NetIQ® CloudAccess and MobileAccess

Installation and Configuration Guide

September 2014

Legal Notice

About this Book and the Library

The *Installation and Configuration Guide* provides conceptual information about the NetIQ CloudAccess (CloudAccess) and NetIQ MobileAccess (MobileAccess) products. This book contains configuration information for the appliance and for the SaaS applications.

NOTE: Many of the topics in this guide are applicable to both CloudAccess and MobileAccess users. However, certain features of the CloudAccess product are not included with the MobileAccess license. Those product features that are visible to MobileAccess users, but are licensed only to CloudAccess users, are clearly marked in this guide.

Intended Audience

This book provides information for individuals responsible for deploying and configuring the appliance and configuring application connectors.

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, as well as definitions for fields in windows of the administration console.

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.

Contents

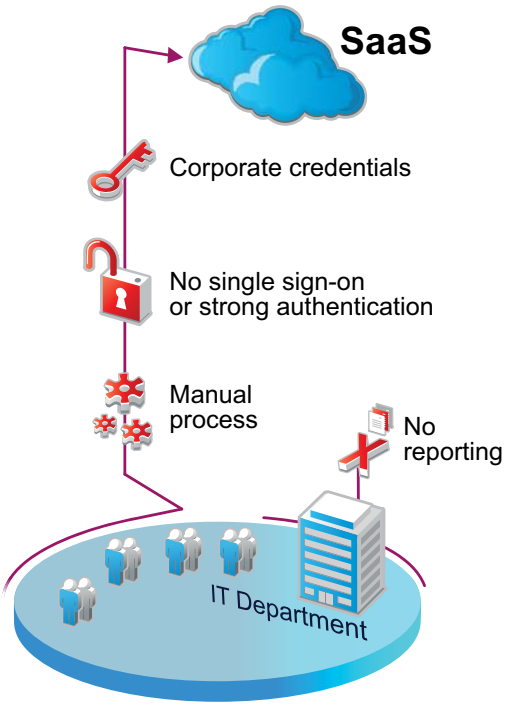
1 Overview of NetIQ CloudAccess

CloudAccess is a virtual appliance that enables you to provide secure access to Software-as-a-Service (SaaS) applications for your corporate users.

1.1 Inherent Problems Using SaaS Applications

Many corporate users want to use SaaS applications to increase business agility. If the corporation does not provide an easy way for users to obtain accounts for SaaS applications, several problems can occur. Figure 1-1 depicts some of these problems.

Figure 1-1 *Problems with Using SaaS Applications in the Corporation*



Common problems include the following:

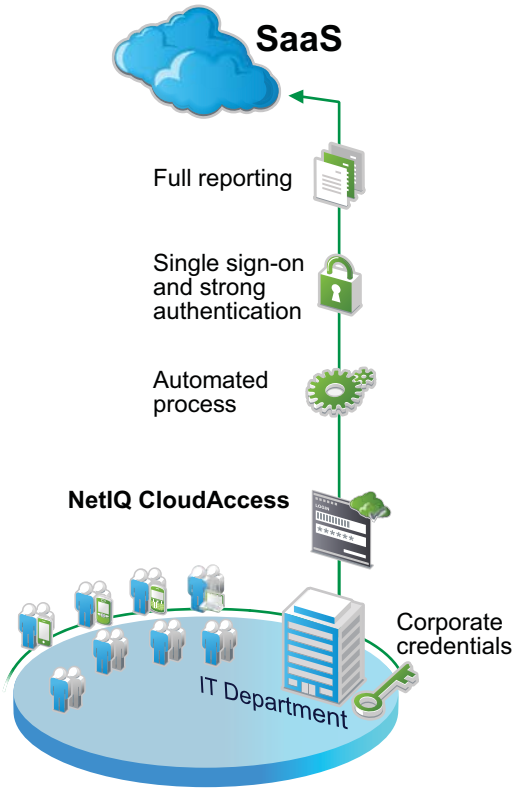
- Users bypass the IT department and create their own accounts in the SaaS application.

- Users must wait for the IT department to create accounts in the SaaS application. It is a manual process, whether the IT department creates the account or the user creates the account.
- Users must remember separate passwords for each SaaS application, and often use their corporate credentials.
- Administrators receive no compliance reports of user activity in the SaaS application.

1.2 The Solution That CloudAccess Provides

CloudAccess provides a simple, secure solution to the problems presented with using SaaS applications.

Figure 1-2 *CloudAccess Solution*



CloudAccess provides the following benefits:

- An automated process to provision user accounts to the SaaS applications
- Secure single sign-on to the SaaS applications without corporate credentials leaving the security realm
- The ability for users to securely access SaaS applications inside or outside of the corporation
- Compliance reporting of users' activities in the SaaS applications

1.3 How CloudAccess Works

CloudAccess is a virtual appliance that provides a web service for users to securely access SaaS applications and other web applications. The appliance performs the following functions:

- **Provisioning:** CloudAccess allows you to map roles (groups) in an identity source, such as Active Directory or eDirectory, to account authorizations in the SaaS applications. CloudAccess leverages group management in the identity source to automatically create and manage the associated user accounts in the SaaS application.
- **Secure Single Sign-on:** CloudAccess authenticates users against identity sources and provides single sign-on to the SaaS applications and other web applications based on the users' entitlements. It also supports Integrated Windows Authentication (Kerberos) for background authentication to CloudAccess. The corporate credentials never leave the firewall. Provisioned users automatically have access to the SaaS applications, if they are logged in to the identity source.
- **Reporting:** CloudAccess provides reports on the usage of the SaaS applications to help enforce corporate policies and prove compliance.
- **Enabling Mobile Devices:** CloudAccess enables mobile devices to securely access the SaaS applications.

NOTE: Whether you have a CloudAccess license or a MobileAccess-only license determines the application connectors you are entitled to use. For more information, see Section 1.5, "Understanding Product Licensing," on page 16.

1.4 How CloudAccess Fits into Your Network

CloudAccess resides behind the corporate firewall in your IT network. Administrators perform tasks in the console using a browser on a workstation inside or outside of the firewall.

You can cluster the CloudAccess appliance. By default, it is a single node cluster, but CloudAccess supports up to a five-node cluster. For more information about clustering, see Section 3.9, "Configuring Clustering," on page 44.

CloudAccess allows you to configure two network adapters for each node in the cluster. You can configure one adapter for the administrative network and a second adapter for the public network. For more information, see Section 3.4, "Configuring Network Options," on page 33.

The user accounts reside in the identity source. CloudAccess provisions those users to the SaaS application. Users can then access the SaaS application resources by logging in with their identity source accounts, whether they are inside or outside the firewall.

1.5 Understanding Product Licensing

If you purchased a full CloudAccess license, your license includes all of the MobileAccess features. Installing the CloudAccess appliance gives you all of the MobileAccess features automatically. For more information about enabling and configuring MobileAccess, see Chapter 4, "Setting Up and Managing MobileAccess," on page 67.

If you purchased MobileAccess without CloudAccess, your license entitles you to a 90-day trial of CloudAccess. At the end of that period, you are expected to purchase the appropriate license for CloudAccess or discontinue use of the CloudAccess features. Your MobileAccess license entitles you to use the following:

- All administrative features related to mobile device management
- All options on the Identity Sources palette
- All options on the Tools palette
- Three connectors on the Applications palette: the connector for NetIQ Access Manager, the Bookmarks connector, and the Simple Proxy connector

Under the MobileAccess license, you may not use any other embedded connectors (such as the connector for Salesforce or the connector for Google Apps) or import any other connectors (such as the connector for WebEx or custom connectors created with the Access Connector Toolkit).

MobileAccess-only customers can upgrade to a full CloudAccess license at any time. For more information about pricing, contact the NetIQ Sales Support team. For licensing purposes, you can upgrade to a full CloudAccess license by adding a single CloudAccess appliance to an existing MobileAccess cluster. However, if you want all nodes in the cluster to display the CloudAccess product name, you must manually replace each MobileAccess node with a CloudAccess node.

2 Installing the Appliance

The CloudAccess and MobileAccess products are both installed as a VMware virtual appliance using files that you download, extract, and deploy into your IT environment. Whether you have a MobileAccess-only license or a full CloudAccess license, you need to install the virtual appliance only once (in a non-clustered environment).

2.1 Installation and Configuration Checklist

Before you begin installing and configuring your appliance, review the following checklist to ensure that you perform steps in the appropriate order.

Table 2-1 *Installation and Configuration Checklist*

❑	Steps	For more information, see...
❑	1. Verify that your environment meets all prerequisites.	Section 2.2, “Product Requirements,” on page 18
❑	2. Verify that your identity source meets all requirements.	Section 2.3, “Identity Source Requirements,” on page 20
❑	3. Gather the information you need to install and configure the appliance.	Section 2.4, “Appliance Installation Worksheet,” on page 28
❑	4. Install the appliance.	Section 2.5, “Deploying the Appliance,” on page 28
❑	5. Initialize the appliance.	Section 2.7, “Initializing the Appliance,” on page 29
❑	6. Configure the appliance.	Chapter 3, “Configuring the Appliance,” on page 31
❑	7. Configure the MobileAccess tool on the appliance.	Section 4.3, “Configuring the MobileAccess Tool on the Appliance,” on page 68
❑	8. Replace the default certificate on the appliance.	Section 4.4, “Replacing the Default Certificate on the Appliance,” on page 69

❑	Steps	For more information, see...
❑	9. (Conditional) Install a self-signed or non-public certificate on the mobile device.	Section 4.4.2, “Installing a Self-Signed Certificate on the Mobile Device,” on page 70
❑	10. Determine which applications users need to be able to access from mobile devices.	
❑	11. Configure the appropriate connectors to enable user access to applications.	Chapter 5, “Configuring Connectors,” on page 77 *NetIQ® CloudAccess Connectors Guide*
❑	12. (Optional) Obtain or create custom icons in `.png` format to represent your appmarked applications.	
❑	13. Configure appmarks for the applications.	Section 5.2, “Configuring Appmarks for Connectors,” on page 85
❑	14. (Conditional) Map any non-public appmarks to the appropriate groups in the identity source.	Section 5.2.8, “Policy Mapping for Non-Public Appmarks,” on page 90
❑	15. (Conditional) If you have configured provisioning connectors, such as Google Apps, map authorizations for the SaaS applications.	Chapter 6, “Mapping Authorizations,” on page 91
❑	16. (Users) Install the MobileAccess app on their mobile devices.	Section 4.5, “Installing MobileAccess on a Mobile Device,” on page 70
❑	17. (Users) Register their mobile devices with the appliance.	Section 4.6, “Registering a Mobile Device with the Appliance,” on page 71

2.2 Product Requirements

Use the information in the following table to verify that your environment meets all requirements before deploying the appliance.

Table 2-2 *Product 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 ◆ 8 GB RAM

Components	Requirements
Cluster	Supported cluster configuration: ◆ Up to a five-node cluster ◆ For optimal performance, each node should reside in the same IP subnet **NOTE:** The L4 switch must be configured with the publicly resolvable DNS of the cluster before you initialize the appliance.
Identity Source	Use one of the following identity sources for users: ◆ Microsoft Active Directory LDAP on Windows Server 2012 R2 or 2008 R2 ◆ NetIQ eDirectory LDAP 8.8 SP7 or 8.8 SP6 ◆ Microsoft SQL Server 2008 or 2014 ◆ Oracle Database 10.1 or 11.1 For more information, see Section 2.3, “Identity Source Requirements,” on page 20.
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 ◆ Safari or Chrome on supported mobile devices **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. Ensure that you allow pop-up messages for the administration console.

Components	Requirements
Mobile Devices	**Administration:** Not supported on mobile devices. **Users:** Supported iOS mobile devices for users: ◆ iPhone with iOS 7.0 or later ◆ iPad or iPad mini with iOS 7.0 or later Supported Android mobile devices for users: ◆ Android mid-density or high-density screen phone ◆ Android 10 inch or 7 inch tablet Supported Android versions: ◆ Ice Cream Sandwich 4.0 ◆ Jelly Bean 4.1 or later ◆ Kit Kat 4.4
Email Clients	For email proxy, CloudAccess supports IMAP, POP3, and SMTP across a variety of desktop and mobile email clients. For example, Windows Live Mail 2011 and the latest version of the Apple Mail Client on iPad or iPhone with iOS 7 or later. **NOTE:** The email ports in the CloudAccess cluster cannot be changed. It may be necessary to adjust the mail protocol or port configuration on the email clients to connect to the email proxy.
DNS	CloudAccess requires that all appliance nodes, administration workstations, end-user workstations, mobile devices, and identity sources be able to resolve the public DNS name of the appliance. The L4 switch must be configured with the publicly resolvable DNS of the cluster before you initialize the appliance.
SaaS Application Requirements	Each SaaS application has different requirements. For more information about the requirements for each SaaS application, see the *NetIQ® CloudAccess Connectors Guide*.

2.3 Identity Source Requirements

Use the information in the following sections to verify that your identity source meets all requirements before you deploy the appliance. For CloudAccess to provision user accounts to the SaaS applications, each user account in the identity source must contain the attributes listed.

2.3.1 Active Directory Requirements

Verify that your Active Directory environment meets the following requirements:

- ❒ Windows Server 2012 R2 or Windows Server 2008 R2.
- ❒ A unique identity for each user account, whether you have one or more domains or identity sources. The appliance uses the sAMAccountName as the unique identifier for the users.

To provision user accounts from Active Directory to the SaaS applications, all of the following attributes must be populated on the Active Directory users:

- First name
- Last name
- Full name (**Display name** is the field that populates this attribute.)
- sAMAccountName or Logon Name (Pre-Windows 2000)
- User Principal Name (UPN)
- Email address

Obtain the following required items:

- The password and the fully distinguished LDAP-formatted name of a user in Active Directory who has read access to the user objects. The appliance will use this user account to make LDAP binds to Active Directory.
- The name and password of a user in Active Directory who becomes the administrator of the appliance. The user must reside in the user search context specified during the appliance initialization procedure.
- The IP address of one or more Active Directory servers that contain the users.
- The context of the users in Active Directory.

2.3.2 eDirectory Requirements

Verify that your eDirectory environment meets the following requirements:

- ❒ eDirectory 8.8 SP7 or eDirectory 8.8 SP6.
- ❒ A unique identity for each user account, whether you have one or more eDirectory trees or identity sources.

To provision user accounts from eDirectory to the SaaS applications, all of the following attributes must be populated on the eDirectory users:

- CN (**Username** is the field that populates this attribute.)
- Given Name (**First name** is the field that populates this attribute.)
- Internet EMail Address
- Surname (**Last name** is the field that populates this attribute.)

Obtain the following required items:

- The password and fully distinguished LDAP-formatted name of a user in eDirectory who has the following rights. The appliance will use this user account to make LDAP binds to eDirectory:
  - **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
- **Group Membership:** compare, read, inherit
- **Surname:** compare, read, inherit

- **Entry Rights:** browse, inherit

- The name and password of a user in eDirectory who becomes the administrator of the appliance. The user must reside in the subtree of the search context for the identity source specified during the initialization of the appliance.
- The IP address of one or more eDirectory servers that contain a replica of the partition holding the user objects and that run NLDAP.
- The context of the users in eDirectory.

2.3.3 JDBC Requirements

In order to use the JDBC database as an identity source, you must know and understand JDBC databases. The information provided in this section is for database administrators.

Meeting the Requirements

Verify that you meet following requirements or obtain the following information before using a JDBC database as an identity source:

- The supported type of JDBC database. (Microsoft SQL Server 2008 or 2014, Oracle Database 10.2 or 11.1)
- The IP address of the JDBC database.
- The port for communication. The default port is 1433 for Microsoft SQL or 1521 for Oracle Database.
- The database name or sid. (`idm` for Microsoft SQL defines as the `sid` in Oracle Database)
- The script files must be installed before you can configure a JDBC database as an identity source. For more information, see "Obtaining the Script Files" on page 23.
- The password for the user name in the sample scripts you install. For more information, see "Obtaining the Script Files" on page 23.

Obtaining the Script Files

In order to use JDBC as an identity source, you must install script files on your JDBC database so that CloudAccess knows what tables to read to access the users and groups information. You download the script files when you configure the JDBC identity source.

You can download the files during the initialization process, if you select JDBC as your identity source, or you can download the scripts when you configure JDBC as an identity source after the appliance is initialized. You download a single zipped file that contains multiple scripts.

The different scripts are:

- **indirect_install:** Installs the schema, which includes the indirect tablespace and `proc_authuser()` stored procedure, as well as the automatic triggers for the `indirect.user` and `indirect.grp` tables.
- **copy_from:** Copies user account information from the database default user store into the indirect.usr table for processing by the connector for JDBC.
- **unistall:** Removes the schema and deletes or drops the connector user accounts in the underlying database.

Populating the Required Columns

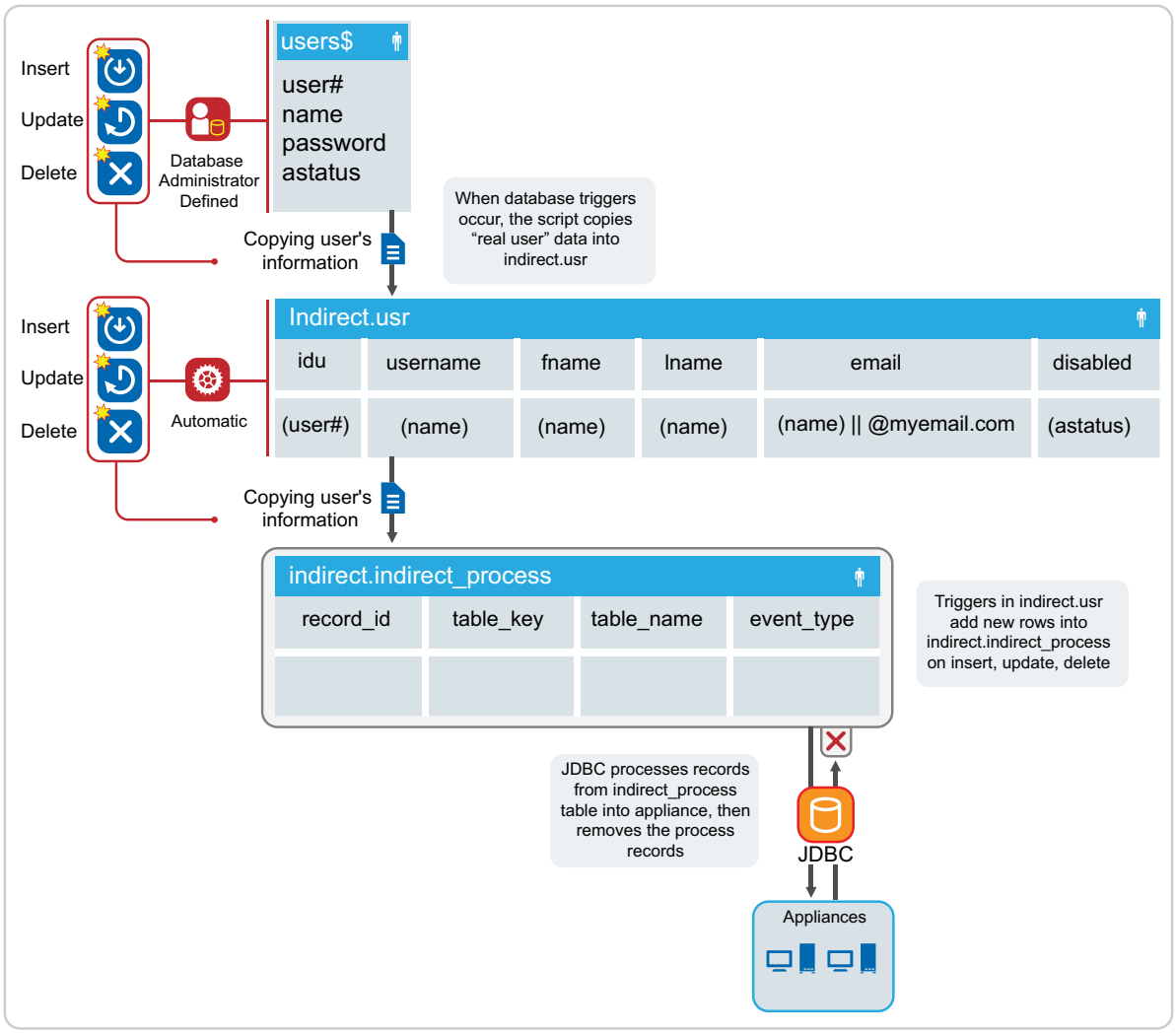
To provision users from the JDBC databases to the SaaS applications, you must have the following columns populated for each user account in the JDBC database:

- `indirect.usr.idu`
- `indirect.usr.username`
- `indirect.usr.fname` (Mandatory only for Google Apps accounts)
- `indirect.usr.lname`
- `indirect.usr.email` (Mandatory only for Salesforce accounts)

Dataflow Information

The connector for JDBC uses indirect tables to gather the needed information. This ensures that the appliance does not work directly with the information in the database. The following graphic depicts how the connector for JDBC obtains the information from the JDBC database. This process is the same no matter what type of database the appliance connects to.

Figure 2-1 *Dataflow of User Information*



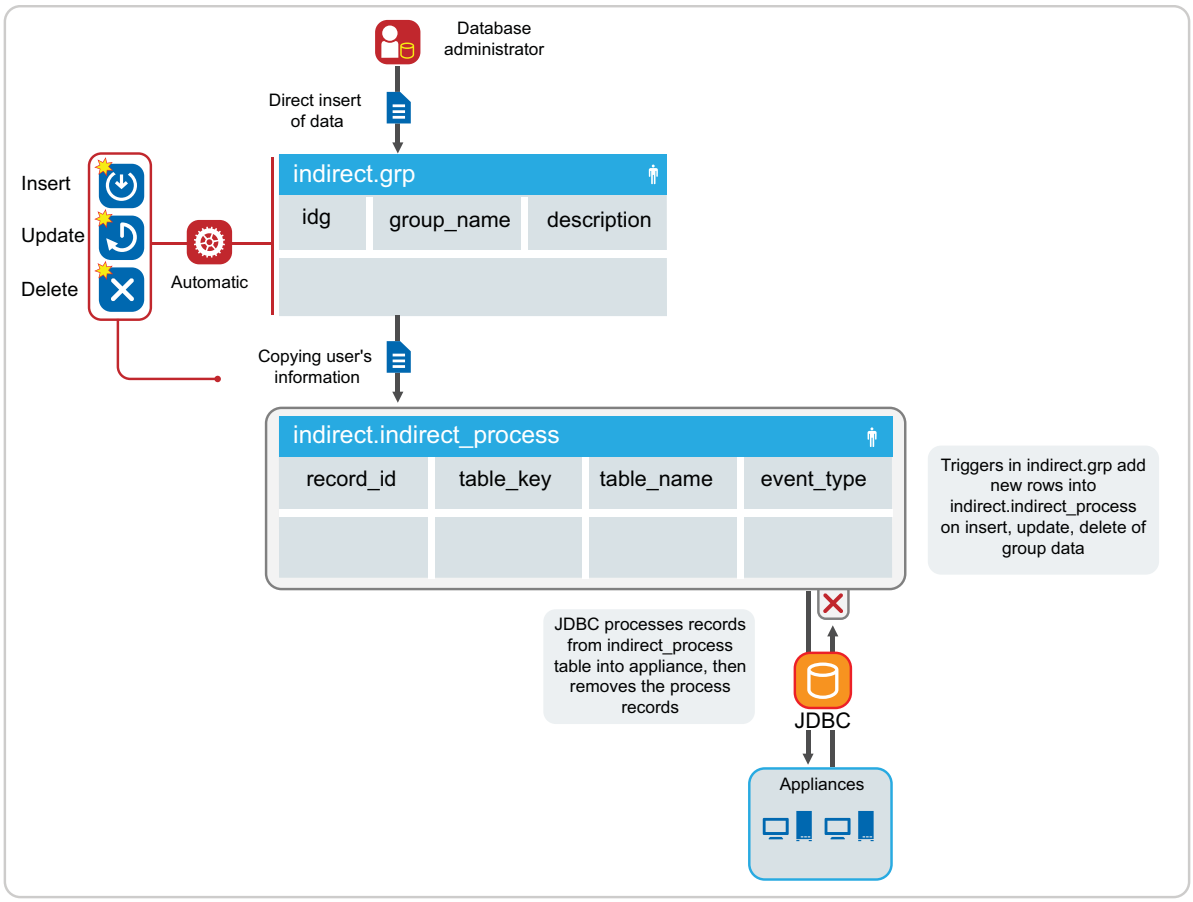
The database administrator creates the user accounts or logs in to the `user$` table. (The dataflow figures are based on the default Oracle security table `user$`.) The database administrator defines triggers or procedures that copy information into the `indirect.usr` table.

