Google Search Appliance

Enabling Windows Integrated Authentication

Google Search Appliance software version 7.2 and later

Google, Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
www.google.com

GSA-WIA_200.02
March 2015

Contents

Enabling Windows Integrated Authentication

By default, Google Search Appliance users who search for and view secure content must enter credentials. In a Windows domain environment, you can configure the search appliance to use one of two methods that remove the need for redundant logins.

The preferred method to enable Windows Integrated Authentication on the search appliance is to enable onboard Kerberos. However, for environments in which Kerberos is not an option, Google SAML Bridge for Windows is provided for Windows integration.

About This Document

This section describes the audience for this document and some additional sources of information.

Audience

This document assumes that you are an experienced Windows administrator. You must have privileges to configure Active Directory and to configure the Internet Information Services (IIS) server that will host SAML Bridge, or access to someone who can do that.

For More Information

For background information on Kerberos refer to these sources:

- The topic "Configuring Crawl and Serve for Kerberos" in the document *Managing Search for Controlled-Access Content*, and the online help topics on the pages cited in that topic.
- A Google search on Kerberos (http://www.google.com/search?q=kerberos) can provide background information on the Kerberos network authentication protocol.

For background information on the technology described in this document, refer to these sources:

- The topic "The SAML Authentication Service Provider Interface (SPI)" in the document *Managing Search for Controlled-Access Content*, and the online help topics on the pages cited in that topic.

- The *Authentication/Authorization for Enterprise SPI Guide*. SAML Bridge is an application of the Google Search Appliance Authentication/Authorization SPI, for which it has the roles of Identity Provider and Policy Decision Point. These terms are explained in the SPI Guide.
- A Google search on SAML (http://www.google.com/search?q=saml) can provide background information on the SAML protocol.

Overview

There are two options for enabling silent authentication in Windows on the Google Search Appliance:

- Enable Kerberos on the search appliance.

  This is called "Kerberizing" the search appliance and is preferred because Kerberos is onboard and easy to configure.

- Use Google SAML Bridge for Windows.

  SAML Bridge mediates between your users and your Windows domain. It is implemented as an ASP.NET website that resides in Windows Internet Information Services (IIS). Scenarios for deployment that require the use of SAML Bridge instead of onboard Kerberos are:

  - Mixed environments in which not all browsers support Kerberos and SAML Bridge is required because it supports NT LAN Manager (NTLM).
  - Environments that do not allow key tab use for Kerberos, which is how the search appliance is "Kerberized".

In addition, you can use either a Kerberized search appliance or SAML Bridge to authorize web content. You do this by using an HTTP head request. While the Kerberos implementation on the search appliance supports IIS websites authorization, it does not support Kerberos constrained delegation. Google SAML Bridge for Windows provides a workaround for this.

Choose one of the following based on how your environment will provide authentication:

- "Enabling Kerberos on the Search Appliance"
- "Using SAML Bridge with the Search Appliance"

Enabling Kerberos on the Search Appliance

On board Kerberos can be used for both crawling and for serving controlled-access content. You must configure the search appliance to use Kerberos authentication at serve time. For information about configuring Kerberos-based authentication for serve, refer to the topics "Configuring Crawl and Serve for Kerberos" and "Kerberos-Based Authentication" in the document *Managing Search for Controlled-Access Content*.

Using SAML Bridge with the Search Appliance

It is preferable to achieve silent authentication by enabling Kerberos on the search appliance (called "Kerberizing"). However, if your implementation requires the use of SAML Bridge for authentication (see examples listed in the "Overview" on page 5, then SAML Bridge can be used to mediate between your users and your Windows domain. SAML Bridge is implemented as an ASP.NET website that resides in IIS.

SAML Bridge can be used to

- Silently Authenticate Users with SAML Bridge
- Authorize Content with SAML Bridge

Note: Although SAML Bridge can be used to authorize content that resides on web servers, this is no longer a common use for it. If your environment requires this, refer to "Authorize Content with SAML Bridge" on page 16 for details.

Silently Authenticate Users with SAML Bridge

The following process describes the role of SAML Bridge in the lifecycle of a search query when SAML bridge is used for authentication:

1. A user performs a secure search.
2. The search appliance redirects the user to SAML Bridge.
3. SAML Bridge authenticates the user.
4. The search appliance gets the user name (and domain, if configured) from SAML Bridge. This is the verified identity.
5. The search appliance passes the verified identity of the search user to the authorization phase.

