NetIQ® CloudAccess and MobileAccess

Installation and Configuration Guide

December 2013

Legal Notice

Contents

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 each field on each window.

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 Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

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

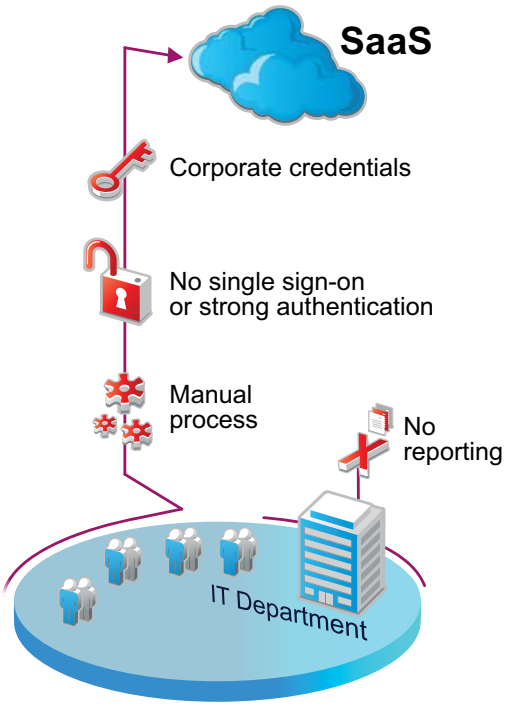
1 Overview of NetIQ CloudAccess

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*



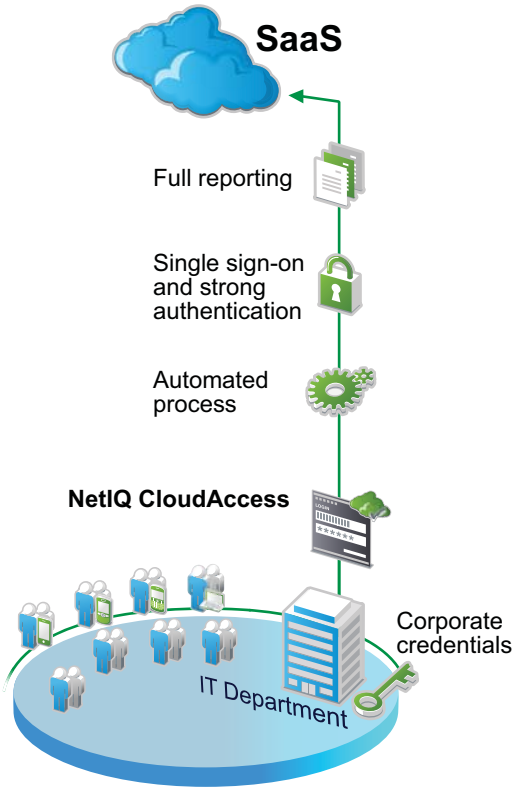
Common problems include the following:

- 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 access the SaaS applications securely. 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. After mapping the authorizations, by leveraging group management in the identity source, CloudAccess automatically creates and manages the associated user accounts in the SaaS application.
- **Secure Single Sign-on:** CloudAccess provides single sign-on to the SaaS applications and supports Integrated Windows Authentication (Kerberos) for background authentication to the CloudAccess identity provider. Provisioned users automatically have access to the SaaS applications, if they are logged in to the identity source. The corporate credentials never leave the firewall.
- **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 3.8, "Configuring Clustering," on page 35.

CloudAccess allows you to configure two NICs for each node in the cluster. You can configure one NIC for the administrative network and a second NIC for the public network. For more information, see Section 3.3, "Configuring Network Options," on page 30.

The user accounts reside in the Active Directory or eDirectory 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 2.0 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 43.

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 Access Manager, the Bookmark 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. For more information, see Section 2.6.2, "Manually Upgrading the Cluster," on page 25.

1.6 Getting Started

Before you can manage CloudAccess and MobileAccess, you must deploy and initialize the appliance. For more information about deploying the appliance, see Section 2.5, "Deploying the Appliance," on page 24. For more information about initializing the appliance, see Section 2.8, "Initializing the Appliance," on page 27.