The `indirect_install .sql` script creates the automatic insert, update, or delete triggers on the `indirect.usr` table. When rows in the `indirect.usr` table are altered, the automatic triggers add a row to the `indirect.indirect_process` table.

The appliance polls the `indirect.indirect_process` table. When the appliance detects rows in the `indirect.indirect_process` table of type `user`, the appliance adds, modifies, or deletes the user account in the applications connected to the appliance.

The appliance then deletes the row from the `indirect.indirect_process` table after the appliance processes the information.

Figure 2-2 *Dataflow of Group Information*

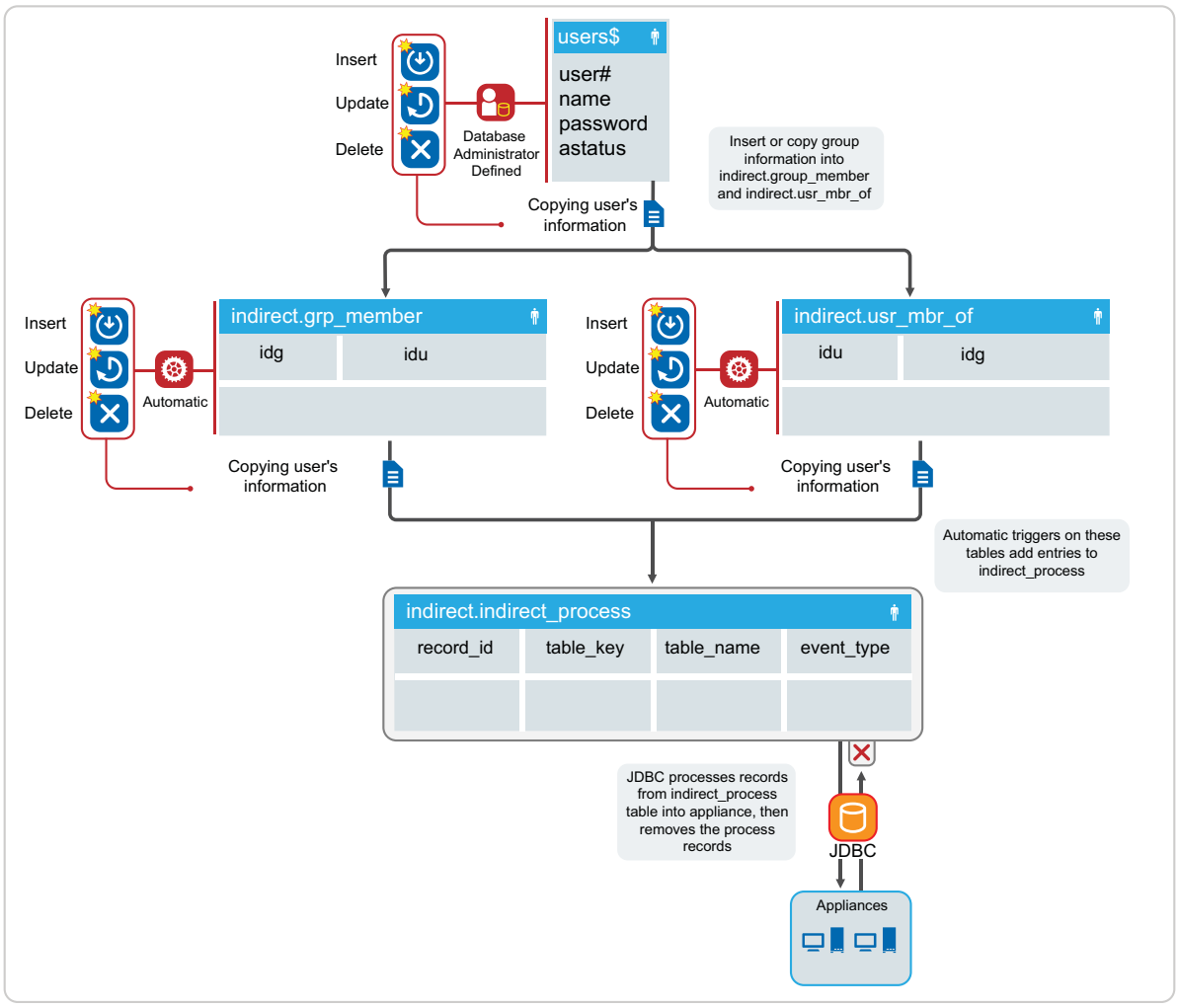


The database administrator performs a direct or triggered insert of data into the `indirect.grp` table.

The `indirect_install .sql` script creates the automatic insert, update, or delete triggers on the `indirect.grp` table. When rows in `indirect.grp` are altered, the automatic triggers add a row to the `indirect.indirect_process` table.

When the appliance detects rows in the `indirector.indirect_process` table of type group, the appliance adds, modifies, or deletes the groups in the applications connected to the appliance. The appliance then deletes the row from the `indirect.indirect_process` table after the appliance processes the information.

Figure 2-3 *Relationship between Users and Groups*



The indirect schema does not have a direct concept of group membership, but maintains a relationship between the `user idu` column and the `group idg` column in the tables `indirect.grp_member` and `indirect.usr_mbr_of table`.

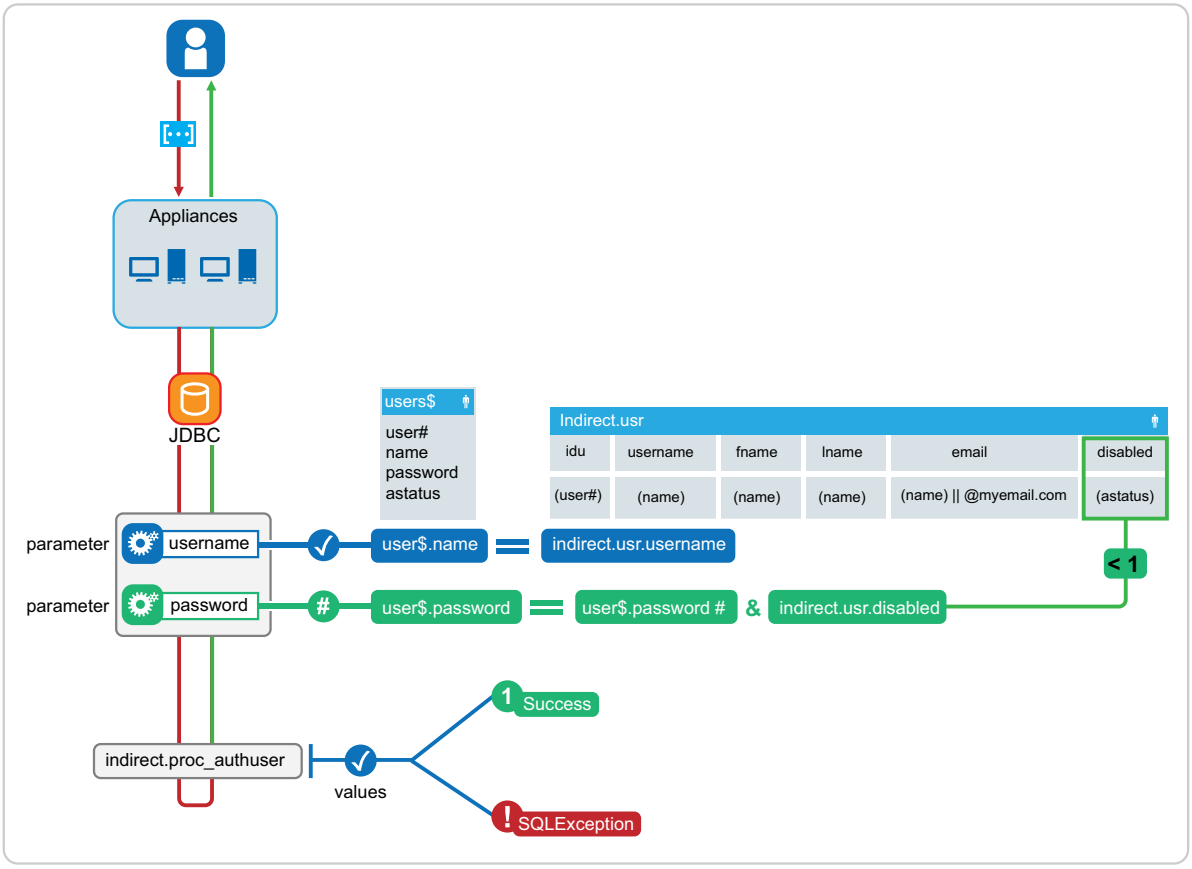
For group membership, the desired group `idg` and user `idu` must exist in both tables. The `indirect install .sql` script creates the automatic insert, update, or delete triggers on the `indirect.grp_member` and `indirect.usr_mbr_of tables`. When rows in these tables are altered, the automatic triggers add a rows to the `indirect.indirect_process` table.

When the appliance detects rows in the `indirector.indirect_process` table for group membership, the appliance adds, modifies, or deletes the group memberships in the applications connected to the appliance. The appliance then deletes the row from the `indirect.indirect_process` table after the connector processes the information.

For example, if the administrator wants to add a user with `idu 6` to a group with `idg 10`, they would have to manually (or through triggers) add entries into both the `grp_member` and `usr_mbr_of` tables.

```
"INSERT INTO indirect.grp_member(idg,idu) VALUES(10,6); INSERT INTO
indirect.usr_mbr_of(idu,idg) VALUES(6,10);"
```

Figure 2-4 *Authentication Process*



To verify authentication credentials, the appliance calls a stored procedure `indirect.proc_authuser` with the parameters of `@username,@password`. The procedure compares the `username` parameter with the default user table (`user$`) and the `indirect.usr.username` fields. If they matched, the process checks the `indirect.usr.disabled` flag (disabled > 0 = disabled). If login is enabled (disabled = 0), the process compares the `password` parameter to the existing password hash in the `user$` table. If the password hash matches, then the process authenticates the user successfully. If any of these conditions are not met, then the process returns an `SQLException` to the appliance, and authentication fails.

You can alter the stored procedure based on the desired schema that the database administrator wishes to use for authentication. The administrator needs to keep in mind that the stored procedure `indirect.proc_authuser(@username,@password)` is hard-coded into the appliance, and expects either a `success (1)` or `SQLException` returned.

2.3.4 Self-Service User Store Requirements

The Self-Service User Store is an internal identity source you can use with the appliance. However, you can only use this identity source after you configure the appliance. The Self-Service User Store cannot be used during the initialization process of the appliance.

There are no specific requirement to use this service. For more information, see Section 3.7.1, “Configuring Self-Service Registration and Password Management,” on page 37.

2.4 Appliance Installation Worksheet

Use the following worksheet to gather the required information to install and configure the appliance.

Table 2-3 *Appliance Installation Worksheet*

Component	❑	Gather the following information:
Networking Information		
	❑	Publicly resolvable DNS name for the appliance
	❑	NTP Server
	❑	DNS server, subnet mask, and gateway
	❑	(Recommended) An SSL certificate signed by a well-known certificate authority (CA)
Identity Sources		
	❑	IP address or DNS name of the server or database that contains the users
	❑	Context of the users (Only for Active Directory and eDirectory)
	❑	Name and password of user with the proper rights to the users

2.5 Deploying the Appliance

Whether you are deploying CloudAccess or MobileAccess, the 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:

- **DHCP environment:** An `*.ovf` file for environments that have a DHCP server.
- **Non-DHCP environment:** 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/).
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 2.7, "Initializing the Appliance," on page 29.

The initial boot configures the appliance. The initial boot could take between five and twenty 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`.

NOTE: Whether you have a MobileAccess-only license or a full CloudAccess license, you need to install only one virtual appliance to access all features. The CloudAccess appliance includes all MobileAccess features.

2.6 Upgrading Your Environment

If you are currently running CloudAccess 2.0 in your environment, you can use the update channel to upgrade to CloudAccess 2.1. For more information, see Section 9.5, "Updating the Appliance," on page 104.

Upgrades from previous versions through the update channel are not supported. If you have a previous version installed, you must manually upgrade to CloudAccess 2.0 and then use the update channel to upgrade to 2.1, or perform a fresh installation of CloudAccess 2.1. For more information about upgrading your environment from CloudAccess 1.5 to CloudAccess 2.0, see "Upgrading Your Environment" in the NetIQ CloudAccess and MobileAccess Installation and Configuration Guide (https://www.netiq.com/documentation/cloudaccess/install_config/data/bookinfo.html) for CloudAccess 2.0 on the NetIQ Documentation website.

2.7 Initializing the Appliance

You must now initialize the appliance.

1 Verify that you meet the requirements listed in Section 2.2, "Product Requirements," on page 18.

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 Provide the following information needed to initialize the appliance:

3a Initialize Appliance

Select **Join Cluster** only if you are initializing an appliance to add to an existing cluster. The first appliance that you configure automatically becomes the master node in the cluster.

3b Step 1 - Network

NTP server - The NTP (Network Time Protocol) server allows appliances to synchronize time with each other. Without this server, the data on the appliances becomes corrupted.

Obtain an IP address automatically - Select this option if you have a DHCP server to provide the IP address of the appliance.

Use the following IP address - Select this option only if you do not have a DHCP server in your environment and you are assigning a static IP address. If you deployed the appliance using the `*-vcenter.ovf` file, the fields are auto-populated with the settings you specified during deployment.

3c Step 2 - Identity Source

Select the identity source that you plan to use.

Username and **Password** - Specify the fully distinguished LDAP format name of a user in the identity source who has Read access to the identity source. For example, in eDirectory this might be `cn=admin,o=netiq`.

Context - Specify the search context of the users in the identity source. For example, `o=netiq`.

Enable LDAP SSL - Specify whether you want to use SSL for communication with an LDAP identity source. If you use SSL, the default port is 636. The default port for non-SSL is 389. You can specify other port numbers as required if the identity source is using a non-default port.

When you set up the identity source for the first time, you specify a single replica of the identity source, but you can add more replicas later if needed.

3d Step 3 - Cluster Information

Public DNS - Specify the public DNS name that is used as the base URL to access the appliance. For example, `nca-01.company.info`.

Admin user name - Specify the user account in the identity source search context who becomes the administrator of the appliance. In eDirectory, this is the CN of the user. In Active Directory, this is the sAMAccountName of the user.

3e Step 4 - Appliance Password

New password / Confirm password - Specify the password for the appliance administrator account. If you lose the connection to the identity source for any reason, you can run through these initialization steps again using the appliance password specified here. You would then specify a different identity source and the user name and password of the new appliance administrator in that new identity source.

4 Click **Finish**.

A successfully initialized appliance automatically redirects the browser to the administration console login page at `https://`*`appliance_dns_name`*`/appliance/index.html`.

5 Log in with the Admin user name specified in **Step 3 - Cluster Information**. The password is the user's password in the identity source.

6 Proceed with Chapter 3, "Configuring the Appliance," on page 31.

You can change the initialization settings at any time if needed. Enter *`appliance_dns_or_IP_address`*`/appliance/Init.html` in a browser to access the initialization settings page. After the appliance has been initialized for the first time, the next time you access the `Init.html` page, CloudAccess prompts you for the appliance password.

Whenever you make changes to the appliance, click **Apply** and wait for the appliance to finish applying your changes. Do not attempt to perform any other administration tasks in the console until the gears have stopped spinning on the appliance icon.

3 Configuring the Appliance

Once you have installed and initialized the appliance, configure the appliance to communicate with the SaaS applications.

3.1 Accessing the Administration Console

After you properly initialize the appliance using the information in Section 2.7, “Initializing the Appliance,” on page 29, the browser automatically redirects you to the administration console at `https://appliance_dns_name/appliance/index.html`. If the initialization does not automatically redirect you, open the page manually to complete the appliance configuration.

To access the administration console:

1. In a supported browser, enter `https://appliance_dns_name/appliance/index.html`.
2. Log in as the administrator of the appliance.

   These credentials are the cluster administrator user name specified during the initialization process and its identity source user password.
3. The first time you log in, the appliance displays the Admin page and might display user count activity on the **Users** bar as users in the search contexts from the identity source are imported and activated. Ensure that this process completes before you configure any application connectors.

Icons at the top of the Admin page allow you to access the other administration pages. If your session times out or you log out, the next time you log in to the appliance, CloudAccess displays the page that you last accessed.

Admin sessions time out by default after 10 minutes. This setting is not currently configurable, but you can adjust the timeout setting for user sessions. For more information, see Section 9.2, "Configuring Session Timeouts," on page 103.

For a list of the different administration pages, see Section 3.2, "Getting Started," on page 32.

3.2 Getting Started

From the Admin page you can use the navigation icons at the top of the page to access other functions in the administration console:

- **Roles:** Configure roles for different users within CloudAccess. For more information, see Section 3.8.2, "Assigning Roles to Users," on page 44.
- **Policy:** Map roles (groups) from the identity source to authorizations from the SaaS applications. For more information, see Chapter 6, "Mapping Authorizations," on page 91.
- **Approval:** Approve or deny authorizations for the SaaS applications. This icon appears only if you have mapped roles to authorizations and selected the option to require approval for accounts, and there are accounts waiting for approval. For more information, see Section 6.8, "Approving Requests," on page 95.
- **Reports:** Report on the user activities to the SaaS applications. For more information, see Chapter 7, "Reporting," on page 97.
- **Devices:** View and manage registered mobile devices. For more information, see Section 4.8, "Managing Mobile Devices," on page 74.

Before you begin any configuration tasks, you should register your appliance. For more information, see Section 3.3, "Registering the Appliance," on page 32.

3.3 Registering the Appliance

CloudAccess 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 on the Admin page 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 Customer Center update channel to download and install software updates, you must register each node in the cluster

separately. The bomb icon remains on the Admin page 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 9.5, "Updating the Appliance," on page 104.

To register your appliance:

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

   The Customer Center is for NetIQ, Novell, and SUSE customers.
2. Click **My Products** > **Products**, then click **CloudAccess**.
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. On the Admin page, click the appliance, 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 appliance in the cluster.

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

3.4 Configuring Network Options

CloudAccess contains a manual routing table, supports two Network Interface Cards (NICs), and provides a forward proxy only for testing purposes.

3.4.1 Configuring the Forward Proxy

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

NOTE: The forward proxy feature has the following limitations:

- The forward proxy is intended only for testing purposes, and is not supported in a production environment.
- When forward proxy is enabled, Simple Proxy connectors work only with web servers or resources (as specified in the **Connects to** field of the connector configuration) that are on the local segment. All simple proxied services must be reachable from the appliance without going through the forward proxy.

To configure the forward proxy:

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

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 clicking **OK** causes the services to restart and you must log in to the appliance again.

3.4.2 Configuring the Second Network Interface

CloudAccess supports two Network Interface Cards (NICs) for each node in the cluster. You can configure one NIC for the administrative network and a second NIC for the public network. However, whether the nodes in a cluster each have one or two NICs configured, the cluster itself has only two DNS names: one for the Admin NICs and one for the Public NICs.

IMPORTANT: If you configure two NICs on one appliance, you must configure all other nodes in the cluster with two NICs.

To configure the second NIC on a node:

1 Log in with an appliance administrator account to the Admin page at `https://`*`appliance_dns_name`*`/appliance/index.html`.

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

3 Click the **Public Interface** tab.

4 Select **Enable Separate Public Interface**.

5 Configure the network settings for your public network and click **OK**.

6 (Conditional) If this is the first node in the cluster with a Public NIC, enter the DNS name for the public network. Modify the keypairs for SSL and SAML as needed and click **OK**.

7 Click **Apply** to save the changes.

8 Click **Close**.

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

3.4.3 Configuring the Routing Table

CloudAccess 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 Log in with an appliance administrator account to the Admin page at `https://`*`appliance_dns_name`*`/appliance/index.html`.

2 Click the node icon, then select **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.

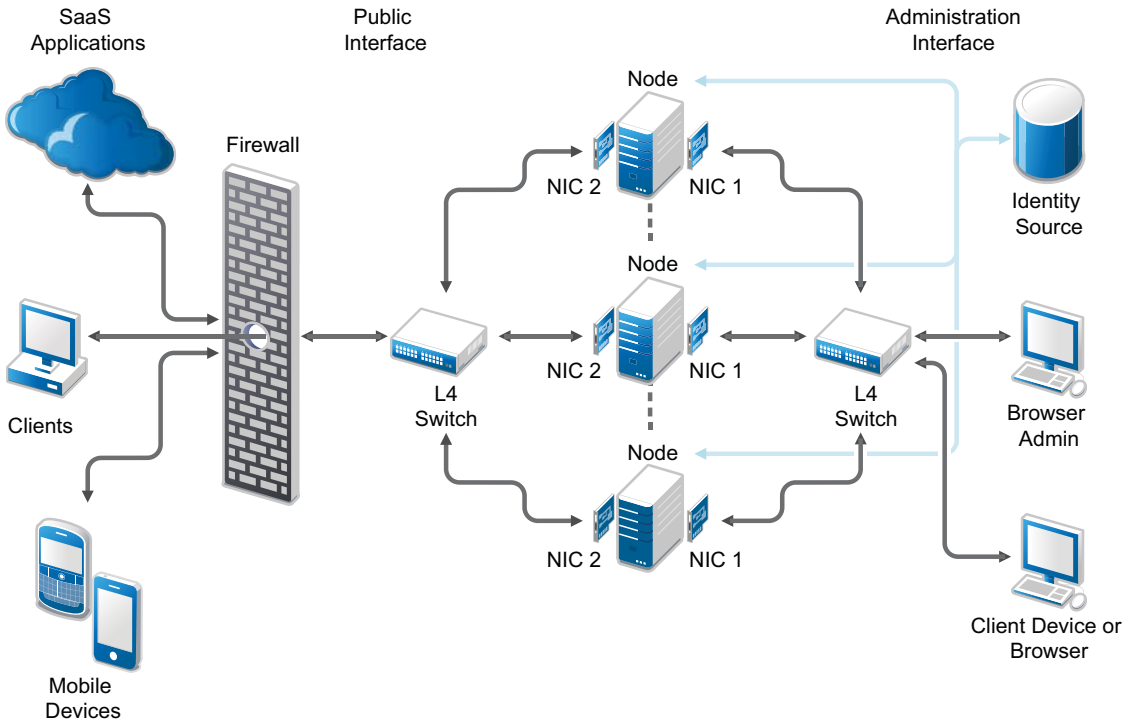
8 Click **Close**.

