NetIQ® SocialAccess

Installation and Configuration Guide

September 2014

Contents

About this Book and the Library

The *Installation and Configuration Guide* for NetIQ® SocialAccess provides step-by-step instructions about how to install and configure the appliance.

Intended Audience

This book provides information for individuals responsible for implementing and administering the SocialAccess appliance. To use this book, you must also understand SAML 2.0.

Other Information in the Library

The library provides the following information resources:

Help

Provides context-sensitive information and step-by-step guidance for common tasks.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Product Overview

NetIQ SocialAccess is an appliance that simplifies a customer's experience accessing resources on the Internet.

1.1 Problems with Customers Accessing Resources on the Internet

Most businesses have an Internet presence and require customers to have an account to access the resources they provide on the Internet. As a customer this means you have multiple accounts and multiple passwords you must remember to access the resources you want on the Internet.

For example, the following graphic depicts the process a customer goes through to gain access to a new website they want to use.

Figure 1-1 *User Accesses a New Website*
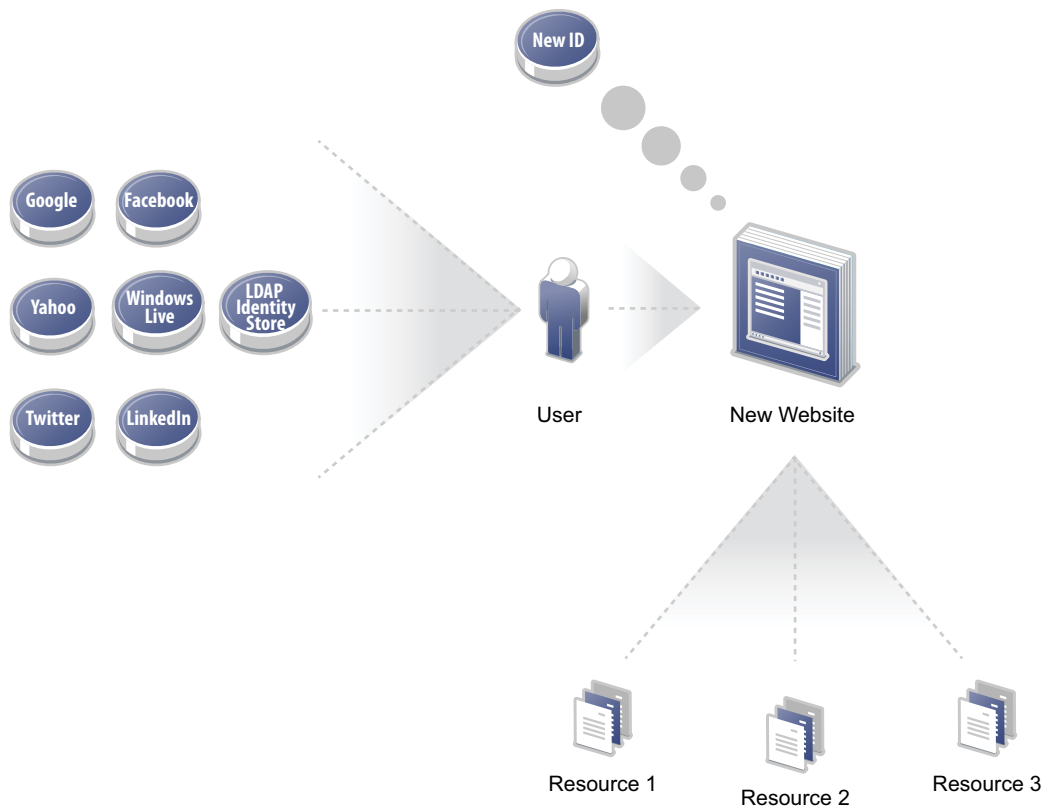
1. The customer already has multiple Internet account IDs and passwords.

2. The customer accesses the new website and the site requires the customer to create another account ID and password.

3. The customer creates a new account ID and password.

4. The customer accesses all of the resources available on the new website.

1.2 The Solution that SocialAccess Provides

SocialAccess provides a solution that allows customers to use existing Internet account IDs and passwords to gain access to a new website. The following graphic depicts the process a customer goes through using the SocialAccess solution.

Figure 1-2   *SocialAccess Solution*
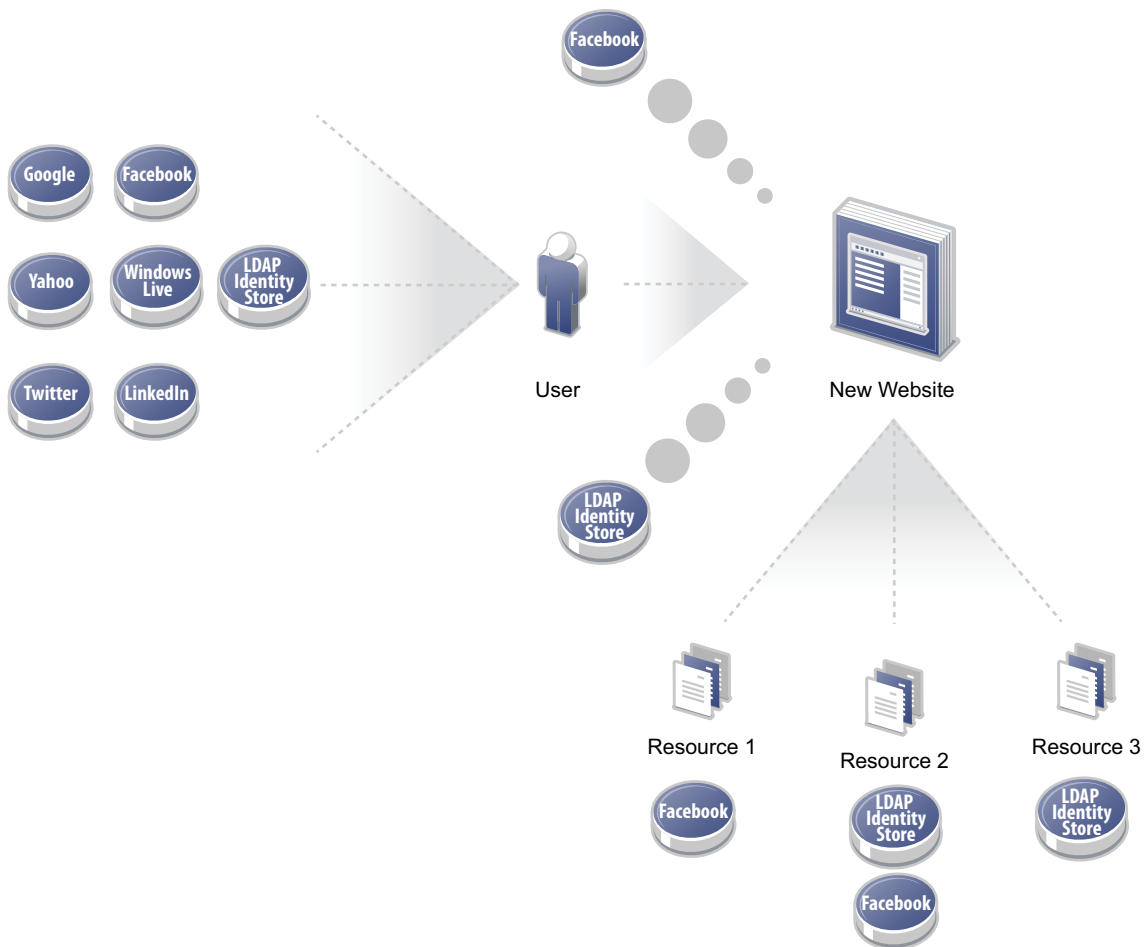
1. The customer already has multiple Internet account IDs and passwords, but wants access to the new website.

2. The customer logs in to SocialAccess.

   SocialAccess displays a landing page with the different options the customer can use to authenticate.

3. The customer enters their existing Internet account ID and password for one of the sites listed. For example, the customer uses their Facebook account ID and password to log into the new website.

4. SocialAccess sends a request to Facebook to obtain customer attributes, which it then sends to the website.

5. SocialAccess grants the customer access to the new website, Resource 1, and Resource 2.

6. If the customer authenticated with the LDAP account ID, instead of Facebook, SocialAccess grants the customer access to the new website, Resource 2, and Resource 3.

SocialAccess controls which resources a customer can access depending on the type of existing account they use to access the new website.

IMPORTANT: SocialAccess does not attempt to log out users from any of the OAuth Providers. Authentication servers used by many OAuth Providers, such as Google, remember sessions and provide the default option for users to stay logged in. Unless users deselect the option to stay signed in, they are not prompted to enter their user name or password again. As a result, in environments with shared workstations, it is likely that a user could inherit another user's session. SocialAccess is intended to be used only for lightly secured resources, but does not guarantee that identities will be audited and corrected like a corporate directory.

1.3 How SocialAccess Works

SocialAccess allows you to configure multiple identity sources that customers can use to authenticate to your business' website. SocialAccess creates a SAML assertion using attributes obtained from the identity sources to allow SAML authentications into the resources associated with your website. For more information about configuring identity sources, see Chapter 4, "Configuring Identity Sources," on page 33.

For a sample network diagram, see Section 3.4.4, "A Sample Network Configuration," on page 22.

2 Installing SocialAccess

SocialAccess is a VMware appliance that you download and deploy into your IT environment.

2.1 Requirements

Use the information in the following table to verify that you meet the requirements for SocialAccess before deploying the appliance.

Table 2-1 *SocialAccess Requirements*

Components	Requirements
VMware	One of the following versions of VMware: ◆ ESXi 5.5 ◆ ESXi 5.1 ◆ ESXi 5.0 (U2 or later)
Node	Minimum hardware requirements for each appliance node in the cluster: ◆ 60 GB disk space ◆ 2 Cores ◆ 4 GB RAM **NOTE:** The default memory allocation is 8 GB, but you can change the memory allocation as needed before powering on the appliance.
Browsers	**Administration:** Supported browsers for administration tasks: ◆ Firefox on Windows 7 or 8.1 ◆ Google Chrome on Windows 7 or 8.1 ◆ Internet Explorer on Windows 7 or 8.1 ◆ Safari on OS X Mavericks or later **Users:** Supported browsers for users: ◆ Firefox on Windows 7 or 8.1 ◆ Google Chrome on Windows 7 or 8.1 ◆ Internet Explorer on Windows 7 or 8.1 ◆ Safari on OS X Mavericks or later **NOTE:** If you experience any issues with a supported browser, ensure that you have the latest version of the browser installed, or try another supported browser. Administering the appliance with Internet Explorer may be slower than with other supported browsers.

Components	Requirements

Cluster	Supported cluster configuration:
	
	    ◆ Up to a five-node cluster
	    ◆ For optimal performance, each node should reside in the same IP subnet

DNS	SocialAccess requires that all appliance nodes, administration workstations, end user workstations, and identity sources be able to resolve the public DNS name of the appliance.

2.2 Deploying the Appliance

The SocialAccess appliance is an Open Virtualization Format (OVF) virtual appliance. You must deploy the appliance to your VMware server.

To configure the appliance, the appliance must obtain an IP address through DHCP or have an assigned static IP address. NetIQ provides two different OVF files for each appliance, to accommodate DHCP and non-DHCP environments:

◆ An `*.ovf` file for environments that have a DHCP server
◆ A `*-vcenter.ovf` file for environments that do not have a DHCP server and need to use a static IP address

To deploy the appliance:

1 Download the appropriate artifact from the NetIQ Downloads Web page (https://dl.netiq.com/index.jsp).

2 (Conditional) If you are using Windows, extract the VMware image to access the available OVF file.

3 (Conditional) If you are using Linux, use the following command to extract the image:

```
tar -zxvf vmware_image.tar.gz
```

4 (Conditional) If you have a DHCP server in your environment, deploy the `*.ovf` file to a specific ESXi host. For more information, see the VMware documentation.

5 (Conditional) If you do not have a DHCP server in your environment:

  5a Deploy the `*-vcenter.ovf` file to a VMware vCenter Server, using either the command line tool "ovftool" or the VMware vSphere client.

  5b Configure the appliance properties, ensuring that you change the `use_dhcp` property to false. Other required properties include the static IP address, subnet mask, default gateway, DNS server, and NTP server name.

    TIP: If you deploy the appliance using the "ovftool," you can configure the appliance properties from the command line and auto-start the VM so you do not have to use the vSphere client to configure the properties before starting the VM.

6 Power on the appliance, then proceed to Section 2.3, "Initializing the Appliance," on page 17.

The initial boot configures the appliance. The initial boot could take between five and ten minutes for the configuration to complete. When the appliance is ready, it displays a welcome message with the initialization URL `https://appliance_ip_address/appliance/Init.html`.

2.3 Initializing the Appliance

You must now initialize the appliance.

1 Verify that you meet the requirements listed in Section 2.1, "Requirements," on page 15.

2 From a supported browser, access the initialization web interface at the URL displayed on the appliance screen after it is deployed.

For example: `https://appliance_ip_address/appliance/Init.html`

NOTE: This URL is case-sensitive, so ensure that you enter the non-variable portions of the URL exactly as illustrated.

---

3 Fill in the fields displayed to initialize the appliance.

4 Click **Finish**.

A successfully initialized appliance automatically redirects the browser to the administration console (`https://appliance_dns_name/appliance/index.html`).

5 Specify the appliance password, then proceed with Chapter 3, "Configuring the Appliance," on page 19.

2.4 Re-initializing the Appliance

If you must re-initialize the appliance, use the following steps:

1 From a supported browser, access the initialization web interface:

`https://appliance_ip_address/appliance/Init.html`

2 Specify the password for the appliance, then change the configuration values as needed.

3 Click **Finish**.

3 Configuring the Appliance

After you have initialized the appliance, you must perform additional configuration for the appliance to work.

3.1 Accessing the Administration Console

After you properly initialize the appliance using the information in Section 2.3, "Initializing the Appliance," on page 17, the browser automatically redirects to the administration console. If not, you can access the console as follows:

1 In a supported browser, specify `https://appliance_dns_name/appliance/index.html`.

2 Specify the appliance password you created during the initialization process.

3.2 Getting Started

Review the following checklist to help you get started using SocialAccess.

Table 3-1 *Getting Started*

☐	Tasks	For more information, see ...
☐	Register the appliance.	Section 3.3, "Registering SocialAccess," on page 20
☐	Configure network options, such as adding a second NIC (network interface card).	Section 3.4, "Configuring Network Options," on page 20
☐	Configure clustering.	Section 3.5, "Configuring Clustering," on page 23
☐	(Optional) Configure event forwarding to Syslog.	Section 3.8, "Configuring SocialAccess to Forward Events to a Syslog Server," on page 30
☐	(Optional) Configure Google Analytics to monitor usage.	Section 3.9, "Using Google Analytics as an External Dashboard," on page 30
☐	Configure identity sources.	Chapter 4, "Configuring Identity Sources," on page 33

3.3 Registering SocialAccess

SocialAccess provides a 30-day trial period. If you do not register the appliance within 30 days after installation, the appliance stops working. The bomb icon in the administration console displays how many days are left in the trial period.

For the purpose of meeting licensing requirements, when you register a single appliance, the cluster as a whole is considered to be registered. However, in order to use the NetIQ Customer Center (NCC) update channel to download and install software updates, you must register each node in the cluster separately. The bomb icon remains in the administration console if there are nodes in the cluster that have not yet been registered for channel updates. For more information about the update channel, see Section 12.4, "Updating the Appliance," on page 86.

To register your appliance:

1. Log in to your Customer Center at http://www.netiq.com/center (http://www.netiq.com/center).

   The Customer Center is for NetIQ, Novell, and SUSE customers.

2. Click **My Products** > **Products**, then click **SocialAccess**.

3. Click the right arrow on the line next to the product to open a details page.

4. Select the **Activation code** value and copy it to the clipboard. You will need this code to register the appliance.

5. Log in to the appliance at `https://appliance_dns_name/appliance/index.html`.

6. Click the appliance node, then click **Register appliance**.

7. Enter the email address you used when you registered with the Customer Center.

8. Paste the Activation Code you copied to the clipboard from the Customer Center.

9. Click **Register**.

10. Repeat Step 6 through Step 9 for each node in the cluster.

When you have successfully registered all nodes in the cluster, the bomb icon disappears.

3.4 Configuring Network Options

SocialAccess contains a manual routing table, supports two NICs, and provides a forward proxy only for testing purposes.

3.4.1 Configuring the Forward Proxy

The forward proxy feature is intended only for testing purposes. The forward proxy is not supported in a production environment.

The forward proxy takes requests coming from the internal network and forwards these requests to the internet.

To configure the forward proxy:

1. Access the administration console at `https://appliance_dns_name/appliance/index.html`, then log in with the password specified during the initialization process.

2. Drag and drop the **Forward Proxy** icon from the **Tools** palette to the **Tools** panel.

3. Use the following information to configure the forward proxy:

   Forward Proxy Server: Specify the IP address and port number for your proxy server.

Ignore List: Specify any IP addresses with the associated DNS names that you want the forward proxy to ignore. For example, `127.0.0.0|localhost`.

4 Click **OK** to save your changes. Note that, as you click **OK**, the services restart and you must log in to the appliance again.

3.4.2 Configuring the Second NIC

SocialAccess allows you to configure two NICs for each node in the cluster. You can configure one NIC for the administrative network and a second NIC for the public network.

When you configure the second NIC, the SocialAccess appliance has only one global DNS name. In order for your users on the private network to access the correct network with the global DNS name for the appliance, you must do additional configuration on your network.

Two options allow users on the private network to access the SocialAccess appliance with the global DNS name:

 ◆ An entry in the local host file on each user's computer that resolves the global DNS name of the appliance to the private network
 ◆ A separate DNS server that routes all internal traffic to the global DNS name of the appliance

To configure the NICs:

1 Access the administration console at `https://appliance_dns_name/appliance/index.html`, then log in with the password specified during the initialization process.

2 Click a node icon, then click **Configure**.

3 To configure the first NIC, click the **Administration Interface** tab, then change the network settings for your administrative network.

4 Click **Apply** to save your changes.

5 To configure the second NIC, click the **Public Interface** tab.

6 Select **Enable Separate Public Interface**.

7 Configure the network settings for your public network.

8 Click **Apply** to save your changes.

9 Click **Close**.

10 Repeat Step 2 through Step 9 for each node in the cluster.

3.4.3 Configuring the Routing Table

SocialAccess provides a routing table for your use if your network has static routes. The routing table allows you to define the next hop in your network for the node in the cluster to reach the desired destination.

To configure the routing table for each node:

1 Access the administration console at `https://appliance_dns_name/appliance/index.html`, then log in with the password specified during the initialization process.

2 Click the node icon, then click **Configure**.

3 Click the **Routing** tab.

4 Specify the appropriate **Reverse Path Filter** setting. Reverse path filtering is used to prevent packets that arrived through one interface from leaving through a different interface. If in doubt, leave the default setting of **Strict mode**, since it prevents users from spoofing IP addresses from local subnets and reduces the likelihood of distributed denial-of-service (DDoS) attacks.

5 Click the plus sign (+) icon to add a route.

6 Define the desired route, then click **OK**.

7 (Optional) Add additional routes.

8 Click **Close**.

9 Repeat Step 2 through Step 8 for each node in the cluster.

3.4.4   A Sample Network Configuration

The following graphic depicts a possible network configuration using SocialAccess.

Figure 3-1   *Sample Network Diagram*
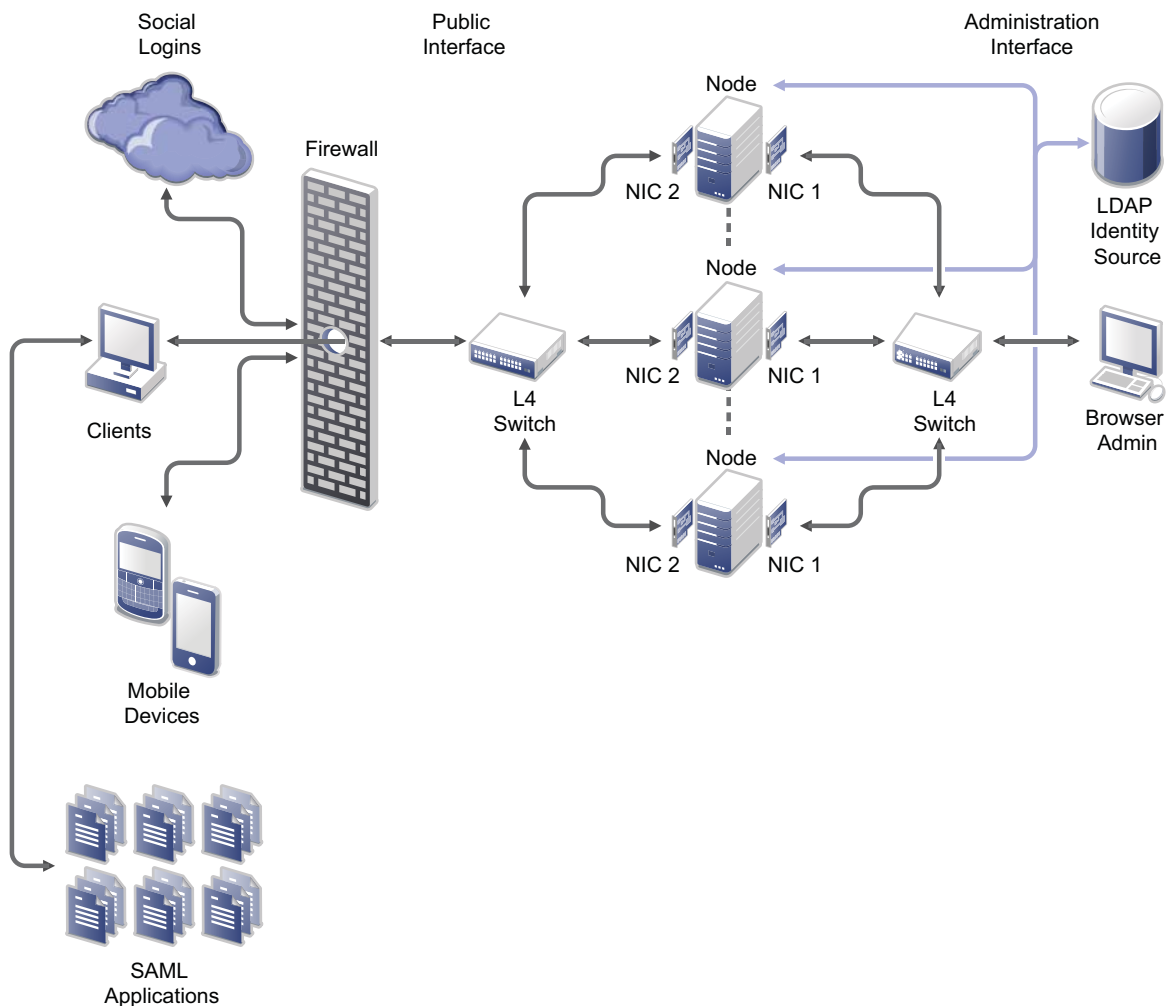
The network diagram shows that each node has both NICs enabled. The first NIC is the administration interface for the node and the second NIC is the public interface of the node. All of the administration and corporate information stays on the administration interface side of the network. All user requests and application requests communicate only on the public interface. This configuration provides a layer of security for your corporate information.