After you have initialized the appliance, the browser automatically redirects to the Admin page. You can also manually access the Admin page as needed. For more information, see Section 3.1, "Accessing the Administration Pages," on page 29. The Admin page allows you to configure and maintain the appliance. From the Admin page you can use navigation icons to access other functions as follows:

- **Roles:** Configure roles for different users within CloudAccess. For more information, see Section 3.7.2, "Assigning Roles to Users," on page 34.
- **Policy:** Map roles (groups) from the identity source to authorizations from the SaaS applications. For more information, see Chapter 8, "Mapping Authorizations," on page 93.
- **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 8.7, "Approving Requests," on page 96.
- **Reports:** Report on the user activities to the SaaS applications. For more information, see Chapter 9, "Reporting," on page 97.
- **Devices:** View and manage registered mobile devices.

Proceed to Section 2.4, "Appliance Installation Worksheet," on page 23 to gather the information required to install and configure the appliance.

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 20
❑	2. Verify that your identity source meets all requirements.	Section 2.3, “Identity Source Requirements,” on page 22
❑	3. Gather the information you need to install and configure the appliance.	Section 2.4, “Appliance Installation Worksheet,” on page 23
❑	4. Install the appliance.	Section 2.5, “Deploying the Appliance,” on page 24
❑	5. Initialize the appliance.	Section 2.8, “Initializing the Appliance,” on page 27
❑	6. Configure the appliance.	Chapter 3, “Configuring the Appliance,” on page 29
❑	7. Configure the MobileAccess tool on the appliance.	Section 4.3, “Configuring the MobileAccess Tool on the Appliance,” on page 44

❑	Steps	For more information, see ...
❑	8. Replace the default certificate on the appliance.	Section 4.4, “Replacing the Default Certificate on the Appliance,” on page 44
❑	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 45
❑	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 57 Chapter 6, “Configuring Additional Embedded Connectors,” on page 77
❑	12. (Optional) Obtain or create custom icons in `.png` format to represent your appmarked applications.	
❑	13. Configure appmarks for the applications.	Section 4.8, “Appmarks,” on page 48
❑	14. (Conditional) Map any non-public appmarks to the appropriate groups in the identity source.	Section 4.8.8, “Policy Mapping for Non-Public Appmarks,” on page 53
❑	15. (Conditional) If you have configured provisioning connectors, such as Google Apps, map authorizations for the SaaS applications.	Chapter 8, “Mapping Authorizations,” on page 93
❑	16. (Users) Install the MobileAccess app on their mobile devices.	Section 4.5, “Installing MobileAccess on a Mobile Device,” on page 46
❑	17. (Users) Register their mobile devices with the appliance.	Section 4.6, “Registering the Mobile Device with the Appliance,” on page 46

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) ◆ ESX 4.1 (U3 or later)

Components	Requirements
Node	Minimum hardware requirements for each appliance node in the cluster: ◆ 60 GB disk space ◆ 2 Cores ◆ 8 GB RAM
Cluster	Supported cluster configuration: ◆ Up to a five-node cluster ◆ Each node must reside in the same IP subnet
Browsers	**Administration:** Supported browsers for administration tasks: ◆ Firefox on Windows 7 ◆ Google Chrome on Windows 7 ◆ Internet Explorer 9 and 10 on Windows 7 **NOTE:** Administering the appliance with Internet Explorer may be slower than with other supported browsers. **Users:** Supported browsers for users: ◆ Firefox on Windows 7 ◆ Internet Explorer 9 and 10 on Windows 7 ◆ Google Chrome on Windows 7 ◆ Safari on Windows 7 ◆ Safari or Chrome on iPad or iPad mini running iOS 6.1 or later
Mobile Devices	**Administration:** Not supported on mobile devices. **Users:** Supported mobile devices for users: ◆ iPhone with iOS 6.1 or later ◆ iPad or iPad mini with iOS 6.1 or later
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 6.1 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.
SaaS Application Requirements	Each SaaS application has different requirements. For more information about the requirements for each SaaS application, see the Chapter 5, “Configuring Connectors,” on page 57.

2.3 Identity Source Requirements

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

Table 2-3 *Identity Source Requirements*

Identity Source	Requirements

Active Directory	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. CloudAccess uses the sAMAccountName as the unique identifier for the users.
	◆ All of the following required Active Directory attributes 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 that has read access to the user objects. CloudAccess will use this user account to make LDAP binds to Active Directory.
	◆ The name and password of a user in Active Directory that 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.