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 CloudAccess with both NICs enabled on each node.

Figure 3-1 *A 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 Changing the Certificates on the Appliance

The appliance contains SSL and SAML self-generated certificates, by default both named ag4csrv1, but NetIQ highly recommends that you replace the default certificates with well-known Certificate Authority signed certificates. The required format for importing a key pair is `.pfx`. This format contains the private key, certificate, and trusted roots required to import.

To change the certificates:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns_name/appliance/index.html`.
2. Click the cluster icon under **Appliances**, then click **Configure**.
3. Delete the default key pairs by clicking the red delete (X) icon next to the SSL key pair and the SAML key pair.
4. Browse to and select the certificates you want to use, then click **OK**.
5. In the Instructions window, click **OK**.
6. Click **Apply** and wait for the configuration changes to be applied to the appliance. Do not perform other administration tasks in the console while the changes are being applied.
7. Close your browser and reopen it to start a new session using the new key pairs.

Expired key pair certificates prohibit changes from being made to this page and make the key pair field red. If the key pair expires, you must re-initialize the appliance before you can upload a new certificate.

3.6 Verifying the Identity Source User Attributes

CloudAccess supports the use of one or more identity sources to authenticate users and for provisioning accounts to the SaaS applications. The initialization process configures the first identity source and adds the identity source to the Admin page.

To successfully provision users to the SaaS applications, you must ensure that each user account contains specific information for the appliance to provision the users. If you are using an LDAP identity source, there are specific attributes that must be populated on the user accounts. If you are using a JDBC database, there are certain columns of information that must be populated. The information for each identity source is different. For more information, see Section 2.3, “Identity Source Requirements,” on page 20.

For security reasons, by default CloudAccess does not allow you to add a user with a user name that is the same as a previously added user. If you attempt to do so, CloudAccess displays the user as not activated. For more information, see Section 10.6, “Troubleshooting Provisioning Issues,” on page 115.

3.7 Configuring Additional Identity Sources

During the initialization process, you configure an identity source. You can add more identity sources after the initialization process completes. However, the user IDs across the identity sources must be unique.

The Self-Service User Store (SSUS) and SAML 2.0 Inbound (SAML2 In) are identity sources that you can only add after your initialize the appliance. Use the following information to configure additional identity sources.

- Section 3.7.1, “Configuring Self-Service Registration and Password Management,” on page 37
- Section 3.7.2, “Configuring Additional Identity Sources,” on page 42
- Section 3.7.3, “Configuring SAML 2.0 Inbound Identity Sources,” on page 42

3.7.1 Configuring Self-Service Registration and Password Management

The Self-Service Registration and Password Management tool (SSRPM) allows you to empower users to register for services and to manage their credentials. It provides selected services from the NetIQ Self-Service Password Reset tool. The Self-Service User Store (SSUS) stores identity and credentials for self-registered user accounts. It is an additional identity source you can use with the appliance.

Enabling a Self-Service User Store (SSUS)

A Self-Service User Store provides self-service registration and password management services. You can enable and activate one Self-Service User Store. After you enable the service, the users can immediately begin to self-register on the SSUS Registration page. Self-registered users can then log in and access public applications from the landing page. Policies are required to allow the self-registered users to access private applications.

By default, SSUS requires new users to have a valid email account to create an SSUS account. Users must be able to receive and respond to a verification email.

You can also configure which service options to support for your SSUS users. The services include a helpdesk, new user, change password, and forgotten password.

To enable the SSUS service:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns_name/appliance/index.html`.
2. In the administration console, drag the **Self-Service User Store** icon from the **Identity Sources** palette and drop it in the **Identity Sources** panel.
3. In the **Identity Sources** panel, click the new identity source, then click **Configure**.
4. On the **Configuration** tab, decide what options you want presented to your users and helpdesk administrators.
5. Click **OK** to enable the Service.
6. In the **System Configuration** panel of the administration console, click **Apply** to activate and start SSUS as a service.
7. Wait for the SSUS service to be activated and started across all nodes in the cluster.

   In the **Appliances** panel, the icon on each node of the cluster spins until the service is ready on the node. Do not apply additional changes until this action is complete on all nodes.

   A round green status icon in the lower left corner of the SSUS service icon indicates that the SSUS is configured and its status is healthy.

To allow the self-registered users to access to a private application that is enabled for SSUS, continue with "Using SSUS as an Authentication Source for an Application" on page 38.

Using SSUS as an Authentication Source for an Application

The applications are not available for SSUS users until you configure policies that authorize SSUS to be an authentication source for them. All SSUS users receive rights to an application when you assign a policy to the SSUS identity source.

Requirements for SSUS Authorizations

Provisioning is not supported for users in an SSUS identity source. For more information, see "Requirements for Provisioning" in the *NetIQ® CloudAccess Connectors Guide*.

Creating an SSUS Policy for a Private Application

An application can have one or more authorizations for its resources. Each authorization can have one or more appmarks associated with it. You grant access to a private application by mapping one or more of its authorizations to the SSUS role. Users can access all of the appmarks associated with an authorization. You cannot control access at the appmark level.

NOTE: You should map authorizations for SSUS roles (groups) only to single sign-on applications. Do not map them to the SaaS applications with account provisioning (Google Apps, Office 365, or Salesforce).

To create a policy that grants access to an application for SSUS users:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns_name/appliance/index.html`.
2. Click **Policy** in the toolbar.
3. On the Policy Mapping page, select **Other Identity Sources** from the drop-down list on the left, then select the **All SSUS Users** role.
4. On the right, select the software-as-a-service application that you want to use for this policy, and then view its authorizations.

   Some applications have multiple authorization options.
5. Drag the **All SSUS Users** role from the left side and drop it on the desired authorization on the right.

   You can also select multiple authorizations under a single application, then drag them from the right and drop them on the **All SSUS Users** role on the left.
6. In the pop-up **Mapping** window, review the mapped settings, then click **OK** to accept the new policy, or click **Cancel** to back out of the setup.

   You can remove an authorization in the list by selecting it, then clicking the **Delete** icon. A strike-through line is drawn through the entry.
7. Under **Other Identity Sources**, view the **Authorization** column for the **All SSUS Users** role to confirm that the **Authorization Stamp** icon appears.
8. Under the application on the right, view the **Policy** column to confirm that the **Policy** icon appears for the mapped authorization.

9 The appmarks for each of the mapped authorizations are available to users at their next login.

10 Repeat Step 4 through Step 9 for each application that you want to use SSUS as an identity source.

Deleting an SSUS Policy for an Application

You can deny access to an application by deleting its SSUS policy. Deleting the policy does not interrupt current sessions. The application is not available to users at their next login.

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

2 Click **Policy** in the toolbar.

3 On the Policy Mapping page, select the **Self-Service User Store** role from the drop-down list on the left, then select the **All SSUS Users** role.

4 In the **All Users** row, click the **Authorization Stamp** icon.

5 In the **Edit All Users Mappings** window, select the authorization you want to remove, then click the **Delete** icon. Repeat this action for every authorization that you want to remove.

A strike-through line is drawn through the entry.

6 Click **OK** to accept the modified settings, or click **Cancel** to back out of the setup.

The application is not available to users at their next login.

Using the Self-Service User Registration and Password Management Services

The users can now self-register for accounts and manage their own credentials. Self-registered users can log in to the landing page for the appliance to access applications.

If you enabled the options during the SSUS configuration, users now see links on the appliance login page to create a new account or a link to reset their password if they have forgotten the password.

The user experience is:

1. The new user accesses the appliance login page.

   `https://appliance_dns_name`

2. The user clicks the link to create a new account.
3. The user follows the on screen prompts to create a new account that includes their name, email address, and a password.
4. After the account is created, the user is prompted to create security questions and answers.

   If the user forgets the account password, the questions and responses are used to verify the user's identity and allow the user to reset the password
5. (Conditional) If the user does not create the security questions and answers now, the user will be prompted to create them when they log in for the first time. If the user does not set up the security questions and answers the appliance will not authenticate the user. The user must set up the security questions and answers to authenticate to the appliance.
6. After the user completes the new account setup, the appliance sends a verification email to the user's email address. The user responds to verify the account creation.
7. The user accesses the login page again.
8. The user logs in with their new user name and password.
9. The user sees and can access the applications that the policies entitle them to see.

After you enable the Self-Service User Store, the Self-Service User Store login page is available for users. On this page, the user can perform the following tasks:

- **Create a New User:** A user can register for the service as a new user. The user provides their name and a valid email address, creates a password, and sets up security questions and responses. After the user responds to a validation message sent to the user's email address, the user can log in and begin using the account.
- **Change Password:** A self-registered user can reset the password for their account at any time. On the user's landing page, there is a **Change Password** icon they click. The user follows the on screen prompts to change their password.
- **Forgotten Password:** If a user forgets their password, they can reset their password after answering the security questions. The user access the login page and they enter their user name. The user then clicks the **Forgotten Password** link and follows the on screen prompts to change their password. The user must successfully reply to the security questions that the user set up for the account.

Providing Helpdesk Services for Self-Registered Users

The Self-Service User Store provides a helpdesk service. If a password expires or a self-registered user is locked out of an account, the password can be reset by an authorized helpdesk user for the SSUS service. The helpdesk user sets a temporary randomized password for the account, and the user is notified of the temporary password by email. This allows the user to log in to the account and reset the temporary password to use a custom password.

- "Adding a User to the Helpdesk Role" on page 40
- "Accessing the SSUS Helpdesk" on page 41
- "Resetting the Password for a Locked Self-Registered User Account" on page 41
- "Deleting a Self-Registered User Account" on page 41

Adding a User to the Helpdesk Role

You must assign a user to the SSUS Helpdesk role to provide helpdesk services for the related self-registered users.

NOTE: You should assign a user from an Identity source other than the SSUS source as the helpdesk user.

Use the following steps to enable the SSUS Helpdesk service.

1. The new user accesses the appliance login page at:

   `https://appliance_dns_name`

2. Click **Roles** in the toolbar.
3. On the Roles page, type the name of a user you want to assign to the Helpdesk role, click **Search**, then select the name.
4. Drag the user name from the left side and drop it on the Helpdesk role on the right.
5. In the pop-up **Add User to Role** window, review the mapped settings, then click **OK** to accept the new role assignment, or click **Cancel** to back out of the setup.
6. After the page refreshes, view the **Role** column for the user to confirm that the **Role** icon appears.
7. Under the Helpdesk role on the right, verify that the authorized user's name appears.

The helpdesk user accesses the helpdesk tools through the landing page. The helpdesk user logs in, and then clicks the **Helpdesk** icon on the landing page.

Accessing the SSUS Helpdesk

The landing page of an authorized helpdesk user displays a **Helpdesk** icon.

To access the Helpdesk from the landing page if you are an authorized helpdesk user:

1. Log in to CloudAccess using your corporate credentials.
2. On the landing page, click the **Helpdesk** icon to go to the Helpdesk page.

Resetting the Password for a Locked Self-Registered User Account

An authorized helpdesk user can use the SSUS Helpdesk service to reset the password for a self-registered user account. Typically, the user needs helpdesk assistance because the account is locked. If the account is not locked, the user can alternatively reset the password by using the **Forgotten Password** option on the Self-Service Registration login page.

To reset the password for an SSUS account as the authorized helpdesk user:

1. Log in to the SSUS Helpdesk as an authorized helpdesk user.
2. On the Helpdesk page, search for an SSUS user account, then click the self-registered user's name.
3. On the Password Policy page, view the password policy settings for the user account, then click **Change Password**.
4. On the Account Information page, confirm the user's information, then click **Change Password**.
5. In the **Random Passwords** window, select a password from the list of randomly generated passwords that satisfies the password policy for this account.

   You can click **More** to choose from additional random passwords.
6. View the confirmation message with the new password, then click **OK**.
7. After the self-registered user receives the temporary password, the user is prompted to reset the password at their next login.

Deleting a Self-Registered User Account

An authorized helpdesk user can use the SSUS Helpdesk service to delete the SSUS account for a self-registered user.

To delete an SSUS account as the authorized helpdesk user:

1. Log in to the SSUS Helpdesk as an authorized helpdesk user.
2. On the Helpdesk page, search for an SSUS user account, then click the self-registered user's name.
3. On the Account Information page, confirm the user's information, then click **Delete Account**.
4. Click **OK** to confirm the account deletion.

3.7.2 Configuring Additional Identity Sources

CloudAccess supports multiple types of identity sources. You can have one or more of each type of identity source configured on your appliance, and you can configure as many identity sources as you need.

The only restrictions are as follows:

- The source for each identity source must be unique. For example, do not configure multiple instances of an identity source for the same Active Directory domain.

and that every user account across the different identity sources must be unique.

For information about requirements and information that are needed to configure an Active Directory, eDirectory, or JDBC database identity source, see Section 2.3, "Identity Source Requirements," on page 20.

NOTE: Although CloudAccess allows you to modify an existing eDirectory or Active Directory connector to point to a different tree, NetIQ does not recommend this approach because it can result in inconsistent display of user and group data. If you want to point a connector to a different tree, delete the existing connector and create a new connector that points to the correct tree.

To change the initial identity source configuration information:

1. Log in with an appliance administrator account to the Admin page at

   `https://appliance_dns_name/appliance/index.html`
2. In the **Identity Sources** panel, click the icon of the identity source that you want to modify, then click **Configure**.
3. Modify the settings as needed, then click **OK** to save the configuration information.
4. Click **Apply** to commit the changes to the appliance.

To add another identity source:

1. Log in with an appliance administrator account to the Admin page at

   `https://appliance_dns_name/appliance/index.html`
2. Drag and drop an identity source icon from the **Identity Sources** palette to the **Identity Sources** panel.
3. Click the identity source icon, then click **Configure**.
4. Complete the fields to configure the new identity source.
5. Click **OK** to save the configuration information.
6. Click **Apply** to commit the changes to the appliance.

3.7.3 Configuring SAML 2.0 Inbound Identity Sources

To allow the appliance to be a SAML 2.0 service provider, you can create a SAML 2.0 Inbound connector using the Access Connector Toolkit. After you export the connector and import it in the appliance, the SAML2 In connector appears as an identity source. You configure an instance of the identity source with information about an appropriate identity provider in order to enable the service provider functionality of the appliance, and to allow the identity provider to send a SAML token to the appliance using the SAML 2.0 POST profile.

After you configure the SAML2 In identity source, the appliance login page provides a link to the login page of the SAML 2.0 identity provider, located to the left of the user name and password login options. The SAML 2.0 users log in through the identity provider to gain access to the appliance landing page.

For more information, see "Creating a SAML 2.0 Inbound (SAML2 In) Connector Template" in the *NetIQ® CloudAccess Connectors Guide*.

3.8 Configuring Roles Management

CloudAccess provides the ability to assign different roles to administrative users in your identity sources. The roles allow administrators to perform certain tasks and deny them access to other tasks.

3.8.1 Defining the Role Types

CloudAccess includes the following types of roles:

- **Appliance Administrator:** The appliance administrator has full rights to all appliance administration pages and role assignments. You assign the first appliance administrator during the initialization of the appliance.
- **Application Owner:** The application owner controls access to the SaaS applications. CloudAccess automatically assigns this role to the user who creates the SaaS application on the Admin page. The application owner can access the following web pages:
  - **Approvals:** The application owner can allow or deny approvals for the users to obtain a SaaS application account.
  - **Policy:** The application owner can map authorizations between the identity source and the SaaS application and optionally require approval for authorizations.
  - **Roles:** The application owner can add or remove users from the application approver role.
- **Application Approver:** The application approver can access the Approvals page and allow or deny approvals for the users to obtain a SaaS application account. CloudAccess automatically assigns this role to the user who creates the SaaS application on the Admin page.
- **Compliance Auditor:** The compliance auditor can access the Reports page and generate, view, and download the reports for the appliance. Users assigned to the appliance administrator role have access to the Reports page automatically.
- **Device Administrator:** The device administrator can view and delete other users' registered mobile devices on the Devices page. A user who has the appliance administrator role automatically has the device administrator role (though the reverse is not the case).
- **Helpdesk:** The helpdesk administrator manages the Self-Service User Store users. The helpdesk user can delete users and reset passwords.

In addition to the default role assignments, you can assign each role to additional users. However, the Roles page never allows you to remove the last appliance administrator role.

3.8.2 Assigning Roles to Users

To assign roles to users:

1. Log in to the Admin page at `https://appliance_dns_name/appliance/index.html` as the appliance administrator or application owner.
2. Click **Roles** on the toolbar.
3. Type the name of a user into the search bar, then click **Search**. Matching users are displayed in the left column.
4. Drag and drop the user to the role you want to assign to that user, then click **OK** to confirm the assignment.

The Roles page displays only the application owner and application approver roles of configured SaaS connectors.

3.9 Configuring Clustering

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

3.9.1 Advantages of Clustering

Clustering in CloudAccess 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: CloudAccess 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 CloudAccess. Each node in the cluster increases the number of possible simultaneous logins.

3.9.2 Managing Nodes in the Cluster

CloudAccess supports up to five nodes in a cluster. You add nodes to the cluster through the initialization process, and perform all other initialization tasks on the Admin page.

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 10.4, "Troubleshooting Different States," on page 110.
2. Download and deploy a new virtual machine (VM) for the new node.

   For more information, see Section 2.5, "Deploying the Appliance," on page 28.
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 2.7, "Initializing the Appliance," on page 29.
4. When initialization is complete, the browser is redirected to `index.html` and a login page appears.
5. Log in to `index.html`.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 there are several background processes 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 the Appliance," on page 32.

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 10.4, "Troubleshooting Different States," on page 110.
2. Verify that all nodes in the cluster are running the same version of CloudAccess. If any nodes need to be updated, ensure that you update the nodes *before* you switch the master node. For more information, see Section 9.5, "Updating the Appliance," on page 104.
3. Take a snapshot of the cluster.

4 Click the node to become the master node on the Admin page, then click **Promote to master**.

An M appears on the front of the node icon indicating 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 start again on the new master and reports start again on the new master. The historical logs are lost. The reporting data is also lost, unless you are using Sentinel Log Manager. For more information, see Section 7.2, "Integrating with Sentinel Log Manager," on page 98.

Removing a Node from the Cluster

You can remove a node from the cluster if something is wrong with the node. However, after you remove 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 45.

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 On the Admin page, click the node you want to remove from the cluster.

4 Click **Remove from cluster**.

The Admin page 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.

3.9.3 Configuring an L4 Switch for Clustering

If you want high availability or load balancing, you must configure an L4 switch for the CloudAccess 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 CloudAccess 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, such as if a user's mobile device changes networks during a session. 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.

3.9.4 Configuring an L4 Switch for Email Proxy

CloudAccess contains an email proxy for users with Google Apps that supports three protocols: SMTP, POP3S, and IMAPS. You must configure your L4 switch to handle these protocols. Use the following high level steps to configure the protocols for your L4 switch. For more information, see your specific L4 documentation.

- "Configuring the SMTP Protocol Handler" on page 47
- "Configuring the POP Protocol Handler" on page 48
- "Configuring the IMAP Protocol Handler" on page 48

Configuring the SMTP Protocol Handler

To configure an SMTP protocol handler for your L4 switch:

1. On your L4 switch, configure a new IP group (traffic group) or use an existing group for the virtual servers in the L4 switch.

   You can use this group for all of the protocols.

2. (Optional) Create a health monitor:
   - **2a** Set the health checking for the pool to **TCP transaction monitor**.
   - **2b** Set the timeout to 30 seconds.
   - **2c** Set the health monitor to separately monitor each node.
3. Create a traffic pool for the SMTP virtual server to use:
   - **3a** Add each appliance node to the pool using the IP address with the port.

     For example: 192.168.1.14:25. The SMTP port is 25.
   - **3b** (Optional) Add the health monitor created in Step 2.
   - **3c** Select your load balancing settings.

     For example: round robin or random
   - **3d** Set the session persistence to **SSL Session ID**.

4 Create a new virtual server:

   4a Specify the protocol as SMTP and the port as 25.

   4b Use the traffic group defined in Step 1 and the pool defined in Step 3 for the virtual server.

5 Start the virtual server.

Configuring the POP Protocol Handler

To configure a POP protocol handler for your L4 switch:

1 On your L4 switch, configure a new IP group (traffic group) or use an existing group for the virtual servers in the L4 switch.

   You can use this group for all of the protocols.

2 (Optional) Create a health monitor:

   2a Set the health checking for the pool to **TCP transaction monitor**.

   2b Set the timeout to 30 seconds.

   2c Set the health monitor to separately monitor each node.

3 Create a traffic pool for the POP virtual server to use:

   3a Add each appliance node to the pool using the IP address with the port.

   For example: 192.168.1.14:995. The POP port is 995.

   3b (Optional) Add the health monitor created in Step 2.

   3c Select your load balancing settings.

   For example: round robin or random

   3d Set the session persistence to **SSL Session ID**.

4 Create a new virtual server:

   4a Specify the protocol as SSL (POP3S) and the port as 995.

   4b Use the traffic group defined in Step 1 and the pool defined in Step 3 for the virtual server.

5 Start the virtual server.

Configuring the IMAP Protocol Handler

To configure an IMAP protocol handler for your L4 switch:

1 On your L4 switch, configure a new IP group (traffic group) or use an existing group for the virtual servers in the L4 switch.

   You can use this group for all of the protocols.

2 (Optional) Create a health monitor:

   2a Set the health checking for the pool to **Connect**.

   2b Set the health monitor to separately monitor each node.

3 Create a traffic pool for the IMAP virtual server to use:

   3a Add each appliance node to the pool using the IP address with the port.

   For example: 192.168.1.14:993. The IMAP port is 993.

   3b (Optional) Add the health monitor created in Step 2.

   3c Select your load balancing settings.

For example: round robin or random.

3d Set the session persistence to **SSL Session ID**.

4 Create a new virtual server:

4a Specify the protocol as SSL (IMAPS) and the port as 993.

4b Use the traffic group defined in Step 1 and the pool defined in Step 3 for the virtual server.

5 Start the virtual server.

3.10 Configuring Integrated Windows Authentication with Kerberos

CloudAccess allows user authentication with either name and password or Integrated Windows Authentication with Kerberos if your identity source is Active Directory. If you choose to use Integrated Windows Authentication, you must configure Kerberos.