Prerequisites for Using SAML Bridge

The following prerequisites apply to the IIS content server that hosts SAML Bridge:

- IIS must be at version 6.0 or later.

  To verify the version of IIS, do this: In the **Start** menu, choose **Administrative Tools > Internet Information Services (IIS) Manager**. In the IIS Manager, choose **Help > About**.

- The server must be running .NET Framework Version 2.0 or later. To verify the version, in the IIS Manager tree view, under the host name, choose **Web Service Extensions**. In the Web Service Extensions panel, look for ASP.NET version 2.0 or later.

Additional prerequisites apply to content servers when using SAML Bridge for Authorization. For details, refer to "Prerequisites for Using SAML Bridge for Authorization" on page 16.

Installing SAML Bridge

You can install SAML Bridge on any IIS server that meets the prerequisites described above.

To install SAML Bridge:

1. Start a web browser and navigate to https://github.com/googlegsa/samlbridge/releases.
2. Download the most recent version of the Google Search Appliance Resource Kit for SharePoint (GSARKS) package for your operating system (x86 or x64).
3. Unzip the package.
4. Locate the installer, which is the file with the extension `msi`.
5. Double-click the installer file. The **Welcome** screen is displayed.
6. Click **Next**.
7. On the **Installer Type** panel, select **Custom** and click **Next**. On the **Custom Setup** panel, SAML Bridge is part of the GSA Resource Kit for SharePoint.
8. Select **GSA Resource Kit for SharePoint**.
9. Click **Next**.

If you're installing SAML Bridge for silent authentication, see "Configuring SAML Bridge in IIS."

If you're installing SAML Bridge to authorize web content, which is no longer a common use but might be needed in some environments as described in the "Overview" on page 5, proceed to "Configuring the Search Appliance to Use SAML Bridge for Authorization" on page 19.

Configuring SAML Bridge in IIS

After you install SAML bridge, proceed to one of the following sections that corresponds to the version of IIS that you use.

- "Configuring SAML Bridge in IIS 6.0"
- "Configuring SAML Bridge in IIS 7 with Windows 2008"

Configuring SAML Bridge in IIS 6.0

SAML Bridge is implemented as a virtual directory that runs in IIS. In SAML Bridge 2.0 and later, the virtual directory is created automatically when you install SAML Bridge, and files in the `saml-bridge` virtual directory have anonymous access. The following instructions apply when you use IIS 6.0.

Configuring the SAML Bridge Virtual Directory as a Web Application

When you install SAML bridge, two virtual directories are created: `gsa-simulator` and `saml-bridge`.

To configure the `saml-bridge` virtual directory as a web application:

1. In the IIS Manager tree view, under the web site `gsa-resource-kit`, find the virtual directory called `saml-bridge`, which the installer created during the installation process.
2. Right click the virtual directory `saml-bridge`, and select **Properties**. The **Properties** dialog box appears, showing the default tab **Virtual Directory**.
3. In the **Application Settings** section, click **Create**.
4. On the **Execute Permissions** drop-down list, ensure that the value is **Scripts only**.
5. Write down the name that appears on the **Application Pool** drop-down menu. You'll use this name when you verify the configuration of the Application Pool.
6. Click the **Directory Security** tab.
7. In the **Authentication and Access Control** region, click **Edit**. The **Authentication Methods** dialog box is displayed.
8. Select **Enable anonymous access** if it is not already selected, and clear any options that are selected in the **Authenticated access** region.
9. Click **OK** to close the **Authentication Methods** dialog box and then click **OK** to close the **Properties** dialog box.

Next, verify the configuration of the SAML Bridge application pool.

Verifying the Configuration in IIS 6.0 of the SAML Bridge Application Pool

This process verifies that the Application Pool Identity for SAML Bridge is Network Service.

1. In the IIS Manager tree view, click to expand **Application Pools**.
2. Right click the name of the application pool that was configured for SAML Bridge and select **Properties**.
3. In the **Properties** dialog box, click the **Identity** tab.
4. In **Application pool identity**, verify that **Predefined** is selected and that **Network Service** is selected in the drop-down menu.
5. Click **OK** to close the **Properties** dialog box.

