempting to negotiate Kerberos authentication, take a packet capture on the client and look for the NEGOTIATE message. The client uses the NEGOTIATE message to communicate the type of authentication it supports to the ProxySG appliance. This will show up as a either a WWW-Authenticate: NEGOTIATE (transparent) or Proxy-Authenticate: NEGOTIATE message. Note that this message alone does not indicate that Kerberos will be used.

```
From 1179 (1244 bytes on wire, 1244 bytes captured)
Ethernet II, Src: 00:50:56:09:35:ed (00:50:56:09:35:ed), Dst: 00:10:00:01:36:48 (00:10:00:01:36:48)
Internet Protocol, Src: 16.94.23.10 (16.94.23.10), Dst: 16.94.23.17 (16.94.23.17)
Transmission Control Protocol, Src Port: http-alt (8080), Dst Port: secure-http-srv (5970), Seq: 1, Ack: 0, Len: 1150
Options: Transfer Protocol

HTTP/1.1 407 Proxy Authentication required

Proxy-Authenticate: NEGOTIATE
```

2. To verify that the client is using Kerberos, take a packet capture from the client and use the display filter to view Kerberos requests. If Kerberos authentication is in use you will see Kerberos requests and responses between the client and the Domain Controller as well as the Kerberos ticket in the GET
Integrate ProxySG Authentication with Active Directory Using IWA

request.

```
Accept: image/gif, image/jpeg, image/pjpeg, image/png, application/x-shockwave-flash, */*
Accept-Language: en-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Host: www.google.com
Proxy-Connection: Keep-Alive
```

```plaintext
<snip>
MechTypes: 3 Items
  MechType: 1.2.840.113550.1.11.12.2 (MS Kerberos)
  MechType: 1.2.840.113550.1.11.12.2 (MS Kerberos)
  MechType: 1.2.840.113550.1.11.13.2.10 (MIMSP - Microsoft NTLM Security Support Provider)
  krb5_ciph: 608204e00609a2864886f7120102010068204ca309204
```
Enable IWA Authentication for SSL Traffic in a Transparent Deployment

After you configure IWA, you must complete the following additional tasks if you are using a transparent proxy deployment and you want to authenticate SSL traffic:

1. Make sure you have an SSL license.

   Although some ProxySG appliance models include an SSL license, other models require that you purchase and install an add-on license. To see whether you have a valid SSL license, launch the ProxySG Management Console and select Maintenance > Licensing > View. You should check that SSL displays in the list of licensed components.

2. Create an HTTPS Reverse Proxy service to listen for authentication requests.
   a. Select Configuration > Services > Proxy Services.
   b. Click New Service.
   c. Enter a unique Name for the service to identify it as your IWA authentication service.
   d. Select HTTPS Reverse Proxy from the Proxy drop-down list.
   e. Select the Keyring that you want to use to establish SSL sessions for this service.
f. To configure the listening port, click New and then configure the service as follows:

- Set **Destination Address** to *Explicit*.
- Set the **Port range** to the port number on which you want this service to listen for incoming authentication requests. Note that you will need to use this same port number in the Virtual URL you define for the realm.
- Set the **Action** to *Intercept*.
- Click **OK** to save the listener settings.

g. Click **OK**.

h. If necessary, configure your firewall to allow traffic between the client workstations and the ProxySG appliance on the port you just configured.

3. Create an IWA realm for authenticating your HTTPS traffic.

You create the realm the same way that you created the IWA realm for your HTTP traffic, with the difference being the URL to which authentication requests are directed:

a. Create the IWA realm as described in "Create an IWA Direct Realm" on page 28 or "Create an IWA BCAA Realm" on page 60.

b. On the **IWA General** tab, set the **Virtual URL** to a URL that points to the HTTPS Reverse Proxy Service you created for IWA authentication. For example, if you configured your HTTPS Reverse Proxy service to listen on port 4433, you would enter a URL such as `https://myproxy:4433`.

c. Make sure your **DNS server** is set up to resolve the hostname to the IP address of the ProxySG appliance.

4. Create the policy rule to enable the appliance to intercept HTTPS traffic.

a. Launch the Visual Policy Manager (VPM) by selecting **Configuration > Policy > Visual Policy Manager > Launch**.

b. Select **Policy > Add SSL Intercept Layer**.

c. Enter a **Layer Name** or accept the default name and then click **OK**. The first policy rule displays with default settings.

d. Right-click the **Action** column and select **Set**.

e. Click **New** and select **Enable HTTPS Interception**.

f. Check the **Issuer Keyring** check box and select the keyring you specified in the HTTPS Reverse Proxy service settings.

g. Click **OK**.
5. Create the policy rule that enables the ProxySG appliance to authenticate client HTTPS requests.
   a. Select **Policy > Add Web Authentication Layer**.
   b. Enter a **Layer Name** or accept the default name and then click **OK**. The first policy rule displays with default settings.
   c. In the **Action** column of the first row, right-click and then select **Set**. The Set Action Object dialog displays.
   d. Click **New** and then select **Authenticate**.
   e. Select the IWA **Realm** from the drop-down list. Make sure you select the realm you created for your HTTPS traffic.
   f. Select the authentication mode from the **Mode** drop-down list. For transparent authentication, you will usually want to select **Origin Cookie Redirect**. This mode redirects the client to the virtual URL for authentication and uses a **cookie surrogate** to reauthenticate clients that have already successfully authenticated. The appliance will automatically downgrade to the **Origin IP Redirect** mode for user agents that do not support cookies.
   g. Click **OK** to close the Add Authenticate Object or Add Force Authenticate object dialog.
   h. Click **OK** to close the Set Action Object dialog.

6. Install the policy rules you created.
   a. Click **Install policy**.
   b. Click **OK** to acknowledge that the policy was successfully installed.
Integrating ProxySG Authentication with Active Directory Using Windows SSO

With Windows SSO authentication, users are authenticated based on their Windows Active Directory logins. Therefore, authentication will only work if your clients are running in a Windows domain environment. In addition, because usernames are derived from IP address mappings, Windows SSO only works well in environments where one IP address maps to one user. Environments with multi-user systems (such as Citrix) or with clients behind NAT devices are not suitable for Windows SSO authentication.

To configure authentication, you must complete the following tasks:

1. Install BCAA on a Windows domain controller (DC) or a member server. Because the appliance cannot communicate directly with a Windows DC, this agent software is required to act as an intermediary between the DC and the appliance. Refer to the BCAA Service Requirements document for more information about installing BCAA.

2. Enable BCAA to begin querying DCs for user logins so that it can begin building an IP address-to-username mapping table. It will use this table to respond to authentication requests from the appliance. See "Configure the Windows SSO Agent on the BCAA Server" on the facing page.

3. Configure the appliance to communicate with BCAA. See Enable Windows SSO Authentication on the Appliance.

4. (optional) Set up authorization. The Windows SSO realm itself cannot perform authorization. If you want to use authorization in conjunction with Windows SSO, you must create an LDAP realm and add it to the Windows SSO realm configuration.

5. Create the policy rules that will enforce authentication and, optionally, authorization.

6. Verify authentication. The best way to verify that authentication is working properly is to look at your reports and make sure that they are displaying user names instead of IP addresses as expected. You can also view authentication statistics to ensure a proper authentication configuration.
Configure the Windows SSO Agent on the BCAA Server

After you install BCAA, you must configure its Windows SSO agent to enable it to begin querying the DCs in your network for user login information. You can optionally specify settings such as which DCs to query (by default, it queries all DCs in the forest) and how long an IP-to-user mapping is valid (called a time-to-live, or TTL, value). The way you configure the agent depends on whether you plan to use Domain Controller Query (DCQ), Client Query (CQ), or both:

- "Configure the Windows SSO Agent for Domain Controller Query" on the next page
- "Configure the Windows SSO Agent for Client Query" on page 89
Configure the Windows SSO Agent for Domain Controller Query

To use Domain Controller Query (DCQ), you must explicitly enable it in the Windows SSO agent configuration on the BCAAAA server as well as in the Windows SSO realm settings on the ProxySG appliance. When you configure the agent, you also specify settings such as which DCs to query (by default, it queries all of them) and how long an IP-to-user mapping is valid (called a time-to-live, or TTL, value) as described in the following procedure. For more information on DCQ, see “About Windows SSO” on page 16.

1. Open the sso.ini file in a text editor. This file is located in the BCAAAA installation directory (C:\Program Files\Blue Coat Systems\BCAAA by default).

2. Enable the agent to begin querying DCs by uncommenting the DCQEnabled=1 line in the DCQSetup section of the file.

3. (Optional) Limit how long IP-to-user mappings are valid. By default, BCAAAA considers all IP-to-user mappings valid for one day (86400 seconds) unless replaced by a new mapping sooner (that is, if another user logs in with an IP address that is already mapped, the old mapping will be replaced by the new one). However, because BCAAAA does not track logouts, it is possible for its IP-to-user mappings to get stale. To change the length of time that a mapping is valid, uncomment the ValidTTL setting in the DCQSetup section of the file and modify the value.

4. (Optional) Limit which DCs BCAAAA queries. By default it queries all DCs in the forest every ten seconds. However, in a large forest that spans WAN links, this can cause excessive bandwidth usage. To prevent this, you can define a list of DCs or an IP address range to which to limit queries by entering values in the DCQDomainControllers section of the file; list the domain controllers you want to query or the IP address ranges of interest. Keep in mind that BCAAAA must query each DC that will handle logins for ProxySG users in order to successfully authenticate them.

5. Save the sso.ini file.

6. Restart the BCAAAA service.
Configure the Windows SSO Agent for Client Query

With Client Query (CQ), the BCAA Agent will directly query the client system to obtain the username of the logged in user. The biggest factor in getting CQ to work is making sure that the client system allows the Windows SSO agent to access its NetBIOS login information on port 445. On many versions of Windows, the Windows firewall blocks remote access to the client workstation through this port; you must unblock this port for CQ to work.

There are no other required configuration steps for getting CQ to work. However, depending on how often IP address-username mappings change within your organization you may want to modify the length of time the agent considers the authentication information valid. This is because the Windows SSO agent does not track logouts and therefore its IP-to-user mappings can get stale; the time-to-live (TTL) settings in the Windows SSO configuration specify how long to consider a mapping valid. By default, all CQ TTL values are set to 15 minutes (900 seconds). If IP address assignments remain fairly static in your environment, you may want to increase the TTL for the authentication credentials to prevent excess traffic between the agent and the client systems. Likewise, if users change IP addresses often, you may want to decrease these values.

1. Open the sso.ini file in a text editor. This file is located in the BCAA installation directory (C:\Program Files\Blue Coat Systems\BCAAA by default).

2. Locate the ClientQuerySetup section of the file and modify the time to live (TTL) settings as appropriate for your network environment. Because the Windows SSO agent cannot monitor logouts, it uses timeout values to limit how long it considers a login valid:
   - ValidTTL—The number of seconds that a successful query is considered valid. During that time, the client will not be requeried (default = 900 seconds).
   - InvalidTTL—The number of seconds after an unsuccessful query before the client will be queried again. During that time, the client will not be requeried and any ProxySG access will be reported by IP address rather than username (default = 900 seconds).
   - DCQTTL—When both DCQ and CQ are enabled, the Windows SSO agent will use a valid DCQ IP address-username mapping if it has one rather than querying the client. This parameter specifies the number of seconds that the Windows SSO agent will consider a DCQ mapping valid. If the DCQ mapping is older than this value, the Windows SSO agent will query the client (default = 900 seconds).