CloudAccess supports the use of only one Kerberos realm. If there are multiple Active Directory domains used as the identity source, all of the domains must use the same realm.

Use the information in the following sections to enable Kerberos authentication between Active Directory and CloudAccess.

- Section 3.10.1, "Configuring the Kerberos User in Active Directory," on page 49
- Section 3.10.2, "Configuring the Appliance to Use Integrated Windows Authentication with Kerberos," on page 50
- Section 3.10.3, "Configuring User Browsers," on page 50

3.10.1 Configuring the Kerberos User in Active Directory

To configure Kerberos on your Active Directory domain:

1 As an Administrator in Active Directory, use MMC to create a new user within the search context specified during the initialization of the appliance.

Name the new user according to the Host and DNS name of the appliance. For example, if the public DNS of the appliance is serv1.cloudaccess.com and the context that has been enabled for cloud is ou=acme corporation,dc=cloudaccess,dc=com, use the following information to create the user:

First name: serv1

User login name: HTTP/serv1.cloudaccess.com

Pre-windows logon name: serv1

Set password: Specify the desired password. For example: Passw0rd

Password never expires: Select this option.

2 Associate the new user with the service principal name.

Any domain or realm references must be uppercase.

2a On the Active Directory server, open a cmd shell.

2b At the command prompt, enter the following:

```
setspn -A HTTP/appliancepublicdns@UPN.SUFFIX newusershortname
```

For example: `setspn -A HTTP/serv1.cloudaccess.com@CLOUDACCESS.COM serv1`

2c Verify setspn by entering `setspn -L shortusername`

For example: `setspn -L serv1`

3 Generate the `keytab` file using the `ktpass` utility.

Any domain or realm references must be uppercase.

3a At the command prompt, enter the following:

```
ktpass /out filename /princ servicePrincipalName /mapuser userPrincipalName
/pass userPassword
```

For example:

```
ktpass /out nidp.keytab /princ HTTP/
serv1.cloudaccess.com@CLOUDACCESS.COM /mapuser serv1@CLOUDACCESS.COM /pass
Passw0rd
```

3b Ignore the message `Warning: pType and account type do not match`.

4 Copy the `nidp.keytab` file created in Step 3 to the browser of the client computer that you are using for administration.

3.10.2 Configuring the Appliance to Use Integrated Windows Authentication with Kerberos

The following steps enable the appliance to use Integrated Windows Authentication (IWA) with Kerberos, if your identity source is Active Directory.

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

2 Click the **Active Directory** icon in the **Identity Sources** palette, then click **Configure**. (Do not drag the icon to the **Identity Sources** panel as you would when configuring the connector for Active Directory itself. These IWA configuration options are global for all connectors for Active Directory.)

3 Select **Integrated Windows Authentication**.

4 Next to the **Keytab** field click **Browse**, then browse to and select the `nidp.keytab` file generated in "Configuring the Kerberos User in Active Directory" on page 49.

5 Click **OK** to save the changes.

6 Click **Apply** to apply the changes to the appliance.

3.10.3 Configuring User Browsers

To complete the Kerberos configuration for Active Directory, configure the user browser. For more information, see Section 8.2, "Configuring End User Browsers for Kerberos Authentication," on page 100.

3.11 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.

Use the information in the following sections to configure your system for reCAPTCHA:

3.11.1 Requirements for reCAPTCHA

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

- ❒ A CloudAccess appliance, installed and configured.
- ❒ One or more supported identity sources, with the connectors enabled and configured.

  The reCAPTCHA tool supports users from Active Directory, eDirectory, and Self-Service User Store (SSUS) identity sources. It does not support users from other types of identity sources, such as users imported from Microsoft SQL Server or Oracle Database type identity sources that use the JDBC identity source connector.

  Each identity source should be configured with an intrusion detection policy. For more information, see Section 3.11.2, "Configuring Intrusion Detection for Failed Logins," on page 51.
- ❒ A Google reCAPTCHA account, configured on the Google reCAPTCHA website. For more information, see Section 3.11.3, "Configuring a Google reCAPTCHA Account," on page 52.

3.11.2 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.

- **SSUS Lock Account After Detection:** The SSUS identity store automatically enables the Lock Account After Detection option. It allows up to 7 consecutive failed login attempts within a 30-minute interval. If the next login attempt also fails within the interval, SSUS locks the account for 15 minutes. After 15 minutes, the system automatically unlocks the account, and the user can log in using a correct user name and password. To log in before the lockout is reset, the user can contact the SSUS Helpdesk and ask the administrator to reset the password.

After you have configured intrusion detection for the supported identity sources, continue with Section 3.11.3, "Configuring a Google reCAPTCHA Account," on page 52.

3.11.3 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 3.11.4, "Configuring the reCAPTCHA Tool," on page 53.

3.11.4 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 service:

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 51.
2. Log in with an appliance administrator account to the Admin page 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.

   The Configuration window opens automatically for the initial configuration. To view or reconfigure the settings later, click the reCAPTCHA tool, then click **Configure**.
5. Configure the reCAPTCHA feature 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 3.11.3, "Configuring a Google reCAPTCHA Account," on page 52.
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.

3.12 Configuring the Time-Based One-Time Password (TOTP) Tool for Two-Factor Authentication Using Google Authenticator

The Time-Based One-Time Password (TOTP) tool in CloudAccess supports the use of one-time passwords (OTPs) for two-factor authentication of users as they access applications through CloudAccess. With two-factor authentication, users must provide two categories of authentication factors before they can access the applications. The authentication factors used by the TOTP tool are:

- **Something the user knows:** The first authentication factor requires *something the user knows*, such as the password for the user's single-sign-on user name.
- **Something the user has:** The second authentication factor requires *something the user has*, such as a mobile device running Google Authenticator to generate time-based one-time passwords.

  Google Authenticator is a free software-token app that users deploy on their mobile devices. Authenticator generates time-based OTPs for authentication, without requiring an Internet connection or cellular service.

If users construct strong passwords and protect them, one-factor authentication can be an effective measure against security breaches. Two-factor authentication provides an additional layer of security to help ensure the identity of a user and reduce the risk of unauthorized access to your applications and data. Users still enjoy the convenience of single sign-on, but the access is more secure.

Figure 3-2 *The Two-Factor Authentication Solution for CloudAccess*

The following sections describe how to set up and use TOTP for CloudAccess:

- Section 3.12.1, "Understanding One-Time Passwords," on page 55
- Section 3.12.2, "How to Use Google Authenticator for TOTP," on page 56
- Section 3.12.3, "Configuring the TOTP Tool," on page 57
- Section 3.12.4, "Registering a Mobile Device with the TOTP Tool for OTP Generation," on page 58
- Section 3.12.5, "Using Two-Factor Authentication at Login," on page 60
- Section 3.12.6, "Resetting a Device (Deregistering a Device)," on page 60

3.12.1 Understanding One-Time Passwords

The one-time password secret keys, code generation, and code verification are based on the industry standard HMAC-SHA1 token algorithm that is defined in the IETF RFC 6238 (http://datatracker.ietf.org/doc/rfc6238/). Each OTP is intended for use by only one user, is valid for a specific period of time, and becomes invalid after the user successfully logs in. It cannot be easily duplicated and reused elsewhere. The entered code is sent securely to CloudAccess through HTTPS (Secure HTTP) encryption on TCP port 443.

With time-based OTP, the TOTP validation server and software-token app use their respective system times to generate OTPs. The TOTP algorithm assumes that the system times are synchronized. To minimize time drift, you should configure the network time protocol (NTP) on the CloudAccess appliance so its clock stays accurate. If you cluster the CloudAccess appliances, ensure that the member nodes in the cluster point to the same centrally located time server. Users should synchronize the clocks on their mobile devices with their service providers' networks, which are typically aligned with atomic clocks.

Time differences between the TOTP validation server and a mobile device can result in a mismatch of the OTP, and subsequent login failure. Common causes include clock time drift, network latency, and slow data entry. To allow for time differences, the Validity Time setting allows a submitted OTP to be considered valid if it matches a server-generated OTP for any time-step that occurs in a specified validity window centered on its received timestamp, plus 30 seconds. A time-step is 30-seconds.

For the TOTP tool, the default validity time setting is 5 minutes. The validity window is 2.5 minutes before and 2.5 minutes after the password's received timestamp, plus 30 seconds. You can specify integer values from 2 to 10. Shorter validity times are considered to be more secure than longer ones.

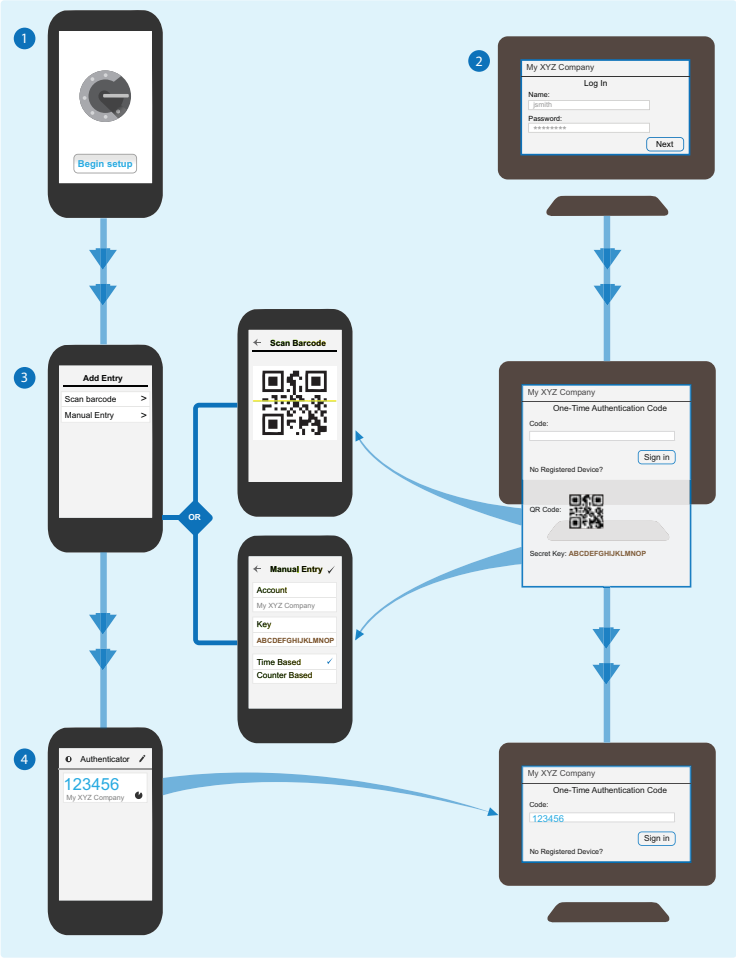
If you enable both the Google ReCAPTCHA tool and the TOTP tool in CloudAccess, ReCAPTCHA works only for the user's login password, and not for the one-time password. The ReCAPTCHA is not used if the OTP is incorrect.

3.12.2 How to Use Google Authenticator for TOTP

You can enable the TOTP validation service for one or more applications. At a user's next login, TOTP prompts the user to register a device to use for the additional authentication. If you enable all applications, the prompt occurs immediately after CloudAccess validates the user's credentials. Otherwise, the prompt occurs when the user first selects any one of the TOTP-enabled applications.

Figure 3-3 illustrates the setup for Google Authenticator on a users mobile device and the registration of the device with TOTP in CloudAccess.

Figure 3-3 *Self-Service Device Registration*



The user registers a device with CloudAccess as follows:

1. The user installs the Google Authenticator app on their mobile device.
2. On a computer, the user logs in to CloudAccess using their corporate user name and password. If the credentials are valid, CloudAccess prompts the user to register a device for one-time passwords.
3. The user registers the mobile device with their CloudAccess account.
    a. TOTP creates a secret key for the user and displays it in text and Quick Response (QR) code format in the computer web browser.

b. On the mobile device, the user starts Google Authenticator and adds an account for CloudAccess.

c. In Google Authenticator, the user scans the Quick Response (QR) code displayed on the browser, or manually enters the security key.

4. The Google Authenticator app generates a 6-digit code, and the user enters the code on the Authentication Code page.

The device registration process is not complete until the user submits a one-time authentication code that was generated using the secret key on the registration page, and the server validates it. If the submitted code does not validate, TOTP re-displays the registration page with the current secret key. The user can generate a new code on the mobile device, and then try again to authenticate. On successful authentication, TOTP stores the shared key with the user's identity information in the related identity source. The user's registered device and its authentication codes apply to all TOTP-enabled applications. Each session requires only a single successful authentication.

TOTP cancels the registration process if the user makes no attempt to register the device and discontinues the login by closing the tab or browser. The next time that the user logs in, CloudAccess generates a new secret key, and prompts the user to register a device with a new key.

For each log in to CloudAccess, the user runs the Google Authenticator app to generate a new 6-digit code for the CloudAccess account. When the app runs, it generates a new 6-digit authentication code every 30 seconds. This code is the one-time password that the user enters for two-factor authentication.

TOTP requires a newly generated authentication code at each subsequent login. If you enable all applications, TOTP prompts for the code immediately after CloudAccess verifies the user's credentials. Otherwise, the prompt occurs when the user first selects any one of the TOTP-enabled applications. The authentication automatically applies to other TOTP-enabled applications for that session.

An administrator can reset a device associated with a user account. This deregisters the device from the account, and invalidates the old key. The next time that the user logs in, CloudAccess generates a new secret key, and prompts the user to register a device with a new key.

3.12.3 Configuring the TOTP Tool

You can enable the Time-Based One-Time Password tool to require users to use two-factor authentication when logging in through CloudAccess.

To configure the TOTP service:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns_name/appliance/index.html`.
2. Drag the **TOTP Tool** icon from the **Tools** palette to the **Tools** panel.

3. Click the **TOTP** icon on the **Tools** panel, then click **Configure**.
4. (Optional) Specify the **Validity Time**.

   Specify an integer value from 2 to 10. The default value is 5. Shorter validity times are considered more secure.

5 Click the **Applications** tab, then select the check box next to one or more applications to enable them for TOTP.

   By default, no applications are enabled for TOTP.

   When a user registers an authentication device, the device and authentication codes apply to all TOTP-enabled applications.

6 Click **OK** to save the setting and enable the TOTP tool.

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

   In the Appliances pane, a green gear icon spins on top of each node until the activation is complete across all nodes in the cluster.

3.12.4 Registering a Mobile Device with the TOTP Tool for OTP Generation

After you enable the TOTP tool, users are prompted to register a device to use for the additional verification the next time they sign in to CloudAccess. Each user must register a mobile device for generating the user's one-time passwords. For the initial setup, the user should use a web browser on a computer other than the mobile device where the one-time passwords will be generated.

The One-Time Authentication code page displays a QR code and its equivalent secret key. The user deploys the Google Authenticator app on a mobile device, and sets up an account for CloudAccess by using the shared key. The user can scan the QR code or manually enter the key. When the app runs, it generates a new one-time password every 30 seconds.

Before registering a device, the following setup is required:

- ❒ The user must be an authorized user of CloudAccess with a valid user name and password.
- ❒ The user must have access to a computer running a supported web browser.

  For a list of supported web browsers, see Browsers in Table 2-2, "Product Requirements," on page 18.
- ❒ The user must use a supported mobile device.

  For a list of supported mobile device platforms, see Mobile Devices in Table 2-2, "Product Requirements," on page 18.
- ❒ The user must install the Google Authenticator app on the mobile device.

To register a mobile device for use with the TOTP tool:

1 (Conditional) If the Google Authenticator mobile app is not already installed on the mobile device, download and install it.

   1a Visit the app store for your mobile device.

   1b Search for Google Authenticator.

   1c Download and install the app.

2 From a computer that will not be used as the OTP device, access CloudAccess either directly or through a SAML2 redirect.

3 On the CloudAccess login page, enter your network user name and password (your normal identity source login credentials).

   A message displays a QR code (and its equivalent secret key) to use for the TOTP registration.

If you are not prepared to register your mobile device at this time, you can cancel the registration process by closing the tab or your browser. On your next login, CloudAccess generates a new secret key, and prompts you to register a device with a new key.

4 On your mobile device, use the Google Authenticator app to scan the displayed QR code, and register the device with CloudAccess. You can alternatively type the secret key.

   4a On your mobile device, open the Google Authenticator app.

   4b Select **Settings** > **Add an account**.

   4c Use either of the following methods to configure the account:

   - **Scan a barcode:**
     1. Select **Scan a barcode**.
     2. Use your device's camera to scan the QR code that appears on the CloudAccess One-Time Authentication Code page.
   - **Enter provided key:**
     1. Select **Time Based**.
     2. Select **Enter provided key**.
     3. Type the 16-character secret key that appears on the CloudAccess One-Time Authentication Code page. The key is case sensitive. Do not add spaces or stray characters.

   4d Specify a unique name for the account.

   4e Tap **Done**.

5 On the mobile device, view the 6-character code that Google Authenticator displays for CloudAccess. This is your OTP.

6 On the computer on the One-Time Authentication Code page, type the OTP, then click **Sign In**.

   CloudAccess confirms that the mobile device is registered, and the login is successful.

   If the code does not validate, the registration page is redisplayed with the current secret key. You can generate a new code, and try again. The code might not validate if you enter an expired code, you do not enter a code, you mistype the code, or you make an error when setting up the secret key for the account in Google Authenticator.

7 To log in to your account from the mobile device, log in to CloudAccess as described in Section 3.12.5, "Using Two-Factor Authentication at Login," on page 60.

   On successful authentication, you can access the apps icons for the authorized services and resources associated with your user identity. Access is granted only for the duration of that session.

To de-register a mobile device:

1 Access CloudAccess either directly or through a SAML2 redirect.

2 Log in and authenticate as described in Section 3.12.5, "Using Two-Factor Authentication at Login," on page 60.

3 Click the **My Devices** icon.

4 In the **Registered Devices** list, select the mobile device.

5 Click the **Delete** icon for the device.

6 In the **Unregister** Device window, click OK to confirm.

   At your next login, CloudAccess prompts you to register a device before you can access applications that require two-factor authentication.

3.12.5 Using Two-Factor Authentication at Login

When two-factor authentication is enabled for CloudAccess, a user must provide login credentials and a one-time authentication code to gain access to TOTP-enabled applications. The code is a 6-digit number generated for CloudAccess by the Google Authenticator app that is running on the user's mobile device. The user must have already registered the mobile device with CloudAccess, as described in Section 3.12.4, "Registering a Mobile Device with the TOTP Tool for OTP Generation," on page 58.

The user should enter the newly generated code as soon as possible after it appears in the Google Authenticator app. Each OTP is intended for use by only one user, is valid for 30 seconds, and becomes invalid after the user successfully logs in. Access is granted only for the duration of that session.

To log in to CloudAccess using two-factor authentication:

1. Access CloudAccess either directly or through a SAML2 redirect.
2. On the login page, enter your network user name and password (your normal identity source login credentials).

   CloudAccess verifies the credentials against a defined identity source. If all applications require two-factor authentication, the One-Time Authentication Code page appears and prompts you to enter the code. Otherwise, CloudAccess displays the page when you first click any one of the applications that require it.
3. Use Google Authenticator to generate a new one-time password, and enter the code on the CloudAccess One-Time Authentication Code page.

   If you enter the password incorrectly, you can try again with the same password until it times out. Google Authenticator generates a new OTP every 30 seconds.

   On successful authentication, you can access the apps icons for the authorized services and resources associated with your user identity. Each session requires only a single successful authentication.

3.12.6 Resetting a Device (Deregistering a Device)

Each user can register a single device to use for generating one-time passwords. Resetting a device for a user's account deregisters the user's current device. The next time the user logs in, the TOTP tool creates a new secret key for the account.

An administrator can reset a device for a user account:

- To allow the user to register a different device
- To revoke access for a registered device that is lost or stolen

Information about a user's registered device and secret key is part of the user's identity information in the identity source. This information is deleted automatically if a user's identity object is permanently deleted from the identity source. The information is stored with the user's object if the user's identity object is disabled.

If the Time-Based One-Time Password tool is disabled, CloudAccess no longer prompts the users for an OTP at login. However, information about a user's registered device and secrete key continue to be stored in the users' identity objects in the identity source. The OTPs generated for the user's CloudAccess account by the Google Authenticator app are no longer needed at login.

After a device is deregistered, the OTPs generated for the user's CloudAccess account by the Google Authenticator app are no longer valid. At the user's next login, the TOTP tool generates a new secret key for the user, and the user must register a device to work with it.

To reset (deregister) a device for a user account as an administrator user:

1. Log in with an appliance administrator account to the CloudAccess Administration Console at `https://appliance_dns_name/appliance/index.html`.
2. Click the **Devices** icon.
3. In the User field, type a few characters of the user name, and then scroll in the window to select the user identity.
4. Under **One-Time Password**, click **Reset**.

3.13 Configuring the Advanced Authentication Tool for Two-Factor Authentication Using NetIQ Advanced Authentication Framework

The Advanced Authentication tool supports the use of one-time passwords (OTPs) for two-factor authentication of users as they access applications through CloudAccess. It works with the NetIQ Advanced Authentication Framework running on a member server in a domain configured as an Active Directory identity source.

With two-factor authentication, users must provide two categories of authentication factors before they can access the applications:

- **Something the user knows:** The first authentication factor requires *something the user knows*, such as the password for the user's single-sign-on user name.
- **Something the user has:** The second authentication factor requires *something the user has*, such as a device to uniquely generate or receive one-time passwords or authentication requests that can be used only for that access moment.

Two-factor authentication provides an additional layer of security that helps ensure the identity of a user and reduce the risk of unauthorized access to your applications. Users still enjoy the convenience of single sign-on, but the access is more secure.

The Advanced Authentication tool supports four types of authentication providers for OTP in the NetIQ Advanced Authentication Framework: OATH OTP, Smartphone, SMS, and Voice Call. For a brief overview of each authentication method, see Section 3.13.2, "Understanding the Authentication Providers," on page 62.

You configure a separate instance of the tool for each authentication provider type you want users to use. For each authentication provider type, you can enable one or more applications, but they must be mutually exclusive of the applications that you enable in other instances. The applications must also be mutually exclusive of applications configured to use the Time-Based One-Time Password tool with Google Authenticator.

At a user's next login, the tool prompts the user for additional authentication, according to the authentication provider type enabled for the application. If you enable all applications for a single authentication provider type, the prompt occurs immediately after CloudAccess validates the user's credentials. Otherwise, the prompt occurs when the user first selects any one of the applications enabled for Advanced Authentication. The authentication automatically applies to all applications for that session that were also enabled for the same type of authentication provider.

For more information about using the NetIQ Advanced Authentication Framework and the supported authentication providers, see the NetIQ Advanced Authentication Framework (https://www.netiq.com/documentation/netiq-advanced-authentication-framework/) documentation website.