3.5 Configuring Clustering

You can cluster the SocialAccess appliance. By default, it is a single node cluster, but SocialAccess supports up to a five-node cluster. You add a node to the cluster by selecting **Join Cluster** during the initialization process.

3.5.1 Clustering Configuration Options

The Cluster icon configuration options are global settings for all nodes in the cluster. For more information about managing these configuration options, see the following sections:

- Section 12.3, "Changing Public DNS Name or NTP Server Settings, or Uploading New Certificates," on page 85
- Section 11.2, "Configuring the Session Timeout for Users," on page 84

3.5.2 Advantages of Clustering

Clustering in SocialAccess offers several advantages. Most of these advantages are available only if you configure an L4 switch or Round-robin DNS. The L4 switch is the best solution.

Disaster Recovery: Adding additional nodes to the cluster provides disaster recovery for your appliance. If one node stops running or becomes corrupt, you can promote another node to master.

High Availability for Authentications: SocialAccess provides high availability for authentications and the single sign-on service, when using an L4 switch in conjunction with clustering. This solution allows users to authenticate in case of problems with the nodes within the cluster. The L4 switch sends authentication requests to the nodes with which it can communicate.

Load Balancing: You can configure the L4 switch to distribute authentications to nodes so one node does not receive all authentication requests while other nodes sit idle.

Scalability: Configuring an L4 switch with clustering increases the scalability of SocialAccess. Each node in the cluster increases the number of possible simultaneous logins.

3.5.3 Managing Nodes in the Cluster

SocialAccess supports up to five nodes in a cluster. You add nodes to the cluster through the initialization process, and perform all other initialization tasks in the administration console.

Adding a Node to the Cluster

To add a node to the cluster:

1 Verify that the cluster is healthy.

- All nodes must be running and communicating.

- All components must be in a green state.
- All failed nodes must be removed from the cluster.

For more information about verifying that your cluster is healthy, see Section 13.3, "Troubleshooting Different States," on page 90.

2 Download and deploy a new virtual machine (VM) for the new node.

For more information, see Section 2.2, "Deploying the Appliance," on page 16.

3 You must now initialize the appliance. Select **Join Cluster** as the first step to initialize the new node, then follow the on-screen prompts.

For more information, see Section 2.3, "Initializing the Appliance," on page 17.

4 When initialization is complete, a login page appears.

5 Log in to the appliance. The new appliance should be displayed in the cluster. Wait until all spinner icons stop processing and all components are green before performing any other tasks.

The cluster is adding the node and several background processes are running. This final step could take up to an hour to complete.

6 Once the node is added to the cluster, register the node. For more information, see Section 3.3, "Registering SocialAccess," on page 20.

Promoting a Node to Master

The first node that you install is the master node of the cluster by default. The master node runs provisioning, reporting, approvals, and policy mapping services. You can promote any node to become the master node.

To promote a node to master:

1 Verify that the cluster is healthy.

For more information, see Section 13.3, "Troubleshooting Different States," on page 90.

2 Verify that all nodes in the cluster are running the same version of SocialAccess. If any nodes need to be updated, ensure that you update the nodes *before* you switch the master node. For more information, see Section 12.4, "Updating the Appliance," on page 86.

3 Take a snapshot of the cluster.

4 Click the node to become the master node in the administration console, then click **Promote to master**.

An "M" appears on the front of the node icon indicating that it is now the master node. This process may take a while to complete. Watch for the node spinner icons to stop and health indicators to turn green before proceeding with any additional configuration changes.

The services move from the old master to the new master. The old master is now just a node in the cluster.

WARNING

- If the old master node is down when you promote another node to master, remove the old master from the cluster, then delete it from the VMware server. Otherwise, the appliance sees two master nodes and becomes corrupted.
- When you switch the master node, the logs and reports start again on the new master. If you do not have Syslog enabled, the historical logs and reporting data are lost. For more information, see Section 3.8, "Configuring SocialAccess to Forward Events to a Syslog Server," on page 30.

Removing a Node from the Cluster

You can remove a node from the cluster if something is wrong with the node. However, after removing a node, you cannot add the same VM instance back into the cluster. You must delete this instance of the appliance from your VMware server, then deploy another instance to the VMware server to add a node back into the cluster.

To remove a node from the cluster:

1. (Conditional) If the node you are removing is the master node, promote another node to be master before you remove the old node. For more information, see "Promoting a Node to Master" on page 24.

2. (Conditional) If you are using an L4 switch, delete the node from the L4 switch. For more information, see the L4 switch documentation.

3. In the administration console, click the node you want to remove from the cluster.

4. Click **Remove from cluster**.

   The administration console immediately shows that the node is gone, but it takes some time for the background processes to finish.

5. Delete the instance of the node from the VMware server.

3.5.4 Configuring an L4 Switch for Clustering

If you want high availability or load balancing, you must configure an L4 switch for the SocialAccess appliance. An L4 switch can be configured in many different ways. Use the following recommendations to configure the L4 switch to work with the appliance.

- **Heartbeat:** Use the following URL to define the heartbeat for the L4 switch:

  `https://`*appliance_ip_address*`/osp/h/heartbeat`

  The L4 switch uses the heartbeat to determine if the nodes in the cluster are running and working properly. The heartbeat URL returns a text message of Success and a 200 response code.

- **Persistence:** Also known as **sticky sessions**, persistence allows all subsequent requests from a client to be sent to the same node. To make this happen, select SSL session ID persistence when configuring the L4 switch.

Session persistence ensures that the same real server is used for the SocialAccess login and the subsequent application single sign-on. Using the same server allows caching for a series of related transactions, which can improve the server performance and reduce the latency of transactions. It removes the delay that might occur if the client sends a request to a new node instead of using the existing session to the same node. To ensure that transactions for the same client are forwarded to the same real server in a load-balanced cluster configuration:

- You can set the L4 switch to use IP-based persistence, which uses the user device's IP address to maintain an affinity between the user session and the same real server in the cluster. IP-based persistence fails if a user's device IP address changes between requests. It also fails if all user devices come through a proxy service where all transactions appear to come from the same IP address.

- You can set the L4 switch to use sticky-bit persistence. Sticky-bit persistence is problematic for L4 switches that do not support stickiness. Sticky sessions also do not work with browsers set to disable cookies.

- You can use a proxy approach for the identity provider nodes that does not depend on the L4 configuration. However, this solution can quickly become chatty.

3.6 Configuring Google reCAPTCHA

The Google reCAPTCHA tool helps protect your user login page against spam, malicious registrations, and other forms of attack where computers disguise themselves as human. It provides an additional layer of security by displaying images of words that users must type in addition to their login credentials. Software bots typically cannot scan the images to provide a response.

Using reCAPTCHA helps prevent automated Denial of Service (DoS) attacks that can impact the performance of the appliance and the identity source. The tool uses the remote Google reCAPTCHA service to provide the images and verify the responses. If a response succeeds, the appliance verifies the user's authentication credentials against the identity source. If a response fails, the appliance fails the login attempt without processing the credentials, and re-displays the login page. Thus, the automated login attempts fail and cannot consume the processing resources of the appliance and identity source.

3.6.1 Requirements for reCAPTCHA

Ensure that your system meets the following requirements before you configure the Google reCAPTCHA tool:

❒ A SocialAccess appliance, installed and configured.

❒ One or more supported identity sources, with the connectors enabled and configured. The reCAPTCHA tool supports users from Active Directory and eDirectory identity sources.

Each identity source should be configured with an intrusion detection policy. For more information, see Section 3.6.2, "Configuring Intrusion Detection for Failed Logins," on page 26.

❒ A Google reCAPTCHA account, configured on the Google reCAPTCHA website. For more information, see Section 3.6.3, "Configuring a Google reCAPTCHA Account," on page 27.

3.6.2 Configuring Intrusion Detection for Failed Logins

Someone who attempts to use more than a few unsuccessful passwords while trying to log on to your system might be a malicious user. reCAPTCHA cannot prevent attacks by anyone who can read the image. It cannot differentiate between malicious users and legitimate users. Using reCAPTCHA cannot prevent coordinated human DoS attacks. If users have unlimited attempts to enter their authentication credentials, reCAPTCHA also cannot help prevent attacks to find passwords.

To help limit the effectiveness of brute force or human attacks that bypass the reCAPTCHA protection, you should enable the user's identity source to respond to this type of potential attack by disabling the account for a preset period of time after a specified number of failed logon attempts.

The supported identity sources have the following built-in intrusion detection systems:

◆ **Active Directory Account Lockout Policy:** Active Directory allows you to specify an account lockout policy for users and global security groups in a domain. Set the policy on the domain group policy object from the domain controller.

To configure the Account Lockout Policy settings:

1. Log in as an Active Directory administrator user to the Windows Server that hosts Active Directory Domain Services (the domain controller).

2. Configure the Account Lockout Policy on the group policy object for the domain controller.

For more information, see the *Account Lockout Policy* (http://technet.microsoft.com/en-us/library/hh994563%28v=ws.10%29.aspx) in the Microsoft TechNet Library. (http://technet.microsoft.com/)

3. Verify that the **Account Lockout Threshold** value is higher than the number of failed login attempts you plan to specify for **Start reCAPTCHA at** in the reCAPTCHA tool.

4. Repeat these steps for each configured Active Directory identity source.

◆ **eDirectory Intruder Lockout Policy:** eDirectory allows you to enable Intruder Detection and specify an Intruder Lockout policy for the container object where your user objects reside.

To configure the eDirectory Intruder Detection and Intruder Lockout Policy:

1. Log in as the eDirectory administrator user to the management console for the eDirectory server.

2. Configure Intruder Detection and the Intruder Lockout policy on the container object where your user objects reside.

   For more information, see "Setting Up Intruder Detection for All Users in a Container" (https://www.netiq.com/documentation/edir88/edir88/data/afxkmdi.html#a3p5g0i) in the *eDirectory 8.8 SP8 Administration Guide*.

3. Verify that the Intruder Lockout value is higher than the number of failed login attempts you plan to specify for **Start reCAPTCHA at** in the reCAPTCHA tool.

4. Repeat these steps for each configured eDirectory identity source.

After you have configured intrusion detection for the supported identity sources, continue with Section 3.6.3, "Configuring a Google reCAPTCHA Account," on page 27.

3.6.3 Configuring a Google reCAPTCHA Account

Before you configure the Google reCAPTCHA tool, you must configure an account to use for your domain at Google reCAPTCHA, and create a public and private key.

To configure a Google reCAPTCHA account to use for your appliance's domain:

1 Access the Google reCAPTCHA (https://www.google.com/recaptcha/) website.

2 Click **Get reCAPTCHA > Sign up Now**.

3 Log in using one of your Google accounts.

   For example, if you use your Gmail account, the reCAPTCHA account is associated with the Gmail account.

4 (Conditional) If this is not your first site, click **Add a New Site**. Otherwise, skip to the next step.

5 Specify a domain.

   Read the **Tips** for more information.

6 Click **Create** to add the domain.

7 Copy the **Public Key** and **Private Key** that the interface displays to use when you configure the identity source.

8 Continue with Section 3.6.4, "Configuring the reCAPTCHA Tool," on page 27.

3.6.4 Configuring the reCAPTCHA Tool

Before you configure the Google reCAPTCHA tool, you must set up intruder detection in the Active Directory and eDirectory identity sources, and create public and private keys for your appliance's domain at the Google reCAPTCHA website.

To configure the reCAPTCHA tool:

1 Using the identity source's native management tools, verify that their intrusion detection setup meets the requirements specified in "Configuring Intrusion Detection for Failed Logins" on page 26.

2 Log in with an appliance administrator account to the SocialAccess administration console at

`https://`*appliance_dns_name*`/appliance/index.html`

3 In the **Identity Sources** panel, verify that you have configured an identity source for Active Directory or eDirectory, or both.

4 Drag and drop the reCAPTCHA tool from the **Tools** palette to the **Tools** panel.

5 Configure the reCAPTCHA tool as follows:

Start reCAPTCHA at: Specify how many failed login attempts must occur before the login page displays the reCAPTCHA prompt. The value should be less than the lockout value set in the identity sources' intrusion detection system.

- If the reCAPTCHA count is set to zero, the login page displays a reCAPTCHA prompt every time for all users. Every login requires user credentials and the reCAPTCHA response.

- If the reCAPTCHA count is greater than zero, the login page displays the reCAPTCHA prompt only after the user login fails the specified number of times in the same browser window.

Public Key: Paste the Public Key value from your reCAPTCHA account configuration for this appliance's domain.

Private Key: Paste the Private Key value from your reCAPTCHA account configuration for this appliance's domain.

For information about the public and private keys for your reCAPTCHA account, see Section 3.6.3, "Configuring a Google reCAPTCHA Account," on page 27.

6 Click **OK** to save the settings and enable the tool.

7 Click **Apply** to activate the configuration.

8 Wait while the service is activated across all nodes in the cluster. Do not attempt other configuration actions until the activation completes successfully.

3.7 Configuring the Authentication Filter to Set Session-Based Identity Information for a User

The SocialAccess single sign-on login is designed to authenticate a user against an identity source and to share this authentication with other protected applications. The authentication process does not provide extended functions to add, remove, or manage a user's identity information for the session. To address this need, SocialAccess provides the Authentication Filter tool.

The Authentication Filter integrates with the SocialAccess single sign-on process. After the user logs in, the filter intercepts the authentication process and sends the user's identity information from the identity source to your custom authentication scripts. You can add, remove, or set values for supported identity attributes. You can also set a cookie. You can interact with the user to gather input for those changes. After all of the encoded rules and associations are complete, SocialAccess stores the modified identity information in the session cache for the web services and applications.

The Authentication Filter tool is compatible with the ExtAPI library and the ExtUI library. It works with multiple scripting languages including PHP, Java, and Perl.

After you create your custom scripts, you must enable and configure the Authentication Filter tool in SocialAccess. The enabled filter automatically runs on each node in a SocialAccess cluster.

For information about creating custom authentication scripts to use with the Authentication Filter, see the *Authentication Filter Technical Reference for NetIQ CloudAccess* (https://www.netiq.com/documentation/cloudaccess/auth-filter_techref/data/auth-filter_techref.html). Although this Technical Reference was written for CloudAccess, the content and examples are equally applicable to SocialAccess.

Before you enable the Authentication Filter, set up your environment to meet the following requirements:

- A SocialAccess 2.1 appliance, installed and configured.
- The Authentication Filter supports only applications that use session-based protocols. The filter stores the altered identity attributes and values in the session attribute cache.

  The Authentication Filter does not support applications that use sessionless protocols, because there is no session attribute cache to store the altered identity attributes and values. For example, the OAuth protocol is a sessionless protocol. Thus, the Authentication Filter does not support applications that use the OAuth Service Provider connector.
- On the ExtAPI server, create a script that uses the ExtAPI library commands to apply session-based authentication rules to an authenticated user's identity information. The Authentication Filter points to the URL for this file.
- If the session-based identity changes require user interaction:
  - On the ExtUI server, create a script that uses the ExtUI library commands to collect the user's session-based identity information, and return control to SocialAccess. The ExtAPI script should redirect the authentication session to the URL for this file.
  - On the ExtAPI server, create a redirect file configured with the ExtUI script's URL.

To enable the Authentication Filter:

1 Log in with an appliance administrator account to the administration console at `https://appliance_dns_name/appliance/index.html`.

2 Drag the **Authentication Filter** icon from the **Tools** palette and drop it in the **Tools** panel.

3 In the **Tools** panel, click the **Authentication Filter** icon, then click **Configure**.

4 In the Edit External Filter window, complete the following information:

Display name: Specify a name for the filter. This name appears in the **Tools** panel of the console.

Connects to: Specify the URL to the script that you want to run during the user SSO login.

For example:

`https://extapi_server_dns:port/path/extapi/index.php`

Use HTTPS for secure SSL transfer of information. If you use an HTTP URL, information is not secure.

Basic Auth User: (Optional) If login is required to access the URL, specify the user name to use in the basic authentication header.

Basic Auth Password: (Conditional) If you specify a user name, specify the password for it.

5 Click **OK** to save and enable the filter settings.

6 Click **Apply** to activate the filter configuration.

7 Wait while the service is activated across all nodes in the cluster. Do not attempt other configuration actions until the activation completes successfully.

In the **Appliances** panel, a green gear icon spins on top of each node until the activation is complete across all nodes in the cluster. In the **Tools** panel, a green status icon appears on the lower-left corner of the service icon. A yellow status icon appears if the URL uses HTTP instead of HTTPS because the traffic is not secure.

3.8 Configuring SocialAccess to Forward Events to a Syslog Server

You can configure SocialAccess to forward login and logout events to a syslog server.

To configure SocialAccess to forward events:

1 Access the administration console at `https://appliance_dns_name/appliance/index.html`, then log in with the password specified during the initialization process.

2 Drag and drop the Syslog tool from the **Tools** palette to the **Tools** panel.

3 In the **Tools** panel, click the Syslog tool, then click **Configure**.

4 Specify the IP address and the port of the syslog server.

5 Select the type of protocol to use: **UDP**, **TCP**, or **TLS**.

6 Click **OK** to save the tool settings.

7 Click **Apply** to activate event forwarding.

3.9 Using Google Analytics as an External Dashboard

SocialAccess enables administrators to use Google Analytics as an external dashboard to monitor and analyze SocialAccess usage. Once you have completed the free Google Analytics registration process for the SocialAccess appliance, data is available for analysis within a few hours. You can also do your own data mining with the API that Google provides. For more information, see the Google Analytics website (http://www.google.com/analytics/).

To set up Google Analytics for SocialAccess:

1 (Conditional) If you do not already have a Google account, set one up on the Google website.

2 Sign in to your Google account and select the option to register for Google Analytics.

3 Select the option to monitor a website and provide the base URL for the SocialAccess appliance. Google Analytics tracks both user and admin logins. For example, `https://appliance_dns`.

4 Specify an account name. This account name is only for managing Google Analytics and does not affect anything in SocialAccess. You can share this account name as needed.

5 Log in to the SocialAccess administration console.

6 Drag the Google Analytics tool from the **Tools** palette to the **Tools** panel.

7 Enter the Tracking ID (not the tracking code) that Google provided during the registration process and click **OK**.

8 Click **Apply** and wait for the appliance to update.

NOTE: If you have any issues with configuring the Google Analytics tool in the administration console, such as the tool being invisible on the Tools palette, verify that you do not have any adblockers running in your browser that may be interfering with administration tasks. You should be able to disable any adblockers on the web page itself.

4 Configuring Identity Sources

After you have configured the appliance, you need to configure the identity sources. SocialAccess uses identity sources for user authentication to SAML applications or of web services. You must configure the identity source and the connector for the identity source for the authentication process to work.

SocialAccess supports a number of identity sources and also provides two templates: OAuth 2.0 and OpenID Connect.

4.1 Configuring Active Directory as an Identity Source

SocialAccess supports Windows Server 2012 R2 and Windows Server 2008 R2.

To configure Active Directory as an identity source:

1 Verify that you have an Active Directory administrator account.

2 Log in to the SocialAccess administration console:

   `https://appliance_dns_name/appliance/index.html`

3 Drag and drop the connector for Active Directory from the **Identity Sources** palette to the **Identity Sources** panel.

4 Click the connector, then click **Configure**.

5 Use the following information to configure the connector for Active Directory:

   Credentials: Specify the fully distinguished LDAP format name and password of the Active Directory administrator account.

   Search Context: Specify the fully distinguished LDAP format of the context where the connector searches for user objects.

   Active Directory Servers: Specify the IP address and LDAP port of the Active Directory server where the user objects reside. Select **Enable LDAP SSL** to use port 636, or the default non-SSL port is 389.

6 (Optional) If you have custom attributes you want to map, click **Advanced Options**, then specify your custom attributes under **Attribute Mappings**.

7 Click **OK**, then click **Apply** to save the configuration.

The connector for Active Directory is now an identity source for user logins. Users and administrators can log in to SocialAccess using either their sAMAccountName or email address in Active Directory.

4.2 Configuring eDirectory as an Identity Source

SocialAccess supports eDirectory 8.8.7 and 8.8.6.

To configure eDirectory as an identity source:

1 Verify that you have an eDirectory administrator account with the following minimum rights for the connector for eDirectory to work:

- ◆ **Property Rights**
    - ◆ **CN:** compare, read, inherit
    - ◆ **Description:** compare, read, inherit
    - ◆ **Given Name:** compare, read, inherit
    - ◆ **GUID:** compare, read, inherit
    - ◆ **Internet Email Address:** compare, read, inherit
    - ◆ **Login Disabled:** compare, read, inherit
    - ◆ **Member:** compare, read, inherit
    - ◆ **Member Of:** compare, read, inherit
    - ◆ **Surname:** compare, read, inherit
- ◆ **Entry Rights:** browse, inherit

2 Log in to the SocialAccess administration console:

`https://`*`appliance_dns_name`*`/appliance/index.html`

3 Drag and drop the connector for eDirectory from the **Identity Sources** palette to the **Identity Sources** panel.

4 Click the connector, then click **Configure**.

5 Use the following information to configure the connector for eDirectory:

Credentials: Specify the fully distinguished LDAP format name and password of the eDirectory administrator account with the minimum rights.

Search Context: Specify the fully distinguished LDAP format of the context where the connector searches for user objects.

eDirectory Server: Specify the IP address and LDAP port of the eDirectory server that contains a Master or Read/Write replica of the partition where the user objects reside. Select **Enable LDAP SSL** to use port 636, or the default non-SSL port is 389.

6 (Optional) If you have custom attributes you want to map, click **Advanced Options**, then specify your custom attributes under **Attribute Mappings**.

7 Click **OK**, then click **Apply** to save the configuration.

The connector for eDirectory is now an identity source for user logins. Users and administrators can log in to SocialAccess using either their CN or email address in eDirectory.

4.3 Configuring reCAPTCHA for Active Directory or eDirectory

You can configure Google reCAPTCHA to work with Active Directory and eDirectory identity sources to provide an additional layer of security for the user login process. After a specified number of failed login attempts by users, reCAPTCHA displays a phrase that users must type in addition to their password. For more information about configuring reCAPTCHA, see Section 3.6, "Configuring Google reCAPTCHA," on page 26.

4.4 Configuring Facebook as an Identity Source

To configure Facebook as an identity source:

1 Install the developer app to your profile from the Facebook Developers (https://developers.facebook.com) website.

2 On the developer site, click **Apps**, then click **Create a New App**.

3 Provide the following information:

- Specify a **Display Name**.
- From the **Category** list, select **Apps for Pages**.

4 Click **Create App**.

5 Click **Settings** in the left pane, then provide the following information:

- In the **App Domains** field, create a new **App Domain** and specify your base DNS name (without `https`) in the format *appliance_dns_name*.
- Specify a **Contact Email** address.
- Click **+Add Platform**, then select **Website**.
- Set the value of the **Site URL** field to your SocialAccess appliance publicly resolvable DNS name. For example, `https://appliance_dns_name`.
- The other fields on this window are not required.
- Click **Save Changes**.

6 Copy the **App ID** value and the **App Secret** value to use when you configure the connector for Facebook.

7 Log in to the SocialAccess administration console:

`https://appliance_dns_name/appliance/index.html`

8 Drag and drop the connector for Facebook from the **Identity Sources** palette to the **Identity Sources** panel.

9 Click the connector, then click **Configure**.

10 Specify the **App ID** and **App Secret** values that you copied from the Facebook configuration.

11 Click **OK**, then click **Apply** to save the configuration.

The connector for Facebook is now an identity source for user logins.