3. Save the sso.ini file.

4. Restart BCAA Agent.
Enable Windows SSO Authorization on the ProxySG Appliance

If you want to use your Windows SSO realm for authorization—that is, to specify what a user can or cannot do based on user name or group membership—you must set up access to the Active Directory (AD) user and group information using an LDAP realm. You can then configure your Windows SSO realm for authorization.

1. In the ProxySG Management Console, select Configuration > Authentication > LDAP > LDAP Realms.

2. Create an LDAP realm.
   a. Click New.
   b. Enter a Realm name.
   c. Select Microsoft Active Directory from the Type of LDAP server drop-down list.
   d. Enter the IP address of the Active Directory server in the Primary server host field.
   e. (Optional) If you are using a port other than the default, enter a value in the Port field.
   f. Click OK.
   g. Click Apply.

3. Specify the base DN(s) where you want the ProxySG to begin its search for user and group information.

   The base DN(s) you enter will depend on how your directory is organized. For example, if you want the ProxySG appliance to search the entire directory for user and group information, you might enter a single entry that points to the folder where all users and groups are located such as cn=Users,dc=acme,dc=com. However, if you want to search for users at the departmental level, you might need to add multiple entries such as ou=sales,dc=acme,dc=com and ou=development, dc=acme,dc=com.

   If you do not know the base DN for your AD server, go to the command line on the AD server and enter the following command:
   ```
   ldifde -f output.txt
   ```
   You can then open the output.txt file that this command generates in a text editor and search for the distinguishedName: entry.

   a. Select the LDAP DN tab.
   b. Click New. The Add LDAP Base DN dialog displays.
c. Enter the base DN that represents the part of your Active Directory tree where you want the ProxySG to begin searching for user or group entries and then click OK.

d. (Optional) If you want to add additional base DNs to search, repeat Step b. For example, if you have different AD servers distributed throughout your organization, you may want to add an entry for each one. Or, if you want to define user and group access at the departmental level, you may want to create a base DN entry for each organizational unit.

e. (Optional) Organize the base DN entries you have added by using the Promote entry or Demote entry buttons to move entries up or down. The ProxySG searches the base DNs in the order listed, starting at the top.

f. Click Apply to save your entries.

4. (Optional) If your AD server does not support anonymous searches, you must specify an Active Directory user that the ProxySG will use to log in to the directory.

   a. Select the LDAP Search & Groups tab.

   b. Deselect Anonymous search allowed.

   c. Enter the fully qualified DN of the AD user the ProxySG should use to log in to the directory in the Search user DN field. For example, cn=BC_Admin,cn=Users,dc=acme,dc=com.

   d. Click Change Password and enter the password for the specified user in the New Password and Confirm new Password fields. Click OK to close the dialog.

   e. Click Apply.

5. Configure the LDAP authorization settings in the Windows SSO realm.


   b. Select the Windows SSO realm from the Realm name drop-down list.

   c. Select the LDAP realm you just created from the Authorization realm name drop-down list.

   d. Click Apply.

You can now create policy rules for authentication and, if configured, authorization. The policy rules are what instruct the ProxySG how to handle client requests after an authentication success or failure.
Validate the Windows SSO Realm Configuration

After you configure an authentication realm on the ProxySG, you must verify that the ProxySG appliance can successfully connect to the authentication server and successfully authenticate a user as follows:

1. In the Management Console, select **Configuration > Authentication > Windows SSO > Agents**.

2. Click **Test Configuration**.

3. When prompted, enter the IP address of a client system in the Windows domain and then click **OK**.

4. The ProxySG appliance will use the realm configuration you supplied to send an authentication request to BCAA and return the results as follows:
   - If the ProxySG and the BCAA server are configured properly, BCAA will return the username associated with the IP address you provided.
   - If the test does not succeed, check that the settings on the **Agents settings** tab as well as the **BCAAA settings** are configured correctly and then test the configuration again.
Create a Windows SSO Authentication Policy

Because Windows SSO does not really authenticate users (that is, it does not challenge users for credentials), it does not issue an HTTP 301/302 redirect or an HTTP 401/407 authentication request to the browser. Therefore, the way you configure the authentication policy does not depend on whether the appliance is deployed explicitly or transparently. Instead it simply checks the client IP address in the request against the IP address-username mapping table maintained by BCAAA. This means that all Windows SSO authentication policies can (and should) use the Proxy-IP authentication mode.

This topic shows how to create a policy using the Visual Policy Manager (VPM). You can also create policy using the Content Policy Language (CPL). Refer to the Content Policy Language Reference for details.

Note that you must create the Windows SSO realm before you can define the authentication policy.

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.


3. Enter a Layer Name or accept the default name and then click OK.

4. In the Action column of the first row, right-click and then select Set. The Set Action Object dialog displays.

5. Click New and then select one of the following authentication objects:
   - **Authenticate**—Use this option if you do not need to log user IDs for denied requests. With this option, if policy causes a request to be denied before the user is authenticated, the user ID associated with the request will not be available for access logging.
   - **Force Authenticate**—Use this option to force the appliance to authenticate requests even if they are denied before authentication would normally occur. This ensures that user IDs are available for access logging.

6. Click OK. The Add Authenticate Object or Add Force Authenticate object dialog displays.

7. Define the authenticate actions as follows:
   a. (Optional) Specify a Name for the authentication object.
   b. Select the Windows SSO Realm from the drop-down list.
   c. Select Proxy IP from the Mode drop-down list.
Integrating ProxySG Authentication with Active Directory Using Windows SSO

   d. Click **OK** to close the Add Authenticate Object or Add Force Authenticate object dialog.
   e. Click **OK** to close the Set Action Object dialog.

8. (Optional) Create an authorization policy. For instructions, see "Configure a Windows SSO Authorization Policy" on the facing page.

9. Install the policy.
   a. Click **Install policy**.
   b. Click **OK** to acknowledge that the policy was successfully installed.
Configure a Windows SSO Authorization Policy

Because a Windows SSO realm simply maps the IP address in a client request to an Active Directory (AD) login name, it does not have any additional information about the user, such as group membership information. Therefore, if you want to use authorization with a Windows SSO realm, you must create an LDAP realm to connect to AD for access to user and group information and then configure the Windows SSO realm to point to the LDAP realm. See "Enable Windows SSO Authorization on the ProxySG Appliance" on page 90 for more information.

This topic shows how to create a policy using the Visual Policy Manager (VPM). You can also create policy using the Content Policy Language (CPL). Refer to the Content Policy Language Reference for details.

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.

2. Create a Web Access Layer.
   b. Enter a Layer Name or accept the default name and then click OK.

3. Specify the user or group to authorize (the source).
   a. In the Source column of the first row, right-click and then select Set. The Set Source Object dialog displays.
   b. Click New and then select the type of LDAP object this rule will authorize:
      - To create a rule for authorizing a group, select Group. The Add Group Object dialog displays.
      - To create rule for authorizing a user, select User. The Add User Object dialog displays.
   c. Select the LDAP realm you created to authorize authenticated Windows SSO users from the Authentication Realm drop-down list.
   d. Specify the LDAP name of the user or group that rule will authorize:
      - If you know the name of the LDAP user or group, enter it in the Group or User field.
      - If you don't know the LDAP name of the user or group, click Browse and select the group from the LDAP Browser.
   e. Click OK to close the Add Group Object or Add User Object dialog.
f. Click OK to close the Set Source Object dialog.

4. Specify whether to allow or deny requests from the specified user or group.
   a. Right-click the Action column.
   b. Select one of the following options:
      - **Allow** Select this option if the default proxy policy for the appliance is set to deny proxy access through the ProxySG. This is the default in a secure web gateway deployment.
      - **Deny** Select this option if the default proxy policy for the appliance is set to allow proxy transactions.

      If you aren’t sure what the default proxy policy is set to on your appliance, go to Configuration > Policy > Policy Options and check the **Default Proxy Policy** setting.

5. (optional) Define any additional parameters that you want this rule to enforce.

6. To create additional authorization rules, repeat Steps 3 through 5.

7. Install the policy.
   a. Click **Install policy**.
   b. Click OK to acknowledge that the policy was successfully installed.
Configure LDAP Authentication

To configure [LDAP authentication](#) on the ProxySG appliance, complete the following tasks:

1. Configure the ProxySG appliance to connect to and perform searches on the LDAP directory. See "Create an LDAP Realm" on the next page.

2. Configure advanced LDAP realm settings. Review the details of your customized LDAP directory configuration and security requirements, and configure your LDAP realm accordingly.
   - Configure the object class attributes and group information to map to your LDAP directory schema. See "Configure the LDAP Realm for Customized Directories" on page 101.
   - Configure resource availability settings, such as refresh and timeout cycles. See "Configure LDAP Realm Resource Availability Settings" on page 103.
   - Connect to an LDAP server using a secure connection (requires an LDAPv3 supported directory). See "Connect to a Secure LDAP Server" on page 105.

3. Verify that the ProxySG appliance is configured for authentication. See "Verify LDAP Directory Connectivity" on page 108.


5. (Optional) Optimize your LDAP searches and group compare operations. See "Optimize Your LDAP Realm" on page 112.
Configure LDAP Authentication

Create an LDAP Realm

The LDAP realm on the ProxySG appliance needs to be configured in order to successfully communicate with and search for entries contained within a specified LDAP directory. To configure the LDAP realm, you'll need to have information about the LDAP hierarchy and the LDAP directory server settings. If you do not have LDAP directory information, you can use a LDAP viewer to review the tree structure and other information details about the LDAP directory. Due to the complexity of LDAP directories, Blue Coat recommends that you retrieve this information from the LDAP directory administrator.

To enable LDAP authentication, you'll need to configure the LDAP authentication realm on the ProxySG appliance to properly communicate with and recognize the directory structure – the complexity of the configuration process depends on your LDAP directory deployment and the schema that you've decided to use. SGOS provides limited default configuration options for more commonly used directories and built-in schemas, but you'll still need to verify that all information is properly retrieved and processed by the appliance.

The procedure below shows the steps to configure the ProxySG appliance to connect with an LDAP directory server using default settings. If you are running a customized LDAP directory, it might be necessary for you to configure additional options or change the default LDAP realm settings on the ProxySG appliance. For more information on these optional configuration items, see "Configure the LDAP Realm for Customized Directories" on page 101.

1. Create an LDAP realm.
   a. Select **Configuration > Authentication > LDAP > LDAP Realms**.
   b. Click **New**.
   c. Enter a **Realm name**.
   d. Select the LDAP directory server you are using from the **Type of LDAP server** drop-down list.
   
   ![Warning](image)
   The User attribute type is automatically selected based on your LDAP directory selection, but you can manually specify the user attributes if you've implemented a customized LDAP schema.
   
   e. Enter **Primary server host** and **Port** values of the LDAP directory server in the **Servers** section. In most cases, LDAP directories uses the default port value of 389.
   
   f. Click **OK**. The realm you just created is added to the **LDAP Realms** tab.
   
   g. Select the **LDAP Servers** tab and then select the **Realm name** to configure.
   
   h. Select the **LDAP Protocol Version** that your LDAP directory uses.
   
   i. Select **Follow referrals** if your LDAP directories are distributed across several LDAP servers using continuation references. This option allows your searches to follow referrals and return all matching entries found during a search operation.
j. Select **Case sensitive** if your LDAP directory uses case-sensitive values for the usernames and passwords.

k. (Optional) If you have an alternate LDAP directory server for failover, enter the **Alternate server host** and **Port** values in the **Servers** section.

l. (Optional) To change the amount of time the appliance will wait for an authentication response from the LDAP directory server before timing out, enter a new value in the **Timeout request after x seconds** field (default 60 seconds).

m. Click **Apply**.