Next, configure the IdP endpoint in IIS for SAML Bridge. Refer to "Configuring the IdP Endpoint in IIS for SAML Bridge" on page 9.

Configuring SAML Bridge in IIS 7 with Windows 2008

SAML Bridge is implemented as a virtual directory that runs in IIS. In SAML Bridge 2.0 and later, the virtual directory is created automatically when you install SAML Bridge, and files in the `saml-bridge` virtual directory have anonymous access. The following steps apply when you use IIS 7.0.

Verifying the .NET Framework Version

To verify the version of .Net framework in Windows 2008:

1. Open IIS Manager.
2. Under **Application Pools**, look for the version in the **.Net framework version** column.
3. Verify that the value is version 2.0 or later.

Verifying the Configuration in IIS 7 of the SAML Bridge Application Pool

This process verifies that the Application Pool Identity for SAML Bridge is Network Service.

1. In the IIS Manager tree view, click to expand the **Application Pools**.
2. Select the name of the application pool that was configured for SAML Bridge and select **Advanced Setting** from the **Actions** pane.
3. Under **Process Model**, verify that the value of **Identity** is set to **Network Service**.
4. Click **OK** to close the dialog box.

Next, configure the IdP endpoint in IIS for SAML Bridge.

Configuring the IdP Endpoint in IIS for SAML Bridge

SAML Bridge supports both POST Binding, which is recommended, and Artifact Binding. As a SAML IdP, SAML Bridge uses different endpoints for these binding types. The endpoint is where the search appliance redirects the client to be authenticated. For POST Binding, `Post.aspx` is the authentication endpoint. For Artifact Binding, `Login.aspx` is the authentication endpoint.

To configure the IdP endpoint so that the user's browser sends Windows login credentials for authentication:

1. In the IIS Manager under **Web Sites**, select `saml-bridge`.
2. Select the **Content** view.
3. Select the appropriate endpoint:
   - If you are using POST Binding (recommended), select `Post.aspx`.
   - If you are using Artifact Binding, select `Login.aspx`.
4. In the **Actions** pane, click **Switch to Features** view, which displays either the `Post.aspx` home or `Login.aspx` home, depending on the endpoint you previously selected.
5. Double-click the **Authentication** icon.
6. Select **Anonymous Authentication** and click **Disable** in the **Actions** pane.
7. Select **Windows Authentication** and click **Enable** in the **Actions** pane.

The endpoint file is treated differently from other files in SAML Bridge. The endpoint file identifies users by enabling authentication. Other files (in particular, `Resolve.aspx` and `Authz.aspx` used for Artifact Binding and authorization) must allow anonymous access in the virtual directory.

Granting Permissions for the SAML Bridge Log File

To grant permission for users to write to the SAML Bridge log file:

1. Right-click the `saml-bridge` web site in IIS and select **Explore**.
2. Right-click the `ac.log` file and select **Properties**.
3. In the **Security** tab click **Add...** . The **Select Users, Computers or Groups** dialog box appears.
4. Click **Check Names**. The `saml-bridge` web site is mapped to everyone in the current domain.
5. Click **OK**.
6. In the **Permissions for Everyone** list, check the box in the **Full Control** row and the **Allow** column.
7. Click **OK.**

Additional Steps to Configure SAML Bridge for POST Binding

POST Binding requires a public key and private key pair that are used to encrypt and decrypt the response message from the SAML IdP. The SAML IdP uses the private key to encrypt the message, and the search appliance uses the public key to decrypt it.

SAML Bridge looks for the certificate located in the server key store. You can follow the standard process of enabling HTTPS for the IIS web site to create a key request, generate a certificate from your certificate authorityCA, and upload it to the IIS server where SAML Bridge is installed. Although the certificate is available for HTTPS serving, SAML Bridge can still use HTTP to serve.

To configure SAML Bridge for POST Binding, you must:

- "Locate the Certificate to Use"
- "Grant SAML Bridge Access to the Certificate"
- "Obtain the Public Key"

Locate the Certificate to Use

If there is a certificate on the server where SAML Bridge is installed, locate the certificate name in the server key store. You must copy the certificate name to the `web.config` file.