4.5 Configuring Google as an Identity Source

To configure Google as an identity source:

1 Log in to Google Cloud Console (https://cloud.google.com/console) and create a new project.

2 Open the project you just created, then navigate to **API & Auth** > **Credentials**.

3 Click **Create New Client ID**.

4 Select **Web Application**.

5 Edit the **Authorized Javascript origin** to be the DNS name of your SocialAccess appliance.

6 Edit the **Redirect URI** to include the URL: `https://dns_name/osp/a/t1/auth/oauth2/landingpad`, then change the *dns_name* to the DNS name of your SocialAccess appliance.

7 Click **Create Client ID**.

8 Copy the **Client ID** value and the **Client Secret** value to use when you configure the connector for Google.

9 Log in to the SocialAccess administration console:

`https://appliance_dns_name/appliance/index.html`

10 Drag and drop the connector for Google from the **Identity Sources** palette to the **Identity Sources** panel.

11 Click the connector, then click **Configure**.

12 Use the following information to configure the connector for Google:

Client ID: Specify the **Client ID** value from the Google configuration.

Client Secret: Specify the **Client Secret** value from the Google configuration.

13 Click **OK**, then click **Apply** to save the configuration.

The connector for Google is now an identity source for user logins.

4.6 Configuring LinkedIn as an Identity Source

To configure LinkedIn as an identity source:

1 Log in to LinkedIn at the LinkedIn Developer website (https://www.linkedin.com/secure/developer).

2 Click **Add New Application**.

3 Create a new application with the following information:

OAuth Accept Redirect URL: Specify `https://dns_name/osp/a/t1/auth/saml2/sso` where the *dns_name* is the DNS name of the SocialAccess appliance.

JavaScript API Domains: Specify `https://dns_name` where the *dns_name* is the DNS name of the SocialAccess appliance.

4 Copy the **API Key** value and the **Secret Key** value to use when you configure the connector for LinkedIn.

5 Log in to the SocialAccess administration console:

`https://appliance_dns_name/appliance/index.html`

6 Drag and drop the connector for LinkedIn from the **Identity Sources** palette to the **Identity Sources** panel.

7 Click the connector, then click **Configure**.

8 Use the following information to configure the connector for LinkedIn:

API Key: Specify the **API Key** value from the LinkedIn configuration.

Secret Key: Specify the **Secret Key** value from the LinkedIn configuration.

9 Click **OK**, then click **Apply** to save the configuration.

The connector for LinkedIn is now an identity source for user logins.

4.7 Configuring MSLive as an Identity Source

To configure MSLive as an identity source:

1 Create an application with a Windows Live login (MS Live) by following the instructions in the MSDN Library Getting Your Client ID for Web Authentication (http://msdn.microsoft.com/en-us/library/bb676626.aspx).

2 Edit the application, then add the DNS name of your SocialAccess appliance as the **Redirect domain** under the **API Settings**.

3 Copy the **Client ID** value and the **Client Secret** value to use when you configure the connector for MSLive.

4 Log in to the SocialAccess administration console:

   `https://appliance_dns_name/appliance/index.html`

5 Drag and drop the connector for MSLive from the **Identity Sources** palette to the **Identity Sources** panel.

6 Click the connector, then click **Configure**.

7 Use the following information to configure the connector for MSLive:

   Client ID: Specify the **Client ID** value from the MSLive configuration.

   Client Secret ID: Specify the **Client Secret** value from the MSLive configuration.

8 Click **OK**, then click **Apply** to save the configuration.

The connector for MSLive is now an identity source for user logins.

4.8 Configuring Twitter as an Identity Source

To configure Twitter as an identity source:

1 Access the Twitter application at the Twitter Developer website (https://dev.twitter.com/apps).

2 Select **Create a new application**.

3 Create a new application with the following information:

   Website: Specify the publicly resolvable DNS name of your SocialAccess appliance.

   callbackURL: Specify `https://dns_name/osp/a/t1/auth/saml2/sso` where the *dns_name* is the DNS name of the SocialAccess appliance.

4 Copy the **Consumer Key** value and the **Consumer Secret** value to use when you configure the connector for Twitter.

5 Log in to the SocialAccess administration console:

   `https://appliance_dns_name/appliance/index.html`

6 Drag and drop the connector for Twitter from the **Identity Sources** palette to the **Identity Sources** panel.

7 Click the connector, then click **Configure**.

8 Use the following information to configure the connector for Twitter:

   Consumer Key: Specify the **Consumer Key** value from the Twitter configuration.

   Consumer Secret: Specify the **Consumer Secret** value from the Twitter configuration.

9 Click **OK**, then click **Apply** to save the configuration.

The connector for Twitter is now an identity source for user logins.

4.9 Configuring Yahoo as an Identity Source

To configure Yahoo as an identity source:

1 Log in to the Yahoo Developer website (http://developer.yahoo.com/).

   You must have a Yahoo developer account to log in to the website.

2 Click your name, then click **My Projects**.

3 Click **Create a Project**, then select **Web-Based**.

4 Create a new application with the following information:

   Home Page URL: Specify `https://dns_name/osp/a/t1/auth/saml2/sso` where the *dns_name* is the DNS name of the SocialAccess appliance.

5 Click **This app requires access to private user data**, then use the following information:

   Application Domain: Specify `http://dns_name`, where the *dns_name* is the DNS name for the SocialAccess appliance.

   Permission Scopes: Enable the appropriate **Social Directory (Profiles)** permission as follows:

   ◆ **Read/Write Public and Private** to get *all* attribute values (ID, UserName, FirstName, LastName, BirthDate, Email, Photo, Gender, Language, StreetAddress, City, State, ZipCode, Country, Phone).

   ◆ **Read Public** or **Read/Write Public** to get only the following attribute values: ID, UserName, BirthDate, Photo, Gender, and Language

6 Copy the **Consumer Key** value and the **Consumer Secret** value to use when you configure the connector for Yahoo.

7 Log in to the SocialAccess administration console:

   `https://appliance_dns_name/appliance/index.html`

8 Drag and drop the connector for Yahoo from the **Identity Sources** palette to the **Identity Sources** panel.

9 Click the connector, then click **Configure**.

10 Use the following information to configure the connector for Yahoo:

   Consumer Key: Specify the **Consumer Key** value from the Yahoo configuration.

   Consumer Secret: Specify the **Consumer Secret** value from the Yahoo configuration.

11 Click **OK**, then click **Apply** to save the configuration.

The connector for Yahoo is now an identity source for user logins.

4.10 Configuring OAuth2 Sites as Identity Sources

SocialAccess provides a generic OAuth2 template. The OAuth2 template allows you to configure OAuth2 sites as identity sources for SocialAccess. For more information about OAuth2, see the OAuth2 website (http://oauth.net/2/).

To use the OAuth2 template:

1 Create an OAuth2 application that represents the SocialAccess appliance on the developer site you want to use as an identity source.

Creating an application does not require any coding.

2 Copy the following information into a document as you create the OAuth2 application to use when configuring the OAuth2 template:

- ◆ Client ID
- ◆ Client Secret ID
- ◆ Authentication URL
- ◆ Token URL or access token
- ◆ Profile URL
- ◆ (Conditional) Profile header
- ◆ Scope separator

3 Log in to the SocialAccess administration console:

`https://`*appliance_dns_name*`/appliance/index.html`

4 Drag and drop the OAuth2 template from the **Identity Sources** palette to the **Identity Sources** panel.

5 Click the template, then click **Configure**.

6 Use the information gathered in Step 2 to create your own connector for OAuth2 following the on-screen prompts.

7 (Optional) You can upload a login card image that is specific to your OAuth2 application in the **Login card image** field. Users see this image when they log in to SocialAccess.

The image can be a `.png`, `.jpg`, or `.gif` file. The file size is 215px x 50px and the file must be under 1 MB in size.

8 Click **OK**, then click **Apply** to save and create the connector for OAuth2.

It is common with some OAuth sources for the Token URL or Profile URL to require the oauth_token variable instead of the expected accessToken variable. To fix this, add the following:

`URL:?oauth_token{$accessToken}`

For example: `https://api.foursquare.com/v2/users/self?oauth_token={$accessToken}`

4.11 Configuring OpenID Connect Sites as Identity Sources

SocialAccess provides a generic OpenID Connect template. The OpenID Connect template allows you to configure OpenID Connect sites as identity sources for SocialAccess. For example, PayPal is an OpenID Connect site.

To use the OpenID Connect template:

1 Create an OpenID Connect application that represents the SocialAccess appliance on the developer site you want to use as an identity source.

Creating an application does not require any coding.

2 Copy the following information into a document as you create the OpenID Connect application to use when configuring the OpenID Connect template:

- ◆ (Optional) Discovery URL
- ◆ (Optional) Register URL
- ◆ Client ID
- ◆ Client Secret ID

- ◆ Authentication URL
- ◆ Token URL
- ◆ Profile URL

3 Log in to the SocialAccess administration console:

`https://appliance_dns_name/appliance/index.html`

4 Drag and drop the OpenID Connect template from the **Identity Sources** palette to the **Identity Sources** panel.

5 Click the template, then click **Configure**.

6 Use the information gathered in Step 2 to create your own connector for OpenID Connect following the on-screen prompts.

7 (Optional) You can upload a login card image that is specific to your OpenID Connect application in the **Card image** field. Users see this image when they log in to SocialAccess.

The image can be a `.png`, `.jpg`, or `.gif` file. The file size is 215px x 50px and the file must be under 1 MB in size.

8 Click **OK**, then click **Apply** to save and create the connector for OpenID Connect.

It is common with some OpenID Connect sources for the Token URL or Profile URL to require the oauth_token variable instead of the expected accessToken variable. To fix this, add the following:

`URL:?oauth_token{$accessToken}`

For example: `https://api.foursquare.com/v2/users/self?oauth_token={$accessToken}`

5 Configuring Application Connectors

SocialAccess provides several application connectors that are included in the appliance. This chapter describes configuration tasks that are common to multiple connectors. For more information about configuring specific connectors, see the following chapters:

In addition to configuring embedded connectors, you can create custom connectors. For more information, see

5.1 Requirements for Connectors

As you configure connectors, ensure that you meet these general setup requirements:

❐ Ensure that the **Display Name** for each configured instance of a connector is unique for the appliance. The name allows you to identify a configured instance of the connector on the Applications panel of the administration console.

❐ The **Federation Instructions** on a connector's Configuration page provide the information that you will use to configure federation for SocialAccess on the service provider site. The information identifies where on the service provider's site to find the federation configuration capability as well as the field values and other guidance that you need to complete the required information.

When you configure the connector, the federation instructions will automatically provide the following information about your appliance as the identity provider:

- The URL for single sign-on

  `https://appliance_dns_name/osp/a/t1/auth/saml2/sso`

- The URL for single logout

  `https://appliance_dns_name/osp/a/t1/auth/app/logout`

- The URL for the identity provider's entityID

  `https://appliance_dns_name/osp/a/t1/auth/saml2/metadata`

- The X.509 signing certificate for the appliance

  The application uses the certificate to set the trust relationship with SocialAccess.

  NOTE: When you copy the appliance's signing certificate, ensure that you include all leading and trailing hyphens in the certificate's Begin and End tags.

5.2 Viewing Connectors for Applications

SocialAccess displays the connectors in the following locations of the administration console:

* **Applications palette:** Displays unconfigured connectors that ship with the appliance.
* **Applications panel:** Displays configured connectors for the applications that you want to make available to users.

5.3 Providing Access to Applications for Users

After you configure the connectors for applications, you must provide a way for users to access the applications. SocialAccess provides the following portal pages for users:

* **Login page:** The login page allows users to enter their corporate credentials for authentication, such as user name and password. SocialAccess authenticates a user against your identity sources.

  The login page also exposes the authentication extensions of the appliance, such as Google reCAPTCHA, if configured.

  The URI for the login page is the public DNS name of the appliance. Provide this URl to your users:

  ```
  https://appliance_dns_name
  ```

* **Landing page:** The landing page contains the appmarks (linked icons) for accessing the applications that a user is entitled to use. The landing page appears after a user enters valid credentials and responds successfully to any additional authentication prompts.

  This page displays appmarks for an application only after the related connector is configured properly and the user has been authenticated. When a user clicks an appmark, SocialAccess shares identity information about the user with the application in order to establish the user's session. For more information about appmarks, see Section 5.4, "Configuring Appmarks for Connectors," on page 42.

5.4 Configuring Appmarks for Connectors

Appmarks are essentially bookmarks for applications. After you configure a connector for an application, you configure one or more appmarks to enable users to access the application in different ways. After a user logs in to SocialAccess, users see the appmarks on the landing page that they are entitled to see, according to the application settings for public access.

You can configure appmarks for any SSO connector. You can even configure multiple appmarks for the same connector. You can copy an existing appmark to create a new one.

NOTE: Appmarks for SSO connectors have no access control associated with them. If users know how to get to a service, they can access the service. Appmarks just add convenience to the user experience.

5.4.1 Understanding Appmark Options

You configure appmarks on the Appmarks tab in the Configuration window for the connector. On the Appmarks tab next to the name of the appmark in the blue bar are several icons for renaming, copying, disabling, or deleting the appmark. Use the mouseover text to identify the icon you want to use. You can view and edit appmark configuration options by clicking the blue bar or the plus sign (+) icon. The following appmark options are available:

Reset

> This button restores the Appmarks tab to the default settings for the connector. Consider using this option if you have configured custom connectors that are not working as expected. Click **OK** and apply the changes to the appliance to see the default appmark settings.

Desktop browser

> Enables the appmark to be visible on the SocialAccess landing page.

Initiate login at

> Specifies whether the URL of the appmark on the landing page is the identity provider-initiated type or the service provider-initiated type. This option is not available for the OAuth2 Resources connector because the OAuth2 Resources connector offers only service provider-initiated authentication. It does not have an IDP-initiated mode.

URL

> The URL that is to be used for the appmark. There are some replacement values that you can use. For more information, see Section 5.4.4, "Using Appmark Variables," on page 45.

Icon

> The icon that represents the application on the landing page. You can use a different custom icon for each connector to improve their usability for users.

5.4.2 Configuring an Appmark

After you have configured a connector for an application, you can configure an appmark to simplify access to that application from the user's landing page.

To configure an appmark:

1 Log in with an appliance administrator account to the administration console:

   `https://appliance_dns_name/appliance/index.html`

2 (Conditional) If you have not already configured the connector for the application, drag it from the **Applications** palette to the **Applications** panel, then provide the appropriate information on the **Configuration** tab. The required information varies depending on the connector.

3 (Conditional) If you have already configured the connector for the application, click the connector on the **Applications** panel and click **Configure**.

4 Click the **Appmarks** tab.

5 Click the plus (+) sign next to the default created appmark.

6 The **Desktop browser** check box is selected by default. Complete the following steps to configure the appmark:

    6a (Conditional) If it is applicable to the connector, select the appropriate option from the **Initiate login at** list.

    6b Leave the default value in the **URL** field.

    6c (Optional) If you want to provide your own icon for the appmark, click the **X** on the **Icon** line to delete the default icon. Then browse to and select a `.png` file to represent the application on the browser's landing page.

7 Click **OK**, then click **Apply**.

The appliance reconfigures with the new change. After this process has completed, users who enter the appliance URL are redirected to a login page. They enter their user name and password and are presented with a landing page containing the appmark icon that links to the application.

5.4.3 Creating Multiple Appmarks for an Application

Application connectors can have multiple appmarks. You can create a new appmark from scratch, or you can copy an existing appmark to save time, especially if you want to create several appmarks and just change one or two options on each one. This procedure assumes you have already configured the connector.

To create a new appmark for a connector:

1 Log in with an appliance administrator account to the administration console:

    `https://`*`appliance_dns_name`*`/appliance/index.html`

2 Click the configured connector on the **Applications** panel, then click **Configure**.

3 Click the **Appmarks** tab, then do one of the following:

    ◆ Click **New**

    ◆ Click the **Copy** icon next to the existing appmark name

4 (Conditional) If you are copying an existing appmark, the **Name** field is pre-populated with `COPY_${DisplayName}`. You have several options:

    ◆ You can accept this default name. (However, note that "COPY_" will be part of the name.)

    ◆ You can change the display name by manually editing the text.

    ◆ You can edit the display name by selecting from available variables. Type ${ at the end of the field, then select a variable from the list. For more information about the available variables, see Section 5.4.4, "Using Appmark Variables," on page 45.

5 Complete the appropriate fields for the appmark. For more information about available options, see Section 5.4.1, "Understanding Appmark Options," on page 43.

6 Click **OK**, then click **Apply** to update the appliance.

5.4.4　Using Appmark Variables

Each connector has different configuration settings and variables, and some appmarks need to contain information from the connector configuration to be useful. When you configure a connector, the Appmarks tab is automatically populated with one or more default appmarks, depending on the connector. The default settings contain some variables in the URL field.

You can use the variables that are available for a connector in the **Name** and **URL** fields if they are of the string type and have a value provided. To insert a variable, type `${` to display the available variables. Use the mouse or press the up/down arrow keys to select a variable. When you press the down arrow key, an additional box shows the resolved value. Press the up arrow key to close the resolved variables box. Some variables may not be resolvable until after you apply your changes on the appliance.

6 Configuring the SAML 2.0 Connector for ADFS

The connector for Active Directory Federation Services (ADFS) provides federated single sign-on access to ADFS with SAML 2.0 through SocialAccess. It does not support provisioning. The connector allows SocialAccess to authenticate a user against an enterprise identity source and to share this authentication with ADFS in order to establish the user's session.

SocialAccess includes this connector with the appliance. The connector appears automatically on the Applications palette in the administration console. After you configure the connector, you must also configure ADFS to work with the connector.

6.1 Requirements

Verify that you meet the following requirements before you import the connector:

❒ An understanding of identity federation using the SAML 2.0 protocol.

For more information about SAML, see the OASIS website (https://wiki.oasis-open.org/security/FrontPage).

❒ An ADFS 2.0 system, installed and configured.

❒ Administrator access to the ADFS system. An understanding of ADFS and its management tools are presumed.

❒ An ADFS user account for each user who wants to authenticate to ADFS through the SocialAccess single sign-on service. The connector for ADFS does not provision user accounts.

❒ The location in the ADFS administration console where you will configure the SAML 2.0 federation for SocialAccess.

When you configure the connector, the **Federation Instructions** provide the information that you will need to set up the federation in ADFS for SocialAccess. This information includes the metadata; a signing certificate for the appliance; the field values to use; and other guidance.

❒ The metadata file from the ADFS 2.0 system.

`https://adfsserver/FederationMetadata/2007-06/FederationMetadata.xml`

You will need the following information from the metadata file:

 ◆ **Assertion Consumer Service URL:** The value in the **AssertionConsumerService** field with the HTTP-POST binding.

 ◆ **EntityID:** The value in the **entityID** field.

 ◆ **Logout URL:** The value in the **SingleLogoutService Location** field with the HTTP-POST binding.

❒ (Optional) An X.509 signing certificate from ADFS is required to support single logout. Communications use SSL regardless of whether you provide this certificate.

6.2 Configuring the Connector

After you import the connector, you must configure it to work with your ADFS system.

1 Log in as an administrator to the SocialAccess administration console:

```
https://appliance_dns_name/appliance/index.html
```

2 Drag and drop the SAML 2.0 connector for ADFS from the **Applications** palette to the **Applications** panel.

3 On the **Configuration** page, specify the configuration properties.

Use the information from the ADFS metadata file. The signing certificate from ADFS is optional.

4 Under **Assertion Attribute Mappings**, map the SAML Assertion attributes to the appropriate attributes in your identity source.

5 Expand the **Federation Instructions**, then copy and paste the instructions into a text file to use during the ADFS configuration for single sign-on.

NOTE: You must use a text editor that does not introduce hard returns or additional white space. For example, use Notepad instead of Wordpad.

6 Click the **Appmarks** tab, then review and edit the default settings for the appmark.

For more information, see Section 5.4, "Configuring Appmarks for Connectors," on page 42.

7 Click **OK** to save the configuration.

8 Click **Apply** to commit the changes to the appliance.

9 Wait until the configuration changes have been applied on each node of the cluster.

10 Log in to ADFS as the ADFS administrator, then configure the SAML 2.0 federation for SocialAccess in the ADFS administration console.

Use the information from the **Federation Instructions** in Step 5 to complete the setup.

NOTE: When you copy the appliance's signing certificate, ensure that you include all leading and trailing hyphens in the certificate's Begin and End tags.

11 After you complete the configuration, users can log in through SocialAccess to single sign-on to the ADFS system. The SocialAccess login page URL is:

```
https://appliance_dns_name
```

12 (Conditional) To allow Service Provider-initiated login, you must specify the Name ID format on the ADFS side. To do this, run the following PowerShell command:

```
Set-ADFSClaimsProviderTrust -TargetName Display Name from Claims
Provider Trust -RequiredNameIdFormat
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
```

13 (Optional) If you want users to connect to SharePoint, proceed to Section 6.4, "Connecting to SharePoint," on page 49.

6.3 Troubleshooting Certificate Errors

If you use a self-signed certificate and certificate chain errors occur, run the following PowerShell command:

```
Set-ADFSClaimsProviderTrust -TargetName Display Name from above -
SigningCertificateRevocationCheck None
```

6.4 Connecting to SharePoint

With additional configuration, the SAML 2.0 connector for ADFS allows users to single sign-on through SocialAccess to SharePoint as well as ADFS.

This section describes how you can leverage the claims-based single sign-on capabilities of ADFS and SharePoint to set up a hub model of federation through ADFS. In this hub, SocialAccess has a trusted relationship with ADFS as the identity provider, and ADFS has a trusted relationship with SharePoint as a claims-based federation provider. SharePoint accepts the claims-based assertions, and allows users to access federated SharePoint web applications. Using roles for claim-based single sign-on makes it easier for SharePoint site administrators to map role and organization claims to SharePoint groups.

To set up the relationships, you define the roles in the connector for ADFS that ADFS and SharePoint will use for the claims-based single sign-on. The connector adds the role information to the identity information in assertions that it sends to ADFS.

In ADFS, you configure claims rules that look for the email address and role of users, and then transform them for use by SharePoint. ADFS applies rules to the assertions from SocialAccess to transform them into role claims that the SharePoint web applications understand, and sends the role claims to SharePoint.

In SharePoint, you configure its Person Picker to look for the roles in the assertions from ADFS. SharePoint validates the assertion information, stores the information in its token cache, and issues a session cookie for the user. By default, SharePoint sets the session lifetime to be the same as the SAML token lifetime. In ADFS, you can specify the web single sign-on lifetime that determines the lifetime of the session cookie. Typically, the cookie expires when the user closes the browser window.

To set up this claims-based single sign-on federation hub:

- The SocialAccess administrator must modify the definition for the connector for ADFS to add two new roles to use for claims-based single sign-on, and then import and configure the modified connector.
- The ADFS administrator must configure a connection between SharePoint and ADFS, and define the rules for passing identity and role information from SocialAccess to SharePoint.
- The SharePoint administrator must modify the SharePoint People Picker to look for the roles in incoming assertions.
- The SharePoint administrator can add users to a SharePoint group based on the users' roles.