2. Specify the base DN (distinguished name) that defines the point where you want the ProxySG to begin its search for user and group information within the LDAP tree.

The base DN you enter depends on how your directory is organized. You can assemble the DN by sequencing the RDNs (relative distinguished name) in a comma separated list beginning at the bottom of the tree leading up to the directory root. Counterintuitively, LDAP directories have the root at the top of the tree; so you'll need to determine the bottom-most point that you wish to search from.

For example, if you want to search the directory for user and group information, you might point to the folder where all users and groups are located such as `cn=Users,dc=bluecoat,dc=com`. However, if you want to search for users at the departmental level, you might add multiple entries such as `ou=sales,dc=bluecoat,dc=com` and `ou=techpubs, dc=bluecoat,dc=com`.

<eDirectory users: make sure that the base DNs point to replica servers and not just servers with a sub-ref on them. Blue Coat does not recommend using a server that only contains subrefs on the replica server.

a. Select the **LDAP DN** tab.

b. Click **New**. The Add LDAP Base DN dialog displays.

c. Enter the base DN that defines the point where a search begins in your LDAP tree and click **OK**. You can assemble the DN by sequencing the RDNs (relative distinguished name) in a comma separated list.

d. (Optional) If you want to add additional base DNs to expand the search areas of the LDAP tree, repeat Step c. For, example, if you have multiple LDAP trees distributed throughout your organization, you may want to add an entry for each one. Or, if you want to define user and group access at the departmental level, you may want to create a base DN entry for each organizational unit.

e. (Optional) Organize the base DN entries you have added by using the **Promote entry** or **Demote entry** buttons to move entries up or down. The ProxySG searches the base DNs in the
Configure LDAP Authentication

order listed, starting at the top.

f. Click **Apply** to save your entries.

3. Specify an LDAP user that the ProxySG will use to log in and search the LDAP directory.

   The LDAP realm defaults to anonymous user searches. However, Blue Coat recommends specifying an LDAP search user with specific administrator rights. Depending on which LDAP directory you’re using and how it is configured, an anonymous search user might not have sufficient access to attributes to return a valid search result.

   For security purposes, you might consider creating an authenticated user with limited access that can only search a particular LDAP tree or a limited set of attributes.

   a. Select the **LDAP Search & Groups** tab.
   
   b. Deselect **Anonymous search allowed**.
   
   c. Enter the fully qualified DN of the LDAP user the ProxySG should use to log in to the directory in the **Search user DN** field. For example, cn=BC_Admin,cn=Users,dc=acme,dc=com.
   
   d. Click **Change Password** and enter the password for the specified user in the **New Password** and **Confirm new Password** fields. Click **OK** to close the dialog.
   
   e. Click **Apply**.
Configure the LDAP Realm for Customized Directories

The ProxySG appliance provides basic configuration settings based on your LDAP directory selection during realm creation. These settings assume a default configuration for your schema, that is, types of objects, attributes of each object type, and the rules that govern the LDAP directory. If you've modified your off the shelf LDAP directory or are using a customized solution, you'll want to review and reconfigure the standard LDAP realm settings to properly correspond to your customizations.

1. Provide additional details about how your LDAP directory organizes information about users and groups.

   For example, if your directory only searches a user object to retrieve information about the group that it is associated with (like iPlanet), you'll need to specify group membership. Alternatively, if a group object contains information about its users, (like Active Directory), you'll need to specify user membership. These settings are typically dependent on the type of LDAP directory you are using. If you are using a customized LDAP directory you must review, and if necessary, manually specify group information; otherwise you might experience authorization difficulties.

   a. In the ProxySG Management Console, select Configuration > Authentication > LDAP > LDAP Search & Groups.

   b. Select a Membership type.

      - **Group** – Specifies that information about your LDAP directory users are only stored within groups objects.

      - **User** – Specifies that information about your LDAP directory groups membership can be stored within user entries.

   c. Enter the Membership attribute used by your LDAP directory. This attribute is used to list the groups that each user is a member of in the LDAP tree.

      Select the type of username to lookup.

      - **Relative** – Indicates that a relative distinguished name (RDN) is used to define the membership attribute. This option is only available for **Group** membership types.

      - **FQDN** – Indicates that a lookup is only performed on a user object that is explicitly defined by a fully qualified distinguished name. FQDN can be selected when the membership type is either **Group** or **User**.

   d. Select **Nested Groups Support** if your LDAP directory has groups that are members of another group. This enables a user that is a member of the 'child' group to be referenced along with the 'parent' group.

      Be sure not to introduce any looped references into your nested groups. For example, a loop
Configure LDAP Authentication

forms if the group member Testgroup has the nested group member Testgroup2, which in turn has the aforementioned Testgroup as a nested member.

- Click **Apply** to set the changes.

2. Add or modify the object class attribute values on the LDAP realm to match those on your LDAP directory.

The contents of a directory entry is defined by the schema, including object types, which typically defines what an object is or represents. These can include entities such as organizations and people, or anything else the LDAP directory administrator defines it as. Because there is some interoperability expected among various LDAP-enabled applications, there are usually some loosely standardized values for the object classes. If your LDAP schema has been customized with new or modified object classes, you'll need to define (or redefine, as the case may be) the values of the object classes to fit your LDAP server schema configuration.

Object class attribute values are used by Blue Coat during a VPM search of an LDAP server. If an administrator wants to browse the groups in a particular realm, the ProxySG appliance searches the LDAP server for objects that have object class attribute values matching those in the group list and in the container list. The list of object class attribute values in the container list is needed so that containers that contain groups can be fetched and expanded correctly. The object class attribute values used in directory entries can differ among LDAP servers. SGOS includes standard object classes used by the LDAP directory. You can redefine the attribute values of the stock object classes to fit your LDAP server schema configuration.

- Select the **LDAP ObjectClasses** tab and then the LDAP realm where the object classes that you want to modify are located.
- Select the type of object that you want to redefine: **container**, **group**, or **user**.
- Click **New** to add a new object class or **Edit** to change the value of an existing object class.
- Enter or edit the object class attribute value(s) that must be available when performing searches on the ProxySG.
- Click **OK** and **Apply** to set the changes.
Configure LDAP Realm Resource Availability Settings

The LDAP realm on the ProxySG appliance is preset with limited timeout and refresh values for various authentication resources. Availability of resources can be adjusted to better suit your environment, user base, and to address security issues. Depending on how your users access LDAP-enabled resources, these settings might become intrusive, forcing users to reauthenticate multiple times during a single session.

1. In the ProxySG Management Console, select **Configuration > Authentication > LDAP > LDAP Realms > LDAP General**.

2. Enter the refresh and timeout values to change how often the ProxySG appliance reauthenticates a client.

   - **Credential refresh time**—(Basic credentials only) Specifies the amount of time the ProxySG appliance will cache Basic credentials (username and password) and use these cached credentials to authenticate the user. By default, basic credentials are good for 900 seconds (15 minutes).

   - **Surrogate refresh time**—After the ProxySG appliance successfully authenticates a client, it caches the client’s IP address or a cookie (depending on the authentication mode that is in use) in its surrogate cache. If it receives subsequent requests from the same client during the surrogate refresh time, it uses the IP address or cookie in its cache to authenticate the user. By default, the surrogate credential is good for 900 seconds (15 minutes).

   - **Authorization refresh time**—The Authorization Refresh Time allows you to manage how often the authorization data is verified with the authentication realm. It has a default setting of 900 seconds (15 minutes). You can configure this in policy for better control over the resources as policy overrides any settings made here.

   - **Inactivity timeout**—When a client request is successfully authenticated, the ProxySG appliance establishes an active session with the client and as long as that session stays active, the ProxySG appliance will not attempt to reauthenticate requests from that client. This setting specifies how long the client session can be inactive before the ProxySG appliance terminates the session; subsequent requests from that client will require authentication. By default, the client can be inactive for 900 seconds (15 minutes).

   - **Rejected credentials time**—(Basic credentials only) Specifies whether to cache failed authentication attempts (bad password, expired account, disabled account, old password, or server down). If the client attempts to connect again during the rejected credentials time, the ProxySG appliance will automatically reject the request for the specified period of time. Enter a value from 1 second (the default) to 10 seconds. Or, to disable this option, enter 0.

3. Specify how the appliance uses cookie surrogates by setting the **Cookies** settings. The cookie settings are only applicable if you plan to use an authentication mode that uses cookie surrogates.

   - **Use persistent cookies**—By default, this option is deselected, which means that the ProxySG
appliance will use session cookies when creating a cookie surrogate for a client. Session cookies are only valid during the current browser session and are deleted when the user closes the browser. Therefore, the ProxySG must reauthenticate the client each time the user starts a new browser session. If you select this option, the appliance will use persistent cookies instead of session cookies. Persistent cookies are stored on the client system and are therefore not deleted at the end of the browser session. When using persistent cookies, the ProxySG appliance will only need to reauthenticate a client when the cookie in its surrogate credential database expires.

- **Verify the IP address in the cookie** – By default, this option is selected which means that the ProxySG appliance will only accept a cookie from a client if the client IP matches the IP address in the surrogate cookie. To enable the appliance to accept cookies from IP addresses that do not match the address in the cookie—for example if you use DHCP—deselect this option.

4. (Transparent proxy only) Specify a URL to which to redirect client requests that require authentication in the **Virtual URL** field.

For best results, the virtual URL you specify must:

- Contain a simple hostname that does not contain any dots (for example, use http://myproxy rather than http://myproxy.acme.com. This allows Internet Explorer to recognize the URL as part of the Intranet zone rather than the Internet zone so that the browser will automatically return credentials when challenged rather than prompting the user.

- Resolve to the IP address of the ProxySG appliance by adding an "A" record to your internal DNS server that associates the virtual URL with the ProxySG appliance IP address.
Connect to a Secure LDAP Server

By default, LDAP traffic between the ProxySG appliance and the LDAP directory server is handled via an insecure connection. You can encrypt traffic by enabling LDAP over SSL (LDAPS) in the LDAP realm. This is accomplished by installing a CA certificate signed by the secure LDAP server onto the ProxySG appliance. After the ProxySG validates the LDAP directory’s server certificate, an encrypted communication channel is established.

Your LDAP directory must conform to LDAPv3 standards to take advantage of LDAPS.

1. Install the CA certificate on the ProxySG appliance to validate the certificate presented by the LDAP directory server.
   a. In the ProxySG Management Console, select Configuration > SSL > CA Certificates.
   b. Click Import and enter a name for the new certificate.
   c. Copy and paste the certificate details into the CA Certificate PEM text box. Be sure to include the entire certificate, beginning with -----BEGIN CERTIFICATE----- and ending with -----
Configure LDAP Authentication

End Certificate------, as shown below.

The CA certificate generated by the secure LDAP server needs to be in a PEM (Privacy Enhanced Mail) Base 64 encoded format.

b. Click OK and Apply to set the changes.

2. Create a CA Certificate List restricting trust to the LDAP CA certificate(s).
   a. Click the CA Certificate Lists tab.
   b. Click New to create a new CA Certificate List. Name the profile so that is readily identifiable.
   c. Select the newly imported certificate from the left column and then click Add >> to place it into the CA Certificate List in the right column.
   d. Click OK and Apply to set the changes.