Use the information in the following sections to configure your system for Advanced Authentication:

- Section 3.13.1, "Requirements for Advanced Authentication," on page 62
- Section 3.13.2, "Understanding the Authentication Providers," on page 62
- Section 3.13.3, "Configuring the Advanced Authentication Tool," on page 64

3.13.1 Requirements for Advanced Authentication

Ensure that your system meets the following requirements before you configure the Advanced Authentication tool:

- ❒ A CloudAccess appliance, installed and configured.
- ❒ An Active Directory identity source, with the identity source connector enabled and configured.
- ❒ A server running NetIQ Advanced Authentication Framework that is an Active Directory member server in the same domain as the Active Directory identity source.
- ❒ The Advanced Authentication tool supports only the following authentication providers: OATH OTP, Smartphone, SMS, and Voice Call. For a brief overview of each authentication method, see Section 3.13.2, "Understanding the Authentication Providers," on page 62.

  Before you configure the Advanced Authentication tool, ensure that you install and configure the authentication providers that you want to use on the NetIQ Advanced Authentication Framework server. For more information, see the following resources:

  - *OATH Authentication Provider Installation Guide* and the *OATH Authentication Provider Configuration Guide*
  - *Smartphone Authentication Provider Installation Guide*
  - *SMS Authentication Provider Installation Guide*
  - *Voice Call Server Authentication Provider Installation Guide*

  For SMS and Voice Call, the user's telephone number that will be used for authentication should be specified in the user's properties in Active Directory.
- ❒ The users in the domain must use the NetIQ Advanced Authentication Framework client or web user interface to enroll or re-enroll for the authenticator providers that you want them to use.
- ❒ Identify the type of authentication provider that you want to use for each of your destination applications.

3.13.2 Understanding the Authentication Providers

Use the information in this section to understand the supported authentication providers for NetIQ Advanced Authentication Framework.

- "OATH OTP" on page 63
- "Smartphone" on page 63
- "SMS" on page 63
- "Voice Call" on page 64

OATH OTP

For the OATH OTP authentication provider, the user enters a 6-digit code as a one-time password on the authentication page. The user commonly generates the time-based one-time passwords (TOTPs) with an OATH TOTP-compliant hardware token (key fob or card) that is associated with the user. A user can alternatively generate TOTPs with the NetIQ Smartphone Authenticator app running on a mobile device. If the code is valid, the user can access the application.

To use software tokens, the user downloads and installs the NetIQ Smartphone Authenticator app on their mobile device. Using the NetIQ Advanced Authentication Framework client or web service, the user must enroll the device for the OATH OTP authentication provider by manually entering a 40-hex digits random code as the shared secret key, or by scanning its related QR (quick response) code. In OATH OTP mode, the Smartphone Authenticator app generates the 6-digit code, without requiring an Internet connection or cellular service.

For more information about supported devices and platforms, see the NetIQ Advanced Authentication Framework (https://www.netiq.com/documentation/netiq-advanced-authentication-framework/) documentation for the OATH OTP authentication provider.

Smartphone

For the Smartphone authentication provider, the user receives a push notification message in the Smartphone Authenticator app running on a mobile device, and can accept or reject the authentication request. If the user accepts the request within the valid interval, the user can access the application.

The user downloads and installs the NetIQ Smartphone Authenticator app on their mobile device. Using the NetIQ Advanced Authentication Framework client or web service, the user must enroll the device for the Smartphone authentication provider by scanning a QR Code. In Smartphone mode, the Smartphone Authenticator app requires an Internet connection or cellular service for the mobile device to receive the push notification message.

For more information about supported devices and platforms, see the NetIQ Advanced Authentication Framework (https://www.netiq.com/documentation/netiq-advanced-authentication-framework/) documentation for the Smartphone authentication provider.

SMS

The SMS authentication provider generates a 6-digit software token for the user, and sends it in an SMS text message to the mobile phone number that is stored in the user's properties in Active Directory. The user's phone receives and displays the message. The user enters the code on the authentication page. If the code is valid, the user can access the application.

You can configure any Internet gateway that supports POST messages to deliver the SMS messages, such as Twilio or Messagebird. To receive the SMS message, the mobile device must have an Internet connection or cellular service, as well as a text-messaging plan. The user's properties in Active Directory must contain a mobile phone number.

For more information, see the NetIQ Advanced Authentication Framework (https://www.netiq.com/documentation/netiq-advanced-authentication-framework/) documentation for the SMS authentication provider.

Voice Call

The Voice Call authentication provider calls the mobile phone number that is stored in the user's properties in Active Directory. The user accepts the call, then enters their personal PIN number to verify the authentication. If the PIN is valid, the user can access the application.

Using the NetIQ Advanced Authentication Framework client or web service, the user must enroll for the Voice Call authentication provider by creating a dedicated unique PIN code to use when confirming an authentication request. The Advanced Authentication Framework administrator configures the required length of the PIN code.

To receive the call, the mobile device must have an Internet connection or cellular service, as well as a voice calling plan. The user's properties in Active Directory must contain a mobile phone number. Because the Voice Call Server works with Twilio Voice, the phone number must be in a country supported by the Twilio Voice platform.

For more information, see the NetIQ Advanced Authentication Framework (https://www.netiq.com/documentation/netiq-advanced-authentication-framework/) documentation for the Voice Call authentication provider.

3.13.3 Configuring the Advanced Authentication Tool

Before you configure the Advanced Authentication tool, ensure that your setup meets the requirements described in Section 3.13.1, "Requirements for Advanced Authentication," on page 62.

To configure the Advanced Authentication tool:

1. Log in with an appliance administrator account to the Admin page at

   `https://appliance_dns_name/appliance/index.html`
2. In the Identity Sources panel, verify that you have configured one Active Directory identity source for a domain where a member server is running NetIQ Advanced Authentication Framework.
3. Drag and drop the Advanced Authentication tool from the **Tools** palette to the **Tools** panel.

   The Configuration window opens automatically for the initial configuration. To view or reconfigure the settings later, click the Advanced Authentication tool, then click **Configure**.
4. Configure the Advanced Authentication feature:

   Authentication type: Select the type of authentication provider that you want to enable for the specified server running the NetIQ Advanced Authentication Framework. For more information, see Section 3.13.2, "Understanding the Authentication Providers," on page 62.

   NAAF host name/port: Specify the hostname of the Active Directory member server running NetIQ Advanced Authentication Framework. The default port number is 8232.
5. Click the **Applications** tab, then select the check box next to one or more applications that require the specification authentication provider.

   You can enable one or more applications for the specified type of authentication provider. However, you must assign each application to only one type of authentication provider.
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.

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

The CloudAccess 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, CloudAccess provides the Authentication Filter tool.

The Authentication Filter integrates with the CloudAccess 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, CloudAccess 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.

For information about creating custom authentication scripts to use with the Authentication Filter, see the *Technical Reference: Authentication Filter for NetIQ CloudAccess*.

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

Before you enable the Authentication Filter, ensure that your enterprise environment meets the following requirements:

- A CloudAccess 2.1 appliance, installed and configured
- The Authentication Filter supports only applications and devices 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 and devices 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 use the OAuth Service Provider connector.
  - Mobile devices use a token-based protocol, which reestablishes the session for each transmission. Thus, there is no session attribute cache for mobile sessions, whether the connector's protocol is session-based or sessionless.
- 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. The ExtAPI server is a web server that supports the programming language for the script file you create.
- 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 CloudAccess. The ExtAPI script should redirect the authentication session to the URL for this file. The ExtUI server is a web server that supports the programming language for the script file you create.
  - 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 CloudAccess administration console at `https://appliance_dns/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 on the main Admin page.

   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. On the Admin page, 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.

3.15 Configuring CloudAccess to Forward Events to a Syslog Server

You can configure CloudAccess to forward various events to a syslog server. Event types that are forwarded include Login, Logout, Register Device, Un-register Device, and Failed Login.

To configure CloudAccess to forward events to a syslog server:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns_name/appliance/index.html`.
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. On the Admin page, click **Apply** to activate event forwarding.

4 Setting Up and Managing MobileAccess

Administrators can now enable user access to SSO, proxy, and SaaS applications from supported mobile devices. For more information about supported mobile devices, see Section 2.2, “Product Requirements,” on page 18.

4.1 Introduction to MobileAccess

MobileAccess features are available for all application connectors that CloudAccess supports. Configurable options in MobileAccess include the following:

- Which applications users should be able to access.
- Whether users can access an application through a desktop browser or a mobile device, or both.
- The preferred viewer for the application on the mobile device.
- Whether users are required to provide a PIN to use the MobileAccess app on their mobile device, and if so, whether they are required to re-enter the PIN after a period of inactivity.

The MobileAccess app that end users install on their mobile devices enables them to access corporate and SaaS applications from those devices. Administrators can also make the MobileAccess app available to users in a private corporate store. Once users have installed the app and registered their device, they can access assigned applications using their corporate user name and password.

Administrators can unregister user mobile devices in the administration console. So, if a registered mobile device is lost or stolen, or an employee leaves the company, you can ensure that unauthorized users cannot access corporate resources. Users can also unregister their own mobile devices if necessary, either from their device or from the appliance administration console.

4.2 Installing and Configuring the MobileAccess Appliance

The prerequisites for the MobileAccess appliance, and the steps for installing and configuring the appliance, are the same as those for CloudAccess.

NOTE: Whether you have a full CloudAccess license or a MobileAccess-only license, you need to install only one appliance to get all features. For more information about product licensing, see Section 1.5, "Understanding Product Licensing," on page 16.

For more information, see the following sections:

- Chapter 2, "Installing the Appliance," on page 17
- Chapter 3, "Configuring the Appliance," on page 31

After you have installed and configured the appliance, you can configure the MobileAccess tool. For more information, see Section 4.3, "Configuring the MobileAccess Tool on the Appliance," on page 68.

4.3 Configuring the MobileAccess Tool on the Appliance

Once you have installed and configured the appliance, you can configure the MobileAccess tool.

To configure the MobileAccess tool:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns_name/appliance/index.html`.
2. Drag the MobileAccess icon from the **Tools** palette to the **Tools** panel.
3. Click the MobileAccess icon on the **Tools** panel and then click **Configure**.
4. In the **Display name** field on the Mobile Application Access window, type your company name. This name appears in the bar at the top of the MobileAccess app window on users' mobile devices.
5. In the **Prompt for Password Re-authentication in x Days** field, specify how long users can continue to use an authenticated password on mobile devices before re-authentication is required.
6. (Optional) On the **PIN Required** bar, specify whether users must set a PIN for the MobileAccess app on their mobile devices, and whether they must re-enter the PIN after a period of inactivity. You can change this requirement at any time. For more information, see Section 4.7, "Understanding the MobileAccess PIN," on page 74.
7. Click **OK**.
8. Click the **Apply** button on the Admin page.
9. Wait for the apply operation to finish. (The gear stops spinning on the appliance when the operation has finished.)
10. Continue with Section 4.4, "Replacing the Default Certificate on the Appliance," on page 69.

4.4 Replacing the Default Certificate on the Appliance

You must change the default certificate that comes with the appliance before you can successfully register mobile devices. For security reasons that are well-documented, as well as for administrator and user convenience, NetIQ highly recommends that you change the default certificate on the appliance to a well-known Certificate Authority signed certificate. For more information, see Section 3.5, "Changing the Certificates on the Appliance," on page 35.

Before you change the certificate on the appliance, ensure that your environment meets the following requirements:

- ❒ The appliance must be installed and running with a DNS entry that points to it.
- ❒ The certificate must be at least 2k key size (4k preferably) using SHA256.
- ❒ The certificate must be signed by a Certificate Authority, preferably a well-known Certificate Authority. If you choose to use a self-signed certificate, it must be flagged as a certificate authority.

If you use a self-signed or non-public CA-signed certificate, users must also install the certificate on their mobile devices. For more information, see the following topics:

- Section 4.4.1, "Generating a Self-Signed Certificate," on page 69
- Section 4.4.2, "Installing a Self-Signed Certificate on the Mobile Device," on page 70

4.4.1 Generating a Self-Signed Certificate

You can generate a self-signed certificate and use it on the appliance, but if you do so, you must also perform the steps in Section 4.4.2, "Installing a Self-Signed Certificate on the Mobile Device," on page 70 to ensure that you can successfully register mobile devices. You can run the Java 7 keytool on a computer other than the appliance to generate the certificate.

To generate a self-signed certificate:

1. Using the Java 7 keytool, use the following commands replacing *name* and *appliance_dns_name*:

   ```
   keytool -genkeypair -keystore name.p12 -storepass changeit -sigalg
   SHA256withRSA -keyalg RSA -keysize 4096 -dname "CN=appliance_dns_name" -
   validity 365 -storetype pkcs12 -ext bc=ca:true
   ```

   name can be anything you want, as long as it is the same between the two commands, and you can find it when you want to upload it.

   appliance_dns_name must be the DNS name of the appliance.

   The output of this command is a `.p12` format file. You can use this file to replace the default certificate on the appliance. (Use the password of `changeit` when the administration console prompts for it.) For more information, see Section 3.5, "Changing the Certificates on the Appliance," on page 35.

2. To get the public certificate from that keyfile (which you will use when you perform the procedure in Section 4.4.2, "Installing a Self-Signed Certificate on the Mobile Device," on page 70) use the following command, replacing *name* with the same value from above:

   ```
   keytool -export -keystore name.p12 -storetype pkcs12 -alias mykey -file
   name.cer -storepass changeit
   ```

   The output of this command is a *name*`.cer` file that you can use later.

4.4.2 Installing a Self-Signed Certificate on the Mobile Device

This procedure is required only if you used the commands in Section 4.4, "Replacing the Default Certificate on the Appliance," on page 69 to generate the certificate. If you are using a certificate signed by a well-known Certificate Authority, you can skip this section.

To install a self-signed certificate on the mobile device:

1. Take the *name*.cer file that you generated in Section 4.4, "Replacing the Default Certificate on the Appliance," on page 69 and email it to the user who has an email account configured on the mobile device. Alternatively, you could put it on a web or FTP site that is accessible from the mobile device.
2. Open the email (or web/FTP site) on the mobile device and tap the certificate attachment.
3. In the Install Profile window, tap **Install**.
4. Read the warning and then tap **Install**.
5. Verify that the certificate says "Trusted" with a green check mark in the Profile Installed window.
6. (Conditional) If the certificate is not trusted, something is wrong with the certificate and the MobileAccess application will not work. Go back and try to generate the certificate again.
7. Tap **Done**.
8. Verify that this procedure worked by entering the appliance DNS name in the Safari address bar and ensuring that there is no warning about an untrusted certificate.

   NOTE: This step does not currently work in Chrome.

This certificate is installed in the Settings > General > Profiles page on the mobile device and can be removed from that location on the device.

The server certificate and the trusted root certificate need to be at least 2k in size.

Once you have replaced the default certificate on the appliance, you can continue with MobileAccess installation and configuration. For more information, see Section 4.5, "Installing MobileAccess on a Mobile Device," on page 70.

4.5 Installing MobileAccess on a Mobile Device

Once an administrator has enabled and configured the MobileAccess tool in the administration console, users must install the MobileAccess app on supported mobile devices before they can access SaaS, SSO, or proxy applications that have been configured for mobile access. If users do not yet have the MobileAccess app installed, they are prompted to do so and redirected to the App Store. Access to the administration console from mobile devices is not supported.

To install the MobileAccess app on a mobile device:

1. Access the App Store on the mobile device.
2. Search for the NetIQ MobileAccess app.
3. Tap **Install**.
4. Continue with Section 4.6, "Registering a Mobile Device with the Appliance," on page 71.

4.6 Registering a Mobile Device with the Appliance

Users can install the NetIQ MobileAccess app on a mobile device to access the single sign-on services of MobileAccess providers and CloudAccess providers. A user can register a device with multiple providers by setting up separate accounts for each one. If a user registers a device with multiple providers, the user must select the account to use for a session from the **Accounts > Providers** list. By default, the app connects the user to the first provider in the list.

Before users can register their mobile device with the appliance, the following prerequisites must be met:

- A MobileAccess appliance or a CloudAccess appliance, installed and configured.
- The MobileAccess tool, enabled and configured on the appliance.
- A signing certificate configured on the appliance.
- Applications, configured and entitlements are configured by mapping authorizations for applications to roles (groups) in the identity source.
- The MobileAccess app, installed by users on their mobile devices. During registration, the mobile device should be connected to a network that does not use HTTP proxy.

4.6.1 iOS Devices

To register a mobile device using a link from the appliance administrator:

1. The administrator sends users an email with a link for the CloudAccess appliance. The link looks like this:

   `comnetiqauth://x-callback-url/register?providerUrl=https://`*`appliance_dns_name`*`/`
2. The user opens the email from the mobile device.
3. The user taps the link.

   The link launches the application with the **Provider** value filled in.
4. The user taps **SignIn** to begin the registration process.
5. On the CloudAccess login page, the user types their corporate credentials for the account, and taps **Sign in**.
6. (Conditional) If the administrator has specified that a PIN is required for the MobileAccess app, the user creates a PIN to be entered when the app launches.

   The user's mobile device is registered.

To register a mobile device manually:

1. The administrator provides users the login URL for the CloudAccess appliance. For example:

   `https://`*`appliance_dns_name`*
2. The user launches the MobileAccess app on their mobile device.
3. The user taps **Accounts**, then taps **Plus** (**+**) to add a new account.
4. The user types the **Provider URL** for the account, then taps **SignIn** to begin the registration process.
5. On the CloudAccess login page, the user types their corporate credentials for the account, and taps **Sign in**.

6 (Conditional) If the administrator has specified that a PIN is required for the MobileAccess app, the user creates a PIN to be entered when the app launches.

The user's mobile device is registered.

To verify that the device is registered with the appliance:

1 The user taps **Accounts** at the bottom of the app window.

2 The user can verify that the device is listed under **Devices**, along with the time of registration.

The device name is the name that is set on the **Settings > General > About** window of the mobile device. Users can change this name, but it is not configurable by the administrator of the CloudAccess appliance.

Tapping the **All Apps** icon displays the icons for configured applications. This page is empty until the administrator configures application connectors to be accessible from mobile devices.

Tapping the **Favorites** icon displays the icons for apps that the user chooses as their favorites. This page is empty until the user adds apps from the All Apps page to the Favorites page.

To add an app to Favorites:

1 On the All Apps page, long-press any app until all of the apps begin to shake.

2 Select the **X** on an app to add it to **Favorites**.

3 Tap **Home** to end the selection process.

After the user adds apps to **Favorites**, MobileAccess opens to the Favorites page. The user can view all applications by tapping **All Apps**.

To deregister a mobile device from the appliance:

1 The user taps **Accounts** at the bottom of the app window.

2 Under **Devices**, the user swipes left on the device name to expose the **Delete** option.

3 The user taps **Delete**.

The user's mobile device is deregistered.

4.6.2 Android Devices

To register a mobile device using the app UI:

1 The administrator provides users the login URL for the CloudAccess appliance. For example:

`https://appliance_dns_name`

2 The user launches the MobileAccess app on their mobile device.

3 If this is the first time the user opens the app, it presents the MobileAccess License Agreement. The user reads the agreement and taps **Accept** to continue.

4 The user taps the **Tools** icon, then taps **Accounts > Add Accounts**.

5 The user types the DNS name or URL for the account, then taps **Sign in** to begin the registration process.

6 On the CloudAccess login page, the user types their corporate credentials for the account, and taps **Sign in**.

7. (Conditional) If the administrator has specified that a PIN is required for the MobileAccess app, the user creates a PIN to be entered when the app launches.

   The user's mobile device is registered.

To register a mobile device using the device settings:

1. The administrator provides users the login URL for the CloudAccess appliance. For example:

   `https://appliance_dns_name`

2. The user launches the **Settings** tool on their mobile device.
3. The user taps **Add Account**.
4. In the list of installed apps, the user taps **MobileAccess**.
5. If this is the first time the user opens the app, it presents the MobileAccess License Agreement. The user reads the agreement and taps **Accept** to continue.
6. The user types the DNS name or URL for the account, then taps **Register** to begin the registration process.
7. On the CloudAccess login page, the user types their corporate credentials for the account, and taps **Sign in**.
8. (Conditional) If the administrator has specified that a PIN is required for the MobileAccess app, the user creates a PIN to be entered when the app launches.

   The user's mobile device is registered. The device opens to the landing page for the provider. This page is empty until the administrator configures application connectors to be accessible from mobile devices.

To verify that the device is registered with the appliance:

1. The user taps the Tools icon to view the Settings page.
2. The user taps **Manage Devices**.
3. The user can verify that the device is listed under **Devices**, along with the time of registration.

   The device name is the name that is set on the **Settings > General > About** window of the mobile device. Users can change this name, but it is not configurable by the administrator of the CloudAccess appliance.

To deregister a mobile device from the appliance using the app interface:

1. The user taps the **Tools** icon to view the Settings page.
2. Under **Accounts**, the user taps **Remove account:** *appliance_dns_name*.

   The user's mobile device is deregistered.

To deregister a mobile device from the appliance using device settings:

1. The user launches the **Settings** tool on their mobile device.
2. Under **Accounts**, the user taps **MobileAccess**.
3. The user taps the menu, then taps **Remove Account**.

   The user's mobile device is deregistered.

4.7 Understanding the MobileAccess PIN

MobileAccess administrators can require users to set a PIN on their mobile devices as a security measure to prevent unauthorized users from accessing protected resources through the MobileAccess app. Administrators can also specify whether users must re-enter the PIN after a period of inactivity on the device.

Users must install the MobileAccess app on the mobile device before they can set the PIN. If a PIN is required, the MobileAccess app prompts users to set the PIN the first time they open the app. Otherwise, users can set, change, or remove the PIN any time by accessing the Settings page from the MobileAccess app.

NOTE: The MobileAccess PIN is unrelated to the built-in device passcode, which is designed to protect other resources on the mobile device.

Even if the administrator does not require users to set a PIN, users can optionally set a PIN on their device. The PIN can be different for each mobile device the user registers. The PIN is not stored anywhere other than on the device itself.

Administrators can change the **PIN Required** setting any time in the administration console. If the administrator specifies that a PIN is required after a mobile device has already been registered, the next time the user launches the MobileAccess app on the mobile device, MobileAccess prompts the user to set a PIN. The app then prompts the user for that PIN each subsequent time the user accesses the app. If the administrator initially requires users to set a PIN and then changes that requirement, users can remove the PIN from their device. However, MobileAccess does not notify users if a PIN is no longer required.

Whether the MobileAccess administrator requires users to set a PIN or a user chooses to set a PIN, by default users can enter their PIN incorrectly five times. On the fifth attempt, the application unregisters the mobile device and removes the current PIN. The user must then reregister the device and reset the PIN. For more information, see Section 4.6, “Registering a Mobile Device with the Appliance,” on page 71.

4.8 Managing Mobile Devices

Administrators who have the Device Administrator role can manage and unregister user devices in the appliance administration console. So, if a registered mobile device is lost or stolen, or an employee leaves the company, you can ensure that unauthorized users cannot access corporate resources.

Users can also unregister their own mobile devices, either from their device or from the administration console. A mobile device that has previously been unregistered can be reregistered by the same user. However, for a different user to use the unregistered mobile device, the user must delete and reinstall the MobileAccess app on the device before reregistering the device.

Use the information in the following sections to help you manage mobile devices:

4.8.1 Unregistering Mobile Devices from the Administration Console

The Devices page lists the devices for the logged-in user by default. If you are logged in with an account that has the Device Administrator role assigned, you have the option to search for and unregister devices that are registered to other users. If you log in with a regular user account, you can view and manage only your own registered devices.