6.4.1 Requirements

Verify that you meet the following requirements:

❒ A SocialAccess appliance, installed and configured.

❒ One server with the following components installed:

  ❒ Windows Server 2008 (or later) with the latest updates.

  ❒ Active Directory with the latest updates.

  ❒ ADFS 2.0 with the latest updates.

❐ A SharePoint 2010 (or later) server with the latest updates, installed in the same domain as the ADFS server.

   ❐ The SharePoint server should be connected to the ADFS server.

   For information about connecting the servers, see the following references in the Microsoft TechNet Library:

   ◆ *How to Configure ADFS v 2.0 in SharePoint Server 2010* (http://technet.microsoft.com/en-us/library/hh305235%28v=office.14%29.aspx).

   ◆ *Configure SAML-based Claims Authentication with ADFS in SharePoint 2013* (http://technet.microsoft.com/en-us/library/hh305235%28v=office.15%29.aspx)

❐ Roles enabled within the SharePoint system using PowerShell scripts.

6.4.2 Adding Roles to the SAML 2.0 Connector for ADFS

You must modify the definitions in a SAML 2.0 connector for ADFS template file to add roles that will be used when ADFS sends role claims to SharePoint. These instructions create two roles: an administrator role called `ADMIN` and a user role called `USER`.

Modifying the SAML 2.0 Connector for ADFS Template

Use the NetIQ Access Connector Toolkit to modify the definitions in the connector for ADFS.

1 Obtain a copy of the ZIP file for the SAML 2.0 connector for ADFS.

2 Log in as a SocialAccess administrator to the Access Connector Toolkit at

   `https://`*appliance_dns_name*`/css/toolkit`

3 Click **Import**, browse to and select the connector's ZIP file, then click **OK**.

4 Click the **Display Name** link for the connector to open it in the Edit Connector Template window.

5 Click the **Assertions** tab, then on the left side of the screen, click the **Attributes** tab.

6 Click **New,** then create a new Role attribute to use for the SharePoint connection.

   6a Define the properties for the Role attribute:

   Name: Specify `http://schemas.microsoft.com/ws/2008/06/identity/claims/role`.

   Display Name: Specify `Role`.

   Encoding: Leave this field blank.

   Data Owner: Leave this field blank.

   Default Value: Leave this field blank.

   Required: Select **false** to make this attribute optional.

   Description: Specify `A role assigned to the user account`.

   Role Attribute: Select **true**, then continue to configure the role definitions.

   6b Under **Roles**, click **New,** specify the following information, then click **Save**.

   Name: Specify `ADMIN`.

   Description: Specify `Administrator Role`.

   6c Under **Roles**, click **New,** specify the following information, then click **Save**.

   Name: Specify `USER`.

   Description: Specify `User Role`.

6d Add or customize any additional roles that you need for the SharePoint environment, and save each one.

6e Click **Save** to save the Role attribute definition.

7 Click **Save** to apply the connector template changes.

8 Click the **Export** icon next to the **Display Name** for the connector template.

9 Save the ZIP file for use on this or another SocialAccess system.

10 Proceed to "Importing the Modified Connector" on page 51.

Importing the Modified Connector

After you modify the SAML 2.0 connector for ADFS, you must import the connector into SocialAccess.

1 Log in as an administrator to the SocialAccess administration console at

   https://*appliance_dns_name*/appliance/index.html

2 On the Admin page, click the **Tools** icon on the toolbar, then click **Import connector template**.

3 Click **Browse,** then browse to and select the ZIP file for the modified SAML 2.0 connector for ADFS.

4 Click **Import**.

   The Applications palette displays the modified SAML 2.0 connector for ADFS.

5 Proceed to "Configuring the Modified Connector" on page 51.

Configuring the Modified Connector

After you export and import the modified connector, you configure the connector by following the steps in Section 6.2, "Configuring the Connector," on page 48.

After you configure a SAML 2.0 connector for ADFS that supports SharePoint roles, you must modify ADFS and SharePoint to accept these roles. Proceed to "Modifying Claims Rules in the ADFS System" on page 51.

6.4.3 Modifying Claims Rules in the ADFS System

Before you begin, ensure that you have configured a connection between ADFS and SharePoint. In ADFS, you must define the claim rules for incoming assertions from SocialAccess and for outgoing assertions sent to SharePoint.

Adding Claims Rules for SharePoint Roles in Incoming Assertions

You must modify the ADFS claim rules between ADFS and SocialAccess. The purpose of these rules is to allow the user's email address and the role to pass through to SharePoint.

To add claim rules for incoming assertions from SocialAccess:

1 Log in to your ADFS system.

2 Access the **Claims Provider Trusts** for SocialAccess.

3 Click **Edit Claim Rules**.

4 Add two rules using the following information:

- ◆ Rule 1
  - ◆ **Claim rule template:** Select **Pass Through or Filter an Incoming Claim**.
  - ◆ **Claim rule name:** Specify `pass nameID`.
  - ◆ **Incoming claim type:** Specify `Name ID`.
  - ◆ **Incoming name ID format:** Specify `Email`.
  - ◆ **Pass through all claim values:** Select this option.
- ◆ Rule 2
  - ◆ **Claim rule template:** Select **Pass Through or Filter an Incoming Claim**.
  - ◆ **Claim rule name:** Specify `pass Roles`.
  - ◆ **Incoming claim type:** Specify `Roles`.
  - ◆ **Pass through all claim values:** Select this option.

5 Exit the Rule editor.

6 Proceed to "Adding Claims Rules for Transforming Assertions for SharePoint" on page 52.

Adding Claims Rules for Transforming Assertions for SharePoint

You must configure ADFS to map the user's Email Address to Login on the SharePoint system, and to send the user's role.

To add claim rules for assertions sent to SharePoint:

1 In the ADFS console, select **Trust Relationships** > **Relying Party Trusts**.

2 Right-click *Name of your SharePoint system*, then select **Edit Claim Rules**.

3 Add two rules with the following information:

- ◆ Rule 1
  - ◆ **Claim rule template:** Select **Transform an Incoming Claim**.
  - ◆ **Claim rule name:** Specify `NameID to EmailAddress`.
  - ◆ **Incoming claim type:** Specify `Name ID`.
  - ◆ **Incoming name ID format:** Specify `Email`.
  - ◆ **Outgoing claim type:** Specify `E-mail Address`.
  - ◆ **Pass through all claim values:** Select this option.
- ◆ Rule 2
  - ◆ **Claim rule template:** Select **Pass Through or Filter an Incoming Claim**.
  - ◆ **Claim rule name:** Specify `pass Roles`.
  - ◆ **Incoming claim type:** Specify `Roles`.
  - ◆ **Pass through all claim values:** Select this option.

4 Exit the Rule editor.

5 Proceed to Section 6.4.4, "Configuring the SharePoint People Picker to Use the Roles," on page 53.

6.4.4 Configuring the SharePoint People Picker to Use the Roles

The default SharePoint People Picker configuration requires a repository of users and groups for the people picker to search. However, in a claims-based access model, the only information SharePoint has is the claims data associated with the current user's SAML assertion.

Before you begin, ensure that you have roles enabled within the SharePoint system using PowerShell scripts.

After you complete the ADFS configuration, you must configure the SharePoint option of **People Picker** to use the roles ADMIN and USER for claims received from ADFS.

1 Where the SharePoint system grants access, select **People Picker**.

2 Under **ADFS**, select **Role**.

3 In the **Find** box, specify either ADMIN or USER.

This field must contain the name of the role you configure the connector to use in Section 6.4.2, "Adding Roles to the SAML 2.0 Connector for ADFS," on page 50.

4 Select the role SharePoint returns, then assign the role to the group within SharePoint.

6.4.5 Troubleshooting SharePoint Issues

Use the following information if you encounter problems.

Issue: Error: The root of the certificate chain is not a trusted root authority.

Solution: You need to change the SharePoint server certificates. For detailed instructions, see *Root Certificate Chain not Trusted* (http://blogs.technet.com/b/speschka/archive/2010/02/13/root-of-certificate-chain-not-trusted-error-with-claims-authentication.aspx).

7 Configuring the Connector for NetIQ Access Manager

The connector for NetIQ Access Manager provides federated single sign-on access to Access Manager with SAML 2.0 through SocialAccess. It does not support provisioning. The connector allows SocialAccess to authenticate a user against your identity sources and to share this authentication with Access Manager in order to establish the user's session.

SocialAccess includes this connector with the appliance. The connector appears automatically on the Applications palette in the administration console. After you configure the connector, you must also configure Access Manager to work with the connector. Although you typically install the Access Manager Identity Server as an identity provider (IdP), you must configure it to be a service provider (SP) that consumes authentication information from SocialAccess.

7.1 Requirements for the Connector for Access Manager

❒ A SocialAccess appliance, installed and configured.

❒ A NetIQ Access Manager 4.0.*x* system, installed and configured.

Ensure that SSL communications are enabled for Identity Server and Access Gateway, and that both components are configured to trust the same signing certificate authority. For more information, see "Enabling SSL Communications" in the *NetIQ Access Manager Setup Guide*. You will use this signing certificate for the Access Manager connector in SocialAccess.

❒ Access Manager user accounts for each user who wants the single sign-on service.

❒ The metadata file from your Access Manager system for SAML 2.0 services:

```
https://<access_manager_identity_server_dns_name>/nidp/saml2/metadata
```

❒ The SSL signing certificate from Access Manager.

IMPORTANT: The configuration assumes that you have configured SSL communications for Access Manager. The SSL signing certificate does not necessarily need to come from an external certificate authority, but you must use the same certificate for the Access Manager connector in SocialAccess when you set up the federation. Each provider must trust the SSL certificate authority.

For information about configuring SSL communications for Access Manager, see "Security and Certificate Management" in the *NetIQ Access Manager Administration Console Guide*.

SSL is used for the secure exchange of authentication information between SocialAccess and Access Manager. When you configure the Access Manager connector in SocialAccess, you must import the trusted root certificate from the Access Manager NIDP Trust Store. Failure to import the certificate causes numerous system errors.

You can download the certificate from the Trusted Roots configuration for Access Manager. Store the file in a location that you can browse to from the SocialAccess appliance.

1. In the Access Manager Administration Console, click **Devices > Identity Servers > ClusterName > Security > Trusted Roots**.

2. Click the signing certificate name.

3. On the Certificate Details page, select **Export Public Certificate**, then click **PEM** as the file type.

   A PEM-encoded file is a Base64-encoded DER certificate that is enclosed between `BEGIN CERTIFICATE` and `END CERTIFICATE` tags.

4. Store the **PEM** file in a location that you can browse to from the SocialAccess appliance when you configure the connector for Access Manager.

You can alternatively copy the certificate information from the `ds:X509Certificate` field in the Access Manager metadata file. Ensure that you add `-----BEGIN CERTIFICATE-----` before the encoded information, and add `-----END CERTIFICATE-----` after the encoded information.

You must use a text editor that does not introduce hard returns or additional white space. For example, use Notepad instead of Wordpad.

❐ If you use an eDirectory identity source for Access Manager and you need to provide access to Access Gateway protected resources that require a user name and password, you must enable Universal Password in eDirectory for the Access Manager LDAP connection.

NOTE: Universal Password Retrieval options must be properly set in the configuration of the Universal Password policy in eDirectory, so that it allows the password to be retrieved from the Access Manager user store.

For more information, see *Unable to retrieve Universal Password from eDirectory using PasswordFetchClass (TID 7007114)* (http://www.novell.com/support/kb/doc.php?id=7007114).

7.2 Configuring the Connector for Access Manager

To provide identity services to Access Manager, SocialAccess must trust Access Manager as a service provider. Establish this trust by enabling and configuring the NetIQ Access Manager connector.

Before you begin, ensure that your system meets the requirements in Section 7.1, "Requirements for the Connector for Access Manager," on page 55.

To configure the connector for Access Manager:

1 Download the metadata file for SAML 2.0 services from your Access Manager system:

`https://<access_manager_identity_server_DNS_name>/nidp/saml2/metadata`

You need information from this file to configure the Access Manager connector.

2 Log in as an administrator to the SocialAccess administration console:

`https://appliance_dns_name/appliance/index.html`

3 Drag and drop the SAML 2.0 connector for NetIQ Access Manager from the **Applications** palette to the **Applications** panel.

4 On the Configuration window, use information from the Access Manager metadata file to specify the following connector settings:

NOTE: The information from the Access Manager metadata file is case sensitive.

Connector Parameter	Value	Metadata Parameter or Description
Display name	*my_nam_sp*	Specify a unique name for your Access Manager service provider.
Assertion consumer service URL	`https://`*idp.example.com*`/nidp/saml2/spassertion_consumer`	Specify the location in the `AssertionConsumerService` section for HTTP-POST bindings.
Destination URL	*https://web_redirect_url*	(Optional) After a successful authentication by the IdP, the web browser is redirected to the secure destination URL.
EntityID	`https://`*idp.example.com*`/nidp/saml2/metadata`	`entityID` Ensure that you specify the ID with lowercase characters.
Logout response URL	`https://`*idp.example.com*`/nidp/saml2/spslo_return`	Specify the response location in the `SingleLogoutService` section for HTTP-POST bindings.
Logout URL	`https://`*idp.example.com*`/nidp/saml2/spslo`	Specify the location in the `SingleLogoutService` section for HTTP-POST bindings.
Signing certificate		Browse to and select the file that contains the Access Manager SSL certificate.

5 In the **Assertion Attribute Mappings** section, select an attribute from the **NameID** list to use for mapping users in the federation.

Specify the identity source attribute that contains a user's name identifier in the Access Manager user store. SocialAccess and Access Manager can use different user stores, as long as you can find an attribute that is consistent between them.

For example, select **X-Custom1**, where you have created a custom mapping of the employee ID attribute to the X-Custom1 attribute in the SocialAccess identity source.

6 Expand **Federation Instructions**, then copy and paste the instructions into a text file to use during the Access Manager configuration.

Use a text editor that does not introduce hard returns or additional white space. For example, use Notepad instead of Wordpad.

7 Click the **Appmarks** tab, then review and edit the default settings for the appmark.

8 Click **OK** to save the configuration.

9 Click **Apply** to commit the changes to the appliance.

10 Wait until the configuration changes have been applied on each node of the SocialAccess cluster.

11 As the Access Manager administrator, configure the SAML 2.0 federation for CloudAccess.

For more information, see Section 7.3, "Configuring Access Manager to Use SocialAccess as an Identity Provider," on page 58.

Use the information from the **Federation Instructions** in Step 6 to complete the setup.

NOTE: When you copy the appliance's signing certificate, ensure that you include all leading and trailing hyphens in the certificate's Begin and End tags.

7.3 Configuring Access Manager to Use SocialAccess as an Identity Provider

After configuring the connector, you must configure Access Manager to use SocialAccess as a trusted external identity provider.

❒ **Create an attribute set to use for the identity provider attributes.**

Access Manager uses attribute sets to provide a common naming scheme for the exchange of authentication information. Using an attribute set reduces the traffic between the identity provider and the service provider's identity source, because the attribute information can be gathered in one request at authentication rather than in a separate request for each attribute when a policy or protected resource needs the attribute information.

For more information, see "Configuring Attribute Sets" in the *NetIQ Access Manager Identity Server Guide*.

❒ **Create an attribute matching expression to use for the identity provider user identification.**

When Access Manager receives an assertion from SocialAccess, it uses the attributes in the assertion to match the user to an identity in your identity sources. You must know which attributes in the identity source are used to uniquely identify the users. Use the same attribute that you specified in the attribute set, such as Ldap Attribute:workforceID.

For more information, see "Configuring User Matching Expressions" in the *NetIQ Access Manager Identity Server Guide*.

❒ **Create an external identity provider for SAML 2.0 that represents SocialAccess.**

SocialAccess acts as an external identity provider to Access Manager. You must establish a trust between them so that two user accounts can be associated with each other without the sites exchanging user data.

For more information, see "Creating a Trusted Service Provider for SAML 2.0" in the *NetIQ Access Manager Identity Server Guide*.

❒ **Create an external authentication contract for the identity provider that represents SocialAccess.**

An external authentication contract allows you to use SocialAccess as the primary authentication method for a resource. The contract can allow users to authenticate only through SocialAccess, or to alternatively authenticate through local contracts of equal or higher authentication levels. The contract defines a string that the identity provider uses to match an incoming authentication request from Access Manager. You can assign a contract to one or more resources.

IMPORTANT: If the protected resources are authenticated primarily by a local contract, but might alternatively be authenticated by SocialAccess, you can modify the local contract you want to use to allow it to be satisfiable by an external provider.

For more information, see "Configuring Authentication Contracts" in the *NetIQ Access Manager Identity Server Guide*.

❏ **Configure a SAML 2.0 authentication request for the identity provider that represents SocialAccess.**

Access Manager uses an authentication request to define the federation method and the authentication contract to use for an external identity provider. This relationship between the identity provider and service provider enables single sign-on and single log-out. To enable the authentication process for SocialAccess, you must create an authentication request that uses the external authentication contract that you created for it. The authentication type in the contract must match the string that the service provider sends in an authentication request.

For more information, see "Configuring an Authentication Request for an Identity Provider" in the *NetIQ Access Manager Identity Server Guide*.

❏ **(Conditional) If you use an eDirectory identity source and the protected applications require a password, configure password retrieval.**

The identity provider contract for SocialAccess does not use a user name and password for the credentials. To allow single sign-on to Access Gateway protected resources that require a user's name and password, you must configure the PasswordFetchClass to retrieve them. You create the class, then create a password retrieval authentication method from the class.

The service provider executes the password retrieval after the identity provider completes the remote authentication and federation. It stores the user name and password with the LDAP credentials, then allows the additional user-specific attributes to be injected in SAML assertions for authentication sent to and consumed by the Access Gateway that protects the back-end resources. This advanced authentication enables users to access the back-end protected resources.

IMPORTANT: The PasswordFetchClass works only with eDirectory user stores where Universal Password is enabled.

For more information, see "Configuring Password Retrieval" in the *NetIQ Access Manager Identity Server Guide*.

❏ **Configure a user identification method to use for the identity provider that represents SocialAccess.**

During the authentication, SocialAccess matches the user with an account in the Access Manager user store. The matching process allows SocialAccess to retrieve information about the user, such as the name, email, roles, and so on. You must specify the user identification method that is used to match the user account at the identity provider (SocialAccess) with a user account at the service provider (Access Manager).

For more information, see "Selecting a User Identification Method for Liberty or SAML 2.0" in the *NetIQ Access Manager Identity Server Guide*.

❏ **Configure attributes for the identity provider that represents SocialAccess.**

You must specify the attributes that SocialAccess can use to match the user to an account in the Access Manager user store. An authentication request and response contain these attributes.

For more information, see "Configuring the Attributes Obtained at Authentication" in the *NetIQ Access Manager Identity Server Guide*.

❏ **Assign the external authentication contract to the protected resources.**

You can use SocialAccess as the identity provider for back-end resources protected by Access Gateway. To do this, use the external authentication contract that you created for SocialAccess as the definition of how users authenticate to the protected resources.

For more information about configuring Access Gateway to protect resources, see "Configuring Protected Resources" in the *NetIQ Access Manager Access Gateway Guide*.

7.4 Configuring Appmarks for Protected Resources in Access Manager

After you have configured the connector for Access Manager and single sign-on SAML 2.0 federation between Access Manager and SocialAccess, you can configure appmarks for protected resources in Access Manager.

The default appmark for the connector for Access Manager uses the Destination URL field from the configuration. If you did not specify the Destination URL, you will end up at the Access Manager home page for the default appmark.

For more information, see Section 5.4, "Configuring Appmarks for Connectors," on page 42.

7.5 Configuring Identity Provider-Initiated Logins

You must complete some additional configuration steps to enable users to log in to the web service while also authenticating to the identity source. A login initiated by the identity provider allows users to start the login process at the SocialAccess login page.

1. The user accesses the IdP-initiated login URL you provide.

   ```
   https://appliance_dns_name
   ```

2. The landing page displays different appmarks for each application configured to work with the appliance.
3. The user clicks the appmark to access the web service.
4. SocialAccess redirects the login to the web service.
5. The user is authenticated to both the identity source and the web service at this point.

You must provide a link to the IdP-initiated login URL for users to access.

```
https://appliance_dns_name
```

You can also copy the auto-generated URL on each icon to provide as a link for the user.

8 Configuring the Connector for OAuth2 Resources

The connector for OAuth 2 Resources provides simple authenticated access to a web service through SocialAccess. The connector allows SocialAccess to authenticate a user against your identity sources and to provide protected access to a destination web service.

SocialAccess includes this connector with the appliance. The connector appears automatically on the Applications palette in the administration console. After you configure the connector, you must also configure the OAuth2 client application.

The connector for OAuth2 Resources offers a simple authentication method as an alternative to federated single sign-on connectors that use SAML 2.0 or WS-Federation protocols. Protocols for federated access management provide a robust trust and security model that is an open standard and widely used. However, it does require the protocol's code to be installed on the protected services. Consider using the connector for OAuth2 Resources for smaller services that do not require the full security and trust that SAML or WS-Federation provides, and just need a simple method to validate and get identity information from a trusted source (the SocialAccess identity provider in this case).

By implementing the open standard OAuth 2.0 protocol, the connector for OAuth2 Resources behaves as an OAuth2 Authorization Server and Resource Server using the Authorization Code flow as detailed in the OAuth 2.0 Authorization Framework document at http://tools.ietf.org/html/rfc6749#section-4.1.

Using this connector, the SocialAccess appliance provides user authentication and all OAuth2 token creation and validation for access to a protected resource.

NOTE: The OAuth2 Resources connector provides SP-initiated authentication. It does not have an IDP-initiated mode.

8.1 Configuring the OAuth2 Client Application

When you configure the connector for OAuth2 Resources in SocialAccess, the Client ID, Client Secret, and OAuth Endpoint URLs are created automatically. This information must then be used to configure the OAuth2 client application. All configuration activities at the OAuth2 client application are out of band.

Enforcement of authorization or access control beyond the initial authentication and token creation process is the responsibility of the OAuth client application. For information about configuring the OAuth client application, refer to your OAuth client application documentation.

8.2 Configuring the Connector for OAuth2 Resources

You can configure instances of the OAuth2 Resources connector in one of the following ways:

- An instance of the connector per OAuth client application. This is the simplest method conceptually and matches how SAML connectors are used.

- Multiple OAuth client applications all configured within a single instance of the OAuth2 Resources connector. This means that all OAuth2 client applications would use the same schema (OpenID Connect or native), and would use the same Client ID and Client Secret. This configuration is simple to configure and maintain, but care should be taken to include only clients of the same trust level in a connector instance. Because all clients share the same client ID and secret, if one of the clients is compromised in any way, they are all compromised. Any of them could also masquerade as another client in some cases.

(Optional) For each OAuth client application, you can manually create appmarks so the SocialAccess landing page shows an icon for connection to the OAuth2 client application. Appmarks should be configured to point to the URL of the OAuth2 client application that will start the OAuth2 authentication process.

To configure the connector for OAuth2 Resources:

1 Log in as an administrator to the SocialAccess administration console:

   https://*appliance_dns_name*/appliance/index.html

2 Drag and drop the **OAuth Resources** connector from the **Applications** palette to the **Applications** panel.

3 In the **Applications** panel, click the new **OAuth Resources** connector and then click **Configure**.

4 On the **Configuration** tab, provide the following information:

   - **Display name**: Clearly identify the connector on the **Applications** panel of the administration console.