3. Create a device profile to use the keyring.
   a. Click Device Profiles from the left pane and then New to create a new device profile. Name the profile so that is readily identifiable.
b. Select the CA Certificate List that you just created from the CCL drop down menu. All other default settings should be retained.

c. Click OK and Apply to set the changes.

4. Enable SSL connections on the ProxySG LDAP realm.

   a. In the ProxySG Management Console, select Configuration > Authentication> LDAP> LDAP Servers and select the realm to configure.

   b. Click the Enable SSL check box.

   c. Set the SSL device profile to the newly created device profile.

   d. Click OK and Apply to set the changes.

5. (Optional) Add an alternate LDAP directory server.

   a. Specify the IP address of the alternate LDAP directory server.

   b. Specify the port. In most cases, LDAPS uses a default port of 636.

   c. Click Apply to set the changes.
Configure LDAP Authentication

Verify LDAP Directory Connectivity

Verify that the ProxySG appliance can successfully authenticate a user located on the LDAP directory server. You can test authentication by entering the username and password of a specific user located in an LDAP realm. Keep in mind, you can only test the credentials of a user that is under the DN(s) that are associated with a particular LDAP realm.

1. In the ProxySG Management Console, select Configuration > Authentication > LDAP > LDAP Realms > LDAP Servers.
2. Click Test Configuration.
3. When prompted, enter the username and password of an LDAP user and then click OK.
4. The appliance sends an authentication request to the configured LDAP directory server and then displays a message indicating whether the authentication succeeded or failed. If the test failed, it could be the result of incorrect user credentials or realm configuration. If the test succeeds, you'll receive a message indicating a successful configuration.
Create a Web Access Policy

After you verify that the ProxySG appliance can successfully communicate with the LDAP directory server, you can create specific rules to govern authenticated users and groups. If you do not add any Web Access authorization rules, every available group (and users associated with the group) can be authenticated for access to the network. The policy below limits the traffic to a specific group that can be granted access to network resources.

When a user from the specified group attempts to access the network using an explicitly configured browser, they are automatically prompted for username and password credentials.

This topic shows how to create a policy using the Visual Policy Manager (VPM). You can also create policy using the Content Policy Language (CPL).

Note that you must create an LDAP realm before you can define the corresponding access policy.

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.

2. Create the policy rule that enables the ProxySG appliance to authenticate client requests.
   b. Enter a Layer Name to distinguish this layer from another layer and then click OK. The first policy rule displays with default settings.

3. Configure the action.
   a. Right-click the Action column and then select Set. The Set Action Object dialog displays.
   b. Click New and then select the Authenticate... object. The Add Authenticate object dialog displays.
   c. Specify a Name for the authentication object you just created.
   d. Select Realm and then select the LDAP realm that you wish to use from the drop-down list.
   e. Select the authentication mode from the Mode drop-down list. Although you can select Auto to have the ProxySG appliance automatically choose an authentication mode, it is usually better to make a selection that is appropriate for your deployment as follows:

      - Explicit deployments—Select Proxy or Proxy IP. The Proxy IP mode reduces the load on the network because it uses an IP surrogate to reauthenticate clients that have...
Configure LDAP Authentication

already successfully authenticated.

- **Transparent deployments**—Select **Origin Cookie Redirect**. This mode redirects the client to the virtual URL for authentication and uses a **cookie surrogate** to reauthenticate clients that have already successfully authenticated. The appliance will automatically downgrade to the **Origin IP Redirect** mode for user agents that do not support cookies.

  f. Click **OK** to close the Add Authenticate Object dialog.
  g. Click **OK** to close the Set Action Object dialog.

4. **(Optional) Restrict source IP addresses to specific test workstations or networks.**
   a. Right-click the **Source** column and then select **Set**... The Set Source Object dialog displays.
   b. Click **New** and then select the **Client IP Address/Subnet**... object. The Add Client IP Address/Subnet object dialog displays.
   c. Specify an **IP Address** or Subnet Mask of the workstation/network that you want to limit the affects of the policy to and click Add. You can add as many IP addresses as you wish.
   d. Click Close when you have finished entering the IP addresses/Subnet masks.
   e. Click **OK** to close the Set Action Object dialog.

5. **Create the policy rule that enables the ProxySG appliance to grant users access to the network.**
   a. Select **Policy > Add Web Access Layer**.
   b. Enter a **Layer Name** or accept the default name and then click **OK**. The first policy rule displays with default settings.

6. **Configure the Web Access policy settings.**
   a. In the **Source** column of the first row, right-click and then select **Set**. The Set Source Object dialog displays.
   b. Click **New** and then select **Group**. The Add Group Object dialog displays.

      Enter the name of the LDAP group that you wish to authorize. Alternatively, you can add a **User** to authorize a specific user instead of an entire group. If you don't know what groups are available, you can view the LDAP directory using an LDAP browser.

   c. Select the LDAP **Realm** from the drop-down list.
   d. Click **OK** to close the Set source object and close the dialog.
   e. Click **OK** to close the Set Action Object dialog.
   f. In the **Action** column of the first row, right-click and then select **Allow**.
7. Install the access policy.
   a. Click **Install policy**.
   b. Click **OK** to acknowledge that the policy was successfully installed.

8. Test the authorization policy by accessing a network resource. Keep in mind, the browser must be configured explicitly to pass through the ProxySG appliance.
   a. Open your default Web browser and configure your browser to explicitly pass requests through the ProxySG appliance.
   b. Visit a Web page, such as www.bluecoat.com.
   c. When prompted, enter the user credentials. If the user is a valid entry in the LDAP group, the URL loads properly within the browser.
Optimize Your LDAP Realm

If you are experiencing poor LDAP performance when performing searches and comparisons, you can perform tune your LDAP realm. The standard LDAP realm settings have been set to provide accurate results over a range of possible configurations. Some of these options might generate unnecessary overhead, depending on how your LDAP directory is configured. Keep in mind you'll need to verify the options you set in the LDAP realm against the LDAP directory configuration, otherwise, the operations might return incorrect values.

1. Specify how you want the LDAP realm to handle alias entries when performing a search operation.

   When an LDAP alias entry points to another entry, the original entry is dereferenced, or removed from the search results; only the entry that was referenced is considered to be found. This dereferencing process can potentially reduce the performance of your LDAP deployment. However, to maximize accuracy of searches, the default setting is Always. You can change the dereferencing method for better search performance, but you'll need to verify that correct results are returned.

   a. Select the LDAP Search & Groups tab.
   b. Select a Dereference aliases option.
      - **Never** — Never dereferences an alias entry. Offers the highest search performance, but should only be selected only when alias entries are not present in the LDAP directory.
      - **Searching** — Dereferences alias entries only after locating the base entry of a search.
      - **Finding** — Dereferences alias entries only while locating the base entry of a search.
      - **Always** — Always dereferences an alias entry. Returns the most accurate search results when alias entries are present, but can cause reduced performance.
   c. Click Apply.

2. Enter an LDAP search filter clause to reduce the number of results that a group search returns.

   This option is only available for LDAP directories that store users within group entries.

   a. In the ProxySG Management Console, select Configuration > Authentication > LDAP > LDAP Realms.
   b. Select the LDAP Search & Groups tab.
   c. Enter a Group constraint filter option.
Configure LDAP Authentication

Constraints must be valid LDAP search filters and are AND’d to the search filter when performing a group search. For more information on valid LDAP search filters, refer to RFC2254.

- **Example 1** – If you enter `cn=p*` into the Group constraint filter field, only groups starting with the letter P are returned.

- **Example 2** – If you enter `cn=proxy` into the Group constraint filter field, only the proxy group is returned.

d. Click **Apply**.

3. Specify whether you want to perform group comparisons on the ProxySG appliance or send each compare operation to the LDAP directory.

   Typically compare operations are sent to the LDAP server for each query; however, if your network is experiencing excessive lag times when performing compares, offloading the operation onto the ProxySG appliance can significantly reduce load times, depending on how your LDAP directory is configured. The default is **Server**. If you have a very large user or groups, you can perform the comparisons on the ProxySG appliance. Depending on the LDAP schema and the number of users and groups, this can result in reduced load on the LDAP server.

   a. Select the **LDAP General** tab.

   b. Select a **Group comparison method** option. The default is **Server**.

      - **Local** – Offloads the compare operations onto the ProxySG after retrieving the LDAP entries. Because the compares are performed locally, this method typically reduces load on the LDAP server

      - **Server** – Queries the LDAP server for each compare operation. Keep in mind, if there are a large number of compare operations to perform, it can result in significant server load.

        There is a small possibility that local compares might produce differing results from server compares. If you suspect erroneous compare results, set to **Server**.

   c. Click **Apply**.
Configure LDAP Authentication

Create an LDAP Existence Check Policy

An LDAP existence check allows the client to verify whether or not a value of the specified LDAP attribute in the user’s entry is present. The LDAP attribute trigger enables you to create a policy rule that checks for the existence of a specific LDAP attribute. If a match is found during the search, the specified action is executed.

This topic shows how to create a policy using the Visual Policy Manager (VPM). You can also create policy using the Content Policy Language (CPL).

1. Launch the VPM.
   a. From the Management Console, select Configuration > Policy > Visual Policy Manager.
   b. Click Launch.
2. Create the policy rule that enables the ProxySG appliance to grant users access to the network.
   a. Select a valid policy layer. The LDAP Attribute Object exists in the Admin Access, SSL Access, Web Access, and Forwarding layers as Source objects. For example, to add an SSL Access layer, select Policy > Add SSL Access Layer. An Add New Layer dialog box appears.
   b. Enter a Layer Name or accept the default name and then click OK. The first policy rule displays with default settings.
3. Configure the settings for the policy rule that you created in the previous step.
   a. In the Source column of the first row, right-click and then select Set. The Set Source Object dialog displays.
   b. Click New and then select LDAP Attribute. The Add LDAP Attribute dialog displays.

       Enter the name of the LDAP attribute object that you wish to apply an action against. If you don't know what attributes are available, you can view the LDAP directory using an LDAP browser.
   c. Select an LDAP Authentication Realm from the drop-down list.
   d. Enter a valid LDAP Attribute Name.
   e. Select Attribute exists to perform a existence check against the value of the specified LDAP attribute from the user’s entry.
   f. Click OK to close the Set Action Object dialog.
   g. In the Action column of the first row, right-click and then select Allow.
4. Install the access policy.
a. Click **Install policy**.

b. Click **OK** to acknowledge that the policy was successfully installed.
Configure LDAP Authentication

Create an LDAP Attribute Comparison Policy

An LDAP compare operation allows the client to verify if a specified entry contains a given attribute. You can perform a compare operation using the VPM, using an attribute trigger. The LDAP attribute trigger enables you to create a policy rule that checks for a string match from an entry. If a valid match is found during the search, the specified action is executed.

This topic shows how to create a policy using the Visual Policy Manager (VPM). You can also create policy using the Content Policy Language (CPL).

1. Launch the VPM.
   a. From the Management Console, select **Configuration > Policy > Visual Policy Manager**.
   b. Click **Launch**.

2. Create the policy rule that enables the ProxySG appliance to grant users access to the network.
   a. Select a valid policy layer. The LDAP Attribute Object exists in the **Admin Access**, **SSL Access**, **Web Access**, and **Forwarding** layers as Source objects. For example, to add an SSL Access layer, select **Policy > Add SSL Access Layer**. An Add New Layer dialog box appears.
   b. Enter a **Layer Name** or accept the default name and then click **OK**. The first policy rule displays with default settings.