To unregister mobile devices from the administration console as a Device Administrator user:

1. Log in to the Admin page of the console at `https://appliance_dns_name/appliance/index.html`.
2. Click **Devices** at the top of the page.
3. (Conditional) If you want to search for the devices belonging to a particular user, enter the user name in the **User** field.
4. Click the trash can icon next to the device you want to unregister, then click **OK** on the confirmation message.

To unregister mobile devices from the Devices page as a regular user:

1. Browse to `https://appliance_dns_name/appliance/Devices.html`.
2. Enter your login credentials when prompted.
3. Click the trash can icon next to the device you want to unregister, then click **OK** on the confirmation message.

Once a mobile device has been unregistered, the device can be registered to a new user. However, the MobileAccess app on the device must first be deleted and reinstalled. For more information, see Section 4.8.3, "Deleting and Reinstalling the MobileAccess App on a Device," on page 76.

4.8.2 Unregistering a Mobile Device from the Device

Users who have previously registered a mobile device can unregister the device if necessary.

To unregister a mobile device from the device:

1. The user launches the MobileAccess app on the device.
2. (Conditional) If a PIN has been set up, the user enters the correct PIN when prompted.
3. The user taps the **Settings** option at the bottom of the application.
4. The user taps the **Unregister** button.

   The device is now unregistered.
5. (Conditional) If the device is going to be reregistered to a different user, the user should clear browser cookies on the device before the device is reregistered.

NOTE: Users can uninstall the MobileAccess app on a mobile device once the device has been unregistered. However, if the MobileAccess app is uninstalled without the device first being unregistered, the device continues to appear on the Devices page of the administration console. The administrator or user can delete the device from the Devices page.

4.8.3 Deleting and Reinstalling the MobileAccess App on a Device

Once a mobile device has been unregistered, the MobileAccess app on the device must be deleted and reinstalled before a different user can reregister the device.

1. Follow Apple's instructions to uninstall the MobileAccess app at the following web page:

   (http://www.apple.com/support/iphone/assistant/application/#section_5)

2. Reinstall the MobileAccess app. For more information, see Section 4.5, "Installing MobileAccess on a Mobile Device," on page 70.

5 Configuring Connectors

CloudAccess provides multiple connectors to SaaS applications. The connector for Google Apps for Business, the connector for Salesforce, and the connector for Microsoft Office 365 enable both account provisioning and single sign-on (SSO). The other available connectors, which are downloadable from NetIQ Downloads (https://dl.netiq.com/), provide only single sign-on capability.

The connectors for Google Apps and Salesforce are embedded in the appliance and are visible on the Admin page of the administration console as soon as you have initialized the appliance. The connector for Office 365 is included with the CloudAccess appliance. However, the administration console displays the connector only after you have installed the connector on the Windows server.

IMPORTANT: The connectors for Google Apps, Salesforce, and Office 365 are CloudAccess-only features and are not included in the MobileAccess-only license. For more information about product licensing, see Section 1.5, "Understanding Product Licensing," on page 16.

CloudAccess also ships with the connector for NetIQ Access Manager, the connector for Bookmarks, the connector for OAuth2 Resources, and the connector for Simple Proxy.

For more information, see the *NetIQ® CloudAccess Connectors Guide*.

5.1 Overview of CloudAccess Connectors

CloudAccess uses connectors to provide single sign-on (SSO) access for users to web resources through CloudAccess. CloudAccess authenticates the users against your identity sources. When the user accesses the link for an application through CloudAccess, CloudAccess shares the authenticated user's identity information with the destination application to establish the user's session. Each user can access only the links they are authorized to use, according to the entitlements you set for each application.

5.1.1 Understanding Single Sign-On Methods

CloudAccess supports single-sign for a variety of web services and applications that have different authentication requirements. The method used for single sign-on depends on the security requirements and capabilities of each destination resource.

Federated Single Sign-On with SAML 2.0 or WS-Federation

Federated single sign-on relies on a trust relationship between an identity provider and a service provider to give a user access to a protected web service or application through CloudAccess. Open standards for federation include SAML 2.0 (Security Assertion Markup Language), WS-Federation (Web Services Federation), and SAML 2.0 Inbound. They provide a vender-neutral means of exchanging user identity, authentication, and attribute information. The service provider trusts the identity provider to validate the user's authentication credentials, and to send identity information about the authenticated user. The service provider accepts the data and uses it to give the user access to the destination service or application. This data exchange is transparent for the user. It allows the user to access the web service or application without providing an additional password.

The following describes the SSO experience for trusted access to an application through CloudAccess:

1. The user provides login credentials directly to CloudAccess, such as their corporate user name and password.
2. CloudAccess authenticates the user's credentials against the identity sources.
3. CloudAccess presents the landing page to the user with links to applications that the user is entitled to use.
4. When a user clicks an application's link, as the identity provider, CloudAccess produces an authentication assertion or token for the service provider that contains the identity attributes needed for the user request.
5. The service provider consumes the assertion or token to establish a security context for the user.
6. The service provider validates the assertion and authorizes the resource request.
7. The service provider establishes a session with the user.

CloudAccess can also provide authentication when the user initiates access to the application from the service provider.

The following describes the SSO experience for trusted access to an application initiated from the service provider:

1. The user attempts to log in to application.
2. The login is redirected to CloudAccess.
3. CloudAccess prompts the user for the user name and password. Or, if Kerberos is configured, CloudAccess performs seamless authentication.
4. CloudAccess verifies the user name and password using the identity sources. Or, if Kerberos is configured, CloudAccess validates the Kerberos token.

5. CloudAccess provides an assertion to application service provider.
6. The service provider validates the assertion and allows the user to access the application.

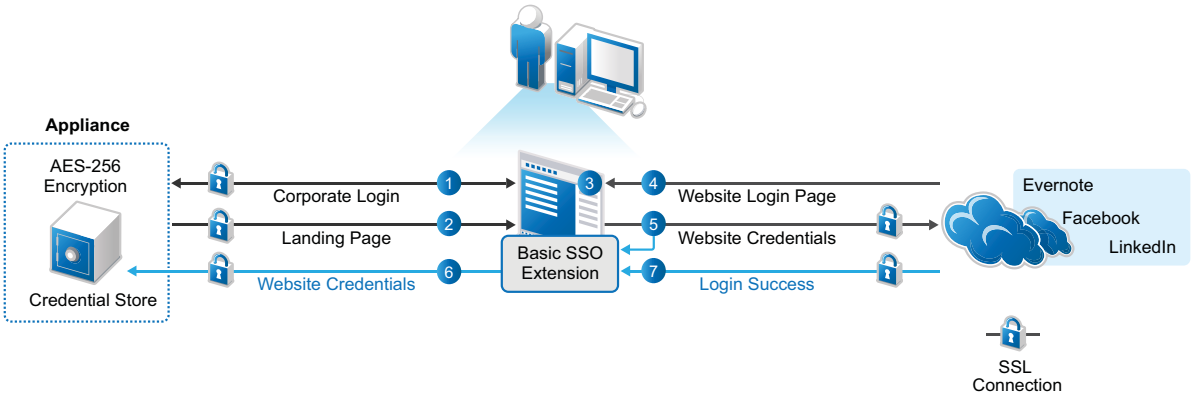
Basic Single Sign-On

Basic single sign-on provides an internal credentials store where users can save their credentials for third-party websites that require a password be sent at login. The destination website's login page must use HTML Forms as the main point of interaction with the user. A user typically has a site-specific user name and password for each destination website. CloudAccess stores the user's credentials for each site in AES-256 encrypted format. After a user authenticates to CloudAccess, the user can access a website without manually re-entering the user's credentials for the site.

Basic SSO connectors work with the Basic SSO extension for the Chrome browser running on the user's computer to securely collect, store, retrieve, and replay the user credentials for a destination website. Users must log in to the website once in order for the extension to capture and store the credentials in the CloudAccess credential store. The user can choose whether to store the credentials for each destination website. If the user does not allow credentials to be saved for a website, the user must enter the site's credentials for each session.

Figure 5-1 depicts the user experience when the user clicks the appmark for a Basic SSO application.

Figure 5-1 *User's First-Time Login to the Website with Basic SSO*



The following describes the experience for Basic SSO the first time the user accesses the app:

1. In a Chrome browser, the user logs in to the CloudAccess login page using their corporate credentials.
2. The user sees the available applications on the landing page.
3. The user clicks the appropriate application icon.

   If the Basic SSO extension for the Chrome browser is not installed on the computer:

   a. The connector prompts the user to install the Basic SSO extension.
   b. The user accepts the prompt, and the appliance opens the Google Play Store in a new tab.
   c. The user installs the Basic SSO extension, then closes the Google Play Store tab to continue.
   d. The user returns to the landing page and clicks the appropriate application icon again.
4. A new tab opens for the login page of the application.
5. The user enters their user name and password for the destination website.

   The user must enter this separate user name and password once.

6. The extension asks if the user wants the credentials to be saved by CloudAccess, and the user allows the credentials to be saved.
    a. The extension captures the user name and password, and sends them to CloudAccess over an SSL connection.

       The extension obfuscates the user name and password with Base64 encoding before transmission.

    b. CloudAccess encrypts the site-specific credentials with AES-256 encryption, and then stores the encrypted data in the credential store that is part of the appliance.

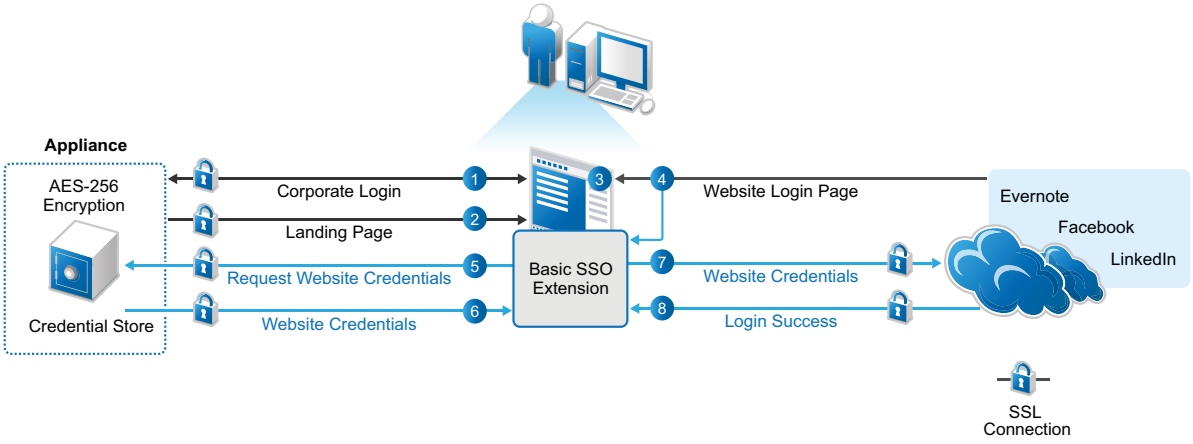
       The appliance encrypts the user name and password with an encryption key that is unique per user.
7. The website returns a success or failure indicator for the login.

   If the login succeeds, the browser opens to the application's website over an SSL connection.

   If the login fails, the browser returns the user to the website's login page to try again, and the extension requests that CloudAccess remove the saved credentials.

After the user allows the password to be stored securely, the user experiences single-sign-on access to the application in subsequent sessions. Figure 5-2 depicts the user experience when the user clicks the appmark for a Basic SSO application and the user's credentials are available in the credentials store.

Figure 5-2 *User's Single Sign-On Access to a Website with Basic SSO*



The following describes the experience for Basic SSO after the user stores credentials:

1. The user logs in to the CloudAccess login page using their corporate credentials.
2. The user sees the available applications on the landing page.
3. The user clicks the appropriate application icon.
4. A new tab opens for the login page of the application.
5. The Basic SSO extension requests that CloudAccess retrieve the user's user name and password for the site from the credential store.
6. CloudAccess retrieves the site-specific encrypted credentials from the credential store, decrypts them, and then sends the user name and password to the application's website over an SSL connection.

   CloudAccess obfuscates the user name and password with Base64 encoding before transmission.
7. CloudAccess logs in the user to the application's website. To the user, it appears as a single sign-on experience.

If the user changes their login credentials for the destination website, the user will be prompted to log in again and the new credentials will be stored using the same process as for the initial setup.

8. The website returns a success indicator for the login, and the browser opens to the application's website over an SSL connection.

OAuth 2.0 Single Sign-On

OAuth 2.0 single sign-on provides simple authenticated access to a protected web service through CloudAccess. CloudAccess behaves as an OAuth 2.0 Authorization Server and Resource Server to provide user authentication and all OAuth2 token creation and validation for access. It uses the Authorization Code flow as detailed in the *OAuth 2.0 Authorization Framework (IETF RFC 6749)* (http://tools.ietf.org/html/rfc6749#section-4.1) document.

CloudAccess supports OAuth 2.0 access in service-provider mode. End users can access the protected resource by browsing to the URL of the OAuth client application. For example, the user can enter the URL directly into the browser and be redirected to log in to CloudAccess, or they can use a bookmark or the landing page appmark after logging in to CloudAccess.

The following describes the experience for OAuth 2.0 access to an application by browsing to the URL:

1. The user accesses the protected resource by entering the URL directly in the browser.
2. The user is redirected to the CloudAccess login page.
3. The user provides login credentials to CloudAccess, such as their corporate user name and password.
4. CloudAccess authenticates the user's credentials against the identity sources.
5. CloudAccess validates the OAuth2 token for the client.
6. The user gains access to the resource.

The following describes the experience for OAuth 2.0 access to an application through CloudAccess:

1. The user provides login credentials directly to CloudAccess, such as their corporate user name and password.
2. CloudAccess authenticates the user's credentials against the identity sources.
3. CloudAccess presents the landing page to the user with links to applications that the user is entitled to use.
4. The user clicks the bookmark or the landing page appmark for the application.
5. CloudAccess validates the OAuth2 token for the client.
6. The user gains access to the resource.

Simple Proxy Single Sign-On

Simple proxy single sign-on provides reverse proxy access to your enterprise web service through CloudAccess. 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 HTTP 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. This proxy solution cannot inject the password. It does not support site redirects.

The following describes the experience for simple proxy access to a web service through CloudAccess:

1. The user provides login credentials directly to CloudAccess, such as their corporate user name and password.
2. CloudAccess authenticates the user's credentials against the identity sources.
3. CloudAccess presents the landing page to the user with links to applications that the user is entitled to use.
4. The user clicks the appmark for the application.
5. (Conditional) CloudAccess sends identity information about the user in query strings and headers.
6. The website validates the resource request.
7. The user gains access to the resource.

Bookmarks

In CloudAccess, you can create bookmarks to web applications through CloudAccess that do not require additional passwords. The bookmarks are accessible from the browser landing page or directly from the MobileAccess app on users' mobile devices.

The following describes the experience for bookmark access to a web application through CloudAccess:

1. The user provides login credentials directly to CloudAccess, such as their corporate user name and password.
2. CloudAccess authenticates the user's credentials against the identity sources.
3. CloudAccess presents the landing page to the user with links to applications that the user is entitled to use.
4. The user clicks the appmark for the bookmark.
5. The user gains access to the resource.

5.1.2 Connectors for Federated Single Sign-On and Provisioning

CloudAccess provides three connectors that enable federated single sign-on and logout as well as account provisioning. The connectors ship with the appliance. You can use these connectors if you have a CloudAccess license as well as an account with the destination service.

- "Connector for Google Apps for Business (SAML 2.0)"
- "Connector for Microsoft Office 365 (SAML 2.0 or WS-Federation)"
- "Connector for Salesforce (SAML 2.0)"

After you initialize the appliance, the connectors for Google Apps and Salesforce are automatically visible in the Applications palette on the Admin page of the administration console. However, the connector for Office 365 is not visible in the palette until you install the connector on the Windows Management Server.

Provisioning is available for users in your corporate identity sources for Active Directory, eDirectory, and JDBC. You must map authorizations for the appropriate roles (groups) to enable their entitlements to the applications. Users must log in with a corporate identity in order to access their provisioned account.

5.1.3 Connectors for Federated Single Sign-On

CloudAccess provides additional connectors that you can use for federated single sign-on to web services and applications through CloudAccess. The connectors support either the SAML 2.0 protocol or the WS-Federation protocol.

The connector for NetIQ Access Manager ships with the appliance. You can use this connector if you have a CloudAccess license or a MobileAccess-only license as well as an account for Access Manager. For more information, see NetIQ Access Manager (SAML 2.0).

You can download additional connectors from NetIQ Downloads (https://dl.netiq.com/). For configuration information, see the following:

- "Connector for Accellion (SAML 2.0)"
- "Connector for ADFS (SAML 2.0)"
- "Connector for ADFS (WS-Federation)"
- "Connector for Azure (WS-Federation)"
- "Connector for Box (SAML 2.0)"
- "Connector for Jive (SAML 2.0)"
- "Connector for ServiceNow (SAML 2.0)"
- "Connector for VMware vCloud (SAML 2.0)"
- "Connector for WebEx (SAML 2.0)"
- "Connector for Zoho (SAML 2.0)"

You can also create custom connectors for federated single sign-on and logout by using the NetIQ Access Connector Toolkit. For more information, see "Creating Custom Connectors".

After you download a connector, you must import it to CloudAccess to make it available in the **Applications** palette in the CloudAccess administration console. You can use these connectors if you have a CloudAccess license as well as an account with the destination service.

5.1.4 Connectors for Basic Single Sign-On

CloudAccess provides many connectors for Basic Single Sign-on (SSO). They allow users to access web services that use forms-based authentication and require that the user's password be sent at login. Examples include social media sites such as Evernote, Linked In, and Facebook. Basic SSO connectors work with the Basic SSO extension for the Chrome browser running on the user's computer.

CloudAccess supports using multiple connectors for Basic SSO. Each instance points to a different destination website. You can use these connectors if you have a CloudAccess license. Users have individual accounts with the destination services.

You can download the connectors for Basic SSO from NetIQ Downloads (https://dl.netiq.com/). After you download a connector, you must import it to CloudAccess to make it available in the **Applications** palette in the CloudAccess administration console. For more information, see "Connectors for Basic SSO".

You can also create custom connectors for Basic SSO by using the NetIQ Access Connector Toolkit. For more information, see "Creating Custom Connectors".

5.1.5 Connector for OAuth 2.0 Single Sign-On

CloudAccess provides a connector for OAuth2 Resources that allows single sign-on with simple OAuth 2.0 authenticated access to a protected web service through CloudAccess. The connector ships with the appliance.

CloudAccess supports using multiple instances of the connector for OAuth2 Resources. Each instance points to a different destination OAuth 2.0 resource, or to a set of OAuth 2.0 resources that have the same authentication requirements. You can use this connector if you have a CloudAccess license as well as an account with the destination service.

For more information, see "Connector for OAuth2 Resources".

5.1.6 Connector for Simple Proxy Single Sign-On

CloudAccess provides a connector for Simple Proxy that gives users reverse proxy access to your enterprise web service through CloudAccess. The connector ships with the appliance.

CloudAccess supports using multiple instances of the connector for Simple Proxy. Each instance points to a different destination website path. You can use this connector if you have a CloudAccess license or a MobileAccess-only license as well as access to the destination web path.

For more information, see "Connector for Simple Proxy".

5.1.7 Connector for Bookmarks

The connector for Bookmarks is a container for simple bookmarks to applications that do not require additional passwords for access. The connector ships with the appliance. You can use this connector if you have a CloudAccess license or a MobileAccess-only license as well as access to the destination web service.

For more information, see "Connector for BookMarks".

5.1.8 Custom Connectors

CloudAccess 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 CloudAccess, 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 "Custom Connector Worksheets".

The Access Connector Toolkit facilitates custom connector development efforts without coding or scripting. You can create connectors for identity-aware SaaS applications that support federated single sign-on and logout or that support basic single sign-on. You can use the toolkit and custom connectors if you have a CloudAccess license as well as appropriate accounts with the destination services.

For more information, see "Creating Custom Connectors".

5.1.9 License Information for Connectors

A CloudAccess license entitles you to use any of the connectors mentioned in this guide, including custom connectors.

A MobileAccess-only license entitles you to use only the following three connectors on the **Applications** palette in the CloudAccess administration console. All other connectors, including custom connectors, are CloudAccess-only features and require a CloudAccess license.

- "Connector for NetIQ Access Manager (SAML 2.0)"
- "Connector for Bookmarks"
- "Connector for Simple Proxy"

For more information, see "Understanding Product Licensing".

5.2 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 CloudAccess, users see the appmarks on the landing page that they are entitled to see, according to the application settings for public access or policy mappings for the application to identity source roles (groups).

You can configure appmarks for any proxy connector, SaaS connector, or SSO connector. You can even configure multiple appmarks for the same connector. For example, you might want to have several appmarks for the various Office 365 applications so users can easily identify them. The connector for Google Apps includes default appmarks for Calendar, Drive, and Mail applications. You can copy an existing appmark to create a new one.

When you configure an appmark, you specify whether you want the application to launch in a desktop browser or on a supported mobile device, or both. If you configure a single appmark to display in both a desktop browser and on a mobile device, the appmark will have the same name, but you can customize the icons so they are different. Appmarks offer significant flexibility, enabling you to customize your users' experience using different view options and variables.

When you configure a new appmark to display on a mobile device, after the appliance is finished applying your change, the user must do a refresh on the mobile device before the appmark appears. To do a refresh, the user does the standard "pull-to-refresh" action on the Applications page in the MobileAccess app. (This action is used in mail and other common applications on the mobile device.)

NOTE: Appmarks for proxy and 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.

Use the information in the following sections to help you understand and configure appmarks:

- Section 5.2.1, "Understanding Appmark Options," on page 86
- Section 5.2.2, "Mobile Device Workflow using Safari or Chrome," on page 87
- Section 5.2.3, "Mobile Device Workflow with Internal Viewer," on page 88
- Section 5.2.4, "Mobile Device Workflow from Bookmarks," on page 88
- Section 5.2.5, "Configuring an Appmark for the Desktop Browser or Mobile Device," on page 88
- Section 5.2.6, "Creating Multiple Appmarks for an Application," on page 89

- Section 5.2.7, “Using Appmark Variables,” on page 90
- Section 5.2.8, “Policy Mapping for Non-Public Appmarks,” on page 90

5.2.1 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 check box 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.

Name

The display name for the appmark. If you want different display names for the appmark on the desktop browser page and on mobile devices, you should create a copy of the appmark and change the name. For more information, see Section 5.2.6, “Creating Multiple Appmarks for an Application,” on page 89.

Public

This option is available only for appmarks configured for Simple Proxy, Bookmark, OAuth2 Resources, and SSO-only type connectors. Public access is disabled by default for all connectors except connectors for Basic SSO. If you select the **Public** option, all users can see and use the appmark. If you deselect the **Public** option, no users can see the appmark until it is mapped to desired identity source roles (groups) in Policy Mapping.

Desktop browser

Enables the appmark to be visible on the CloudAccess 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 appears only for the full provisioning connectors (Google Apps, Salesforce, and Office 365) and the SSO-only connectors, such as Box or Accellion.