   - **Schema**: Specify whether the attributes that SocialAccess sends to the OAuth client follow OpenID Connect standard naming or use the Native schema names defined internally on the appliance.

   - **Allowed OAuth Client URI(s)**: Specify the whole path or just the host name for the OAuth2 client application. Using only the host name allows all paths on that domain. Since OAuth2 depends on SSL as one of its core security mechanisms, HTTPS should always be specified. For more information about configuring redirect URIs, see the following document: http://tools.ietf.org/html/rfc6749#section-10.6.

   - **OAuth Details (Client ID and Client Secret)**: Use this information to configure the OAuth2 client application.

   - **OAuth Endpoints (Auth URL, Token URL, and Profile URL)**: Use this information to configure the OAuth2 client application.

5 Click the **Appmarks** tab, then review and edit the default settings for the appmark.

6 Click **OK** to save the configuration.

7 Click **Apply** to commit the changes to the appliance.

8 Wait until the configuration changes have been applied on each node of the SocialAccess cluster.

After the OAuth2 Resources connector and OAuth client application have been configured, end users can access the protected resource by browsing to the URL of the OAuth client application (by entering the URL directly into the browser, using a bookmark or the landing page appmark, and so forth). If the user is not already authenticated to the SocialAccess appliance, the browser is redirected

to the SocialAccess login page and the user is prompted for login credentials. After a successful authentication or if the user is already authenticated to the appliance and is authorized to access the protected resource, the user gains access to the resource.

8.3 Supported OpenID Connect Schema

The OAuth Resources connector supports the OpenID Connect schema names listed in the following table.

Table 8-1 *OpenID Connect Schema*

Member	Type	Description
name	string	End user's full name in displayable form including all name parts, possibly including titles and suffixes, ordered according to the user's locale and preferences.
given_name	string	Given name(s) or first name(s) of the end user. Note that in some cultures, people can have multiple given names; all can be present, with the names being separated by space characters.
family_name	string	Surname(s) or last name(s) of the end user. Note that in some cultures, people can have multiple family names or no family name; all can be present, with the names being separated by space characters.
middle_name	string	Middle name(s) of the end user. Note that in some cultures, people can have multiple middle names; all can be present, with the names being separated by space characters. Also note that in some cultures, middle names are not used.
preferred_username	string	Shorthand name that the end user wishes to be referred to at the RP, such as janedoe or j.doe. This value *may* be any valid JSON string including special characters such as @, /, or whitespace. This value *must not* be relied upon to be unique by the RP. (See Section 2.5.3 (http://openid.net/specs/ openid-connect-basic-1_0-28.html#claim.stability) of the OpenID Connect Basic Client Profile 1.0 document.)
picture	string	URL of the end user's profile picture. This URL *must* refer to an image file (for example, a PNG, JPEG, or GIF image file), rather than to a Web page containing an image. Note that this URL *should* specifically reference a profile photo of the end user suitable for displaying when describing the end user, rather than an arbitrary photo taken by the end user.
email	string	end user's preferred email address. Its value *must* conform to the RFC 5322 (http://openid.net/specs/openid-connect-basic-1_0-28.html#RFC5322) addr-spec syntax. This value *must not* be relied upon to be unique by the RP, as discussed in Section 2.5.3 (http://openid.net/specs/openid-connect-basic-1_0-28.html#claim.stability) of the OpenID Connect Basic Client Profile 1.0 document.
gender	string	End user's gender. Values defined by this specification are female and male. Other values *may* be used when neither of the defined values is applicable.

Member	Type	Description
birthdate	string	End user's birthday, represented as an ISO 8601:2004 (http://openid.net/specs/openid-connect-basic-1_0-28.html#ISO8601-2004)[ISO8601-2004] YYYY-MM-DD format. The year *may* be 0000, indicating that it is omitted. To represent only the year, YYYY format is allowed. Note that depending on the underlying platform's date related function, providing just year can result in varying month and day, so the implementers need to take this factor into account to correctly process the dates.
locale	string	End user's locale, represented as a BCP47 (http://openid.net/specs/openid-connect-basic-1_0-28.html#RFC5646) [RFC5646] language tag. This is typically an ISO 639-1 Alpha-2 (http://openid.net/specs/openid-connect-basic-1_0-28.html#ISO3166-1) [ISO639 1] language code in lowercase and an ISO 3166-1 Alpha-2 (http://openid.net/specs/openid-connect-basic-1_0-28.html#ISO3166-1) [ISO3166 1] country code in uppercase, separated by a dash. For example, en-US or fr-CA. As a compatibility note, some implementations have used an underscore as the separator rather than a dash, for example, en_US; Implementations *may* choose to accept this locale syntax as well.
phone_number	string	End user's preferred telephone number. E.164 (http://openid.net/specs/openid-connect-basic-1_0-28.html#E.164) [E.164] is *recommended* as the format of this Claim, for example, +1 (425) 555-1212 or +56 (2) 687 2400. If the phone number contains an extension, it is *recommended* that the extension be represented using the RFC 3966 (http://openid.net/specs/openid-connect-basic-1_0-28.html#RFC3966) [RFC3966] extension syntax, for example, +1 (604) 555-1234;ext=5678.

9 Configuring the Connector for Simple Proxy

The connector for Simple Proxy provides reverse proxy access to your enterprise web service through SocialAccess. The connector allows SocialAccess to authenticate a user against your identity sources and to provide protected access to a destination web service. You can configure the connector to protect access to the document root of the web server, or to protect access only to a path within the document root of the web server.

Every web server is different. Two common simple proxy scenarios are:

- **Simple website:** If your web server provides a single web service, you can protect access to the entire site by creating a connector for Simple Proxy. The connector points to the document root of the web server.

- **Multiple-service website:** If your server provides multiple web services, you can create a separate connector for Simple Proxy for each destination web service. Each connector points to a different independent path within the document root of the web server.

If the web service requires user identity information to control access or content, you can configure the connector to inject the authenticated user's identity attributes in query strings and headers sent to the web service. However, the connector cannot be used to provide single sign-on for web services that require passwords for access. It does not support provisioning.

This connector is embedded with the SocialAccess appliance, and is located on the Applications palette in the administration console. Each cluster supports multiple connectors for Simple Proxy.

9.1 Requirements for Simple Proxy

The connector for Simple Proxy enables reverse proxy access to an enterprise web server behind your firewall. It can support web services that employ user identity information to control access or display if you enable the identity injection policies that insert an authenticated user's identity attributes in query strings or headers of requests it sends to the web server. For more information, see Section 9.2, "Viewing or Customizing the Attributes for Identity Injection," on page 66.

For each proxy web service, the web service's content should be self-contained in that path. If the service depends on files that reside in parallel paths on the web server, you can specify a path at a higher level in the document root's directory structure, or reorganize the site's contents as needed.

The connector for Simple Proxy does not support the following:

- **Protected resources that require a password:** This proxy solution cannot be used with protected web services or applications that require an LDAP password to be included in the identity injection. The appliance cannot send a user's password for a proxy application to the back end web service.

  If the web server needs the user's password, you must find a workaround. For example, you could specify a static string that is accepted for all users.

- **Site redirects:** This proxy solution does not support site redirects to locations outside the protected path. It cannot follow paths to alternate websites.

IMPORTANT: The Access Gateway for NetIQ Access Manager provides solutions for more complex reverse proxies that support password injection and redirects. For more information, see "Managing Reverse Proxies and Authentication" in the *NetIQ Access Manager Access Gateway Guide*.

Before you configure a connector for Simple Proxy, ensure that your setup meets the following requirements:

❒ A SocialAccess system, installed and configured.

❒ A web server, configured and running behind the corporate firewall. Ensure that you have configured the authentication procedures and identity injection policy for the web service.

  You need the following information:

  - The primary DNS name or IP address of the web server.
  - Alternative DNS names or IP addresses for the web server, if any.
  - The port number that the web server uses to listen for requests, such as 8080 (non-secure) or 8443 (secure SSL).
  - If the web server requires secure communications with HTTPS.

    If you use HTTPS, the value that you specify for the web server's DNS name or IP address in the connector must match the CN in the web server's SSL certificate.

❒ Determine which web services you need to protect for your web server, and which users require access to each one.

9.2 Viewing or Customizing the Attributes for Identity Injection

The connector for Simple Proxy can inject an authenticated user's identity attributes in query strings and headers of communications sent from the appliance to the destination web service. The web server might use this information to determine whether the user should have access to the resource. It can also use the identity information to customize content on the web page. For example, when a user whose first name is Joe (as specified in the identity source) navigates to the destination web page, he might see "Welcome: Joe" at the top of his browser window.

9.2.1 Understanding Identity Attributes

In the connector for Simple Proxy, you can enable or disable the following identity injection policies. Both policies are enabled by default.

- **Inject Identity in Query:** If you enable this option, when a user navigates to the connector's destination web service, the service receives all of the user's identity attributes in the query string.

  WARNING: Injecting attributes in the query string could exceed the maximum URL length of 2083 characters.

- **Inject Identity in Header:** If you enable this option, when a user navigates to the connector's destination web service, the service receives all of the user's identity attributes as custom headers.

If you enable an injection policy, the connector sends all of the user's identity attributes, even if the values are unavailable (empty). For some applications, this is still useful information and the web service can use it to make access or display decisions.

WARNING: If you use HTTP for communications between the connector and the web service, the injected identity attributes are available as clear text to network packet sniffers.

Although the proxy service runs behind the firewall, consider configuring the connector's web service URL with HTTPS to protect the communication stream to the web service. If you use HTTPS, the value that you specify for the web server's DNS name or IP address in the connector must match the CN in the web server's SSL certificate.

The attribute values in the query strings parameters or header parameters sent to the web server are based on the following options in the identity source user interface:

Identity Source Parameter	Query String Parameter	Header Parameter
ID	ID	X-ID
Email	Email	X-Email
User name	UserName	X-UserName
First name	FirstName	X-FirstName
Middle name	MiddleName	X-MiddleName
Last name	LastName	X-LastName
Full name	FullName	X-FullName
Preferred name	PreferredName	X-PreferredName
Generational qualifier	GenerationalQualifier	X-GenerationalQualifier
Gender	Gender	X-Gender
Phone	Phone	X-Phone
Birthdate	BirthDate	X-BirthDate
Street address	StreetAddress	X-StreetAddress
City	City	X-City
State	State	X-State
ZIP code	ZipCode	X-ZipCode
Country	Country	X-Country
Language	Language	X-Language
Identity Type	IdentityType	X-IdentityType
X-Custom1	XCustom1	X-XCustom1
X-Custom2	XCustom2	X-XCustom2
X-Custom3	XCustom3	X-XCustom3
X-Custom4	XCustom4	X-XCustom4
X-Custom5	XCustom5	X-XCustom5

The IdentityType parameter for query strings and headers indicates the type of identity source that the appliance uses to authenticate the user, such as Active Directory, eDirectory, and JDBC.

9.2.2 Viewing Identity Attribute Mappings to Identity Source Attributes

In your identity source, the identity attributes are mapped to identity source attributes. You can view mappings in your identity source connector. For example, in eDirectory, ID is mapped to the `guid` attribute, `User name` is mapped to the `cn`, and so on. You can change these mappings as needed for your environment, but any changes you make are global. You cannot change them on a per proxy or app basis.

To view identity attribute mappings in an identity source:

1 Log in as an administrator to the SocialAccess administration console:

    https://*appliance_dns_name*/appliance/index.html

2 In the **Identity Sources** panel, click the identity source, then click **Configure**.

3 Expand **Advanced Options**.

4 In the **Attribute Mappings** section, expand **Default** to view the list of the mappings of identity attributes to identity source attributes.

5 If you modify the settings, click **OK** to save your changes, then click **Apply**.

    Do not continue until the changes are applied to all nodes of the appliance cluster.

6 Repeat this process for each identity source that manages users who will access the destination web server.

9.2.3 Configuring Custom Identity Attributes

An identity injection sends all identity attributes. You cannot specify only a subset of attributes, add attributes, or remove attributes. However, you can map the X-Custom<1-5> attributes to attributes in your identity source. Ensure that you map the appropriate identity source attribute to each custom attribute across all of the identity sources for users who will access the destination web server.

To configure custom identity attributes in your identity source:

1 Log in as an administrator to the SocialAccess administration console:

    https://*appliance_dns_name*/appliance/index.html

2 In the **Identity Sources** panel, click the identity source, then click **Configure**.

3 Expand **Advanced Options**, then use the **Attribute Mappings** section to map custom attributes (X-Custom<1-5>) to attributes in your identity source.

4 Click **OK** to save your changes, then click **Apply**.

    Do not continue until the changes are applied to all nodes of the appliance cluster.

5 Repeat this setup for each identity source that manages users who will access the destination web server.

9.3 Configuring the Connector for Simple Proxy

Each connector for Simple Proxy can protect only a single web location. If the connector is set to protect the document root, then users can access all files served by the website. If the connector is set to protect a path under the document root, users can access only those files that reside in the path or its subdirectories.

To configure the connector for Simple Proxy:

1 Log in as an administrator to the SocialAccess administration console:

    https://*appliance_dns_name*/appliance/index.html

2 Drag and drop the connector for Simple Proxy from the **Applications** palette to the **Applications** panel.

3 On the **Configuration** tab, provide the following information:

Display name: Specify the display name for the reverse proxy service. This name is also the default name of the appmark that appears on the user landing page.

Local path: Specify a unique path on the appliance that will be used in the URL to associate traffic for the remote web service, such as `/myservice` or `servicexyz`. The path will be appended to the DNS name of the cluster for accessing the resource, and will be removed from the request before forwarding it to the web server.

The local path must be unique across all connectors for Simple Proxy that you configure on the appliance. You can use alphanumeric characters a to z and 0 to 9, forward slashes (/), hyphens (-), and underscores (_). Spaces, uppercase characters, and other special characters are not supported. The path is not case sensitive. There is no length limit, but you should consider length restrictions for URLs and file system pathnames when you specify the character string.

Connects to: Specify the URL of the destination web service that you want to protect.

You can use HTTP (not secure) or HTTPS (secure) in the URL, depending on requirements of the web server. If you use HTTPS, the value that you specify for the DNS name or IP address must match the CN in the web server's SSL certificate. The connector automatically finds the SSL certificate and installs it for you if the URL uses HTTPS.

You can specify the IP address or DNS name of the web server. Specify the port number if it is needed to access the location.

Do one of the following:

- ◆ Specify the root of the web server in order to protect all resources in the document root of the web server, including its subdirectories and their content.

  For example, you can specify the URL in any of the following formats:

  ```
  http://10.20.30.40
  http://10.20.30.40:8080
  https://myweb.example.com
  https://myweb.example.com:8443
  ```

- ◆ Specify a path within the document root of the web server in order to protect only the resources in that path, including its subdirectories and their content.

  For example, you can specify the URL in any of the following formats:

  ```
  http://10.20.30.40/path_to_protect
  http://10.20.30.40:8080/path_to_protect
  https://myweb.example.com/path_to_protect
  https://myweb.example.com:8443/path_to_protect
  ```

Inject Identity in Query: Select this option to include the user identity attributes in the query strings that are sent to the **Connects to** URL. For more information, see Section 9.2, "Viewing or Customizing the Attributes for Identity Injection," on page 66.

WARNING: Injecting attributes in the query string could exceed the maximum URL length of 2083 characters.

Inject Identity in Headers: Select this option to include the user identity attributes in the headers that are sent to the **Connects to** URL. For more information, see Section 9.2, "Viewing or Customizing the Attributes for Identity Injection," on page 66.

4 Expand **Advanced Options**, then configure the **Rewriter Options**.

The rewriter parses and searches the web content that passes through the appliance for URL references that qualify to be rewritten. URL references are rewritten when they meet the following conditions:

Strip Local path from query string: Enables URL references specified in the query strings to be rewritten with the published DNS name.

Strip Local path from POST data: Enables URL references specified in the post data to be rewritten with the published DNS name.

Strip Local path from REFERRER header: Enables URL references specified in the referrer headers to be rewritten with the published DNS name.

Alternative Host Names: URL references that match entries in this list are rewritten with the published DNS name. You can use any of the following formats. The entries are not case sensitive.

```
site.example.com
myhostname
10.10.2.10
http://<dns_name_or_ip_address>
http://<dns_name_or_ip_address>:port
https://<dns_name_or_ip_address>
https://<dns_name_or_ip_address>:port
```

You need to include names in this list if your web servers have any of the following configurations:

- If you have a cluster of web servers that are not sharing the same DNS name, you need to add their DNS names to this list.

- If your web server obtains content from another web server, the DNS name for this additional web server needs to be added to the list.

- If the web server listens on one port (for example, 80), and redirects the request to a secure port (for example, 443), the DNS name needs to be added to the list. This allows the response to be sent in the format that the user expects.

- If an application is written to use a private hostname, you need to add the private hostname to the list. For example, `http://<hostname>/index.html`.

5 Click the **Appmarks** tab, then review and edit the default settings for the appmark.

6 Click **OK** to save the configuration.

7 Click **Apply** to commit the changes to the appliance.

8 Wait until the configuration changes have been applied on each node of the SocialAccess cluster.

10 Creating Custom Connectors with the Access Connector Toolkit

SocialAccess provides the NetIQ Access Connector Toolkit (ACT) that allows you to create custom connectors. If you need help creating a custom connector to use with SocialAccess, Priority Support customers have the option to open a service request with NetIQ Technical Support (NTS) (http://www.netiq.com/support). NTS is available to provide toolkit support as well as to configure the connectors to work with integrated applications. Additional information from the SaaS provider is usually required.

NOTE: Before you contact NetIQ Technical Support, please complete the appropriate worksheet for the connector type that you want to create. See Appendix A, "Custom Connector Worksheets," on page 95.

The Access Connector Toolkit facilitates custom connector development efforts without coding or scripting. You can create custom connectors for identity-aware web services or applications that use the following authentication methods for single sign-on:

- SAML 2.0
- WS-Federation
- SAML 2.0 Inbound (SAML-In)

NOTE: Although the Access Connector Toolkit displays options for creating custom connectors for web services or applications that use Basic SSO (forms-based) authentication for single sign-on, SocialAccess does not support Basic SSO custom connectors.

After you create a connector, you must export it from the toolkit as a file that you can import into SocialAccess. You can use the SocialAccess administration console to import and enable the connector, and to create appmarks for the web service or application.

10.1 Accessing the Access Connector Toolkit

The Access Connector Toolkit is a web application that you access through the SocialAccess appliance. It requires administrator credentials.

To access the toolkit:

1 Log in as a SocialAccess administrator to the Access Connector Toolkit:

   `https://`*`appliance_dns_name`*`/css/toolkit`

10.2 Toolkit Requirements

The Access Connector Toolkit is a web application that ships with SocialAccess. You can use the Access Connector Toolkit to create custom connectors if you have a SocialAccess license as well as appropriate accounts with the destination services.

10.2.1 Toolkit Compatibility

The Access Connector Toolkit contains new functionality for the SocialAccess 2.1 release. In order to update an existing custom connector template with the new functions, you can import the template into the new toolkit, and then export the template again. The updated connector template contains the new functionality.

Templates that you create with the new toolkit are not backwards compatible with prior releases of the toolkit. You cannot import a connector from SocialAccess 2.1 into a toolkit that came with a prior version of SocialAccess. The import fails.

10.2.2 Provisioning Support

Provisioning is supported only through connectors created by NetIQ. At this time, you cannot create a custom connector template that supports provisioning user accounts to the connected system.

10.3 Federation Requirements for the Application Service Provider

As you explore the features of the Access Connector Toolkit, refer to the definitions in this section to understand the type of information you will need to collect from the destination web service or application.

assertion

A SAML 2.0 assertion is a package of identity attributes for an authenticated user that is sent from the trusted identity provider to the service provider.

assertion properties

The properties of the assertion include the following information:

- The recipient of the assertion.
- The LDAP identity attribute to use when federating users with the destination application service provider. Does the NameID require an email address format, or does it require unspecified format?
- The URL where SocialAccess should redirect the end user's session after the user logs in successfully with the URL provided on the connector configuration page.
- The binding method to use for identity information sent to the destination provider. For SAML 2.0, the only supported binding method is POST.

assertion attributes

The provider should provide a technical document that describes the attributes that are required for an assertion, such as the user's name or email address. It can include the attributes that are required to assign roles. The SAML assertion typically requires the nameID attribute. You must map the SAML assertion attributes to the matching attributes in your identity source.

entityID

The entityID is a field from the metadata that uniquely identifies that particular service provider, such as *sp_domain_name*.

For example:

google.com

The entity ID might use information from the federation instructions, or from a setting completed on the Configuration page when you deploy the connector.

federation instructions

The federation instructions provide the information that you will use to configure federation for SocialAccess on the service provider site. The information identifies where on the service provider's site to find the federation configuration capability as well as the field values and other guidance that you need to complete the required information.

When you configure the connector, the federation instructions will automatically provide the following information about your appliance as the identity provider:

- The URL for single sign-on

  `https://appliance_dns_name/osp/a/t1/auth/saml2/sso`

- The URL for single logout

  `https://appliance_dns_name/osp/a/t1/auth/app/logout`

- The URL for the identity provider's entityID

  `https://appliance_dns_name/osp/a/t1/auth/saml2/metadata`

- The X.509 signing certificate for the appliance

  The web service or application uses the certificate to set the trust relationship with SocialAccess.

  NOTE: When you copy the appliance's signing certificate, ensure that you include all leading and trailing hyphens in the certificate's Begin and End tags.

It provides the following information about your appliance if the login is initiated by the service-provider, such for connectors that use the WS-Federation protocol:

- The WS-Federation Passive URL
- The X.509 signing certificate for the appliance

metadata

The metadata is the configuration information that the application service provider uses to establish communications with the identity provider in an federation trust relationship. This usually includes a login URL or a customer-specific domain name, which is called the Assertion Consumer Service URL. Service providers allow you to export the required metadata to an XML file, or they provide the metadata in a public URL. The auto-generated metadata file from the service provider will not work as is. You must manually change the values to match your actual deployment environment.

The metadata usually includes the following information:

- The entityID for the service provider.
- The URL that receives the user identity information.
  - For SAML 2.0, the Assertion Consumer Service URL is where the assertion is posted by the browser. For example:

    `https://www.google.com/a/${customer-domain}/acs`

- For WS-Federation, the Login URL is where the security token is posted by the browser. It corresponds to the `PassiveRequestorEndpoint` field from the metadata.

- For SAML-In, the Single Sign-on Service URL is where the AuthnRequest will be posted. It corresponds to the `SingleSignOnService` field with a Post binding from the metadata.

  `https://accessmanager.base.url/nidp/saml2/sso`

- The logout URL corresponds to the `SingleLogoutService` field from the metadata.

- The logout URL Binding (HTTP Post or Redirect)

  The logout response URL

- The X.509 signing certificate

protocol binding

The protocol binding is the method used for transmitting assertions between the authenticating identity provider and the service provider. SocialAccess supports the Redirect and Post bindings for service-provider-initiated SSO, and the Post binding for identity-provider-initiated SSO.

nameID

The nameID is the attribute in the identity source that uniquely identifies the user. You must know whether this attribute requires the email address format or an unspecified format.

new settings

The new settings are appliance-specific settings that you want to allow the administrators to set when they configure the connector for an appliance.