3. Configure the settings for the policy rule that you created in the previous step.
   a. In the **Source** column of the first row, right-click and then select **Set**. The Set Source Object dialog displays.
   b. Click **New** and then select **LDAP Attribute**. The Add LDAP Attribute dialog displays.

      Enter the name of the LDAP attribute object that you wish to apply an action against.
      If you don't know what attributes are available, you can [view the LDAP directory using an LDAP browser](#).

   c. Select an LDAP **Authentication Realm** from the drop-down list.
   d. Enter a valid LDAP **Attribute Name**.
   e. Select **Attribute value match** to perform a string comparison against the value of the specified LDAP attribute from the user’s entry.
   f. Specify a value with which to compare the LDAP attribute name.
   g. Select a comparison filter from the drop down.
   h. Click **OK** to close the Set Action Object dialog.


Configure LDAP Authentication

i. In the **Action** column of the first row, right-click and then select **Allow**.

4. Install the access policy.
   a. Click **Install policy**.
   b. Click **OK** to acknowledge that the policy was successfully installed.
Configure SAML Authentication

Before you configure SAML, make sure that you meet the requirements. The following procedures assume that you have installed and configured the administration software for your IDP.

1. Save a local copy of the IDP’s configuration data by exporting the IDP metadata file.

2. Prepare the appliance for SAML authentication:
   a. Import certificates to the CCL.
   b. Create an HTTPS reverse proxy service for the HTTPS POST endpoint.
   c. Define assertion attributes to specify which data the IDP should use to authenticate users.
   d. Create the SAML realm.
   e. After you create the SAML realm, configure general settings.

3. (Optional) To authorize users through one or more SAML realms, specify the criteria to use when searching for users.

4. Configure your IDP:
   - "Configure AD FS" on page 129
   - Configure Oracle
   - "Configure SiteMinder" on page 132
   - (Supported in SGOS 6.5.2 and later) "Configure Shibboleth" on page 140

5. Include the realm in your policy.
Export the IDP Metadata File

To export the IDP metadata file, log in to the IDP’s administration software.

Exporting IDP metadata entails saving the XML document to disk. It is important to save the metadata file without opening it in a browser first. Browsers do not necessarily support XML file structure and may change the XML tags.

If you use SiteMinder, Oracle, or Shibboleth, you will need to copy and paste the metadata file contents to the CLI using the inline idp-metadata command. Because XML files are text-based, it is best to use a text editor such as Notepad to open the file to copy its contents.

To ensure that the SAML realm is configured correctly, Blue Coat recommends that you import metadata instead of entering the information manually. If there are issues with realm configuration, the Authentication debug log shows the following error: The SAML realm configuration is invalid.

Export Metadata from AD FS

1. Log in to the AD FS MMC.
2. Select Endpoints and look under Metadata for the URL beside the Federation Metadata type.
3. Copy the URL and paste it into a browser address bar.
4. Save the XML file to a location that the appliance can access.

Export Metadata from SiteMinder

Before you can export metadata, make sure that you have created a SAML 2.0 IDP. This assumes that you have already created the IDP (entity) in SiteMinder.

1. Log in to the CA Federation Manager.
2. Select Federation > Entities.
3. Beside the entity you created, select Action > Export Metadata.
4. In the Partnership Name field, enter a name to identify the partnership between the ProxySG appliance and SiteMinder. You will refer to this partnership name later, when you configure the partnership in SiteMinder.
5. Click Export. SiteMinder generates the metadata document.
6. Save the XML file to a location that the appliance can access.
Configure SAML Authentication

Export Metadata from Oracle

1. Log in to the Oracle Enterprise Manager.
2. In the navigation tree on the left, select Identity and Access > OIF.
3. On the main page, select Oracle Identity Federation > Administration > Security and Trust.
4. Click the Provider Metadata tab.
5. In the Generate Metadata section, select Identity Provider from the Provider Type menu.
6. Select SAML 2.0 from the Protocol menu.
7. Click Generate. OIF generates the metadata document.
8. Save the XML file to a location that the appliance can access.

Export Metadata from Shibboleth

1. On the server where Shibboleth is installed, browse to the <shibboleth>/metadata folder.
2. Copy the idp-metadata.xml file.
3. Save the XML file to a location that the appliance can access.
Configure the CCL

The ProxySG appliance CCL must contain at least a root certification authority (CA) certificate, but depending on other considerations, you may require more certificates. Determine which certificates you must import to the CCL:

- Root CA certificate—**Required.** Add the certificate for the root CA that issued the IDP’s signing certificate to the CCL.

- IDP’s signing certificate—**Required if self-signed.** If the IDP’s signing certificate is self-signed, add it to the CCL. CA-signed certificates are included in SAML assertions.

- Intermediate CA certificate—**Optional.** You must import intermediate CA certificates to the ProxySG appliance, but it is not necessary to add them to the CCL. For instructions on importing certificates to the appliance, refer to the "Importing CA Certificates" section in the "Managing X.509 Certificates" chapter in the *SGOS Administration Guide.*

In explicit deployments, if you do not add the certificate for the CA that issued the IDP’s certificate to the appliance’s CCL, HTTPS connections to the IDP fail.
Set up an HTTPS Reverse Proxy Service

You should create an HTTPS reverse proxy service only if the SAML realm uses an HTTPS, rather than HTTP, POST endpoint.

Determine whether to use an HTTP or HTTPS POST endpoint:

- If you use AD FS, the POST endpoint must use HTTPS.
- If you use SiteMinder or Oracle, the POST endpoint can use either HTTPS or HTTP.
- If you want greater security, use an HTTPS POST endpoint.

Regardless of which IDP you use, Blue Coat recommends using an HTTPS POST endpoint.

Create an HTTPS reverse proxy service to act as the SAML realm’s HTTPS POST endpoint. The IDP redirects browsers to this service when it creates assertions.

SSL connections require a certificate and a private key. Browsers must trust the certificate that the HTTPS reverse proxy service uses, and the certificate’s Subject value must match the Virtual host configured in the SAML realm (see "Configure the SAML Realm" on page 125). If the names do not match, SSL hostname mismatch errors occur.

For instructions on creating the HTTPS reverse proxy service, refer to the Reverse Proxy Deployment WebGuide.
Define Assertion Attributes

The ProxySG appliance maps policy conditions to assertion attribute values. If you require more attributes than the ones included in SAML assertions, you can define them in the SAML realm.

1. In the Management Console, select **Configuration > Authentication > SAML > Attributes**.
2. Click **New**. The console displays the Add SAML Attribute dialog.
3. Enter attribute settings:
   - **Attribute name**—This is the name of the attribute as it appears in the appliance and IDP configuration, and when referring to the attribute in the attribute.<name>= policy condition. The name must be unique.
   - **Attribute data type**—Select case-exact-string or case-ignore-string. The appliance uses this setting to match assertion attribute values with policy conditions.
   - **SAML name**—This is the name of the attribute as it will appear in assertions from the IDP, in the Name= XML attribute of the <Attribute> element. For example, an assertion might include the line <saml:Attribute Name="mail"> where mail is the SAML attribute name.
4. Click **OK**, and then click **Apply**.

Starting in SGOS 6.6.2.x, you can forward SAML attributes in SAML 2.0 assertions through HTTP headers to back-end servers by creating substitution policy. See "SAML Attribute Substitutions" below.

SAML Attribute Substitutions

(Introduced in SGOS 6.6.2.x) You can forward SAML attributes (including the user name) in SAML 2.0 assertions through HTTP headers to back-end servers by creating substitution policy. The SAML substitution uses the following CPL syntax:

```cpl
$(saml.attribute.<name>)
```

To forward SAML attributes using substitution policy:

1. In the SAML realm configured on the appliance, define the attribute you want to forward.
   
   If you remove an attribute that is referenced in policy, the appliance issues a warning the next time that policy is compiled.

2. In the VPM, add a Web Access Layer.

3. In the Source column, add a **SAML Attribute** object that specifies the attribute to forward.
Configure SAML Authentication

If the attribute you specify does not exist in the SAML realm, the appliance issues a warning when it compiles policy.

4. In the Action column, add a Control Request Header or Control Response Header object. Select Set Value and enter the substitution:

\[
\$(\text{saml.attribute.<name>})
\]

where \text{<name>} is the name of the attribute to forward.

5. Install the policy.

After you install the substitution policy, the appliance evaluates the configured policy rules and modifies the HTTP request/response headers with the additional x-header fields corresponding to attribute names with the attribute values. When the appliance compiles policy, it validates the field attribute \text{<name>} against configured SAML attributes.

You can alternatively add the substitution policy through the #inline policy command or CPL. For information on those methods, refer to the Command Line Interface Reference and the Content Policy Language Reference, respectively.
Configure the SAML Realm

1. In the Management Console, select **Configuration > Authentication > SAML.**

2. Click **New.**

3. On the Add SAML Realm dialog, in the **Realm name** field, enter a name for the realm. The realm name identifies the realm in areas of the Management Console such as logs and the Visual Policy Manager.

4. Select the trusted CCL. From the **Federated IDP CCL** menu, select the CCL you created in "Configure the CCL" on page 121.

5. Specify configuration parameters:
   - (AD FS only) Use preconfigured settings for the IDP. Copy and paste the URL for the metadata into the **Federated IDP metadata URL** field.
   - (SiteMinder, Shibboleth, and Oracle) Import metadata through the `#(config saml <realm-name>)inline idp-metadata <XML>` CLI command.

6. From the **Encryption keyring (optional)** menu, select the keyring to use for decrypting encrypted assertions.

7. (Optional) If you require that assertions from the IDP be encrypted, mark the **Require encryption** check box. If you mark the check box, the ProxySG appliance rejects unencrypted assertions. Note that as long as the encryption keyring is configured, the appliance attempts to decrypt encrypted assertions whether or not the **Require encryption** check box is marked.

8. Specify the hostname for the SAML endpoint; in other words, point to the HTTPS reverse proxy listener you set up. In the **Virtual host** field, enter the host and port in format `<hostname_or_IP_address>:<port_number>`. The hostname must match the name of the SSL certificate for the HTTPS reverse proxy service. See "Set up an HTTPS Reverse Proxy Service" on page 122.

9. (Optional) Define limits for assertions’ timestamps. Assertions with timestamps that fall outside of these limits are invalid.
   - Specify an interval before the current time. Assertions stamped before this interval are invalid. In the **Not before** field, specify the number of seconds. The default value is 60.
   - Specify an interval after the current time. Assertions stamped after this interval are invalid. In the **Not after** field, specify the number of seconds. The default value is 60.

10. (If applicable) If you defined your own assertion attributes ("Define Assertion Attributes" on page 123), select them from the following menus:
   - **SAML user attribute**—This is the attribute containing the relative username. If you do not specify the attribute, the appliance uses the SAML Name ID value for the username.
   - **SAML fullname attribute**—This is the attribute containing the full username.
Configure SAML Authentication

- **SAML group attribute**—This is the name of the group membership attribute. Values of this attribute match the group= policy condition.

11. (Optional; available in SGOS 6.5.2 and later) Select an **SSL device profile** to use to communicate with the IDP when the redirect/POST URL uses HTTPS.

12. (Optional; available in SGOS 6.5.2 and later) If the client cannot be redirected to, or communicate directly with, the IDP—for example, if a firewall exists between users and the IDP—select **Disable client redirects** to disable the appliance’s ability to redirect the browser to the IDP for authentication. When you disable client redirects, the appliance handles all communication with the IDP and OCS on behalf of the client.