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 5.2.7, “Using Appmark Variables,” on page 90.

Icon

The icon that appears on the landing page. Within the same appmark, you can use different icons for the landing page and for mobile devices. You can use a different custom icon for each connector to improve their usability for users.

iOS devices

Enables the appmark to be visible on supported iOS mobile devices in the MobileAccess app on the Applications page.

Android devices

Enables the appmark to be visible on supported Android mobile devices in the MobileAccess app on the Applications page.

Launch with

Specifies how to launch the application on the mobile device. Options include the following:

- **Safari:** When the user opens the MobileAccess app on the mobile device and taps the appmark, the MobileAccess app launches Safari and directs it to the application.
- **Chrome:** When the user opens the MobileAccess app on the mobile device and taps the appmark, the MobileAccess app launches Chrome and directs it to the application. If Chrome is not installed on the mobile device, the user is taken to the App Store to install it.
- **Internal viewer:** When the user opens the MobileAccess app on the mobile device and taps the appmark, the MobileAccess app opens an embedded HTML viewer and directs it to the application. This view is similar to the Safari and Chrome options, except that the user does not have to leave the MobileAccess window. The application opens within the MobileAccess app window, and the user can tap the app name (as defined by the administrator when configuring the tool in the appliance) on the navigation bar in the top left corner of the screen to go back to the app home page and easily switch to another protected resource.
- **Native application:** Use this option specifically for mobile apps. When the user opens the MobileAccess app on the mobile device and taps the appmark, MobileAccess opens the mobile app itself.

Launch URL

Use for the **Native application** option. This is the URL such as `fb://profile` that will launch another application installed on the device.

App installer URL

(Optional) You can use this option if you selected the **Native application** option. This is the URL to install the application if it is missing on the mobile device.

URL

The URL that is to be used for the appmark. This can be different from the desktop URL if there is a mobile-specific version of the page.

Icon

The icon that represents the application in the MobileAccess app. Appmark icons for mobile devices should be in `.png` file format and ideally 72 x 72 pixels to ensure they display correctly. Square icons size well on mobile devices. Each icon should convey a good visual image of the application it represents.

5.2.2 Mobile Device Workflow using Safari or Chrome

When you select **Safari** or **Chrome** from the appmark **Launch with** list, MobileAccess opens the application in a new tab in the browser by using the MobileAccess proxy.

The browser workflow on the mobile device is as follows:

1. The end user opens the MobileAccess app on the mobile device.
2. (Conditional) If it is configured, the user is prompted for and enters an application PIN.
3. The user sees a list of protected resources and selects a protected resource.
4. The MobileAccess app starts Safari or Chrome and directs it to the protected resource via the MobileAccess proxy by opening a new tab in the browser.

5. The end user is allowed access to the protected resource.
6. In Google Chrome, the user can tap the button in the top left of the navigation bar to close the current tab and return to the MobileAccess app.

5.2.3 Mobile Device Workflow with Internal Viewer

When you select **Internal viewer** from the appmark **Launch with** list, MobileAccess opens an embedded HTML viewer and directs it to the protected resource by using the MobileAccess proxy.

The workflow on the mobile device is as follows:

1. The end user opens the MobileAccess app on the mobile device.
2. (Conditional) If it is configured, the user is prompted for and enters an application PIN.
3. The user sees a list of protected resources and selects a protected resource.
4. The MobileAccess app opens an embedded HTML viewer and directs it to the protected resource using the MobileAccess proxy.
5. The end user is allowed access to the protected resource.

5.2.4 Mobile Device Workflow from Bookmarks

When a user opens a protected bookmarked application in a Safari browser, MobileAccess prompts the user for the application PIN, then allows the user to access the bookmarked application.

The workflow using bookmarks on the mobile device is as follows:

1. The end user opens Safari on the mobile device.
2. The end user selects a bookmark that points to a URL protected by MobileAccess (i.e., a protected resource).
3. The end user is redirected to the MobileAccess app.
4. (Conditional) If it is configured, the user is prompted for and enters an application PIN.
5. The end user is redirected back to Safari and the bookmarked URL (protected resource).
6. The end user is seamlessly allowed access to that bookmarked application.

5.2.5 Configuring an Appmark for the Desktop Browser or Mobile Device

After you have configured a connector for a proxy, SaaS, or SSO application, you can configure an appmark to simplify access to that application from the user's landing page or from a mobile device, or both.

To configure an appmark:

1. Log in with an appliance administrator account to the Admin page at

   `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.
3. Click the configured connector on the **Applications** panel and click **Configure**.
4. (Conditional) If you have not already configured the connector, provide the appropriate information on the **Configuration** tab. The required information varies depending on the connector.

5 Click the **Appmarks** tab.

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

7 (Conditional) Select the **Public** check box if you want the appmark to appear for all users, regardless of their entitlement to the application.

8 (Conditional) If you want the appmark to be available on the user's landing page, select the **Desktop browser** check box and complete the following steps:

8a (Conditional) If it is applicable to the connector, select the appropriate option from the **Initiate login at** list.

8b Leave the default value in the **URL** field.

8c (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.

9 (Conditional) If you want the appmark to be available on the user's mobile device, select the **iOS devices** or **Android devices** check box and complete the following steps.

9a Select an option from the **Launch with** list to specify how you want users to access the application on their mobile device. For more information about the available options, see Section 5.2.1, "Understanding Appmark Options," on page 86.

9b (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 mobile device. You can use different icons for the landing page and mobile devices.

10 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.

5.2.6 Creating Multiple Appmarks for an Application

Application connectors can have multiple appmarks. For example, you might create several appmarks for different Office 365 or Google Apps applications. 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 Admin page at

`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 5.2.7, “Using Appmark Variables,” on page 90.

5 Specify whether the application should be accessible from a desktop browser or a mobile device, or both, and complete the appropriate fields. For more information about available options, see Section 5.2.1, “Understanding Appmark Options,” on page 86.

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

5.2.7 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.

5.2.8 Policy Mapping for Non-Public Appmarks

Appmarks for proxy and SSO applications are intended only for display and convenience. They are not connected to any authorization policy or access control list (ACL). The SSO and proxy appmark URLs are still available to be used by anyone who knows the link in the URL field. However, selecting or deselecting the **Public** option when configuring an appmark determines whether the appmark actually appears for the users in a group. If you deselect the **Public** check box, the appmark is not available for users until you map the appmark to one or more groups in your configured identity source. After mapping is completed, users in those mapped groups can see the appmark on the landing page or mobile device.

The following procedure assumes that you have already configured an appmark and applied the change on the appliance.

To map an appmark to a group in your identity source:

1 Switch to the Policy page of the administration console.

2 On the left side, locate the identity source that has the desired group (listed as Role Name) from the list.

3 On the right side, select **Other Applications** from the list.

4 Select the Authorization Name of the appmark and drag it to a Role Name.

5 In the mapping window, there are no approvals for appmarks because there is no account provisioning in this process. Users who are included in the group are automatically approved. Click **OK** to continue.

Now when users who are in the mapped group do a refresh in the MobileAccess app or access the landing page, they see the new appmark icon. Users who are not in the mapped group do not see the

icon.

6 Mapping Authorizations

Most companies define their business policies through authorization assignments. Examples of authorizations are groups, roles, and profiles. These authorizations are different depending on each SaaS application. For more information, see Section 6.1, “Supported Roles and Authorizations,” on page 91.

Authorizations give users access to resources. CloudAccess provides a simple solution that allows you to map your identity source roles (groups) to the SaaS application authorizations and approve or deny access to those authorizations.

Authorization categories are available for the connector types that provision users (Office 365, Google Apps, and Salesforce). If you use connector types that provide only authentication and they require mapped authorizations for entitlements instead of Public access, their authorizations are available in the Other Applications category. By default, Public access is disabled for all connectors, except for the connectors for Basic SSO.

The Policy Mapping page maps the authorizations from the SaaS applications to the roles (groups) in the identity sources and allows you to select whether the authorization requires an approval. If approval is required, the Approval page allows you to accept or deny the authorization request.

6.1 Supported Roles and Authorizations

Each identity source can contain different roles that appear on the Policy Mapping page.

- **Active Directory:** groups, local groups, and global groups
- **eDirectory:** group
- **Other Identity Sources:** roles for JDBC and SSUS identity sources

Each application contains different authorizations that appear on the Policy Mapping page.

- **Google Apps:** user and groups
- **Office 365:** account, groups, and license
- **Salesforce:** groups, roles, and profiles (account types)

- **Other Applications:** appmarks for Bookmarks, Simple Proxy, or other applications that require mapped authorizations for entitlements instead of Public access.

Provisioning applications support mapped authorizations only for users in Active Directory, eDirectory, and JDBC identity sources. For more information, see "Requirements for Provisioning" in the *NetIQ® CloudAccess Connectors Guide*.

6.2 Prerequisites

Verify that you meet the following prerequisites before mapping SaaS application authorizations to the identity source groups:

- ❒ Configure the appropriate connectors for your environment. For more information, see Chapter 5, "Configuring Connectors," on page 77.
- ❒ Ensure that roles (groups) in the identity source exist.
- ❒ Populate the required attributes on the users in the identity source. For more information, see Section 3.6, "Verifying the Identity Source User Attributes," on page 36.

6.3 Loading Authorizations

In order to map an authorization, you must load the authorization into the Policy Mapping page.

To verify that applications are available for mapping authorizations:

1. Verify that you have configured the SaaS application connectors that provision users.

   For more information, see Chapter 5, "Configuring Connectors," on page 77.
2. Log in to the Admin page using the application administrator credentials you specified when you created the SaaS application connector.
3. Click **Policy** to open the Policy Mapping page.
4. In the right pane, click the down arrow next to the connector, then select your SaaS application connector, or select **Other Applications** and select the application.

   If the Policy Mapping page does not display the SaaS application connector, you did not configure the connector properly. For example, if the **Public** policy is enabled for a connector, the application does not appear in the list. For more information, see Chapter 5, "Configuring Connectors," on page 77.

Successfully completing these steps populates the Policy Mapping page with the SaaS application's authorizations.

6.4 Reloading Authorizations

When you perform a switch master with the cluster nodes, or if authorizations change in the SaaS applications, or you add new roles in the identity sources, you must reload the authorizations on the Policy Mapping page.

To reload authorizations:

1. To reload roles (groups) from the identity sources, click the **Reload table** icon at the end of the Identity Source table.
2. To reload authorizations from the SaaS applications, click the **Reload table** icon at the end of the Authorizations table.

6.5 Mapping Authorizations

After the authorizations load, map the SaaS application authorizations to the identity source roles (groups).

To map authorizations:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns_name/appliance/index.html`.
2. Click **Policy** at the top of the page.
3. In the right pane of the Policy Mapping page, click the down arrow, then select the desired SaaS connector, or select **Other Applications** and select the application.
4. In the **Role Name** column on the left, select the role (group) from the identity source you want to map to an authorization from the selected SaaS connector.
5. In the right pane, drag and drop the desired authorization from the SaaS connector to the left mapping pane.

   or

   In the left pane, drag and drop the desired group from the identity source to the right mapping pane.
6. (Optional) Click the **Approvals** icon to specify that an approval is required to grant access.

   NetIQ recommends a maximum of 2,000 simultaneous approvals. For more information about approvals, see Section 6.8, "Approving Requests," on page 95.
7. Click **OK** to map the SaaS authorization to the identity source group.

The mapping grants access for users who are members of the identity source roles to the SaaS application authorization. When you add new users to the role (group) that is mapped to a SaaS account authorization, and the request is then approved (if approval is required), the users will see the associated appmark on the landing page or the MobileAccess application page. If **Prompt Before Provisioning** is not enabled, the accounts are provisioned automatically. If **Prompt Before Provisioning** is enabled (available for Salesforce and Google Apps only) users are prompted to create a new SaaS account or to claim an existing account the first time they click or tap the appmark. For information, see "How CloudAccess Provisions User Accounts" in the *NetIQ® CloudAccess Connectors Guide*.

6.6 Understanding Google Apps Mappings

Mapped placement of newly provisioned users to a sub-organization overrides the default placement in the top-level organization. On the Policy page, you can map the User Account authorization and a User Placement authorization value to the same identity source group. Once users are added to the appropriate identity source group, which triggers user account provisioning to Google Apps, new users are placed in the organization that you mapped to the identity source group in Policy Mapping.

IMPORTANT: Pay careful attention when mapping User Placement authorization values to identity source groups on the Policy page to ensure that users are placed in the intended Google Apps organizations. Google Apps allows each user to be placed in only one organization at a time. If you grant a User Placement authorization to a user, and then grant another User Placement authorization to the same user, the first value is overwritten when the user is moved in the Google Apps organizational unit structure.

In addition, if you revoke a User Placement authorization for a user, even if that user has multiple User Placement authorizations, that user is moved to the default organization specified in the Google Apps connector configuration. (Because Google Apps allows a user to be placed into only one organization at a time, when a User Placement authorization value is overwritten, there is only one value that is removed, which moves the user back to the default placement.) If you want to move that user from the default location back into a new Google Apps sub-organization, you must add the user back to the appropriate identity source group and perform policy mappings again.

If you revoke a User Account authorization for a user after the user has been provisioned into Google Apps and one or more User Placement authorizations have been granted to the user, that user is placed in suspended mode in Google Apps. No placement activity takes place as long as the user account is suspended; the user simply remains in the Google Apps organization that they were in before the suspension. When you re-grant the User Account authorization, the account is moved to the "active user" state. If you performed a User Placement authorization change while the user account was suspended, the user is moved to the appropriate organization once the account is reactivated.

6.7 A Mapping Example

Use the following example of authorization mapping to understand how mapping works.

1. In Active Directory:
   - **1a** Create a group named GoogleAppsUsers.
   - **1b** Add users to the GoogleAppsUsers group.
2. In Google Apps for Business, create a Google Apps Account group.
3. In CloudAccess, configure the connector for Google Apps.
4. On the Policy Mapping page:
   - **4a** Load the authorizations for the connector for Google Apps.
   - **4b** In the **Role Name** column, select the connector for Active Directory.
   - **4c** In the right pane, select the connector for Google Apps.
   - **4d** Drag and drop the Google Apps Account into the left pane, over the GoogleAppsUsers group.
   - **4e** Click **OK**.

     The appliance automatically provisions all users in the GoogleAppsUsers group to the Google Apps Account group. Note that if the **Prompt Before Provisioning** option is enabled in the connector for Google Apps configuration, users are prompted the first time they log in to either create an account or specify an existing account.
5. In Active Directory, create a new user, then add the user to the GoogleAppsUsers group.

   The user is automatically added to the Google Apps Account group and has access to Google Apps for Business.

6.8 Approving Requests

CloudAccess provides the ability to approve or deny requests to the SaaS applications. During the configuration of the connector, you specified an application owner. The application owner approves or denies requests for access to the SaaS applications. The application owner knows who should have access to the SaaS applications, whereas the appliance administrator might not have this knowledge.

The **Approval** icon appears in the administration console only if you have mapped roles and selected the option to require approval for the account. When there are accounts waiting for approval, CloudAccess adds the **Approval** icon.

By default, CloudAccess automatically provisions users according to mapped authorizations. To enable approvals so that automatic provisioning does not occur, click the **i** (Configure Authorizations Policies) icon when you map the roles (groups) from the identity source to the SaaS applications authorizations on the Policy Mapping page. Now an application owner must grant approval before provisioning can occur.

To grant approval:

1. Log in to the Admin page at `https://`*`appliance_dns_name`*`/appliance/index.html` as the application owner.
2. Click the **Approvals** tab.
3. Select the desired approval request.
4. Click **Approve** or **Deny**.

NOTE: Users who have been deleted from the identity source may still appear on the Approval page. If you know that certain users have been deleted, you can simply deny approval for those users. However, approving requests for users who have been deleted does *not* result in account provisioning for those users in the SaaS applications.

NetIQ recommends a maximum of 2,000 simultaneous approvals.

7 Reporting

CloudAccess provides reports of users' activity through the appliance. You can run, download, and save various reports on the **Reports** tab in the administration console. CloudAccess also provides the option to use Google Analytics as an external dashboard, or to forward events to Sentinel Log Manager.

7.1 Using Google Analytics as an External Dashboard

CloudAccess enables administrators to use Google Analytics as an external dashboard to monitor and analyze CloudAccess usage. Once you have completed the free Google Analytics registration process for the CloudAccess 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/?gclid=CJCt792Y07kCFUlp7AodDBwALA).

To set up Google Analytics for CloudAccess:

1. (Conditional) If you do not already have a Google account, set one up on the Google web site.
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 CloudAccess appliance. Google Analytics tracks both user and admin logins. For example, `https://appliance_dns_name`.
4. Specify an account name. This account name is only for managing Google Analytics and does not affect anything in CloudAccess. You can share this account name as needed.
5. Log in to the CloudAccess administration console.
6. On the Admin page, drag the Google Analytics icon 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 ad blockers running in your browser that might be interfering with administration tasks. You should be able to disable any ad blockers on the web page itself.

7.2 Integrating with Sentinel Log Manager

The CloudAccess appliance can forward events to Sentinel Log Manager 1.2.x if you want more detailed reports.

To integrate the appliance with Sentinel Log Manager:

1. Configure Sentinel Link in Sentinel Log Manager.

   For more information, see Sentinel Link Overview Guide (http://www.novell.com/documentation/sentinel70/sentinel_link_overview/data/bookinfo.html).

2. Open TCP port 1290 on the Sentinel Log Manager server.

   2a. To change the port, use `ssh` and log in to the Sentinel Log Manager server as `root`.

   2b. At the command prompt, enter `yast firewall`.

   2c. Select **Advanced** > **Allowed Services**, then manually add port 1290 to the list of TCP ports.

3. On the Admin page in CloudAccess, drag and drop the Sentinel icon from the **Tools** palette to the **Tools** panel.

4. Click the Sentinel icon, then click **Configure**.

5. Specify the IP address and port of the Sentinel Link server, then click **OK** and **Apply** to save the changes.

The CloudAccess appliance appears as another event source in Sentinel Log Manager.

8 Configuring the End User Experience

CloudAccess allows you to configure the end user's email client or mobile devices to use the single sign-on authentication to access the SaaS applications. This increases the security of your company's information stored in the SaaS applications because users authenticate with their corporate credentials, but these credentials are never stored in the SaaS applications.

Configure each user's email client or mobile device to point to the CloudAccess appliance. The appliance acts as a proxy, so when users access the SaaS applications, the appliance automatically logs users in to the SaaS application.

CloudAccess also allows you to customize the login, logout, and landing pages so they display your company's branding instead of the default NetIQ branding.

8.1 Configuring Email Clients

You can configure any supported email client to point to CloudAccess. The email clients allow you to receive email from multiple sources in one location. For a list of supported clients, see "Email Clients" on page 20.

NOTE: The following procedure lists typical ports for email clients, but ports may vary depending on your environment.

To configure your email client to use a CloudAccess email account:

1. Access your email client.
2. Create a new email account using the following information to configure CloudAccess as your email source:

   Incoming email server (IMAP/POP): Specify the IP address or hostname of your appliance.

   Incoming email server username: Specify your identity source enterprise logon name for the account name.

   Incoming email server password: Specify your identity source password.

   If your password changes, you must change the password in the email account.

   Outgoing email server (SMTP): Specify the IP address or hostname of your appliance.

   SSL: You must select **SSL** for IMAP (port 993), POP (port 995), and SMTP (port 25).

   The SMTP server requires authentication.

   For more information, see the appropriate documentation for the email client you are using.

8.2 Configuring End User Browsers for Kerberos Authentication

If you are using Windows Integrated Authentication for Kerberos authentication to CloudAccess, each end user browser must be configured to use Kerberos authentication.

To configure Kerberos authentication for web browsers:

1. Add the user computers to the Active Directory domain.

   For instructions, see your Active Directory documentation.
2. Log in to the Active Directory domain, rather than the computer.
3. (Conditional) If you are using Internet Explorer, configure the browser to trust the appliance:
   - **3a** Click **Tools** > **Internet Options** > **Security** > **Local intranet** > **Sites** > **Advanced**.
   - **3b** In the **Add this website to the zone** field, enter the Base URL for the appliance, then click **Add**.

     In the configuration example, this URL is `serv1.cloudaccess.com`.
   - **3c** Click **Close**, then click **OK**.
   - **3d** Click **Tools** > **Internet Options** > **Advanced**.
   - **3e** Verify in the Security section that **Enable Integrated Windows Authentication** is selected, then click **OK**.
   - **3f** Restart the browser.
4. (Conditional) If you are using Firefox, configure the browser to trust the appliance:
   - **4a** In the URL field, specify `about:config`.
   - **4b** In the **Filter** field, specify **network.n**.
   - **4c** Double-click `network.negotiate-auth.trusted-uris`.

     This preference lists the sites that are permitted to engage in SPNEGO Authentication with the browser. Specify a comma-delimited list of trusted domains or URLs.

     For this example configuration, add `serv1.cloudaccess.com` to the list.
   - **4d** Click **OK**, then restart your browser.

8.3 Customizing Branding on User-Facing Pages

CloudAccess 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 2.7, “Initializing the Appliance,” on page 29.

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 administration console at `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 CloudAccess 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.

9 Maintenance Tasks

CloudAccess 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.

9.1 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. On the Admin page, click the Cluster icon at the bottom of the page, then click **Change cluster password**.
2. Type your old password, then type your new password twice and click **OK**.

9.2 Configuring Session Timeouts

The admin session timeout is set to 10 minutes and is not configurable. The user session timeout is also set to 10 minutes by default, but it is configurable.

To change the user session timeout:

1. On the Admin page, click the Cluster icon at the bottom of the page, then click **Configure**.
2. Adjust the setting in the **User session timeout** field as needed, then click **OK**.

9.3 Changing the IP Address

You can change whether a node uses a DHCP IP address or a static IP address on the Admin page.

To change the IP address:

1. Click the node icon, then click **Configure**.
2. Select whether the appliance uses a DHCP IP address 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.
3. Click **OK** to save the changes.
4. Click **Apply** to apply the changes to the appliance.

9.4 Changing the Public DNS Name or NTP Server Settings, or Uploading New Certificates

The appliance contains self-generated certificates. You can upload custom certificates through this interface. You can also change the public DNS name or NTP server if necessary.

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns_name/appliance/index.html`.
2. Click the cluster icon under **Appliances**, 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. If the key pair expires, you must re-initialize the appliance before you can upload a new certificate.

9.5 Updating the Appliance

CloudAccess provides an update channel for keeping your appliances current 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 the Appliance,” on page 32.

When an update is available for one or more nodes in the cluster, the CloudAccess Admin page 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 Admin page with an administrator account. Other consoles do not display the flag icon.

CloudAccess 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** on the Admin page. You can download and install an update as soon as the flag appears on the Admin page, or you can wait for CloudAccess to download the update that night, to minimize network impact due to possible size of an update.

WARNING: If you download and update in the same step and the download is interrupted or incomplete, the update fails. The appliance might become unresponsive or seem to be in a restart loop. If this occurs, download the update, then go back to the snapshot and try again to apply the 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 CloudAccess.