For example:

- Customer-specific sections of the Assertion Consumer Service URL

- Connector-specific setting, such as a customer domain

security token

A WS-Federation security token is a package of identity attributes for an authenticated user that is sent from the trusted identity provider to the service provider. The provider should provide a technical document that describes the attributes that are required for the token, such as the user's name or email address. It can include the attributes that are required to assign roles.

signing certificate

The signing certificate is the X.509 certificate that identifies SocialAccess to the service provider. If you specify that the certificate is required by the service provider, the template automatically retrieves the appliance's certificate and inserts it in the Federation Instructions when you deploy the connector. You use the certificate when you set up the federated single sign-on for the application.

template properties

The template properties define the following information for the connector:

- Type of connector and type name (based on the template wizard)

- The unique name for the template file (target name)

- A brief description used as the connector name

- A 3-digit version number (ex: 1.0.0)

- A custom graphic to use for the icon that represents the connector in the SocialAccess administration console.

10.4 Creating a SAML 2.0 Connector Template

To create a connector for single sign-on with SAML 2.0, you can use the SAML2 option in the Access Connector Toolkit.

10.4.1 SAML 2.0 Requirements for the Application Service Provider

To create a custom SAML 2.0 connector, the application that connects to SocialAccess must meet the following protocol-specific requirements:

❒ Support identity federation using the SAML 2.0 protocol.

For more information about SAML, see the OASIS website (https://wiki.oasis-open.org/security/FrontPage).

❒ Support the SAML web browser single sign-on profile, with the Redirect and POST bindings for service-provider-initiated SSO, and the POST binding for identity-provider-initiated SSO.

❒ Provide a capability in the application's administration console that allows you to enable and configure SAML SSO with SocialAccess as the identity provider.

❒ Provide technical documents that describe the application's SAML federation requirements, metadata, and assertions.

10.4.2 Planning for a SAML 2.0 Connector

Before you attempt to create the SAML 2.0 connector, you must collect information about the destination web service or application. For more information, see Section 10.3, "Federation Requirements for the Application Service Provider," on page 72.

Ask the application service provider the following types of questions to gather the required information:

- What does your SAML assertion look like?
- Do you have a SAML metadata document? What fields, if any, are customer-specific?
- Does your service support the SAML single logout protocol?
- What are the required configuration steps in your application to set up federation?
- What information do you provide to customers when they are setting up federation with their identity source?

10.4.3 Creating a SAML 2.0 Connector Template for an Application

A SAML 2.0 connector template consists of multiple components for federation, metadata, and assertion information.

To create a custom SAML 2.0 connector:

1 Log in as an administrator to the Access Connector Toolkit:

   `https://appliance_dns_name/css/toolkit`

2 Click **New** > **SAML2**.

   The connector **Type** is `SAML2`. The **Type Name** is `Generic SAML2 Connector`.

3 On the **Template** tab, complete the following information:

- ◆ Template properties
- ◆ Whether the service provider requires a signing certificate
- ◆ Federation instructions for the service provider
- ◆ New settings that need to be collected on the Configuration page of the connector

4 Click the **Metadata** tab, then use one of the following methods to specify the metadata:

- ◆ Select **Request**, then specify the source URL to retrieve the metadata.
- ◆ Complete the fields to manually generate the metadata.
- ◆ Import the values from a file or URL, and modify them for your deployment environment.

5 Click the **Assertion** tab, then define the properties and attributes required for the assertion.

    5a On the **Properties** subtab, specify the properties for the assertion.

    5b On the **Attributes** subtab, click **New**, specify and define the identity attribute, then click **Save**.

    5c (Conditional) If the service provider requires other identity attributes for an assertion, repeat Step 5b to map the SAML assertion attribute to an attribute in your identity source.

6 (Optional) If it is supported, create the provisioning definitions. For more information, see Section 10.2.2, "Provisioning Support," on page 72.

7 Click **Save** to save the new connector template.

8 Proceed to Section 10.8, "Exporting a Connector Template," on page 80 to finish creating the new connector.

10.5 Creating a WS-Federation Connector Template

To create a connector for single sign-on with WS-Federation, you can use the WS-Fed option in the Access Connector Toolkit.

10.5.1 WS-Federation Requirements for the Application Service Provider

To create a custom WS-Federation connector, the destination application that connects to SocialAccess must meet the following protocol-specific requirements:

❒ Support identity federation using the WS-Federation protocol.

    For more information about WS-Federation, see the OASIS website (http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html) or see the MSDN Library article (http://msdn.microsoft.com/en-us/library/bb498017.aspx).

❒ Support for the WS-Federation Passive Requestor Profile.

❒ Provide a capability in the application's administration console that allows the customer to enable and configure WS-Federation SSO.

❒ Provide technical documents that describe the application's WS-Federation federation requirements, metadata, and security tokens.

10.5.2 Planning for a WS-Federation Connector

Before you attempt to create a WS-Federation connector, you must collect information about the destination web service or application. For more information, see Section 10.3, "Federation Requirements for the Application Service Provider," on page 72.

Ask the web service or application vendors the following types of questions to gather the required information:

- What does your WS-Federation security token look like?
- Do you have a WS-Federation metadata document? What fields, if any, are customer-specific?
- What are the required configuration steps in your application to set up federation?
- What is the information that you provide to customers when they are setting up federation with their identity source?

10.5.3 Creating a WS-Federation Connector Template for an Application

A WS-Federation connector template consists of multiple components for federation, metadata, and assertion information.

To create a custom connector:

1 Log in as an administrator to the Access Connector Toolkit:

    https://*appliance_dns_name*/css/toolkit

2 Click **New** > **WSFed**.

    The connector **Type** is `WS-Fed`. The **Type Name** is `Generic WS-Fed Connector`.

3 On the **Template** tab, complete the following information:
    - Template properties
    - Whether the service provider requires a signing certificate
    - Federation instructions for the service provider
    - New settings that need to be collected on the Configuration page of the connector

4 Click the **Metadata** tab, then use one of the following methods to specify the metadata:
    - Select **Request**, then specify the source URL to retrieve the metadata.
    - Complete the fields to manually generate the metadata.
    - Import the values from a file or URL, and modify them for your deployment environment.

5 Click the **Assertion** tab, then define the properties and attributes required for the security token.

    5a On the **Properties** subtab, specify the properties for the assertion.

    5b On the **Attributes** subtab, click **Predefined**, click the identity attribute, modify the definition if needed, then click **Save**.

    If a predefined option does not exist, use **New** to define it.

    5c (Conditional) If the service provider requires other identity attributes for an assertion, repeat Step 5b to map the WS-Federation attribute to an attribute in your identity source.

6 (Optional) Create the provisioning definitions. For more information, see Section 10.2.2, "Provisioning Support," on page 72.

7 Click **Save** to save the new connector template.

8 Proceed to Section 10.8, "Exporting a Connector Template," on page 80 to finish creating the new connector.

10.6 Creating a SAML 2.0 Inbound Connector Template

To create a connector for single sign-on with SAML 2.0 Inbound, you can use the SAML2 In option in the Access Connector Toolkit.

IMPORTANT: Connectors that you create in the Access Connector Toolkit using the SAML2 In option work only for users that you create on the SocialAccess appliance. SAML2 Inbound connectors will not work in SocialAccess with existing user accounts.

10.6.1 SAML2 In Requirements for the Application Service Provider

To create a custom SAML 2.0 Inbound connector, the destination application that connects to SocialAccess must meet the following protocol-specific requirements:

❑ Support identity federation using the SAML 2.0 protocol.

For more information about SAML, see the OASIS website (https://wiki.oasis-open.org/security/FrontPage).

❑ Support the SAML web browser single sign-on profile, with the Redirect and POST bindings for service-provider-initiated SSO, and the POST binding for identity-provider-initiated SSO.

❑ Provide a capability in the application's administration console that allows the customer to enable and configure SAML SSO.

❑ Provide technical documents that describe SAML federation requirements, metadata, and assertions.

10.6.2 Planning for a SAML2 In Connector

Before you attempt to create the connector, you must collect information about the destination web service or application. For more information, see Section 10.3, "Federation Requirements for the Application Service Provider," on page 72.

Ask the web service or application vendors the following types of questions to gather the required information:

- What does your SAML assertion look like?
- Do you have a SAML metadata document? What fields, if any, are customer-specific?
- Does your service support the SAML single logout protocol?
- What are the required configuration steps in your application to set up federation?
- What is the information that you provide to customers when they are setting up federation?

10.6.3 Creating a SAML2 In Connector for an Application

A SAML2 In connector template consists of multiple components for federation, metadata, and assertion information.

To create a custom connector template:

1 Log in as an administrator to the Access Connector Toolkit:

   https://*appliance_dns_name*/css/toolkit

2 Click **New** > **SAML2 In**.

   The connector **Type** is SAML2 In. The **Type Name** is Generic SAML2 In Connector.

3 On the **Template** tab, complete the following information:

   - Template properties
   - Whether the service provider requires a signing certificate
   - Federation instructions for the service provider
   - New settings that need to be collected on the Configuration page of the connector

4 Click the **Metadata** tab, then use one of the following methods to specify the metadata:

   - Select **Request**, then specify the source URL to retrieve the metadata.
   - Complete the fields to manually generate the metadata.
   - Import the values from a file or URL, and modify them for your deployment environment.

5 Click the **Assertion** tab, then define the properties and attributes required for the security token.

   5a On the **Properties** subtab, specify the properties for the assertion.

   5b On the **Attributes** subtab, click **Predefined**, click the identity attribute, modify the definition if needed, then click **Save**.

   If a predefined option does not exist, use **New** to define it.

   5c (Conditional) If the service provider requires other identity attributes for an assertion, repeat Step 5b to map the WS-Federation attribute to an attribute in your identity source.

6 Click **Save** to save the new connector template.

7 Proceed to Section 10.8, "Exporting a Connector Template," on page 80 to finish creating the new connector.

10.7 Modifying a Connector

You can modify the definition information for a connector by importing it in the Access Connector Toolkit. For example, you can import an existing connector to update its definition to the latest features available for connectors.

1 Obtain a copy of the connector's ZIP file.

2 Log in as a SocialAccess administrator to the Access Connector Toolkit:

   https://*appliance_dns_name*/css/toolkit

3 Click **Import**, browse to and select the connector's ZIP file, then click **OK**.

   The connector appears in the list of connector templates.

4 Click the **Edit** icon next to the **Display Name** for the connector template to open it in the Edit Connector Template window.

5 Modify the connector template settings as desired.

6 Click **Save** to apply the changes.

7 Click the **Export** icon next to the **Display Name** for the connector template.

8 Save the ZIP file for use on this or another SocialAccess system.

9 Proceed to Section 10.9, "Importing and Configuring Custom Connectors," on page 80.

10.8 Exporting a Connector Template

After you create a connector template, you must use the Access Connector Toolkit to export it in a compressed ZIP file that you can import to any SocialAccess system. You then import the connector template in the SocialAccess administration console to make it available in the **Applications** palette.

To export the connector template:

1 Log in as a SocialAccess administrator to the Access Connector Toolkit:

    https://*appliance_dns_name*/css/toolkit

2 Click the **Export** icon next to the **Display Name** for the connector template.

3 Save the ZIP file for use on this or another SocialAccess system.

4 Proceed to Section 10.9, "Importing and Configuring Custom Connectors," on page 80.

10.9 Importing and Configuring Custom Connectors

SocialAccess allows you to import and configure custom connectors that you create with the Access Connector Toolkit, or that are created for you by NetIQ Technical Support or NetIQ partners.

After you export a custom connector, you must import its ZIP file to SocialAccess to make it available in the **Applications** palette of the administration console. Thereafter, you can enable and manage the connector as you do the connectors for applications that shipped with the appliance. The custom connector might require additional configuration, depending on the single sign-on method you use.

The destination application might also require additional configuration, depending on the application and the federation method.

To import and configure a custom connector:

1 Copy the custom connector ZIP file to the computer where you administer SocialAccess.

2 Log in as an administrator to the SocialAccess administration console:

    https://*appliance_dns_name*/appliance/index.html

3 Click the **Tools** icon on the toolbar, then click **Import connector template**.

4 Browse to and select the custom connector ZIP file, then click **Import**.

5 Drag and drop the new custom connector from the **Applications** palette to the **Applications** panel.

6 (Conditional) For connectors that provide federated single sign-on, complete the connector settings on the **Configuration** tab.

The steps to configure the connector are determined by the information you added to the connector template.

7 (Conditional) For connectors that provide federated single sign-on, expand the **Federation Instructions**, then copy and paste the instructions into a text file to use when you configure the destination application.

> **NOTE:** You must use a text editor that does not introduce hard returns or additional white space. For example, use Notepad instead of Wordpad.

8 Click the **Appmarks** tab, then review and edit the default settings for the appmark.

9 Click **OK** to save the configuration.

10 Click **Apply** to commit the changes to the appliance.

11 Wait until the configuration changes have been applied on each node of the SocialAccess cluster.

12 (Conditional) For connectors that provide federated single sign-on, configure the destination application for the appropriate federation method.

11 Customizing the End User Experience

After you have completed the configuration of the identity sources and the connectors for the SAML applications, you can perform additional customization such as rebranding, if appropriate.

11.1 Customizing Branding on User-Facing Pages

SocialAccess allows you to customize user-facing pages, such as the login page, so users see your company branding instead of the default NetIQ branding. After you have customized those pages, you can modify them as needed to meet new company requirements. Customizing the user pages does not affect any pages in the administration console itself.

IMPORTANT: Performing advanced branding customization requires advanced JavaServer Pages (JSP) knowledge. Before you make any changes, ensure that you have a good snapshot of your appliance that you can revert to if necessary. If you upload a bad branding file and are unable to log in to the administration console, you can re-run the appliance initialization to restore the default login pages. For more information, see Section 2.4, "Re-initializing the Appliance," on page 17.

To customize branding for users:

1 (Conditional) If you plan to perform extensive rebranding, take a snapshot of the appliance.

2 Log in with an appliance administrator account to the SocialAccess administration console:

`https://`*appliance_dns_name*`/appliance/index.html`

3 On the toolbar, click the Tools icon, then click **End user branding**.

4 (Conditional) If you want to customize the login page that users see, complete the following steps:

   4a Click **Basic Customization**.

   4b Change the title and background colors by specifying HTML color codes.

   4c Change the default image by either not showing the image, or uploading a new image.

   The user interface changes the image size to automatically display the best size for the image.

   4d Click **OK** to save the changes and then click **Apply**.

5 (Conditional) If you want to perform more extensive rebranding, complete the following steps:

   5a Click **Advanced Customization**.

   5b Click **Download default end user login code**.

   5c Save the file to your local computer.

   5d Save a backup copy of the file.

   5e Unzip the downloaded file and locate the `.jsp` files in the `osp\jsp` subdirectory.

5f Modify the desired `.jsp` pages. The default text for the login page is located in the `osp\resources\oidp_custom_resources_en_US.properties` file.

5g Zip up the files again, but include only the `images` and `jsp` directories.

5h Log in to the administration console again.

5i On the toolbar, click the **Tools** icon, then click **End user branding**.

5j (Conditional) If you are customizing pages for the first time, click **Browse**, then browse to and select the modified file.

5k (Conditional) If you are updating previously customized pages, delete the name of the existing file. Click **Browse**, then browse to and select the `.zip` file that contains the newly modified `.jsp` files.

5l Wait until the file name changes to a hexadecimal value, then click **OK**.

5m Click **Apply**.

The pages now display the branding you customized in the `.jsp` files.

11.2   Configuring the Session Timeout for Users

When a user logs into SocialAccess, the default session timeout is 10 minutes. You can change this session timeout value through the administration console.

To change the session timeout for users:

1 Log in to the administration console:

`https://`*appliance_dns_name*`/appliance/index.html`

2 Click the Cluster icon in the lower left corner of the screen.

3 Click **Configure**.

4 Change the **User session timeout** field value. The value for the field is in minutes.

5 Click **OK**, then click **Apply** to save the changes.

12 Maintenance Tasks

SocialAccess allows you to change various appliance configuration settings as needed. For example, moving your appliance from a staging configuration to a production environment requires changes to the networking components.

12.1 Changing the Cluster Password

You can change the administrator password for the cluster as needed. The administrator password is the same for all nodes in the cluster.

To change the cluster password:

1 Log in with an appliance administrator account to the administration console:

   `https://appliance_dns_name/appliance/index.html`

2 Click the Cluster icon at the bottom of the page, then click **Change cluster password**.

3 Type your old password, then type your new password twice and click **OK**.

12.2 Changing the IP Address

You can change whether a node uses DHCP or a static IP address.

1 Log in with an appliance administrator account to the administration console:

   `https://appliance_dns_name/appliance/index.html`

2 Click the node icon, then click **Configure**.

3 Select whether the appliance uses DHCP or a static IP address.

   If you select to use a static IP address, you can change the required values for the subnet mask, default gateway, and the DNS server.

4 Click **OK** to save the changes, then click **Apply** to apply the changes to the appliance.

If you have additional networking options configured, see .

12.3 Changing Public DNS Name or NTP Server Settings, or Uploading New Certificates

The appliance contains self-generated certificates. You can upload custom certificates through the administration console.

1 Log in with an appliance administrator account to the administration console:

```
https://appliance_dns_name/appliance/index.html
```

2 Click the cluster icon, then click **Configure**.

3 Change the key pairs, NTP server, or public DNS name, then click **OK**.

4 Click **Apply** to apply the changes to the appliance.

Expired key pair certificates prohibit changes from being made to this page and make the key pair field red.

12.4   Updating the Appliance

SocialAccess provides an update channel for keeping your appliances up to date with the latest security fixes, bug fixes, and feature updates. Updates work only if you have registered each node in the cluster. For more information, see Section 3.3, "Registering SocialAccess," on page 20.

When an update is available for one or more nodes in the cluster, the SocialAccess administration console displays a flag icon in the upper right corner of the window. You can also configure the appliance to send an email notification when an update is available. When you click the flag icon, you can see the version of the pending update, instructions on how to apply the update, and the Release Notes associated with the update patch.

The flag icon for the update channel appears only if you are logged in to the administration console with an administrator account. Other consoles do not display the flag icon.

SocialAccess automatically checks the NCC channel for updates once daily at 11:23:23 p.m. and downloads any available update. You can also manually check for updates any time by clicking **Tools > Check for updates** in the administration console. You can download and install an update as soon as the flag appears in the administration console, or you can wait for SocialAccess to download the update that night, to minimize network impact due to possible size of an update. NetIQ recommends always keeping your appliance up to date. However, updates are cumulative, so if you miss an update you can just install the next one when it is available.

IMPORTANT: If you apply an update to one node, you must apply the update to all the other nodes in the cluster. Update one node at a time. Ensure that the update was successful and the node is still working properly before you begin updating the next node. Do not perform any other administrative tasks requiring an **Apply** command, and do not switch the master node, until all nodes have been successfully updated to the same version of SocialAccess.

This process allows you to run in a mixed environment while updating each node. Once you have applied all available channel updates, the flag icon goes away.

To apply an update:

1 Take a snapshot of each node in the cluster to create a backup.

2 Click the appropriate node, then click **Apply update**.

SocialAccess displays status messages during the installation of the update and the rebooting of the node.

3 After the update completes and the node restarts, click **About** on the node to verify the updated version.

4 Verify the health of the updated node and all of the nodes in the cluster. Make sure all icons are green.

For more information, see Section 13.1, "Displaying Health," on page 89.

5 Repeat Step 2 through Step 4 for each node in the cluster.

6 When you are sure all of the nodes in the cluster are working as expected, delete the snapshot.

12.5 Recovering from a Disaster

Use snapshots of the nodes to recover from a disaster. It is important to take snapshots of each node in the cluster regularly so you do not lose information.

To recover from a disaster:

1 On a regular basis, take snapshots of the nodes in the cluster.

  1a Power off the working node, then take a snapshot. NetIQ recommends this method, but it requires that you shut down and restart the node in order to take the snapshot.

    or

    Take a snapshot of the running node, ensuring that you include the virtual machine's memory. Including the memory in the snapshot requires more time and space to store the snapshot, but taking a snapshot of a running node without the memory can result in corruption.

  1b Repeat Step 1a for each node in the cluster, within a short time.

2 When a failure happens, restore the master node snapshot first.

3 Restore the other nodes in the cluster.

Use these steps only for disaster recovery. Never restore one snapshot. SocialAccess contains a database that is time-sensitive. Restoring only one node and not the others causes corruption in the appliance.

13 Troubleshooting SocialAccess

Use the information in the following sections to troubleshoot any issues you might encounter in SocialAccess.

13.1 Displaying Health

SocialAccess displays health for each node and for the cluster in the administration console. Hover the mouse over each node to display the health status of the node. If you want more details, click the node, then click **Show health.**

Show health displays the status for each component of the appliance. If the status is anything other than green (healthy), use the troubleshooting tools to determine what is wrong.

13.2 Troubleshooting Tools

SocialAccess provides troubleshooting tools if you encounter problems.

To access these tools:

1 Log in to the administration console:

   `https://`*`appliance_dns_name`*`/appliance/index.html`

2 Under **Appliances**, click the node, then click **Enter troubleshooting mode**.

3 Click the node again, then click **Troubleshooting tools**.

4 Select one or more of the troubleshooting scenarios listed.

5 Duplicate the error or condition.

6 Click **Download SocialAccess Log Files** to download the logs.

After you obtain the logs, turn off troubleshooting mode by clicking the node again and then clicking **Exit troubleshooting mode**. Leaving the logs running affects the performance of your appliance.

All of the log files in Table 13-1 are included in the download, no matter what scenario you select. The scenario that you select determines the amount of data that the log files display. Search the appropriate log file for errors while troubleshooting issues.

Table 13-1 *Troubleshooting Log Files*

Feature	Logs
Initialization or commands	`ConfigurationReplicator.log`
	`ConfigurationReplicator_RL.log`
	`messages`
	`boot*`
	`packageoperations.log`
	`ag4c_configure.out`
	`ag4c.sh.out`
Forward proxy	`access.log`
Administration console	`adminui.log`
Registration	`register.log`
Updates	`zypper.log`
	`downloadUpdate.log`
	`afterUpdate.log`
	`beforeUpdate.log`
	`rpmsAfterUpdate.log`
	`rpmsBeforeUpdate.log`
	`rpmsUpdateDiff.log`
	`300_appliance_SnapshotUconPackages.sh.log`
Custom Connectors	`catalina.out`
End User Authentication	`catalina.out`

13.3 Troubleshooting Different States

SocialAccess displays indicators for the current state of the different components. The display refreshes every five minutes. SocialAccess might not immediately display the change.

The following sections list the different components, the possible states, and troubleshooting steps to take when the state changes.

13.3.1 Front Panel of the Node

The indicator on the front panel of the node displays the health state of the node.

Figure 13-1 *Front Panel*

The states are:

Green: The node is healthy.

Yellow: The node cannot communicate with the other nodes within the five minute refresh.

Red: The node cannot communicate with the other nodes within two of the five minute refresh cycles.

Clear: The node is initializing or the state of the node is unknown.