If there is not a ready-to-use certificate, you must create one. The certificate for SAML POST Binding can be generated the same way it is for HTTPS serving in IIS. See http://technet.microsoft.com/en-us/library/cc753127(v=ws.10).aspx for details on generating a certificate in Windows.

To locate the name of the certificate on the server and copy the certificate name to the `web.config` file:

1. Select **Run** in the **Start** menu, and type `mmc` to display the management console.
2. Choose **File > Add/Remove Snap-in**, and click **Add** to select a certificate to add. A wizard displays, which lets you choose the account to manage certificates.
3. Choose **Computer Account**, and click **Next.**

4. Select **Local Computer**, and click **Finish**.
5. In the previous dialog box, click **Close**, and then click **OK** to return to the main window.
6. In the certificates tree, navigate to and expand the node named **Personal**. This is where certificates are stored in IIS.
7. Double click the certificate to display its properties.
8. In the **Details** tab, locate the **Friendly Name** attribute, and copy it as the value for the `certificate_friendly_name` attribute in the SAML Bridge `web.config` file.

Also, note the value of the **Subject** attribute in the **Details** tab. You will need it in the next step to grant SAML Bridge access to the certificate.

Grant SAML Bridge Access to the Certificate

In order for SAML Bridge to load the certificate that contains the private key, the Application Pool Identity that runs SAML Bridge requires permission to access the certificate. Check permissions using the WinnHttpCertCfg tool, which you might have to download.

To list accounts that have access to this certificate, type:

```
winhttpcertcfg -l -c LOCAL_MACHINE\My -s
any_word_in_the_subject_attribute_of_the_certificate
```

To grant the Network Service account access to the certificate, type:

```
winhttpcertcfg -g -c LOCAL_MACHINE\My -s
any_word_in_the_subject_attribute_of_the_certificate -a "Network Service"
```

Obtain the Public Key

You must copy the public key in text format into the SAML configuration in the search appliance Admin Console: **Search > Secure Search > Universal Login Auth Mechanisms > SAML** tab (**Public Key of IDP** field). If the public key is in PEM format, you can obtain the base64 encoded text from the certificate. If the certificate is not in PEM format, you must convert it to PEM format.

If the certificate is also used for HTTPS, you can use FireFox. Open a FireFox browser, and go to the website where the certificate is used for HTTPS.

To convert a certificate to PEM format:

1. Open a FireFox browser, and click the lock icon that appears in the status bar. The **Certificate Viewer** window displays.
2. Click **View Certificate**,
3. In the **Details** tab, click **Export**.
4. Click **Save**.

Verifying the SAML Bridge Configuration

This step verifies that the SAML Bridge Application Pool is using Network Service and that SAML Bridge can obtain a user's identity.

In the address field of an Internet Explorer browser, enter one of the following depending on the type of binding you are using:

- For POST Binding (recommended): `http://your_saml_bridge_host:port/saml-bridge/Post.aspx`
- For Artifact Binding: `http://your_saml_bridge_host:port/saml-bridge/Login.aspx`.

You'll see a response such as the following, which assumes that your domain is `saml` and your Windows account is `davidd`.

```
Application Pool Identity = NT AUTHORITY\NETWORK SERVICE
Your Windows account  =  saml\davidd
Use Login.aspx?subject=user@domain to test impersonation
```

The NETWORK SERVICE keyword shows that SAML Bridge is properly configured to use Network Service. If Application Pool Identity is not set to Network Service, follow steps in "Verifying the Configuration in IIS 6.0 of the SAML Bridge Application Pool" on page 8 or "Verifying the Configuration in IIS 7 of the SAML Bridge Application Pool" on page 9, depending on the version of IIS you use.

In the response, you'll see your own domain and login information, because you accessed the file. When the system is in use, the file obtains the domain and login information for each authenticated user.

Configuring the Search Appliance to use SAML Bridge for Authentication

When you configure the search appliance to use SAML Bridge for authentication, you configure it to use the authentication SPI.

To configure the search appliance, do the following:

1. In the search appliance Admin Console, click **Search > Secure Search > Universal Login Auth Mechanisms**.
2. In the **SAML** tab, select the credential group from the drop-down list.
3. Type a value in the **Mechanism Name** field.