13. (If you selected **Disable client redirects** in the previous step) Determine if you want to prevent the appliance from adding a BCSI-SWR- prefix to IDP cookies; this prefix prevents IDP cookies and OCS cookies from having the same name.
   The **Prefix IDP cookies** option is available and enabled by default when you select **Disable client redirects**; clear the **Prefix IDP cookies** option if you do not want to add the prefix to cookies.

14. Click **OK** to save the realm.
Configure General Settings

1. In the Management Console, select Configure > Authentication > SAML > SAML General.
2. From the Realm name menu, select the SAML realm.
3. Configure the following as required.
   - **Display name**—Set the display name of the realm.
   - **Refresh Times**—Do one of the following.
     - Mark the **Use the same refresh time for all** check box to set the same refresh time for credentials and surrogates.
     - Enter different refresh times (in seconds) for credentials and surrogates.
   - **Inactivity timeout**—Enter the number of seconds a session can be inactive before it times out.
   - **Rejected credentials time**—Enter a refresh time (in seconds) for rejected credentials.
   - **Cookies**—Do one or both of the following:
     - **Use persistent cookies**—Mark this to use persistent cookies; leave this unmarked to use session cookies.
     - **Verify the IP address in the cookie**—Mark this to enable verification of cookies’ IP addresses.
   - **Challenge user after logout**—Mark this to enable challenging after logout. For example, if this setting is enabled and a user logs out of a web site, the user must enter credentials again the next time they access the web site.
4. Click **Apply** to save your changes to general SAML settings.
Configure SAML Authorization

1. In the Management Console, select Configuration > Authentication > SAML > Authorization.

2. From the Realm name drop-down list, select the SAML realm for which you want to configure authorization settings.

3. (If applicable) To authorize with the current realm, mark the Self check box. If you select Self, the Authorization username is set automatically to Use FQDN.

4. If you use LDAP for authorization and Use FQDN is selected, ensure that the SAML fullname attribute (see "Configure the SAML Realm" on page 125) contains the user's distinguished name. Later, you must also configure the IDP to send the distinguished name in assertions.

To authorize with another realm, go to the next step.

5. (If applicable) Select the realm with which to authorize from the Authorization realm name menu. Then, choose one of the following options:

   - **Authorization username**—Enter the username in the field.
   - **Use FQDN**—Use the fully-qualified domain name (FQDN).
   - **Determine by search**—Determine the username by LDAP search. Specify the following.
     - **LDAP search realm name**—Enter the name of the LDAP search realm.
     - **Search filter**—Specify the LDAP search filter.
     - **User attribute or FQDN**—Specify either the LDAP attribute name or the FQDN as the username attribute for search results.
     - **Set Users to Ignore**—Add, edit, or remove usernames from the list of users to ignore when determining authorization.

6. Click **Apply** to save your changes to SAML authorization settings.

Policy Conditions

The ProxySG appliance uses existing policy conditions to make authorization decisions for the user. These policy conditions map to assertion attribute values.

- **group=**

The group= condition maps to the values of the SAML group attribute setting specified in the realm.

- **attribute.<name>=**

The attribute.<name>= condition maps to the values of the Attribute name setting specified in the realm.
Configure AD FS

The following steps comprise the minimum required settings to create trust between the ProxySG appliance and AD FS. For other settings that you may require for your deployment, refer to the AD FS documentation.

To perform the procedures in this section, you must be logged in with administrator credentials on the AD FS server.

**Step 1 - Import the ProxySG Certificate to AD FS’s Trust List**

Before the AD FS server can import metadata from the SAML realm, AD FS has to trust the ProxySG appliance’s default certificate. To create trust, add the certificate to AD FS’s trust list.

The following procedure describes how to add the certificate to AD FS’s trust list in Microsoft Internet Explorer 9.x.

1. In the browser, select **Tools > Internet Options > Content**.
2. Click **Certificates**, and then click **Import**.
3. When you are prompted to specify a store in which to install the certificate, select **Trusted Root Certification Authorities**.
   
   If you do not select the Trusted Root Certification Authorities store, any error messages that occur may be inaccurate or unintuitive.

**Step 2 - Import ProxySG Metadata to AD FS**

1. In the AD FS MCC, select **AD FS 2.0 > Trust Relationships > Relying Party Trusts**.
2. Select Relying Party Trusts, right click, and then select **Add Relying Party Trust**.
3. The MMC displays a wizard. Click **Start**.
4. Make sure that **Import data about the relying party published online or on a local network** is selected.
5. In the **Federation metadata address (host name or URL)** field, enter the following URL:
   
   https://<IP-address>:8082/saml/metadata/<realm-name>/sp
   
   In the URL, `<IP-address>` is the address of the appliance, and `<realm-name>` is the name of the SAML realm.
6. Click **Next**.

   If an error message displays when you click **Next**, verify that you imported the certificate correctly and verify that the hostname you specified in the URL in the previous step matches the certificate’s **Subject** value.

   In addition, if AD FS fails to validate the certificate, a generic error message displays; the message does not indicate that the certificate is invalid.
Configure SAML Authentication

7. Enter a display name for the relying party trust and then click Next.

8. To allow access to the appliance for all users, select Permit all users to access this relying party. Do not select this option if you want to limit access to the appliance to authorized users. Click Next.

9. Review your settings and click Next.

10. Make sure that Open the Edit Claim Rules is selected, and then click Close. AD FS prompts you to edit claim rules.

**Step 3 - Set up Claim Rules for Assertions**

1. In the AD FS MMC, select AD FS 2.0 > Trust Relationships > Relying Party Trust.

2. Select the relying party trust that you created in Step 2, right click, and click Edit Claim Rules.

3. The MMC displays a dialog. Click Add Rule.

4. Make sure that Send LDAP Attributes as Claims is selected for Claim rule template, and then click Next.

5. Configure the rule. You can configure the rule to send any attribute, but this procedure describes the following:

**Send User Identity**

The procedures for configuring assertion attributes refer to the attribute’s SAML name. The SAML name is the name that you specified for the attribute in "Define Assertion Attributes" on page 123.

The following procedure tells you how to pass the User Principal Name attribute in the SAML Name ID assertion.

1. Specify the following in the claim rule wizard:
   - In the Claim rule name field, enter the attribute’s SAML name.
   - For Attribute store, select Active Directory for the attribute store.
   - For LDAP Attribute, select the User-Principal-Name attribute.
   - For Outgoing Claim Type, select Name ID.

2. Click Finish, and then click OK.

3. (If required) To add another claim rule, repeat steps 2 through 4 in Step 3.

**Send Distinguished Name**

If you use LDAP for authorization, you must configure a claim rule to send the distinguished name in assertions.
1. Specify the following in the claim rule wizard:
   - In the Claim rule name field, enter the attribute's SAML name.
   - For Attribute store, select Active Directory for the attribute store.
   - For LDAP Attribute, enter distinguishedname in lower case. (You can type in the drop-down menu.)
     Due to a limitation in AD FS, the attribute name disappears if you enter the name once and then go to next field. When this happens, enter the attribute name again exactly as it is shown above.
   - For Outgoing Claim Type, enter DN.

2. Click Finish, and then click OK.

3. (If required) To add another claim rule, repeat steps 2 through 4 in Step 3.

**Send Group Membership**

You can set up AD FS to send group memberships in assertions. Create another claim rule to specify the attribute, and then add an attribute in SAML.

1. Specify the following in the claim rule wizard:
   - In the Claim rule name field, enter the attribute’s SAML name.
   - For Attribute store, select Active Directory for the attribute store.
   - For LDAP Attribute, select the Token Groups-Unqualified Names attribute.
   - For Outgoing Claim Type, select Group.

2. Click Finish, and then click OK.

3. (If required) To add another claim rule, repeat steps 2 through 4 in Step 3.
Configure SAML Authentication

Configure SiteMinder

The following steps comprise the minimum required settings to create a partnership between the ProxySG and SiteMinder. For other settings that you may require for your deployment, refer to the CA SiteMinder documentation.

To perform the procedures in this section, you must be logged in with administrator credentials on the SiteMinder server.

Step 1 - Import Metadata to SiteMinder

1. In a browser, go to the following URL to export ProxySG appliance metadata:
   https://<IP-address>:8082/saml/metadata/<realm-name>/sp
2. Save the file to disk.
3. In the CA Federation Manager, select Federation > Entities.
4. Click Import Metadata.
5. Beside the Metadata file field, browse to the metadata file you saved in the first step.
6. Make sure that the following are selected:
   - For Import As, select Remote Entity.
   - For Operation, select Create New.
7. Click Next.
8. In the Entity Name field, enter a name for the appliance as a service provider.
9. Click Next. (The Import Certificates step is skipped if the appliance metadata doesn’t contain a certificate.)
10. Confirm your settings, and then click Finish.

Step 2 - Configure the Partnership Between SiteMinder and the ProxySG

1. Select Federation > Partnerships.
2. Locate the partnership you created when you exported SiteMinder metadata ("Export the IDP Metadata File" on page 119). Beside the partnership name, select Action > Edit.
3. Specify the following:
   - For Remote SP, select the remote entity you specified when you imported appliance metadata.
   - From Available Directories, select the LDAP directories you want to use. On the right, you can move directories up or down to dictate the search order.
4. Click Next.

5. (Optional) On the Federation Users step, specify search filters or users to exclude from accessing the appliance.

6. Click Next. The next step is Assertion Configuration; see Step 3.

Step 3 - Configure Assertions

After you configure the partnership, you are at the Assertion Configuration step. To send user attributes in SAML assertions:

1. In the Name ID section, for Name ID Format, select the identity format to be passed in SAML assertions.

2. For Name ID Type, select User Attribute.

3. In the Value field, specify the primary user attribute, for example, sAMAccountName for Active Directory.

4. In the Assertion Attributes section, click Add Row.

Configure attributes for the assertion. You send any attribute in assertions, but this procedure describes the following:

The procedures for configuring assertion attributes refer to the attribute’s SAML name. The SAML name is the name that you specified for the attribute in "Define Assertion Attributes" on page 123.

Send User Identity

1. In the Assertion Attribute field, enter the attribute’s SAML name.

2. For Type, select User Attribute.

3. For Value, enter the name of the attribute you want to send.

4. Click Next or add another attribute.

5. To add another attribute, click Add Row in the Assertion Attributes section.

Send Group Membership

Add the memberOf attribute to send group membership information in assertions.

1. In the Assertion Attribute field, enter the attribute’s SAML name.

2. For Type, select User Attribute.

3. For Value, enter memberOf.
Configure SAML Authentication

4. If any users are members of multiple groups, change the **Value** to `FMATTR:memberOf`. If you do not modify the attribute value, SiteMinder incorrectly adds the attribute to the assertion, combining all attribute values in a single XML element.

5. Click **Next** or add another attribute.

6. To add another attribute, click **Add Row** in the Assertion Attributes section.

**Send Distinguished Name**

If you use LDAP for authorization, you must configure SiteMinder to send the distinguished name in assertions.

1. In the Assertion Attribute field, enter the attribute’s SAML name.

2. For Type, select **User Attribute**.

3. For Value, enter `distinguishedName`.

4. Click Next or add another attribute.

5. To add another attribute, click **Add Row** in the Assertion Attributes section.

**Step 4 - Select Authentication Mode**

1. After you configure assertions, you are at the SSO and SLO step.

2. In the SSO section, select **HTTP-POST** for the SSO Binding.

3. Click **Next**.

**Step 5 - Configure Signing and Encryption**

After you select the authentication mode, you are at the Signature and Encryption step.