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 desired node, then click **Apply update**.

   CloudAccess 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 10.2, “Displaying Health,” on page 107.
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.

9.6 Shutting Down or Rebooting a Node

You can shut down or reboot a node in the cluster if necessary.

NOTE: If you shut down the node in a single node cluster, the administration console becomes inaccessible. You must then use vSphere to power on the node. Similarly, if you reboot the node in a single node cluster, the administration console is inaccessible until the reboot is complete.

To shut down or reboot a node:

1. Log in with an appliance administrator account to the Admin page at `https://`*`appliance_dns_name`*`/appliance/index.html`.
2. Click the node that you want to shut down or reboot, then click **Shutdown/Reboot** on the menu.
3. In the confirmation window, click **Shutdown** or **Reboot**.
4. (Conditional) Wait for the node to reboot, or use vSphere to power the node back on.

9.7 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. CloudAccess contains a database that is time-sensitive. Restoring one node only and not the others causes corruption in the appliance.

10 Troubleshooting CloudAccess

The CloudAccess administration console displays health status information for the system, the nodes, and the cluster on the Admin page. This section describes the health status indicators, how to troubleshoot health issues, and how to work around known issues.

10.1 Troubleshooting the Appliance Initialization

If the appliance initialization fails, the user interface displays a link for log files. Click the link to download the log files that provide information about the failure.

10.2 Displaying Health

CloudAccess displays health status information for each node and for the cluster at the bottom of the Admin page. Hover the mouse over each node to display the health status of the node. If you want more details, click the node, then select **Show Health.** CloudAccess refreshes health status information every five minutes.

When you click **Show Health**, CloudAccess 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.

10.3 Using Troubleshooting Tools

CloudAccess provides troubleshooting tools to help you resolve problems.

To access these tools:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns_name/appliance/index.html`.
2. Under **Appliances**, click the node icon, then click **Enter troubleshooting mode**.
3. Click the node icon again, then click **Troubleshooting tools**.
4. Select one or more of the troubleshooting scenarios listed.
5. Duplicate the error or condition.
6. Click **Download CloudAccess Log Files** to download the logs.

After you obtain the logs, turn off troubleshooting mode by clicking the node icon again and then clicking **Exit troubleshooting mode**. Leaving the logs running affects the performance of your appliance.

All of the log files in Table 10-1 are included in the download, no matter what scenario you select. The scenario you select determines the amount of data displayed in the log files. Search the appropriate log file for errors while troubleshooting issues.

Table 10-1 *Troubleshooting Log Files*

Feature	Logs
Initialization or commands	`ConfigurationReplicator.log`
	`ConfigurationReplicator_RL.log`
	`messages`
	`boot*`
	`packageoperations.log`
	`dserv.log`
	`firewall`
Forward proxy	`access.log`
Admin.html UI	`adminui.log`
Registration	`register.log`

Feature	Logs
Updates	zypper.log
	downloadUpdate.log
	afterUpdate.log
	beforeUpdate.log
	rpmsAfterUpdate.log
	rpmsBeforeUpdate.log
	rpmsUpdateDiff.log
	300_appliance_SnapshotUconPackages.sh.log
Identity Source Provisioning	bis_AD_<*xxxxx*>.log
	bis_AD_<*xxxxx*>_RL.log
	ConnectorLogs.txt
	bis_EDIR_h2q3p.log
	bis_EDIR_h2q3p_RL.log
Provisioning to the SaaS Applications	connectors_SFORCE_<*xxxxx*>_RL.log
	connectors_GOOGLEAPPS_<*xxxxx*>.log
	connectors_GOOGLEAPPS_<*xxxxx*>_RL.log
	connectors_O365_<*xxxxx*>.log
	connectors_O365_<*xxxxx*>_RL.log
	ConnectorLogs.txt
Mapping	RolesandResourceServiceDriver.log
	UserApplicationDriver.log
Approvals	jboss.log
Reporting	ManagedSystemGatewayDriver.log
	DataCollectionServiceDriver.log
Mobile Devices	mail
	mail.err
	mail.info
Custom Connectors	catalina.out
End User Authentication	catalina.out

10.4 Troubleshooting Different States

CloudAccess displays indicators for the current state of the different appliance components. The display refreshes every five minutes. CloudAccess might not immediately display the change.

The following sections list the different components, the possible states, and troubleshooting steps you can take when the state changes.

10.4.1 Master Node Health

The master node is responsible for all administration functions in CloudAccess. If the master node is not running, the following functions do not work: provisioning or deleting user accounts, mapping authorizations, system roles, approvals, and reporting. Other nodes in the cluster continue to capture and cache events, but do not send those events to the master node until it is running again. Similarly, event forwarding to Sentinel does not work as long as the master node is down.

10.4.2 Front Panel of the Node

The indicator on the front panel of the node displays the health state of the node.

Figure 10-1 *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 select **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 10.3, “Using Troubleshooting Tools,” on page 108.

4. Restart the appliance, then wait at least another five minute cycle for all nodes to display the current state.

10.4.3 Top of the Node

The indicator on the top of the node shows whether the **Apply** commands completed successfully.

Figure 10-2 *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 of the last **Apply** command made on the node.
3. Restart the appliance, then wait at least another five minute cycle for all nodes to display the current state.

10.4.4 Identity Source

The health indicator for the identity source is the small icon in the lower left corner.

Figure 10-3 *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 CloudAccess interface 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 10-1 on page 108 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 Admin page, then click **Configure** on the identity source.
   b. Click the **Refresh** icon next to the identity source server.

10.4.5 Applications

The health indicator for an application connector is the small icon in the lower left corner.

Figure 10-4 *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 **Provisioning**.

   If **Provisioning** is yellow or red, CloudAccess displays helpful information to help troubleshoot the issue.
2. Use the troubleshooting tools to gather logs, then look at the provisioning logs listed in Table 10-1 on page 108 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.

10.4.6 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 following tools do not have a health indicator: Google Analytics, Mobile, and Time-Based One-Time Password (TOTP).

Figure 10-5 *Tool Indicator*

For all tools, the **Question Mark** icon indicates that the tool is in an unconfigured state.

Advanced Authentication: The states for the Advanced Authentication tool are as follows:

- **Green circle:** The connection to the NetIQ Advanced Authentication Framework is healthy, and only Active Directory identity sources exist in the configuration.
- **Yellow triangle:** The connection to the NetIQ Advanced Authentication Framework is healthy. The triangle indicator serves as a warning that identity source types other than Active Directory exist in the configuration and are not supported with the Advanced Authentication Framework authentication providers.
- **Red circle:** The connection to the NetIQ Advanced Authentication Framework is not working. The Advanced Authentication Framework server is unreachable.

Authentication Filter: The states for the Authentication Filter tool are as follows:

- **Green circle:** The connection to the destination ExtAPI script uses HTTPS. The traffic is secure.
- **Yellow triangle:** The connection to the destination ExtAPI script uses HTTP. The traffic is not secure.
- **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 for test environments only.
- **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 3.11.1, “Requirements for reCAPTCHA,” on page 51.
- **Red circle:** None of the configured identity sources are valid for use with reCAPTCHA.

Sentinel and Syslog: The states for the Sentinel and Syslog tools 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.

10.5 Troubleshooting Networking Issues

As an appliance administrator or network administrator, you may need to troubleshoot some basic networking issues before you can successfully initialize the CloudAccess appliance. For example, if your appliance boots onto the network and gets the wrong IP address or falls back to the default IP address, you can use a basic set of commands in the network troubleshooting console to help you resolve these issues.

The console is in a `chroot` jail environment that gives you temporary connectivity to the appliance. You can use the `cat` command to check files such as `/etc/resolv.conf` and `/etc/hosts`, which exist in memory in the `chroot` environment. When you run the initialization process, the real files are updated on the system. Similarly, actions such as updating the IP address or route are not persistent and are reset if you reboot the appliance. You must run through the initialization process to set them permanently.

NOTE: As long as you have not yet completed the initialization process on the appliance, you automatically have console access without login credentials. Logins to the troubleshooting console are no longer available once you have completed the initialization process. However, you can change network settings after this point using the Init screens.

To troubleshoot network issues:

1. Using the vSphere client console or a similar tool, access the troubleshooting console.
2. (Optional) Press the Tab key twice to see all available commands. Some commonly used and supported commands are listed below.
3. (Conditional) Use the following steps if you need to change appliance network settings:
   - **3a** Delete the default route: `route del default`
   - **3b** Create an alias with the IP address that you want to use: `ifconfig eth0:0 IP_address netmask subnet`
   - **3c** Enter `ifconfig` again to verify that the address is now available.
   - **3d** Add a route: `route add default gw gateway_IP eth0:0`
   - **3e** Check connectivity to various resources: for example, `ping gateway_IP` or `ping www.google.com`
   - **3f** (Conditional) If DNS name resolution is not functioning correctly, add an entry to the `/etc/resolve.conf` file as follows: `echo "nameserver 0.0.0.0" > /etc/resolv.conf`

     At this point, you should have connectivity to the appliance. You can run through the initialization process and configure the appropriate settings permanently.
   - **3g** In a browser, enter `https://IP_address/appliance/Init.html`, replacing *IP_address* with the IP address that you used for your alias.
   - **3h** At the certificate warning prompt, add an exception.
   - **3i** In Step 1 - Network of the initialization process, replace the default network values with your preferred IP address and other network settings and click **Next**.
   - **3j** After CloudAccess validates your entries, click **OK** to apply the new settings. CloudAccess applies the settings permanently and restarts services as needed.

If you return to the troubleshooting console, it now displays your preferred IP address. You can use the `ifconfig` command to verify that the new settings are working correctly.

3k Continue with the remaining initialization steps.

Supported commands include the following:

- `arp`
- `bash`
- `cat`
- `date`
- `echo`
- `ifconfig`
- `ip`
- `mkdir`
- `netcat`
- `nslookup`
- `ping`
- `pwd`
- `rm`
- `route`
- `sntp`
- `traceroute`

The following table provides examples of some common actions and commands.

Table 10-2 *Examples*

Action	Command
Set the IP address of the appliance.	`ifconfig eth0 static_IP netmask netmask up`
Delete the default route.	`route del default`
Set the default route (or gateway).	`route add default gw gw_IP eth0`
Update the time.	`sntp -P no -v -r pool.ntp.org`
Check networking.	`ping 8.8.8.8` `traceroute 8.8.8.8`
Verify that DNS is working.	`nslookup www.google.com`

10.6 Troubleshooting Provisioning Issues

Actions that are taken on users and groups in the identity source might not be reflected in the SaaS applications (Google Apps, Salesforce, and Office 365). The following table lists the actions in the identity sources and the corresponding actions in the SaaS applications.

Table 10-3 *Provisioning Actions*

Identity Sources	SaaS Applications
Delete a user. (Or disable a user account.)	Disables the SaaS account. **NOTE:** In the MobileAccess app an iOS device, the user continues to have access to the SaaS account until the in-progress user session times out.
Remove a user from the authorized group.	Disables the SaaS account.
Create a user.	◆ Creates an account for the user in the SaaS application, if the user is a member of a group with mapped SaaS authorizations. or ◆ Users are prompted to validate their information when they log in the first time.
Move a user from out of the search context into the search context.	Creates an account for the user in the SaaS application, if the user is a member of a group with mapped SaaS authorizations.
Move a user out of the search context.	Disables the SaaS account.

By default, CloudAccess establishes identity based on an internal unique ID in the identity source, not based on the user name, and does not support recreating users with the same name unless they also have the same internal unique ID. Once a user has been mapped and provisioned, if you delete the user from the identity source and then recreate that user with the same name, you will not be able to cache and activate the user in CloudAccess or provision the user to SaaS applications. When CloudAccess is unable to cache users properly, the Cached User Status Bar indicates this status with a lower number of active users than cached users.

IMPORTANT: CloudAccess does provide a **Relaxed user matching** option under **Advanced Options** on the configuration window for the identity source. If you select this option, CloudAccess matches users based on CN or sAMAccountName instead of the internal unique ID. This option enables you to recreate previously deleted users so CloudAccess can manage them again, but you must ensure that you do not create different users with the same CN or sAMAccountName as previously deleted users. Otherwise, those users will have access to the previously deleted users' cloud application data.

10.7 Troubleshooting Mobile Device Issues

Device Registration: The user might not be able to register a mobile device if the device is connected to a network that uses HTTP proxy. The user receives the following error message: `Unable to parse metadata`. To workaround this issue, the user can register the device from a different network that does not use HTTP proxy.

10.8 Troubleshooting CloudAccess Login Failures

When a user is unable to log in to the CloudAccess appliance, the login page displays the message `Login failed, please try again`. Some causes of a login failure might not be obvious to either a user or a CloudAccess administrator, such as when multiple users have the same email address.

To help administrators determine the cause of the failure, the error message provides mouseover text containing an ID. You can download the `/var/log/tomcat7/catalina.out` log file and then search the log file for the ID provided in the error message. For more information about downloading log files, see Section 10.3, "Using Troubleshooting Tools," on page 108.

10.9 Troubleshooting Authentications or Single Sign-On Issues

There can be multiple reasons why authentications to the SaaS applications (Google Apps, Salesforce, and Office 365) fail.

Time Synchronization: CloudAccess depends on timestamps to function correctly. Synchronize time between the VMware host, the appliance, and the workstations. Download the authentication or single sign-on logs. In the `catalina.out` file, search for the error `clock skew`.

SAML Authentications: Firefox contains a SAML debug add-on you can use to view the SAML authentication between CloudAccess and the SaaS applications. Download the add-on SAML tracer (https://addons.mozilla.org/en-US/firefox/addon/saml-tracer/) to view the SAML request.

Master Node Down: If the master node is not running, users who already have accounts can log in to SaaS applications, but CloudAccess cannot provision new users. So, if new users attempt to log in to SaaS applications and receive an error indicating they should contact their system administrator, verify that the master node is running.

10.10 Troubleshooting Connector Issues

For information about viewing the current health status of a connector, see Section 10.4.5, "Applications," on page 112.

For information about accessing log files for connectors, see Table 10-1, "Troubleshooting Log Files," on page 108.

For information about troubleshooting a specific connector, see the connector's information in the *NetIQ® CloudAccess Connectors Guide*.

10.11 Troubleshooting JDBC Identity Source Issues

If you are having problems with your JDBC identity source, use the following information.

Question: I have copied all of my users into the indirect.usr table, the **user count** on my appliance Admin page has increased, but my users cannot log in. The **user count** never reconciles to the same number.

I also see one of the following messages in the `catalina.out` file: `mssqljdbc count: 20`, or `oraclejdbc count: 20`.

Answer: The connector for JDBC uses triggered publications, meaning the connector will only cache the users in the indirect.usr table if some event (insert, update, delete) has occurred on the indirect.usr table entry, so that the built-in triggers will add the rows to the indirect.indirect_process table for the connector to consume and process.

To trigger a synchronization of the existing users in the indirect.usr table, you must perform a trigger action. For example, run an SQL query that would touch the records and trigger an update.

```
UPDATE indirect.usr SET disabled = disabled WHERE idu IS NOT NULL
```

Question: I cannot seem to use a user from my real user database tables as an appliance administrator when I run the initialization process for the appliance. The administrator user name keeps coming back invalid and turning red, even though the user exists in my database login table.

Answer: The connector for JDBC only connects directly to the indirect tables. The issue is that the administrative user who you wish to use during the initialization process has not been copied from the real user database tables to the indirect.usr table. `Copy/select into` the desired administrative user to the indirect.usr table.

Question: I have changed the `indirec.proc_authuser` stored procedure to use my desired tables for authentication, but I am still getting a login failure.

Answer: There are two separate ways that the stored procedure verifies the user name and password parameters passed to the `proc_authuser` stored procedure.

- **Oracle:** The password parameter is hashed and then compared to the existing password with the default settings.
- **MSSQL:** The stored procedure uses the `PWDCOMPARE` built-in function with the default settings.

In some cases, when customizing the stored procedure, the password might not be encrypted. In cases like this, the `password=` clause in the stored procedure might also need to be altered.

A Open Source Licenses

A.1 Open Source Components

A.1.1 Apache 2.4.0-12

See Section A.2.1, “Apache 2.0 License,” on page 128.

A.1.2 Apache Common Codec 1.8

See Section A.2.1, “Apache 2.0 License,” on page 128

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).

A.1.3 Apache Common IO 2.4

See Section A.2.1, “Apache 2.0 License,” on page 128.

This product includes software developed by

The Apache Software Foundation (http://www.apache.org/).

A.1.4 Apache Commons Logging 1.1.1

See Section A.2.1, “Apache 2.0 License,” on page 128.

A.1.5 Apache Portable Runtime 1.4.2

See Section A.2.1, “Apache 2.0 License,” on page 128.

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.

A.1.6 Bouncy Castle 1.5-149

See Section A.2.2, “BouncyCastle - Adaptation of the MIT X11 License,” on page 131.

Copyright (c) 2000 - 2012 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

A.1.7 commons-csv 1.0

See Section A.2.1, “Apache 2.0 License,” on page 128.

Copyright © 2014 The Apache Software Foundation.

A.1.8 dom4j 1.6.1

See Section A.2.3, “BSD Style License,” on page 132.

Copyright 2001-2005 (C) MetaStuff, Ltd. All Rights Reserved.

A.1.9 dovecot20-backend-pgsql-2.0.20-31.1

See Section A.2.4, “MIT,” on page 132 Dovcot - MIT.

See Section A.2.5, “LGPL V2.1,” on page 133 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.

A.1.10 dovecot20-backend-mysql-2.0.20-31.1

See Section A.2.4, “MIT,” on page 132 Dovcot - MIT.

See Section A.2.5, “LGPL V2.1,” on page 133 Dovecot - LGPL V2.1.

See Section A.1.9, “dovecot20-backend-pgsql-2.0.20-31.1,” on page 121.

A.1.11 dovecot20-backend-sqlite-2.0.20-31.1

See Section A.2.4, “MIT,” on page 132 Dovcot - MIT.

See Section A.2.5, “LGPL V2.1,” on page 133 Dovecot - LGPL V2.1.

See Section A.1.9, “dovecot20-backend-pgsql-2.0.20-31.1,” on page 121.

A.1.12 dovecot20-2.0.20-31.1

See Section A.2.4, “MIT,” on page 132 Dovcot - MIT.

See Section A.2.5, “LGPL V2.1,” on page 133 Dovecot - LGPL V2.1.

See Section A.1.9, “dovecot20-backend-pgsql-2.0.20-31.1,” on page 121.

A.1.13 dovecot20-devel-2.0.20-31.1

See Section A.2.4, “MIT,” on page 132 Dovcot - Mit.

See Section A.2.5, “LGPL V2.1,” on page 133 Dovecot - Lgpl V2.1.

See Section A.1.9, “dovecot20-backend-pgsql-2.0.20-31.1,” on page 121.

A.1.14 GTM-OAuth2 v2

See Section A.2.1, “Apache 2.0 License,” on page 128.

Copyright (c) 2011 Google Inc.

A.1.15 GWT 2.4.0

See Section A.2.1, “Apache 2.0 License,” on page 128.

A.1.16 GWT Mosaic 0.4.0-rc4

See Section A.2.1, “Apache 2.0 License,” on page 128.

A.1.17 gwtupload 0.6

See Section A.2.1, “Apache 2.0 License,” on page 128.

A.1.18 Hibernate 3

See Section A.2.5, “LGPL V2.1,” on page 133.

A.1.19 httpclient 4.1.2

See Section A.2.1, “Apache 2.0 License,” on page 128.

A.1.20 JavaMail 1.4.3

See Section A.2.6, “Javamail,” on page 139.

A.1.21 JavaService 2.0.10

See Section A.2.7, “JavaService,” on page 144.

See Section A.2.5, “LGPL V2.1,” on page 133.

Copyright owner John Rutter

A.1.22 Jaxb 2.2

See Section A.2.8, “COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0,” on page 145.

See Section A.2.9, “GPL V2 + classpath exception dual license.,” on page 150.

A.1.23 jersey 1.17

See Section A.2.8, “COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0,” on page 145.

See Section A.2.9, “GPL V2 + classpath exception dual license.,” on page 150.

A.1.24 jQuery 1.8

See Section A.2.4, “MIT,” on page 132.

A.1.25 jQuery SmartBanner

See Section A.2.4, “MIT,” on page 132.

A.1.26 jtds 1.3.1

See Section A.2.12, “GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999,” on page 158.

A.1.27 KKPasscodeLock 0.2.2

See Section A.2.1, “Apache 2.0 License,” on page 128.

A.1.28 libvmtools 9.2.3-113-1

See Section A.2.12, “GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999,” on page 158.

See Section A.2.13, “GNU GENERAL PUBLIC LICENSE Version 2,” on page 165.

See Section A.1.33, “Open-vm-tools 9.2.3-113.1,” on page 125.

A.1.29 log4j 1.2.15

See Section A.2.1, “Apache 2.0 License,” on page 128.

Copyright (c) The Apache Software Foundation

A.1.30 OpenInChromeController

See Section A.2.14, “OpenInChromeController,” on page 169.

BSD Style License (OpenInChrome)

Copyright 2013, Google Inc. All rights reserved.

A.1.31 OpenSAML 2.0

See Section A.2.1, “Apache 2.0 License,” on page 128.

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.

A.1.32 OpenSSL 1.0.1i

See Section A.2.11, “OpenSSL License and SSLeay License,” on page 156.

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Copyright (c) 1995-1998 Eric Young (eay@cryptsoft.com) * All rights reserved.

A.1.33 Open-vm-tools 9.2.3-113.1

See Section A.2.12, “GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999,” on page 158.

See Section A.2.13, “GNU GENERAL PUBLIC LICENSE Version 2,” on page 165.

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

A.1.34 Recaptcha4j 0.0.8

See Section A.2.1, "Apache 2.0 License," on page 128.

Copyright 2007 Soren Davidsen, Taneshare Networks.

A.1.35 snmp4j

See Section A.2.1, "Apache 2.0 License," on page 128.

Copyright unknown/unpublished

A.1.36 Tomcat 7.0.27-10.2

See Section A.2.1, "Apache 2.0 License," on page 128.

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.

A.1.37 WSS4J 1.4.2

See Section A.2.1, "Apache 2.0 License," on page 128.

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).

A.1.38 Xalan 2.7.1

See Section A.2.1, “Apache 2.0 License,” on page 128.

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.

A.1.39 Xerces 2.9.1

See Section A.2.1, “Apache 2.0 License,” on page 128.

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.

A.1.40 XMLSec 1.4.6

See Section A.2.1, “Apache 2.0 License,” on page 128.

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.

A.1.41 Zlib 1.2.3

See Section A.2.15, “Zlib 1.2.3,” on page 170.

Copyright (c) 1995-2005 Jean-loup Gailly and Mark Adler

A.1.42 Zxing 2.3.0

See Section A.2.1, “Apache 2.0 License,” on page 128.

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

A.2 Open Source Licenses

A.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.

A.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.

A.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.

A.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.

A.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!

A.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.

A.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.
 */
```

A.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.

A.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)

A.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.

A.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.]
 */
```

A.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!

A.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.

A.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.

A.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

*/

A.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.