   The name you enter will appear as an Authentication ID on the **Search > Secure Search > Flexible Authorization** page. The Mechanism Name enables you to instruct the authorization mechanism to use a session identity from a specific credential group or instance of an authentication mechanism.
4. Type a value in the **IDP Entity ID** field.

   The IDP Entity ID uniquely identifies the SAML Bridge installation. To locate this value, navigate to the `saml-bridge` virtual directory and open the `web.config` file. If this value is blank in the `web.config` file, use the host name for this value.
5. In the **Login URL** field, type the login URL of SAML Bridge, which is in the format:

   `http(s)://saml-hostname:port/saml-bridge/Login.aspx`

6. Specify the binding in which the search appliance communicates with the SAML Bridge server:
   - If you're using POST Binding, which is recommended, enter the Public Key of IDP. Leave Artifact Resolver URL blank. The POST Binding URL is in the format:

     `http(s)://saml-hostname:port/saml-bridge/Post.aspx`
   - If you're using Artifact Binding, enter the Artifact Resolver URL. *Do not* specify a Public Key of IDP. The Artifact Resolver URL is in the format:

     `http(s)://saml-hostname:port/saml-bridge/Resolve.aspx`
7. Click **Save**.

Completing the Configuration Process

Follow steps in this section to complete the configuration process.

Checking Time Synchronization

The system clock of the SAML Bridge host and the system clock of the search appliance must be synchronized to prevent the search appliance from invalidating authentication responses. The search appliance treats an authentication response as invalid if the timestamp of the response is not close to the time of the search appliance system clock.

Verify that these system clocks are synchronized.

If your environment uses Network Time Protocol (NTP), do the following:

1. Check that an NTP server is running on your network.
2. Test that the search appliance is configured to use NTP:
   a. In the search appliance Admin Console, go to **Administration > Network Settings**.
   b. Ensure that the NTP server is specified.
   c. Use the **Network Diagnostics** box to test connectivity between the search appliance and the NTP server.
3. Check that the NTP service is running on the SAML Bridge host, on the content servers, and on the domain controller.

Ensuring Connectivity Between the Google Search Appliance and SAML Bridge

Verify that the two systems can communicate with each other:

1. In the Admin Console, go to **Administrator > Network Settings**.
2. In Network Diagnostics, enter the URL for the `Login.aspx` file in the **URLs to Test** box as follows, where *`your_ac_host`* is the name of the host on which SAML Bridge is installed:

   `http://your_ac_host:port/virtual_directory_name/Login.aspx`
3. Click **Update and Perform Diagnostics**.

If you discover problems here, check for network connectivity issues as you would for any two hosts.

Enable SSL on SAML Bridge

SSL is required by the SAML artifact consumer URL on the Google Search Appliance but not by the search page or SAML Bridge. However, if you do not enable SSL on both the search appliance and SAML Bridge host, secure searches display warnings about redirection to secured sites from non-secured sites. Therefore, Google recommends that you enable SSL on both the search appliance and SAML Bridge.

For information on how to enable SSL for the search appliance, in the Admin Console, click **Administration > SSL Settings**. Use the online help that is available from that page for information.

For information on how to enable SSL for SAML Bridge, refer to the Microsoft IIS documentation.

Performing a Test Search

Perform a search of secure content. You should not be prompted to log in. You can now proceed to configure policy ACLs or a connector for authorization.

Troubleshooting SAML Bridge for Authentication

This section contains some troubleshooting tips that apply to authentication. Some general tips for narrowing your problem are:

- If one account can't be impersonated, try a different account.
- If one URL doesn't work, try another.
- If one content server can't be authorized, set up a simple web server and use it as the content server.
- Set the log level in the SAML Bridge `web.config` file to 'debug', and then view the `ac.log` file for log messages.
- Monitor these additional files: the web server log, the Windows audit events in the event viewer, and the results produced by Kerberos tracing tools.