1. In the Signature section, for Signing Private Key Alias, select the key that is used to sign assertions.

2. Alternatively, or if there is no private key in the certificate data store, you can generate a signing key or import one from a PKCS#12 (private key and certificate) file.

3. For Post Signature Options, select **Sign Assertion**.

4. Make sure that **Require Signed Authentication Requests** is not selected.

5. Click **Next**.

6. Confirm your settings and click **Finish**.

**Step 6 - Send Encrypted Assertions**

If SiteMinder will be sending encrypted assertions to the ProxySG appliance, create an encryption keyring in the SAML realm. For instructions, see "Creating a Keyring" in the "Managing X.509 Certificates" chapter in the **SGOS Administration Guide**. Then, export appliance metadata. Importing the metadata to SiteMinder
imports the certificate from the keyring.

You can select the **Show key pair** option so that you can view and copy the keyring as a backup. Backing up the keyring lets you easily import it again should you need to back up the appliance configuration later.

1. In the Oracle Enterprise Manager, select **Federation > Partnerships**.
2. Beside the partnership you created, select **Action > Edit**.
3. Select the **Signature and Encryption** step.
4. In the Encryption section, select **Encrypt Assertion**.
5. Beside Encryption Certificate Alias, click **Import** and browse to the certificate you exported.
6. Click **Next**.
7. Click **Finish**.

**Step 7- Activate the Partnership**

After you have defined the partnership, you must activate it. If users attempt to authenticate while the partnership is not activated, SiteMinder provides an HTTP 500 error message without an explanation of the cause of the error.

1. In the CA Federation Manager, select **Federation > Partnerships**.
2. Beside the partnership you created, select **Action > Activate**. The Federation Manager displays a confirmation dialog. Click **Yes**.
   After you activate a partnership, you cannot edit it unless you deactivate it first (**Action > Deactivate**).
   After you have edited the partnership, it is in an inactive state until you activate it again.
3. Confirm the settings and then click **Finish**.
4. Beside the partnership, select **Action > Activate**.
Configure SAML Authentication

Configure Oracle

The following steps comprise the minimum required settings for federation between the ProxySG appliance and Oracle. For other settings that you may require for your deployment, refer to the Oracle documentation.

To perform the procedures in this section, you must be logged in with administrator credentials on the Oracle server.

Step 1 - Import Metadata in Oracle

1. Go the following URL to export appliance metadata:
   https://<IP-address>:8082/saml/metadata/<realm-name>/sp
2. Save the file to disk.
3. In the Oracle Enterprise Manager, select Oracle Identity Federation > Administration > Federations.
4. In the table of Trusted Providers, click Add.
5. In the Add Trusted Provider dialog, beside Metadata Location, click Choose File and browse to the location of the metadata file that you saved in step 2.
6. Click OK.

Step 2 - Set up Federation Between the ProxySG Appliance and Oracle

To set up federation, first configure the appliance as a service provider. Then, configure Oracle as the identity provider.

1. In the Oracle Enterprise Manager, select Oracle Identity Federation > Administration > Federations.
2. In the table of Trusted Providers, select the Provider ID you added when the appliance metadata was imported, and then click Edit.

Step 3 - Select Update Provider Manually

1. For Provider Types, make sure that both Service Provider and Authentication Requester are selected.
3. In the list of attributes, select Email Address and clear all other selections.
4. Click Apply.
5. Select Oracle Identity Federation > Administration > Identity Provider.
6. On the SAML 2.0 tab, select Enable Identity Provider.
Configure SAML Authentication

7. In the Assertion Settings section, select **Send Signed Assertion**.
8. Click **Apply**.

**Step 4 - Set up Attribute Mappings**

When you set up attribute mapping, you specify the name with which an attribute should be defined in the SAML assertions.

1. In the Oracle Enterprise Manager, select **Oracle Identity Federation > Administration > Federations**.
2. Select the Provider ID for the appliance and then click **Edit**.
3. On the Oracle Identity Federation Settings tab, next to Attribute Mappings and Filters, click **Edit**.
4. Configure the assertion. You can send any attribute, but this procedure describes the following:

**Send User Identity**

1. On the Name Mappings tab, click **Add**.
2. On the Add Attribute Name Mapping dialog, specify the following:
   - For **User Attribute Name**, enter `sAMAccountName`.
   - For **Assertion Attribute Name**, enter the attribute’s SAML name.
   - Select **Send with SSO Assertion** in order for the attribute to appear in the assertion.
3. Click **OK**.
4. Click **OK** to save your changes. Alternatively, click **Add** to add another attribute.

**Send Distinguished Name**

The procedures for configuring assertion attributes refer to the attribute’s SAML name. The SAML name is the name that you specified for the attribute in "Define Assertion Attributes" on page 123.

1. Click **Add**.
2. On the Add Attribute Name Mapping dialog, specify the following:
   - For **User Attribute Name**, enter `distinguishedName`.
   - For **Assertion Attribute Name**, enter the attribute’s SAML name.
   - Select **Send with SSO Assertion** in order for the attribute to appear in the assertion.
3. Click **OK**.
4. Click **OK** to save your changes. Alternatively, click **Add** to add another attribute.
Configure SAML Authentication

**Send Group Membership**
Add the memberOf attribute to send group membership information in assertions.

1. Click **Add**.
2. On the Add Attribute Name Mapping dialog, specify the following:
   - For User Attribute Name, enter *memberOf*.
   - For Assertion Attribute Name, enter the attribute’s SAML name.
   - Select **Send with SSO Assertion** in order for the attribute to appear in the assertion.
3. Click **OK**.
4. Click **OK** to save your changes. Alternatively, click **Add** to add another attribute.

**Step 5 - Sign Outgoing Assertions**
If you have not already set up Oracle with a signing certificate, select a keystore to sign outgoing assertions. If you have already set up a signing certificate, skip this step.

1. In the Oracle Enterprise Manager, select **Oracle Identity Federation > Administration > Security and Trust**.
2. Click **Wallet**.
3. Click **Update**.
4. In the Update Wallet dialog, in the Signature section, select a keystore that contains the certificate and private key to use for signing outgoing assertions.
5. Click **OK**.

**Step 6 - Send Encrypted Assertions**
If Oracle will be sending encrypted assertions to the ProxySG appliance, create an encryption keyring in the SAML realm. For instructions, refer to "Creating a Keyring" in the "Managing X.509 Certificates" chapter in the SGOS Administration Guide. Then, export appliance metadata. Importing the metadata to Oracle imports the certificate from the keyring.

To send encrypted assertions after you have imported the certificate:

1. In the Oracle Enterprise Manager, select **Oracle Identity Federation > Administration > Federations**.
2. In the table of Trusted Providers, select the Provider ID for the appliance, and then click **Edit**.
3. On the Oracle Identity Federation Settings tab, scroll down to **Identity Provider/Authority Settings**.
4. Verify the following options.

- In the Assertion Settings list, select **Send Encrypted Assertions**.
- In the Protocol Settings list, select **Include Signing Certificate in XML Signatures**.
- In the Messages to Send/Require Signed list, beside Response with Assertion - HTTP POST, clear **Send Signed**.

5. Click **Apply**.

Be sure to update the metadata after enabling encrypted assertions if the last metadata file you uploaded didn't include the encryption keyring.
Configure Shibboleth

You can configure Shibboleth as an IDP in SGOS 6.5.2 and later.

The following steps comprise the minimum required settings to create a partnership between the ProxySG appliance and Shibboleth. For other settings that you may require for your deployment, refer to the Shibboleth documentation.

**Step 1 - Import Shibboleth’s Certificate to the ProxySG Appliance**

1. Copy the contents of `<shibboleth>/conf/idp.cert`.
2. In the Management Console, select **Configuration > SSL > CA Certificates**. Click **Import**.
3. Click **Paste from Clipboard**. Click **OK**.
4. Include this certificate in a CCL. See "Configure the CCL" on page 121.

**Step 2 - Configure the Partnership**

1. Download the ProxySG’s SAML realm metadata. It is located in https://<IP_address>:8082/saml/metadata/<realm-name>/sp.
2. In the Management Console, select **Statistics > Advanced**. The console displays a list of advanced URLs.
3. Scroll to SAML2 and look for **SP metadata for SAML2 realms**. Make note of the following metadata:
   - The ID ("entityID" in EntityDescriptor element)
   - The virtual protocol, hostname, and port number ("Location" attribute in "AssertionConsumerServiceElement")

   You require this information for the next step.
4. Copy the metadata to `<shibboleth>/metadata/<my-metadata>.xml`.
5. Add a new relying party in Shibboleth. Add the following in `<shibboleth>/conf/relying-party.xml`

```
<rp:RelyingParty provider="<virtual-host>/saml/<realm-name>" id="<virtual-host>/saml/<realm-name>" defaultSigningCredentialRef="IdPCredential">
  <rp:ProfileConfiguration xsi:type="saml:SAML2SSOProfile" includeAttributeStatement="true" assertionLifetime="PT5M" assertionProxyCount="0" signResponses="never" signAssertions="always" encryptAssertions="never" encryptNameIds="never"/>
</rp:RelyingParty>
```
Note that the "id" attribute must be unique among other existing metadata providers.

```
<metadata:MetadataProvider id="<an id>
"xsi:type="metadata:ResourceBackedMetadataProvider">
<metadata:MetadataResource xsi:type="resource:FilesystemResource"
file="<shibboleth>/metadata/<my-metadata>.xml"/>
</metadata:MetadataProvider>
```
Add the Realm to Policy

After completing SAML realm configuration, you can install policy using content policy language (CPL). Be aware that the examples below are just part of a comprehensive authentication policy.

The following examples assume that the default policy condition is allow.

Refer to the Content Policy Language Reference for details about CPL and how transactions trigger the evaluation of policy file layers.

SAML realms do not work with any "form" authentication mode.

To allow every SAML-authenticated user access to the ProxySG appliance:

```xml
<Proxy>
 authenticate(<realm-name>)
</Proxy>
```

To specify group membership as the determining factor in granting access to the appliance:

```xml
<Proxy>
 authenticate(<realm-name>)
</Proxy>
<Proxy>
 group="saml_users" ALLOW
deny
</Proxy>
```

In the previous examples, `<realm-name>` is the name of the SAML realm you created.
How can I verify authentication and troubleshoot authentication problems?

To ensure that authentication is working properly and to troubleshoot authentication problems, you can view user login statistics. You can choose to display all logged in users, filter the display of logged in users by username, realm, or IP address, or use a combination of these filters to display only the users you are interested in.

1. In the ProxySG Management Console, select **Statistics > Authentication**.

2. (Optional) If you only want to view login statistics for a particular realm, select a **Realm** from the drop-down list.

   (Optional) To filter logins by user name pattern, enter a regular expression in the **User pattern** field to display the usernames that match the pattern. You can use the following operators when specifying a user pattern:

<table>
<thead>
<tr>
<th>Operator</th>
<th>Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>Zero or more characters</td>
</tr>
<tr>
<td>?</td>
<td>Exactly one character</td>
</tr>
<tr>
<td>[x-y]</td>
<td>Any character in the character range from x to y</td>
</tr>
</tbody>
</table>

3. (Optional) To filter logins by address, enter an IP address or subnet to match in the IP prefix field. The IP address subnet notation is based on Classless Inter-Domain Routing (CIDR), a way of interpreting IP addresses. For example:
   - 1.2.3.4: represents the IP address 1.2.3.4
   - 1.2.3.0/24: represents the subnet 1.2.3.0 with netmask 255.255.255.0

4. To display all authenticated user logins (or, those that match the defined filters, if any) click one of the following:
   - **Display by user**—Displays login statistics by username.
   - **Display by IP**—Displays login statistics by IP address.