Perform the following troubleshooting steps in the order listed if the state is anything but green:

1. Wait at least five minutes for the display to refresh and display the current state.
2. Click the node, then click **Show health**.

    Show health displays which part of the appliance is having issues.
3. If Show health displays a problem, use the troubleshooting tools to gather logs.

    For more information, see Section 13.2, "Troubleshooting Tools," on page 89.
4. Restart the appliance, then wait at least another five minute cycle for all nodes to display the current state.

13.3.2 Top of the Node

The indicator on the top of the node shows whether the **Apply** commands completed successfully.

Figure 13-2 *Top of the Node*

The states are:

Green: All **Apply** commands completed successfully.

Red: The **Apply** commands did not complete successfully.

Perform the following troubleshooting steps in the order listed if the state is red:

1. Mouse over the top of the node to see the status of the last **Apply** command made on the node.
2. If there is not enough information in the summary, click **Enter troubleshooting mode** on the node, then mouse over the node again.

The troubleshooting mode displays a details summary for the last **Apply** command made on the node.

3. Reboot the appliance, then wait at least another five minute cycle for all nodes to display the current state.

13.3.3 Identity Source

The health indicator for the identity source is the small icon in the lower left corner.

Figure 13-3 *Identity Source Indicator*

The states are:

Green: The connector to the identity source is healthy.

Yellow: The connector has communication problems with the identity source.

Red: The connector to the identity source is unhealthy or contains errors.

Question mark: The state of the connector to the identity source is unknown.

Perform the following troubleshooting steps in the order listed:

1. If the connector is green, but the SocialAccess console is not displaying users, verify that the identity source servers are running and communicating properly.

2. Use the troubleshooting tools to gather logs, then look at the identity source provisioning logs listed in Table 13-1 on page 90 for errors. The ConnectorLogs.txt file maps the display name of the connector with the log name of the connector, if there is more than one identity source connector.

3. Click **Show health** on the master node, then expand **Operational**.

   If these items are yellow or red, the interface displays helpful information to help troubleshoot the issue.

4. If you are using LDAPS to communicate with the identity source, verify the LDAP certificates are not expired. You refresh the certificates as follows:

   a. Log in to the administration console, then click **Configure** on the identity source.

   b. Click the **Refresh** icon next to the identity source server.

13.3.4   Applications

The health indicator for an application connector is the small icon in the lower left corner.

Figure 13-4   *Application Indicator*

The states are as follows:

Green: The connector to the application is healthy.

Yellow: The connector to the application contains warnings.

Red: The connector to the application contains errors or cannot communicate with the application.

Question mark: The connector to the application is in an unknown state.

Perform the following troubleshooting steps in the order listed:

1. Click **Show health** on the master node, then expand **Operational**, and check the status of **Connectors**.
2. Use the troubleshooting tools to gather logs, then look at the logs listed in for errors.
3. Make a cosmetic change to the application connector configuration, then click **Apply**.

   By forcing an **Apply**, the appliance refreshes the application connector state and this can resolve the issue.

13.3.5   Tools

The health indicator for a tool is the small icon in the lower left corner. Only tools that report health have an indicator. The Google Analytics tool does not have a health indicator.

Figure 13-5   *Tool Indicator*

For all tools, the **Question Mark** icon indicates that the tool is in an unconfigured state.

Authentication Filter: The states for the Authentication Filter tool are as follows:

- **Green circle:** The connection to the destination ExtAPI script is healthy.
- **Red circle:** The connection to the destination ExtAPI script is not working. The ExtAPI script is unreachable.

Forward Proxy: The states for the Forward Proxy tool are as follows:

- **Yellow triangle:** The connection to or through the proxy is healthy. The triangle indicator serves as a warning that use of Forward Proxy is intended only for test environments.
- **Red circle:** The connection to or through the proxy is not working. The proxy device is unreachable.

Google reCAPTCHA: The states for the Google reCAPTCHA tool are as follows:

- **Green circle:** All of the configured identity sources are valid for use with reCAPTCHA.
- **Yellow triangle:** One or more of the configured identity sources are not valid for use with reCAPTCHA. For more information, see Section 3.6.1, "Requirements for reCAPTCHA," on page 26.
- **Red circle:** None of the configured identity sources are valid for use with reCAPTCHA.

Syslog: The states for the Syslog tool are as follows:

- **Green circle:** The connection to the specified address:port is healthy.
- **Red circle:** The connection to the specified address:port is not working.

13.4 Troubleshooting Authentications

There can be multiple reasons why authentications to the SAML applications fail.

Time Synchronization: SocialAccess depends on timestamps to function correctly. Synchronize time between the VMware host, the appliance, and the workstations. Download the authentication logs. In the `catalina.out` file, search for the error `clock skew`.

SAML Authentications: Firefox contains a SAML debug add-on that you can use to view the SAML authentication between SocialAccess and the SAML applications. Download the add-on SAML tracer (https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/) to view the SAML request.

A Custom Connector Worksheets

SocialAccess provides the NetIQ Access Connector Toolkit (ACT) that allows you to create custom connectors. If you need help creating a custom connector to use with SocialAccess, Priority Support customers have the option to open a service request with NetIQ Technical Support (NTS) (http://www.netiq.com/support). NTS is available to provide toolkit support as well as to configure the connectors to work with integrated applications. Additional information from the SaaS provider is usually required.

Before you contact NetIQ Technical Support, please complete the appropriate worksheet for the connector type that you want to create. The more information that you can provide, the better and more quickly NTS can help you create the connector.

A.1 Worksheet for SAML or WS-Federation Custom Connectors

For a SAML or WS-Federation custom connector, the destination service provider for the application is the trusted partner. Each connector requires information about how they support federation for the SAML protocol or WS-Federation protocol.

Table A-1 *Worksheet for a SAML or WS-Federation Custom Connector*

☐	**Gather the following information:**
☐	Which federation specifications will be used with various trusted partners? ☐ WS-Federation ☐ SAML 2.0 ☐ SAML 1.*x*
☐	Is the metadata (SAML/WS-Federation) from the trusted partner available?
☐	What profiles will you use to federate with your partners? ☐ WS-Federation Passive Requestor profile ☐ Browser POST profile ☐ Browser Artifact profile
☐	Is encryption of the assertions required? If so, which transport security protocols and certificates will be used?
☐	What user information is required by your partner for SSO? For example: email address, CN, and so on.

❑	**Gather the following information:**
❑	What name identifier format does your partner expect?
	❑ Persistent
	❑ Transient
	❑ Email address
	❑ Unspecified
❑	What attributes are required by your partner? Does a sample assertion exist from the trusted partner?
❑	To what URL on the partner side should an assertion or a claim be sent? (Assertion Consumer Service URL)
❑	To what URL on the partner side should a logout request be sent? (Logout URL and/or Logout Response URL)
❑	Do users need to be redirected to a specific application URL after an assertion has been successfully validated? (Destination URL)
❑	What are the contact details for the trusted partner (or partners), should we need to get them involved?
❑	All information needed by the trusted partner is available via the metadata at `https://`*`appliance_dns_name`*`/osp/a/t1/auth/saml2/metadata`

A.2 Worksheet for SAML In Custom Connectors

For a SAML Inbound (SAML In) custom connector, the identity provider is the trusted partner. Each connector requires information about how they support SAML federation.

Table A-2 *Worksheet for a SAML Inbound Custom Connector*

❑	**Gather the following information:**
❑	Which federation specifications will be used with various trusted partners?
	❑ SAML 2.0
	❑ SAML 1.*x*
❑	Is the SAML metadata from the trusted partner available?
❑	What profiles will you use to federate with your partners?
	❑ Browser POST profile
	❑ Browser Artifact profile
❑	Which transport security protocols and certificates will be used? Assertions must be signed, and may be encrypted.
❑	What user information does the partner send for SSO? For example: email address, CN, and so on.

☐ **Gather the following information:**

☐ What name identifier format does your partner send with an assertion?

    ☐ Persistent

    ☐ Transient

    ☐ Email address

    ☐ Unspecified

☐ What attributes does your partner send? Does a sample assertion exist from the trusted partner?

☐ To what URL on the partner side should a logout request be sent? (Logout URL and/or Logout Response URL)

☐ What are the contact details for the trusted partner (or partners), should we need to get them involved?

☐ All information needed by the trusted partner is available via the metadata at

`https://`*`appliance_dns_name`*`/osp/a/t1/auth/saml2/metadata`

B B Open Source Licenses

B.1 Open Source Components

B.1.1   Apache 2.4.0-12

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright (c) 2001-2009, The Apache Software Foundation

B.1.2   Apache Common Codec 1.8

See Section B.2.1, "Apache 2.0 License," on page 108

Apache Commons Codec (TM) software provides implementations of common encoders and decoders such as Base64, Hex, Phonetic and URLs.

Download: (http://commons.apache.org/proper/commons-codec/archives/1.8/index.html).

B.1.3   Apache Common IO 2.4

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright 2002-2012 The Apache Software Foundation

This product includes software developed by

The Apache Software Foundation (http://www.apache.org/).

B.1.4   Apache Commons Logging 1.1.1

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright 2002-2012 The Apache Software Foundation

B.1.5   Apache Portable Runtime 1.4.2

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright (c) 2009 The Apache Software Foundation. This product includes software developed by The Apache Software Foundation (http://www.apache.org/).

Portions of this software were developed at the National Center for Supercomputing Applications (NCSA) at the University of Illinois at Urbana-Champaign.

This software contains code derived from the RSA Data Security Inc. MD5 Message-Digest Algorithm.

This software contains code derived from UNIX V7, Copyright(C) Caldera International Inc.

B.1.6   Bouncy Castle 1.5-149

See Section B.2.2, "BouncyCastle - Adaptation of the MIT X11 License," on page 111.

Copyright (c) 2000 - 2012 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

B.1.7   commons-csv 1.0

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright © 2014 The Apache Software Foundation.

B.1.8   dom4j 1.6.1

See Section B.2.3, "BSD Style License," on page 112.

Copyright 2001-2005 (C) MetaStuff, Ltd. All Rights Reserved.

B.1.9   dovecot20-backend-pgsql-2.0.20-31.1

See Section B.2.4, "MIT," on page 112 Dovcot - MIT.

See Section B.2.5, "LGPL V2.1," on page 113 Dovecot - LGPL V2.1.

Everything in src/lib/, src/auth/, src/lib-sql/ and src/lib-ntlm/ is under MIT license (see COPYING.MIT) unless otherwise mentioned at the beginning of the file.

Everything else is LGPLv2.1 (see COPYING.LGPL) unless otherwise mentioned at the beginning of the file.

Current exceptions are: src/lib/md5.c : Public Domain

AUTHORS file:

Timo Sirainen <tss@iki.fi>

Solar Designer <solar@openwall.com> (src/lib/md5.c, src/auth/passdb-pam.c)

Andrey Panin <pazke@donpac.ru> (src/auth/mech-apop.c, src/auth/mech-login.c, src/lib-ntlm/*, src/auth/mech-ntlm.c, src/auth/mech-rpa.c)

Joshua Goodall <joshua@roughtrade.net> (src/auth/mech-cram-md5.c, src/doveadm/doveadm-pw.c)

Jelmer Vernooij <jelmer@samba.org> (src/auth/mech-gssapi.c)

Vaclav Haisman <v.haisman@sh.cvut.cz> (src/lib/ioloop-kqueue.c, src/lib/ioloop-notify-kqueue.c)

Portions Copyright (c) 2008 Apple Inc. All rights reserved.

Grepping 'Patch by' from ChangeLog shows up more people.

src/lib/sha1.c and sha2.c:

Copyright (C) 1995, 1996, 1997, and 1998 WIDE Project.

Copyright (C) 2005, 2007 Olivier Gay <olivier.gay@a3.epfl.ch>

src/lib/UnicodeData.txt:

Copyright (C) 1991-2007 Unicode, Inc. All rights reserved. Distributed under the Terms of Use in http://www.unicode.org/copyright.html.

B.1.10 dovecot20-backend-mysql-2.0.20-31.1

See Section B.2.4, "MIT," on page 112 Dovcot - MIT.

See Section B.2.5, "LGPL V2.1," on page 113 Dovecot - LGPL V2.1.

See Section B.1.9, "dovecot20-backend-pgsql-2.0.20-31.1," on page 101.

B.1.11 dovecot20-backend-sqlite-2.0.20-31.1

See Section B.2.4, "MIT," on page 112 Dovcot - MIT.

See Section B.2.5, "LGPL V2.1," on page 113 Dovecot - LGPL V2.1.

See Section B.1.9, "dovecot20-backend-pgsql-2.0.20-31.1," on page 101.

B.1.12 dovecot20-2.0.20-31.1

See Section B.2.4, "MIT," on page 112 Dovcot - MIT.

See Section B.2.5, "LGPL V2.1," on page 113 Dovecot - LGPL V2.1.

See Section B.1.9, "dovecot20-backend-pgsql-2.0.20-31.1," on page 101.

B.1.13 dovecot20-devel-2.0.20-31.1

See Section B.2.4, "MIT," on page 112 Dovcot - Mit.

See Section B.2.5, "LGPL V2.1," on page 113 Dovecot - Lgpl V2.1.

See Section B.1.9, "dovecot20-backend-pgsql-2.0.20-31.1," on page 101.

B.1.14 GTM-OAuth2 v2

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright (c) 2011 Google Inc.

B.1.15   GWT 2.4.0

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright (c) Google, Inc. 2009. All rights reserved. All other product, service names, brands, or trademarks, are the property of their respective owners.

B.1.16   GWT Mosaic 0.4.0-rc4

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright (c) Google, Inc. 2009. All rights reserved. All other product, service names, brands, or trademarks, are the property of their respective owners.

B.1.17   gwtupload 0.6

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright 2009 Manolo Carrasco (Manuel Carrasco MoÃ±ino)

B.1.18   Hibernate 3

See Section B.2.5, "LGPL V2.1," on page 113.

Copyright © 2007 by Red Hat, Inc. This copyrighted material is made available to anyone wishing to use, modify, copy, or redistribute it subject to the terms and conditions of the GNU Lesser General Public License, as published by the Free Software Foundation.

B.1.19   httpclient 4.1.2

See Section B.2.1, "Apache 2.0 License," on page 108.

Apache HttpComponents Client Copyright 1999-2009 The Apache Software Foundation. This product includes software developed by The Apache Software Foundation (http://www.apache.org/).

This project contains annotations derived from JCIP-ANNOTATIONS

Copyright (c) 2005 Brian Goetz and Tim Peierls. See http://www.jcip.net

Apache HttpComponents Core – HttpCore

Copyright 2006-2009 The Apache Software Foundation

This product includes software developed by The Apache Software Foundation (http://www.apache.org /).

B.1.20   JavaMail 1.4.3

See Section B.2.6, "Javamail," on page 119.

Copyright © 2009 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc.

B.1.21 JavaService 2.0.10

See Section B.2.7, "JavaService," on page 124.

See Section B.2.5, "LGPL V2.1," on page 113.

Copyright owner John Rutter

B.1.22 Jaxb 2.2

See Section B.2.8, "COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0," on page 125.

See Section B.2.9, "GPL V2 + classpath exception dual license.," on page 130.

Copyright © 2010, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

B.1.23 jersey 1.17

See Section B.2.8, "COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0," on page 125.

See Section B.2.9, "GPL V2 + classpath exception dual license.," on page 130.

Copyright © 2010, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

B.1.24 jQuery 1.8

See Section B.2.4, "MIT," on page 112.

Copyright 2014 jQuery Foundation and other contributors

https://jquery.org/license

B.1.25 jQuery SmartBanner

See Section B.2.4, "MIT," on page 112.

Copyright (c) Arnold Daniels <arnold@jasny.net>

B.1.26 jtds 1.3.1

See Section B.2.12, "GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999," on page 138.

B.1.27 KKPasscodeLock 0.2.2

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright 2011 Adar Porat

B.1.28   libvmtools 9.2.3-113-1

See Section B.2.12, "GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999," on page 138.

See Section B.2.13, "GNU GENERAL PUBLIC LICENSE Version 2," on page 145.

See Section B.1.33, "Open-vm-tools 9.2.3-113.1," on page 105.

B.1.29   log4j 1.2.15

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright (c) The Apache Software Foundation

B.1.30   OpenInChromeController

See Section B.2.14, "OpenInChromeController," on page 149.

BSD Style License (OpenInChrome)

Copyright 2013, Google Inc. All rights reserved.

B.1.31   OpenSAML 2.0

See Section B.2.1, "Apache 2.0 License," on page 108.

We wish to acknowledge the following copyrighted works that make up portions of this software:

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/).

This project uses libraries covered by the Lesser GNU Public License. Source code for these libraries is available on request.

B.1.32   OpenSSL 1.0.1i

See Section B.2.11, "OpenSSL License and SSLeay License," on page 136.

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Copyright (c) 1995-1998 Eric Young (eay@cryptsoft.com) * All rights reserved.

B.1.33   Open-vm-tools 9.2.3-113.1

See Section B.2.12, "GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999," on page 138.

See Section B.2.13, "GNU GENERAL PUBLIC LICENSE Version 2," on page 145.

Copyright (C) 2009 VMware, Inc. All rights reserved.

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation version 2 and no later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

B.1.34 Recaptcha4j 0.0.8

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright 2007 Soren Davidsen, Taneshare Networks.

B.1.35 snmp4j

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright unknown/unpublished

B.1.36 Tomcat 7.0.27-10.2

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright 1999-2012 The Apache Software Foundation

This product includes software developed by The Apache Software Foundation (http://www.apache.org/).

The Windows Installer is built with the Nullsoft Scriptable Install System (NSIS), which is open source software. The original software and related information is available at http://nsis.sourceforge.net.

Java compilation software for JSP pages is provided by Eclipse, which is open source software. The original software and related information is available at http://www.eclipse.org.

For the bayeux implementation

The org.apache.cometd.bayeux API is derivative work originating at the Dojo Foundation

* Copyright 2007-2008 Guy Molinari

* Copyright 2007-2008 Filip Hanik

* Copyright 2007 Dojo Foundation

* Copyright 2007 Mort Bay Consulting Pty. Ltd.

B.1.37 WSS4J 1.4.2

See Section B.2.1, "Apache 2.0 License," on page 108.

Apache WebServices – WSS4J Copyright © 2004-2009 The Apache Software Foundation

This product includes software developed by The Apache Software Foundation (http://www.apache.org/).

This product includes software Copyright University of Southampton IT Innovation Centre, 2006 (http://www.it-innovation.soton.ac.uk).

B.1.38   Xalan 2.7.1

See Section B.2.1, "Apache 2.0 License," on page 108.

This product includes software developed by The Apache Software Foundation (http://www.apache.org/).

Portions of this software was originally based on the following: software copyright (c) 1999-2002, Lotus Development Corporation., http://www.lotus.com.

software copyright (c) 2001-2002, Sun Microsystems., http://www.sun.com.

software copyright (c) 2003, IBM Corporation., http://www.ibm.com

Voluntary contributions made by Ovidiu Predescu (ovidiu@cup.hp.com) on behalf of the Apache Software Foundation and was originally developed at Hewlett Packard Company.

B.1.39   Xerces 2.9.1

See Section B.2.1, "Apache 2.0 License," on page 108.

This product includes software developed by The Apache Software Foundation (http://www.apache.org/).

Apache Xalan (Xalan serializer) Copyright 1999-2006 The Apache Software Foundation Apache XML Commons Resolver Copyright 2006 The Apache Software Foundation. Portions of this software was originally based on the following:

software copyright (c) 1999-2002, Lotus Development Corporation., http://www.lotus.com.

software copyright (c) 2001-2002, Sun Microsystems., http://www.sun.com.

software copyright (c) 2003, IBM Corporation., http://www.ibm.comVoluntary contributions made by Ovidiu Predescu (ovidiu@cup.hp.com) on behalf of the Apache Software Foundation and was originally developed at Hewlett Packard Company.

B.1.40   XMLSec 1.4.6

See Section B.2.1, "Apache 2.0 License," on page 108.

Copyright (c) 2002 Aleksey Sanin. All Rights Reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions.

B.1.41   Zlib 1.2.3

See Section B.2.15, "Zlib 1.2.3," on page 150.

Copyright (c) 1995-2005 Jean-loup Gailly and Mark Adler

B.1.42 Zxing 2.3.0

See

Barcode4J

Copyright 2002-2010 Jeremias Märki

Copyright 2005-2006 Dietmar Bürkle

Portions of this software were contributed under section 5 of the Apache License. Contributors are listed under: http://barcode4j.sourceforge.net/contributors.html

B.2 Open Source Licenses

B.2.1 Apache 2.0 License

The Apache 2.0 license is available at http://www.apache.org/licenses (http://www.apache.org/licenses/LICENSE-2.0.txt).

Apache License

Version 2.0, January 2004

https://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including across-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

   a. You must give any other recipients of the Work or Derivative Works a copy of this License; and

   b. You must cause any modified files to carry prominent notices stating that You changed the files; and

   c. You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

   d. If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

   You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in

accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

B.2.2   BouncyCastle - Adaptation of the MIT X11 License

The BouncyCastle license is available at http://www.bouncycastle.org/license.html (http://www.bouncycastle.org/licence.html).

Please note: our license is an adaptation of the MIT X11 License and should be read as such.

LICENSE

Copyright (c) 2000 - 2012 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies LICof the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

B.2.3 BSD Style License

The BSD style license is available at http://dom4j.sourceforge.net/dom4j-1.6.1/license.html (http://dom4j.sourceforge.net/dom4j-1.6.1/license.html).

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.The name "DOM4J" must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact dom4j-info@metastuff.com.Products derived from this Software may not be called "DOM4J" nor may "DOM4J" appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.Due credit should be given to the DOM4J Project - http://dom4j.sourceforge.netTHIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL METASTUFF, LTD. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 2001-2005 (C) MetaStuff, Ltd. All Rights Reserved.

B.2.4 MIT

The MIT license is available at http://www.dovecot.org/doc/COPYING.MIT (http://www.dovecot.org/doc/COPYING.MIT).

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

B.2.5   LGPL V2.1

The LGPL V2.1 license is available at http://www.dovecot.org/doc/COPYING.LGPL (http://www.dovecot.org/doc/COPYING.LGPL).

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output fromsuch a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- ◆ a. The modified work must itself be a software library.
- ◆ b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- ◆ c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- ◆ d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

  (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- ◆ a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

- c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

- d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

- e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

- b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from

the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

- <one line to give the library's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

- This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

- This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

- You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

- Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

- <signature of Ty Coon>, 1 April 1990 Ty Coon, President of Vice

That's all there is to it!

B.2.6 Javamail

Sun Microsystems, Inc. ("Sun") ENTITLEMENT for SOFTWARE

Licensee/Company: Entity receiving Software.

Effective Date: Date of delivery of the Software to You.

Software: JavaMail 1.4.3

License Term: Perpetual (subject to termination under the SLA).

Licensed Unit: Software Copy.

Licensed unit Count: Unlimited.

Permitted Uses:

1. You may reproduce and use the Software for Your own Individual, Commercial and Research and Instructional Use only for the purposes of designing, developing, testing, and running Your applets and applications ("Programs").

2. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software's documentation, You may reproduce and distribute portions of Software identified as a redistributable in the documentation (each a "Redistributable"), provided that You comply with the following (note that You may be entitled to reproduce and distribute other portions of the Software not defined in the documentation as a Redistributable under certain other licenses as described in the THIRDPARTYLICENSEREADME, if applicable):

   a. You distribute Redistributable complete and unmodified and only bundled as part of Your Programs,

   b. Your Programs add significant and primary functionality to the Redistributable,

   c. You distribute Redistributable for the sole purpose of running Your Programs,

   d. You do not distribute additional software intended to replace any component(s) of the Redistributable,

   e. You do not remove or alter any proprietary legends or notices contained in or on the Redistributable.

   f. You only distribute the Redistributable subject to a license agreement that protects Sun's interests consistent with the terms contained in this Agreement, and

   g. You agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys' fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Redistributable.

3. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize Your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as "java", "javax", "sun" or similar convention as specified by Sun in any naming convention designation.

4. No Diagnostic, Maintenance, Repair or Technical Support Services. The scope of Your license does not include any right, express or implied, (i) to access, copy, distribute, display or use the Software to provide diagnostic, maintenance, repair or technical support services for Sun softwa re or Sun hardware on behalf of any third party for Your direct or indirect commercial gain or advantage, without Sun's prior written authorization, or (ii) for any third party to access, copy, distribute, display or use the Software to provide diagnostic, maintenance, repair or technical support services for Sun software or Sun hardware on Your behalf for such party's direct or indirect commercial gain or advantage, without Sun's prior written authorization. The limitations set forth in this paragraph apply to any and all error corrections, patches, updates, and upgrades to the Software You may receive, access, download or otherwise obtain from Sun.

5. Records and Documentation. During the term of the SLA and Entitlement, and for a period of three (3) years thereafter, You agree to keep proper records and documentation of Your compliance with the SLA and Entitlement. Upon Sun's reasonable request, You will provide copies of such records and documentation to Sun for the purpose of confirming Your compliance with the terms and conditions of the SLA and Entitlement. This section will survive any termination of the SLA and Entitlement. You may terminate this SLA and Entitlement at any time by destroying all copies of the Software in which case the obligations set forth in Section 7 of the SLA shall apply.

Sun Microsystems, Inc. ("Sun")

SOFTWARE LICENSE AGREEMENT

READ THE TERMS OF THIS AGREEMENT ("AGREEMENT") CAREFULLY BEFORE OPENING SOFTWARE MEDIA PACKAGE. BY OPENING SOFTWARE MEDIA PACKAGE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE "DECLINE" (OR "EXIT") BUTTON AT THE END OF THIS AGREEMENT. IF YOU HAVE SEPARATELY AGREED TO LICENSE TERMS ("MASTER TERMS") FOR YOUR LICENSE TO THIS SOFTWARE, THEN SECTIONS 1-6 OF THIS AGREEMENT ("SUPPLEMENTAL LICENSE TERMS") SHALL SUPPLEMENT AND SUPERSEDE THE MASTER TERMS IN RELATION TO THIS SOFTWARE.

1. Definitions.

   a. "Entitlement" means the collective set of applicable documents authorized by Sun evidencing your obligation to pay associated fees (if any) for the license, associated Services, and the authorized scope of use of Software under this Agreement.

   b. "Licensed Unit" means the unit of measure by which your use of Software and/or Service is licensed, as described in your Entitlement.

   c. "Permitted Use" means the licensed Software use(s) authorized in this Agreement as specified in your Entitlement. The Permitted Use for any bundled Sun software not specified in your Entitlement will be evaluation use as provided in Section 3.

   d. "Service" means the service(s) that Sun or its delegate will provide, if any, as selected in your Entitlement and as further described in the applicable service listings at www.sun.com/service/servicelist.

   e. "Software" means the Sun software described in your Entitlement. Also, certain software may be included for evaluation use under Section 3.

   f. "You" and "Your" means the individual or legal entity specified in the Entitlement, or for evaluation purposes, the entity performing the evaluation.

2. License Grant and Entitlement.

   Subject to the terms of your Entitlement, Sun grants you a nonexclusive, nontransferable limited license to use Software for its Permitted Use for the license term. Your Entitlement will specify (a) Software licensed, (b) the Permitted Use, (c) the license term, and (d) the Licensed Units.

   Additionally, if your Entitlement includes Services, then it will also specify the (e) Service and (f) service term.

   If your rights to Software or Services are limited in duration and the date such rights begin is other than the purchase date, your Entitlement will provide that beginning date(s).

   The Entitlement may be delivered to you in various ways depending on the manner in which you obtain Software and Services, for example, the Entitlement may be provided in your receipt, invoice or your contract with Sun or authorized Sun reseller. It may also be in electronic format if you download Software.

3. Permitted Use.

As selected in your Entitlement, one or more of the following Permitted Uses will apply to your use of Software. Unless you have an Entitlement that expressly permits it, you may not use Software for any of the other Permitted Uses. If you don't have an Entitlement, or if your Entitlement doesn't cover additional software delivered to you, then such software is for your Evaluation Use.

a. Evaluation Use. You may evaluate Software internally for a period of 90 days from your first use.

b. Research and Instructional Use. You may use Software internally to design, develop and test, and also to provide instruction on such uses.

c. Individual Use. You may use Software internally for personal, individual use.

d. Commercial Use. You may use Software internally for your own commercial purposes.

e. Service Provider Use. You may make Software functionality accessible (but not by providing Software itself or through outsourcing services) to your end users in an extranet deployment, but not to your affiliated companies or to government agencies.

4. Licensed Units.

Your Permitted Use is limited to the number of Licensed Units stated in your Entitlement. If you require additional Licensed Units, you will need additional Entitlement(s).

5. Restrictions.

(a) The copies of Software provided to you under this Agreement are licensed, not sold, to you by Sun. Sun reserves all rights not expressly granted. (b) You may make a single archival copy of Software, but otherwise may not copy, modify, or distribute Software. However if the Sun documentation accompanying Software lists specific portions of Software, such as header files, class libraries, reference source code, and/or redistributable files, that may be handled differently, you may do so only as provided in the Sun documentation. (c) You may not rent, lease, lend or encumber Software. (d) Unless enforcement is prohibited by applicable law, you may not decompile, or reverse engineer Software. (e) The terms and conditions of this Agreement will apply to any Software updates, provided to you at Sun's discretion, that replace and/or supplement the original Software, unless such update contains a separate license. (f) You may not publish or provide the results of any benchmark or comparison tests run on Software to any third party without the prior written consent of Sun. (g) Software is confidential and copyrighted. (h) Unless otherwise specified, if Software is delivered with embedded or bundled software that enables functionality of Software, you may not use such software on a stand-alone basis or use any portion of such software to interoperate with any program(s) other than Software. (i) Software may contain programs that perform automated collection of system data and/or automated software updating services. System data collected through such programs may be used by Sun, its subcontractors, and its service delivery partners for the purpose of providing you with remote system services and/or improving Sun's software and systems. (j) Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility and Sun and its licensors disclaim any express or implied warranty of fitness for such uses. (k) No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement.

6. Java Compatibility and Open Source.

Software may contain Java technology. You may not create additional classes to, or modifications of, the Java technology, except under compatibility requirements available under a separate agreement available at www.java.net.

Sun supports and benefits from the global community of open source developers, and thanks the community for its important contributions and open standards-based technology, which Sun has adopted into many of its products.

Please note that portions of Software may be provided with notices and open source licenses from such communities and third parties that govern the use of those portions, and any licenses granted hereunder do not alter any rights and obligations you may have under such open source licenses, however, the disclaimer of warranty and limitation of liability provisions in this Agreement will apply to all Software in this distribution.

7. Term and Termination.

   The license and service term are set forth in your Entitlement(s). Your rights under this Agreement will terminate immediately without notice from Sun if you materially breach it or take any action in derogation of Sun's and/or its licensors' rights to Software. Sun may terminate this Agreement should any Software become, or in Sun's reasonable opinion likely to become, the subject of a claim of intellectual property infringement or trade secret misappropriation. Upon termination, you will cease use of, and destroy, Software and confirm compliance in writing to Sun. Sections 1, 5, 6, 7, and 9-15 will survive termination of the Agreement.

8. Limited Warranty.

   Sun warrants to you that for a period of 90 days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Some states do not allow limitations on certain implied warranties, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

9. Disclaimer of Warranty.

   UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

10. Limitation of Liability.

    TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement. The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

11. Export Regulations.

    All Software, documents, technical data, and any other materials delivered under this Agreement are subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws and regulations and acknowledge that you have the responsibility to obtain any licenses to export, re-export, or import as may be required after delivery to you.

12. U.S. Government Restricted Rights.

    If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

13. Governing Law.

Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

14. Severability.

If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

15. Integration.

This Agreement, including any terms contained in your Entitlement, is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.

Please contact Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054 if you have questions.

B.2.7 JavaService

This software is currently covered by two open source licenses:

```
/*
 * JavaService - Windows NT Service Daemon for Java applications
 *
 * Copyright (C) 2004 Multiplan Consultants Ltd.
 *
 *
 * This library is free software; you can redistribute it and/or
 * modify it under the terms of the GNU Lesser General Public
 * License as published by the Free Software Foundation; either
 * version 2.1 of the License, or (at your option) any later version.
 *
 * This library is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the GNU
 * Lesser General Public License for more details.
 *
 * You should have received a copy of the GNU Lesser General Public
 * License along with this library; if not, write to the Free Software
 * Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307  USA
 *
 *
 * Information about the JavaService software is available at the ObjectWeb
 * web site. Refer to http://javaservice.objectweb.org for more details.
 *
 *
 * This software is derived from earlier work by Alexandria Software Consulting,
 * (no longer contactable) which was released under a BSD-style license in 2001.
 * The text of that original license is reproduced below for reference.
 *
 */
```

```
/*
 *
 * JavaService - License
 *
 * By downloading and/or using this software you agree to abide by the following
license:
 *
 * Copyright (c) 2000, Alexandria Software Consulting
 *
 * All rights reserved. Redistribution and use in source and binary forms, with or
without
 * modification, are permitted provided that the following conditions are met:
 *
 * Redistributions of source code must retain the above copyright notice, this list
of
 * conditions, and the following disclaimer.
 * Neither name of Alexandria Software Consulting nor the names of the contributors
may be
 * used to endorse or promote products derived from this software without specific
prior
 * written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND
ANY
 * EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED
WARRANTIES
 * OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO
EVENT
 * SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT,
 * INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED
 * TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
OR
 * BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN
 * CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING
IN ANY
 * WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH
DAMAGE.
 */
```

B.2.8 COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0

The CDDL license is available at http://glassfish.java.net/public/CDDL+GPL.html (http://glassfish.java.net/public/CDDL+GPL.html).

1. Definitions.

1.1. "Contributor" means each individual or entity that creates or contributes to the creation of Modifications.

1.2. "Contributor Version" means the combination of the Original Software, prior Modifications used by a Contributor (if any), and the Modifications made by that particular Contributor.

1.3. "Covered Software" means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original Software with files containing Modifications, in each case including portions thereof.

1.4. "Executable" means the Covered Software in any form other than Source Code.

1.5. "Initial Developer" means the individual or entity that first makes Original Software available under this License.

1.6. "Larger Work" means a work which combines Covered Software or portions thereof with code not governed by the terms of this License.

1.7. "License" means this document.

1.8. "Licensable" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "Modifications" means the Source Code and Executable form of any of the following:

- ◆ A. Any file that results from an addition to, deletion from or modification of the contents of a file containing Original Software or previous Modifications;
- ◆ B. Any new file that contains any part of the Original Software or previous Modification; or
- ◆ C. Any new file that is contributed or otherwise made available under the terms of this License.

1.10. "Original Software" means the Source Code and Executable form of computer software code that is originally released under this License.

1.11. "Patent Claims" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.12. "Source Code" means (a) the common form of computer software code in which modifications are made and (b) associated documentation included in or with such code.

1.13. "You" (or "Your") means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50%) of the outstanding shares or beneficial ownership of such entity.

2. License Grants.

2.1. The Initial Developer Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, the Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license:

- ◆ (a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer, to use, reproduce, modify, display, perform, sublicense and distribute the Original Software (or portions thereof), with or without Modifications, and/or as part of a Larger Work; and
- ◆ (b) under Patent Claims infringed by the making, using or selling of Original Software, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Software (or portions thereof).
- ◆ (c) The licenses granted in Sections 2.1(a) and (b) are effective on the date Initial Developer first distributes or otherwise makes the Original Software available to a third party under the terms of this License.
- ◆ (d) Notwithstanding Section 2.1(b) above, no patent license is granted: (1) for code that You delete from the Original Software, or (2) for infringements caused by: (i) the modification of the Original Software, or (ii) the combination of the Original Software with other software or devices.

2.2 Contributor Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

- ◆ (a) under intellectual property rights (other than patent or trademark) Licensable by Contributor to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof), either on an unmodified basis, with other Modifications, as Covered Software and/or as part of a Larger Work; and

- ◆ (b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: (1) Modifications made by that Contributor (or portions thereof); and (2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

- ◆ (c) The licenses granted in Sections 2.2(a) and 2.2(b) are effective on the date Contributor first distributes or otherwise makes the Modifications available to a third party.

- ◆ (d) Notwithstanding Section 2.2(b) above, no patent license is granted: (1) for any code that Contributor has deleted from the Contributor Version; (2) for infringements caused by: (i) third party modifications of Contributor Version, or (ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or (3) under Patent Claims infringed by Covered Software in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Availability of Source Code.

Any Covered Software that You distribute or otherwise make available in Executable form must also be made available in Source Code form and that Source Code form must be distributed only under the terms of this License. You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available. You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

3.2. Modifications.

The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

3.3. Required Notices.

You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

3.4. Application of Additional Terms.

You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients' rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, you may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty,

support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.5. Distribution of Executable Versions.

You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable form does not attempt to limit or alter the recipient's rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form under a different license, You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.6. Larger Works.

You may create a Larger Work by combining Covered Software with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Software.

4. Versions of the License.

4.1. New Versions.

Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

4.2. Effect of New Versions.

You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any subsequent version of the License, You must distribute and make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

4.3. Modified Versions.

When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

5. DISCLAIMER OF WARRANTY.

COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY

NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

6. TERMINATION.

6.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

6.2. If You assert a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You assert such claim is referred to as "Participant") alleging that the Participant Software (meaning the Contributor Version where the Participant is a Contributor or the Original Software where the Participant is the Initial Developer) directly or indirectly infringes any patent, then any and all rights granted directly or indirectly to You by such Participant, the Initial Developer (if the Initial Developer is not the Participant) and all Contributors under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively and automatically at the expiration of such 60 day notice period, unless if within such 60 day period You withdraw Your claim with respect to the Participant Software against such Participant either unilaterally or pursuant to a written agreement with Participant.

6.3. In the event of termination under Sections 6.1 or 6.2 above, all end user licenses that have been validly granted by You or any distributor hereunder prior to termination (excluding licenses granted to You by any distributor) shall survive termination.

7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED SOFTWARE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

8. U.S. GOVERNMENT END USERS.

The Covered Software is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" (as that term is defined at 48 C.F.R. § 252.227-7014(a)(1)) and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Software with only those rights set forth herein. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFAR, or other clause or provision that addresses Government rights in computer software under this License.

9. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by the law of the jurisdiction specified in a notice contained within the Original Software (except to the extent applicable law, if any, provides otherwise), excluding such jurisdiction's conflict-of-law provisions. Any litigation relating to this License shall be subject to the jurisdiction of the courts located in the jurisdiction and venue specified in a notice contained within the Original Software, with the losing party responsible for costs, including, without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License. You agree that You alone are responsible for compliance with the United States export administration regulations (and the export control laws and regulation of any other countries) when You use, distribute or otherwise make available any Covered Software.

10. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

NOTICE PURSUANT TO SECTION 9 OF THE COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL)

The code released under the CDDL shall be governed by the laws of the State of California (excluding conflict-of-law provisions). Any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California and the state courts of the State of California, with venue lying in Santa Clara County, California.

B.2.9 GPL V2 + classpath exception dual license.

This license is available here http://glassfish.java.net/public/CDDL+GPL.html (http://glassfish.java.net/public/CDDL+GPL.html).

The GNU General Public License (GPL) Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

   b. You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

   c. If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there

is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a. Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b. Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c. Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

   If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

One line to give the program's name and a brief idea of what it does.

Copyright (C)

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

"CLASSPATH" EXCEPTION TO THE GPL VERSION 2

Certain source files distributed by Sun Microsystems, Inc. are subject to the following clarification and special exception to the GPL Version 2, but only where Sun has expressly included in the particular source file's header the words "Sun designates this particular file as subject to the "Classpath" exception as provided by Sun in the License file that accompanied this code."

Linking this library statically or dynamically with other modules is making a combined work based on this library. Thus, the terms and conditions of the GNU General Public License Version 2 cover the whole combination.

As a special exception, the copyright holders of this library give you permission to link this library with independent modules to produce an executable, regardless of the license terms of these independent modules, and to copy and distribute the resulting executable under terms of your choice, provided that you also meet, for each linked independent module, the terms and conditions of the license of that module.? An independent module is a module which is not derived from or based on this library.? If you modify this library, you may extend this exception to your version of the library, but you are not obligated to do so.? If you do not wish to do so, delete this exception statement from your version.

Terms of Use; Privacy Policy; Copyright ©2008-2012 (revision 20121116.2af7adc)

B.2.10   Microsoft Public License MS-PL

Microsoft Public License MS-PL

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

   The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law.

   A "contribution" is the original software, or any additions or changes to the software.

   A "contributor" is any person that distributes its contribution under this license.

   "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

    a. Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

    b. Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

    a. No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

    b. If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

    c. If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

    d. If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

    e. The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

B.2.11   OpenSSL License and SSLeay License

```
LICENSE ISSUES
  ==============

  The OpenSSL toolkit stays under a dual license, i.e. both the conditions of
  the OpenSSL License and the original SSLeay license apply to the toolkit.
  See below for the actual license texts. Actually both licenses are BSD-style
  Open Source licenses. In case of any license issues related to OpenSSL
  please contact openssl-core@openssl.org.

  OpenSSL License
  ---------------

/* ====================================================================
 * Copyright (c) 1998-2008 The OpenSSL Project.  All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * 1. Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in
 *    the documentation and/or other materials provided with the
 *    distribution.
 *
```

```
 * 3. All advertising materials mentioning features or use of this
 *    software must display the following acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
 *
 * 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
 *    endorse or promote products derived from this software without
 *    prior written permission. For written permission, please contact
 *    openssl-core@openssl.org.
 *
 * 5. Products derived from this software may not be called "OpenSSL"
 *    nor may "OpenSSL" appear in their names without prior written
 *    permission of the OpenSSL Project.
 *
 * 6. Redistributions of any form whatsoever must retain the following
 *    acknowledgment:
 *    "This product includes software developed by the OpenSSL Project
 *    for use in the OpenSSL Toolkit (http://www.openssl.org/)"
 *
 * THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
 * EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED.  IN NO EVENT SHALL THE OpenSSL PROJECT OR
 * ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
 * SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
 * NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
 * LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
 * STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
 * ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
 * OF THE POSSIBILITY OF SUCH DAMAGE.
 * ====================================================================
 *
 * This product includes cryptographic software written by Eric Young
 * (eay@cryptsoft.com).  This product includes software written by Tim
 * Hudson (tjh@cryptsoft.com).
 *
 */

Original SSLeay License
-----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
 * All rights reserved.
 *
 * This package is an SSL implementation written
 * by Eric Young (eay@cryptsoft.com).
 * The implementation was written so as to conform with Netscapes SSL.
 *
 * This library is free for commercial and non-commercial use as long as
 * the following conditions are aheared to.  The following conditions
 * apply to all code found in this distribution, be it the RC4, RSA,
 * lhash, DES, etc., code; not just the SSL code.  The SSL documentation
 * included with this distribution is covered by the same copyright terms
 * except that the holder is Tim Hudson (tjh@cryptsoft.com).
 *
 * Copyright remains Eric Young's, and as such any Copyright notices in
 * the code are not to be removed.
 * If this package is used in a product, Eric Young should be given attribution
 * as the author of the parts of the library used.
 * This can be in the form of a textual message at program startup or
 * in documentation (online or textual) provided with the package.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 * 1. Redistributions of source code must retain the copyright
 *    notice, this list of conditions and the following disclaimer.
 * 2. Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
```

```
 *     documentation and/or other materials provided with the distribution.
 * 3. All advertising materials mentioning features or use of this software
 *    must display the following acknowledgement:
 *    "This product includes cryptographic software written by
 *     Eric Young (eay@cryptsoft.com)"
 *    The word 'cryptographic' can be left out if the rouines from the library
 *    being used are not cryptographic related :-).
 * 4. If you include any Windows specific code (or a derivative thereof) from
 *    the apps directory (application code) you must include an acknowledgement:
 *    "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"
 *
 * THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
 * ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
 * IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
 * ARE DISCLAIMED.  IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
 * FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
 * DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
 * OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
 * HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
 * LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
 * OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
 * SUCH DAMAGE.
 *
 * The licence and distribution terms for any publically available version or
 * derivative of this code cannot be changed.  i.e. this code cannot simply be
 * copied and put under another distribution licence
 * [including the GNU Public Licence.]
 */
```

B.2.12   GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- (a) The modified work must itself be a software library.
- (b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
- (c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
- (d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

  (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work

based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

- ◆ a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

- ◆ b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

- ◆ c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

- ◆ d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

- ◆ e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

- ◆ a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

- ◆ b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

- <one line to give the library's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

- This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

- This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

- You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

- ◆ Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker

- ◆ <signature of Ty Coon>, 1 April 1990 Ty Coon, President of Vice

That's all there is to it!

B.2.13   GNU GENERAL PUBLIC LICENSE Version 2

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

- a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

- b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

- c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

- ◆ a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- ◆ b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

- ◆ c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. HE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

- <one line to give the program's name and a brief idea of what it does.> Copyright (C) <year> <name of author>

- This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

- This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

- You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

- Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

- Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

- <signature of Ty Coon>, 1 April 1989 Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

B.2.14   OpenInChromeController

BSD Style License (OpenInChrome)

Copyright 2013, Google Inc. All rights reserved.

The license is available at https://github.com/GoogleChrome/OpenInChrome/blob/master/LICENSE.txt (https://github.com/GoogleChrome/OpenInChrome/blob/master/LICENSE.txt)

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of Google Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

B.2.15   Zlib 1.2.3

Zlib license

Copyright (c) 1995-2005 Jean-loup Gailly and Mark Adler

The Zlib license is available at http://www.zlib.net/zlib_license.html (http://www.zlib.net/zlib_license.html)

/* zlib.h -- interface of the 'zlib' general purpose compression library version 1.2.8, April 28th, 2013

Copyright (C) 1995-2013 Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly   Mark Adler

jloup@gzip.org   madler@alumni.caltech.edu

*/

B.3 Obtaining a Copy of the Media

The chapter lists the Open Source material contained in this release and the full text of the open source license that applies to each. NetIQ offers to provide a DVD containing the source code for each open source component included in this product governed by GPL, LGPL and CDDL licenses. The request for the source code should be addressed to: Legal Department, NetIQ Corporation., 515 Post Oak Boulevard, Suite 1200, Houston, TX 77027 USA. With the request, please include the name of the product and the version of the product. There is a charge of $10.00 USD for each request to cover cost of media and shipping.