You Are Prompted When Testing Impersonation

Problem

When you test impersonation (see "Verifying the SAML Bridge Configuration") by accessing one of the following URLs, you are prompted to enter your username and password when you should *not* be prompted:

`http://`*`your_saml_bridge_host:port`*`/saml-bridge/Post.aspx` (POST Binding)

or

`http://`*`your_saml_bridge_host:port`*`/saml-bridge/Login.aspx` (Artifact Binding)

Resolution

If you enter credentials and are granted access, the cause of this problem can be one of the following:

- Security for the `.aspx` file might be configured incorrectly.
- Your Internet Explorer browser is using enhanced security settings, and the SAML Bridge host is not recognized as an Intranet site.

If you enter credentials but are not granted access, the Kerberos configuration may be incorrect and might have duplicate SPNs configured. Contact Microsoft Support.

Only Some Accounts Can Be Impersonated

Problem

When you test impersonation (see "Verifying the SAML Bridge Configuration"), some users can be impersonated but others cannot.

Suggestion

There are many reasons why user security can be inconsistent. One method to resolve this problem is as follows:

1. Select a couple of users from the group that can be impersonated and a couple of users from the group that cannot be impersonated.
2. Open the Active Directory Users and Computers console.
3. Click **View > Advanced**.
4. Select a user account that cannot be impersonated and double click to display the **Properties** window.
5. Select the **Security Window**.
6. By default, the permissions for Authenticated Users is Read.
7. If the user you selected does not have Read access, grant that user Read access.
8. Click **Apply** and then click **OK**.

More Troubleshooting Steps

For more troubleshooting steps, visit the SAML Bridge wiki (http://code.google.com/p/google-saml-bridge-for-windows/wiki/SAMLBridgeFAQsTroubleshooting).

Authorize Content with SAML Bridge

Although SAML Bridge can also be used to authorize content that resides on web servers, this is no longer a common use for it. If you will be using SAML Bridge for authorization because your environment requires it as described in the “Overview” on page 5, follow steps in this section to meet prerequisites for installing and configuring it.

The following process describes the role of SAML Bridge in the lifecycle of a search query when SAML Bridge is used for authorization:

1. A user creates a search query that includes secure content.
2. The search appliance authenticates the user and passes the verified identity to the authorization process.
3. The search appliance determines the search results for the user. If the results include secure content, the search appliance uses the Authorization SPI to send an authorization request to SAML Bridge. SAML Bridge then verifies the user's permissions to view the results.
4. SAML Bridge checks the user's access to the search results content by impersonating the user to the content server.
5. If SAML bridge is using NTLM, it sends a headrequest on the user's behalf to content server.
6. If SAML Bridge is using Kerberos, it obtains a Kerberos ticket to use on the user's behalf. This is possible because the domain server is configured to enable SAML Bridge to impersonate the user to the content server.
7. SAML bridge tells the search appliance which documents the user can access.

Review “Authentication/Authorization for Enterprise SPI Guide” for more details about communications between search appliance and SAML Bridge host.

Prerequisites for Using SAML Bridge for Authorization

If you are using SAML Bridge for authorization, the following prerequisites apply:

- “Content Server Kerberos Prerequisites”
- “Active Directory and Domain Controller Prerequisites”
- “Modifying the Windows Registry”
- “Granting ‘Act as Part of the Operating System’ Privilege”

Content Server Kerberos Prerequisites

When SAML bridge is used for authorization, Kerberos must be running on each content server whose content requires authorization.

To verify whether Kerberos is being used, you can use tools such as Windows Network Monitor or tcp trace or a browser extension that shows HTTP headers. You can view the headers that result from any communication with the content server. The content server should send the following header when Kerberos is in use.

```
WWW-Authenticate: Negotiate
```

For example, in the following header, look for the Negotiate header in the server responses.

```
GET /ac/login.aspx HTTP/1.1
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Accept-Language: en-us
UA-CPU: x86
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET
CLR 1.1.4322; .NET CLR 2.0.50727)
Host: myhost
Connection: Keep-Alive

HTTP/1.1 401 Unauthorized
Content-Length: 1656
Content-Type: text/html
Server: Microsoft-IIS/6.0
WWW-Authenticate: Negotiate
WWW-Authenticate: NTLM
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Date: Monday, 15 Nov 2010 21:26:01 GMT
```

You can refer to an unsupported Wiki page on configuring Kerberos for more information (http://code.google.com/p/google-saml-bridge-for-windows/wiki/ConfigKerberos).