Optimize IWA Authentication

When planning your deployment of IWA-based authentication, consider the following points.

Causes of Authentication Delays

The following items are common causes of authentication delays:

**Queued Client Workers**
Blue Coat ProxySG Authentication Guide

If the ProxySG appliance receives NTLM authentication requests faster than the Domain Controller (DC) can process them, HTTP client workers will queue, waiting on authentication. That results in a slow browsing experience for users. If enough requests queue, some will time out, resulting in users receiving an exception page being returned to the browser.

Domain Controller Instability

If a configured DC goes offline, the ProxySG appliance will connect to the alternate DC, and will periodically attempt to reconnect to the primary in the background. If the alternate is also offline, the ProxySG appliance will connect to the fastest DC available, as determined by an LDAP Ping.

Symantec recommends using the primary and alternate Domain Controller configuration to deploy a dedicated DC physically near each ProxySG appliance for low network latency.

Using Read-Only Domain Controllers

Read-only (R/O) DCs can be configured as the preferred and alternate DC. However, it’s important to ensure that the R/O Domain Controllers use an Active Directory Password Replication Policy that allows them to hold the password hashes for users authenticating to the ProxySG appliance. If the R/O Domain Controller doesn’t have the password hash for an authenticating user, then it must forward the authentication request to an R/W Domain Controller, which can introduce substantial latency.

Trusted Domain Configurations

A trusted domain is a domain that has a trust relationship with the domain used by the IWA-Direct realm. To NTLM-authenticate those users, the ProxySG appliance sends the authentication request over the same Schannel connection as the others. In other words, the request is sent to a DC in the domain of the IWA-Direct realm, and that Domain Controller must then forward the request to a DC from the user’s domain. That can introduce substantial latency if the DC from the user’s domain is slow to respond.

Report Statistics to Watch

You can identify authentication speed issues by monitoring the access logs your ProxySG appliances produce. The x-cs-auth-domain field contains the user’s domain, and the x-server-auth-time field contains the amount of time it took to process the authentication request. Consult your Symantec Reporter documentation for steps to create a custom report with these log fields.

Optimal Authentication Configuration

Symantec recommends the following authentication settings:

- Increase Schannel connections for IWA-Direct
  IWA-Direct allows you to increase the number of concurrent Schannel connections that the ProxySG appliance will make to each DC. That setting is called Max Concurrent API, and can be found in the ProxySG Management Console under Configuration > Authentication > Windows Domains. The default value is 2, but it can be set as high as 150.

- Increase Max Concurrent API setting for IWA-BCAAA
  IWA-BCAAA performs NTLM authentications by invoking a Windows system call to SSPI (Security Support Provider Interface). SSPI invokes Netlogon, and Netlogon manages the Schannel connection. For IWA-BCAAA deployments,
Max Concurrent API is controlled through a Netlogon registry setting. Microsoft has documented that setting here: https://support.microsoft.com/en-us/help/2688798/how-to-do-performance-tuning-for-ntlm-authentication-by-using-the-maxc

Preferred and alternate DCs cannot be configured for IWA-BCAAA, because BCAA doesn’t have control over which DC Windows chooses for Schannel.
Why don’t my reports show user names for blocked requests?

Whether or not your reports show user names for blocked requests depends on the order in which denial and authentication occur in the policies you have defined. When the ProxySG intercepts a client request, it uses the URL to determine the content category and, if the category is blocked based on your content filtering policies, the request will be denied before the user has been authenticated and the user name is therefore not available for logging. This is because Deny has precedence over authentication.

To force requests to be authenticated even in the case where the request is denied, you must include the authenticate.force(yes) property in the Proxy layer of your policy. For example, in the following example, requests for gambling websites will be denied before authentication occurs:

```plaintext
define subnet corporate_subnet
    10.10.12.0/24
end
<Proxy>
    client.address= ! corporate_subnet deny ; filter out strangers
    authenticate (MyRealm) ; this has lower precedence than deny
<Proxy>
    category=Gambling exception (content_filter_denied)
```

However, by adding the authenticate.force(yes) property, you can ensure that authentication will occur before the request is denied, allowing you to log the user names of the users who attempt to access gambling sites:

```plaintext
define subnet corporate_subnet
    10.10.12.0/24
end
<Proxy>
    client.address= ! corporate_subnet deny ; filter out strangers
    authenticate(MyRealm) authenticate.force(yes) ; this has higher precedence than deny
<Proxy>
    category=Gambling exception (content_filter_denied)
```
Why are users being prompted to authenticate?

One of the main benefits of IWA is that it can provide a single sign-on experience for users. When configured properly, the user agent or browser will automatically provide the client’s domain credentials when challenged by the ProxySG appliance. Although you cannot guarantee that single sign-on will work in all situations, make sure you have taken the following steps to enable single sign-on:

- **Configure the IWA realm** to allow Kerberos and/or NTLM credentials. When using Basic credentials, the user will always be prompted to authenticate.

- Ensure that users are logging in to their workstations using domain credentials rather than local credentials. The ProxySG appliance can only use domain credentials to authenticate users.

- Ensure that the client browsers support IWA single sign-on. At this time only Internet Explorer (IE) and Firefox support single sign-on.

- Make sure the **client browsers are configured to automatically provide credentials** to the ProxySG appliance.

- Create a DNS "A" record that maps the ProxySG appliance fully qualified domain name (FQDN) with its IP address. In explicit deployments, the DNS A record should map the FQDN in the browser explicit proxy configuration; in transparent deployments, the DNS A record should map the Virtual URL in the IWA realm configuration to the IP address of the ProxySG appliance.

- Ensure that clients are using the DNS server you configured. To test this, ping the FQDN you specified in the DNS configuration from a client system and ensure that it resolves to the correct IP address.
Configure SAML Authentication

Why is the BCAA upgrade uninstalling previous BCAA versions?

**Problem:** When I try to upgrade my BCAA server, the installation wizard indicates that it is uninstalling the previous versions of the software. However, I still need the previous versions to support the appliances that I do not plan to upgrade yet. What should I do?

**Resolution:** Although the BCAA installation wizard says that it is uninstalling previous versions of BCAA during an upgrade, it will not remove the bcaa.ini and bcaa-nn.exe files for each version that was previously installed. This allows it to continue to run any previous versions of BCAA that were installed on the server. After upgrading, your BCAA server will continue to work with all SGOS versions it previously worked with.
Why are connections dropping with a default Deny policy?

**Problem:** If you have set up a SAML realm, users might experience dropped connections if the ProxySG appliance uses the default policy of Deny. When the policy is set to Deny, the appliance intercepts and denies requests to the IDP.

**Resolution:** Install the following policy to allow requests to the IDP:

```
<Proxy>
 authenticate(<realm-name>)
<Proxy>
 allow group=saml_users
<Proxy>
 allow url.host=<hostname>
```

In the previous policy example, `<realm-name>` is the name of the SAML realm and `<hostname>` is the hostname of the IDP.
BCAAA Service Requirements

Refer to the following documentation for details on operating system and BCAA compatibility:

- BCAA 6.1.x Service Requirements
- BCAA 5.5.x Service Requirements

The information in these documents supersedes any and all other BCAA information.
Locate Browser Proxy Settings

If you are using an explicit proxy deployment, you must set up each client Web browser to use the ProxySG appliance as its proxy server.

Use the following table to help you locate the browser proxy settings:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Proxy Configuration Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>Tools &gt; Internet Options &gt; Connections &gt; LAN Settings</td>
</tr>
<tr>
<td>Firefox</td>
<td>Tools &gt; Options &gt; Advanced &gt; Network &gt; Settings &gt; Manual Proxy Configuration</td>
</tr>
<tr>
<td>Chrome</td>
<td>Options &gt; Under the Hood &gt; Change proxy settings &gt; LAN settings</td>
</tr>
<tr>
<td>Safari (Macintosh)</td>
<td>Apple menu &gt; System Preferences &gt; Internet &amp; Wireless &gt; Network &gt; Advanced &gt; Proxies</td>
</tr>
<tr>
<td>Safari (Windows)</td>
<td>Settings menu &gt; Preferences &gt; Advanced &gt; Proxies &gt; Change Settings &gt; LAN settings</td>
</tr>
</tbody>
</table>
SAML Reference

This section describes key concepts and terms in SAML authentication.

Federation and Metadata

The entities (IDP and SP) must federate before authentication can occur. During federation, configuration data is exchanged in metadata files. Each entity publishes information about itself in these files and publishes them to a specific location, for example, on the internet or a network drive. When the entities share metadata, they establish and agree on the parameters that they will use for authentication requests and responses. They also share information such as:

- Entity IDs, which entities use to identify themselves to each other. For example, the Entity ID tells the IDP if an authentication request comes from a federated relying party.
- The SSO POST endpoint and SSO redirect endpoint to which entities send assertions during authentication.
- Each entity's public key certificate, which is used to validate assertions.
- Whether each entity requires encryption. If one of the entities requires encrypted assertions, it will publish a separate encryption certificate.

The appliance may consume encrypted assertions from the IDP, but it does not encrypt authentication requests that it sends to the IDP.

Assertions

The appliance and the IDP exchange data in XML documents called assertions. After a user is authenticated, the IDP sends an authentication assertion and the appliance establishes an authenticated session with the appropriate authorization for the user.

The appliance processes SAML authentication responses from the IDP; these responses may contain assertion attributes that describe the authenticated user. For example, `<saml:Attribute Name="mail">` is an assertion attribute that contains the user's email address inside the `<saml:AttributeValue>` element.

You can configure the appliance to use assertion attributes in authorization decisions. For more information on attributes, see "Define Assertion Attributes" on page 123.

Profiles and Bindings

A profile contains information about how SAML supports a defined use case. For example, the Web Browser SSO Profile enables single sign-on authentication for resources on the internet.

SAML 2.0 includes protocol-specific bindings, which describe how SAML data is exchanged over those protocols. In SGOS 6.5, SAML authentication supports the following for the Web Browser SSO Profile:
- The HTTP POST binding for authentication responses
- The HTTP POST binding and the redirect binding for authentication requests
Backing up the ProxySG Appliance

You may need to back up the ProxySG appliance configuration and save the backup file (called an archive) on a remote system, which you can restore in the unlikely event of system failure or replacement. For more information on configuration backups, refer to "Backing Up the Configuration" in the "Backing up the Configuration" chapter in the SGOS Administration Guide.

Step 1 - Save Keyrings Before Backing up the Configuration

Backing up the configuration does not automatically save keyring data; thus, you must save all keyrings and certificates before creating a configuration archive.

1. In the command line interface (CLI), enter configuration mode and issue the following command:
   
   ```
   #(config ssl)show ssl keypair <keyring_name>
   ```

2. Copy and paste the output from the command into a text editor. You will copy and paste this text into the CLI after you restore the appliance.

Step 2 - Import Saved Keyrings After Restoring the Configuration

After restoring the ProxySG appliance, but before applying the archived configuration, issue the following CLI command:

```
   #(config ssl)inline keyring show <keyring_name> <eof marker>
   <copy and paste text here>
   <eof marker>
```

You should now be able to apply the archived configuration without having to create and import a new keyring.

Step 3 - Re-Import the Appliance Certificate to the Trust List (AD FS only)

To establish an HTTPS connection to the ProxySG appliance, AD FS must trust the default certificate set in the Management Console; however, after you back up and restore a configuration archive, you must re-import the certificate to AD FS. For instructions, see "Configure AD FS" on page 129.