Important: If SAML Bridge is only used for authentication, Kerberos is not required on the content servers. However, because the search appliance requires the authorization service to be specified to allow the basic authentication prompt to be muted, you must properly configure SAML Bridge for authorization. To do this, perform the steps in "Active Directory and Domain Controller Prerequisites" on page 17 on the domain controller machine, and perform the steps in "Granting 'Act as Part of the Operating System' Privilege" on page 18.

Active Directory and Domain Controller Prerequisites

The domain controller that is running Active Directory must meet the following requirements:

- Windows Server 2003 Kerberos Extension must be available. Kerberos is used for authentication between SAML Bridge and the content server.
- The domain functional level must be set to Windows Server 2003. Refer to the Microsoft Technet site for instructions about how to raise the domain functional level.
- Active Directory must be configured to permit SAML Bridge to use delegated credentials from the user to access server content.

To configure Active Directory to permit SAML Bridge to use delegated credentials:

1. Open the Microsoft Management Console (MMC) **Active Directory Users and Computers** snap-in.
2. In the tree view, click **Computers**.
3. In the right pane, select the server hosting SAML Bridge, right click, and select **Properties**.
4. In the **Properties** dialog box, click the **Delegation** tab.
5. Select **Trust this computer for delegation to specified services only**.
6. Select **Use any authentication protocol**.
7. Click **Add**. The **Add Services** dialog box appears.
8. Click **Users or Computers**. The **Select Users or Computers** dialog box appears.

9. Under **Enter the object names to select**, enter the Service Principal Name (SPN) for the Kerberized content server to which the SAML Bridge host will delegate.

    - If you are using Network Service to run an HTTP service, enter the name of the content server.
    - If you are using a domain account to run an HTTP service, enter the name of the domain account.
    - If you are using Microsoft Cluster Server to run a CIFS server, enter the Network Name of the group that contains the file share.

10. Optionally, click **Check Names** to verify that you entered the name correctly.

11. Click **OK**. The **Add Services** dialog box reappears, showing the available services for the object whose SPN you specified.

12. To select one or more services to which SAML Bridge will delegate, first identify the service type, and then select the name in the **User or Computer** column.

    To find the service type if the content server is a web server or SharePoint server, the service will be listed in the **Service Type** column as HTTP.

    To select the name of the services in the **User or Computer** column:

    - If users will access the content server using the NetBIOS name, select that name.
    - If users will access the content server using a DNS alias, select the DNS alias.
    - If the content server is a load balanced web server, select the associated virtual host name. You'll also need to select the NetBIOS name of each physical server represented by the virtual host.

13. Click **OK**. The **Properties** dialog box reappears. Under **Services to which this account can present delegated credentials**, you can view the list of services that you just specified.

14. Click **OK** to close the **Properties** dialog box and then close the **Active Directory Users and Computers** snap-in.

Modifying the Windows Registry

This step is required only if the same IIS server is both a SAML Bridge host and a content server.

To avoid problems that occur when SAML Bridge attempts to access the local web files, you'll need to update the Registry, by following the instructions in Microsoft KB article 896861 (http://support.microsoft.com/kb/896861/).

Granting 'Act as Part of the Operating System' Privilege

When the search appliance sends an authorization request with a user name, SAML Bridge can generate a Windows token by impersonation. However, it can use the token to access remote resources only if it has the privilege to 'Act as part of the operating system'. The Network Service that represents the identity of the SAML Bridge Application Pool must now be configured to act as part of the operating system, if it is not already configured that way.

In some environments, you cannot configure a host individually, because the domain controller sets security settings for all hosts in the domain. If your environment is set up that way, you'll need to get access to the domain controller or ask the administrator to perform this configuration.

If you can configure the SAML Bridge host, follow these steps:

1. Select **Control Panel > Administrative Tools > Local Security Settings.**

2. In the left panel, select **Security Settings > Local Policies > User Rights Assignment**.

3. Open **Act as part of operating system**.
4. In the **Act as part of the operating system Properties** dialog box, click **Add User or Group.**
5. In the **Add User or Group** dialog box, enter **Network Service** and click **OK**. The **Act as part of the operating system Properties** dialog box reappears, with **Network Service** in the box.
6. Click **OK** to close the **Properties** dialog box.

Once the prerequisites are met, refer to the steps for "Installing SAML Bridge" on page 7.

Configuring the Search Appliance to Use SAML Bridge for Authorization

To configure the search appliance to use SAML Bridge for authorization, add a SAML rule for a URL pattern that the search appliance can use to send a SAML authorization request to the Policy Decision Point.

To configure the search appliance to use SAML for authorization:

1. In the search appliance Admin Console, click **Search > Secure Search > Flexible Authorization**.
2. Choose **SAML** from the pull-down menu, and click **Add another rule**. The **Add Flexible Authorization Rule** page appears.
3. In the **URL Pattern** field, type the URL pattern identifying the protected content.
4. Select an **Authentication ID** from the pull-down menu or accept the default credential group. By selecting the Authentication ID, you are instructing the authorization mechanism to use a session identity from a specific credential group or instance of an authentication mechanism.
5. If you want to override the default value of 3 seconds for making a network connection, enter the time in seconds in the **Timeout** field.
6. In the **Authorization service ID** field, enter the Entity ID of the SAML server.
7. In the **Authorization service URL** field, enter:

   `http(s)://saml-hostname:port/saml-bridge/Authz.aspx`

8. Check **Use batched SAML AuthZ requests** to send multiple URLs for authorization in a single AuthZ HTTP request for improved serve time performance (recommended).
9. Click **Save**.
10. On the **Flexible Authorization** page, select the added rule and click **Move Up** to move it ahead of the HEADREQUEST rule. This causes the SAML rule to take precedence over the HEADREQUEST rule.
11. Click **Save Rules Order**.

Continue to "Completing the Configuration Process" on page 13.

Troubleshooting SAML Bridge for Authorization

This section contains some troubleshooting tips that apply to authorization. For general tips to narrow your problem, refer to "Troubleshooting SAML Bridge for Authentication" on page 14. For more troubleshooting steps, visit the SAML Bridge wiki (http://code.google.com/p/google-saml-bridge-for-windows/wiki/SAMLBridgeFAQsTroubleshooting).

Authorization Testing Results in Indeterminate Status

Problem

When you run an authorization test, the permit code 'Indeterminate' appears and the following messages appear in the `ac.log` file.

```
3/13/2007 5:17:59 PM, GetPermission: after WindowsIdentity
3/13/2007 5:17:59 PM, GetPermission: AuthImpl::caught exception
3/13/2007 5:17:59 PM, GetPermission: Either a required impersonation level was
not provided, or the provided impersonation level is invalid.
```

Suggestion

This error indicates that the host on which SAML Bridge resides might have an incompatible version of the .NET framework. Refer to the section "Prerequisites for Using SAML Bridge" on page 6 for the correct version.

If you've checked the .NET version and determined that it meets the requirements, you can reconfigure the .NET framework for IIS as follows:

```
cd C:\WINDOWS\Microsoft.NET\Framework\your-version\
aspnet_regiis.exe -i
```

When your IIS server is reconfigured to use the specified version of .NET, the following message displays:

```
Finished installing ASP.NET (2.0.50727).
```

Authorization Error

Problem

The log file lists a 401 error (unauthorized):

```
1/4/2007 9:14:19 AM, GetURL: GetURL =http://host.domain.domain.com:82/deny.html
1/4/2007 9:14:19 AM, GetURL: inside GetURL internal
1/4/2007 9:14:19 AM, GetURL: Sending a Head request to target URL
1/4/2007 9:14:19 AM, GetPermission: AuthImpl::caught WebException
1/4/2007 9:14:19 AM, GetPermission: e = System.Net.WebException: The remote
            server returned an error: (401) Unauthorized.
      at System.Net.HttpWebRequest.CheckFinalStatus()
      at System.Net.HttpWebRequest.EndGetResponse(IAsyncResult asyncResult)
      at System.Net.HttpWebRequest.GetResponse()
      at SAMLServices.Common.GetURL(String url, ICredentials cred)
      at SAMLServices.Common.GetURL(String url)
      at SAMLServices.Wia.AuthImpl.GetPermission(String url, String subject)
```

Suggestion

This problem indicates a Kerberos configuration error. Check that Kerberos is properly configured, following steps in "Content Server Kerberos Prerequisites" on page 16.