Identity Source	Requirements
eDirectory	Verify that your eDirectory environment meets the following requirements: ◆ eDirectory 8.8.7 or eDirectory 8.8.6. ◆ All of the following required eDirectory attributes 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 that has the following rights. CloudAccess 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 that 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.

2.4 Appliance Installation Worksheet

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

- ❒ **Networking Information:** Gather the following 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:** Gather the following identity source (Active Directory or eDirectory) information:
  - ❒ IP address or DNS name of the server that contains the users
  - ❒ Context of the users
  - ❒ Name and password of a 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 deploy the appliance:

1. If you are using Windows, extract the VMware image.

   or

   If you are using Linux, use the following command to extract the image:

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

2. Deploy the CloudAccess or MobileAccess virtual appliance.

   For more information, see the VMware documentation.

3. If you do not have a DHCP server in your environment, skip to Section 2.7, "Configuring the Appliance Without a DHCP Server," on page 27.

   or

   Power on the appliance, then proceed to Section 2.8, "Initializing the Appliance," on page 27.

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

There are some major considerations that will determine the best way for you to upgrade your environment from CloudAccess 1.5 to CloudAccess 2.0. Before you begin the upgrade process, review the following sections and plan your upgrade carefully to minimize impact to users:

- Section 2.6.1, "Upgrade Considerations," on page 25
- Section 2.6.2, "Manually Upgrading the Cluster," on page 25
- Section 2.6.3, "Upgrading SaaS Connectors," on page 26

2.6.1 Upgrade Considerations

Review the following important considerations before beginning your upgrade:

- With the new appmarks in CloudAccess 2.0, the 2.0 nodes in a cluster being upgraded from 1.5 will not be available to service end-user authentications until after all nodes have been upgraded (replaced) to 2.0. If you need to allow the cluster to service end-user authentications while the upgrade is in progress, you must prevent end-user traffic from accessing the version 2.0 nodes (using L4 or other round-robin configuration) until you have completed the upgrade procedure and you have reset and mapped the appmarks for the SaaS connectors.
- If you implemented custom branding in the CloudAccess 1.5 cluster, that branding is not compatible with CloudAccess 2.0. After you have upgraded all nodes (by replacing them with 2.0 nodes), you will have to manually download compatible 2.0 branding files, customize them, and re-import them into your 2.0 environment.
- As always, you must not attempt to apply any configuration changes in the administration console while the cluster is in a mixed-version state.

If your hardware capacity allows, NetIQ highly recommends upgrading from CloudAccess 1.5 to 2.0 by building a full 2.0 replacement cluster while the 1.5 cluster is still available. Configure and verify appmarks and mappings, customize and verify branding if applicable, then switch over to the 2.0 cluster by changing the L4 or similar configuration.

If building a full 2.0 replacement cluster is not possible due to hardware or other constraints, upgrade your cluster by replacing the nodes one by one. For more information, see Section 2.6.2, “Manually Upgrading the Cluster,” on page 25.

2.6.2 Manually Upgrading the Cluster

Updating your CloudAccess 1.5 environment to CloudAccess 2.0 requires manual steps. Upgrading an existing cluster through the update channel is not supported in this release.

NOTE: You can also use these steps to upgrade a MobileAccess-only cluster to a full CloudAccess environment.

To upgrade your cluster:

1. Verify that your existing cluster is healthy and stable.

   For more information about health indicators, see Section 12.3, “Troubleshooting Different States,” on page 109.
2. Take a snapshot of each node in the cluster, including the master node, to create a backup.
3. Add a CloudAccess 2.0 node to the cluster using the Initialization process. For more information, see Section 2.8, “Initializing the Appliance,” on page 27.
4. Allow the cluster to adjust to the new node. Wait until all spinners have stopped, all nodes are displaying steady green, and connector health icons are green. This adjustment period may take several minutes.

   IMPORTANT: Do not make any configuration changes to the cluster while in this mixed-version state. In addition, do not add the 2.0 node to the L4 or DNS round-robin configuration yet.

   ---
5. Promote the 2.0 node to master. For more information, see “Promoting a Node to Master” on page 36.

6 Wait for all spinners to stop and all health indicators to turn green. This process may take several minutes.

7 Shut down the old master node.

8 In the administration console, click the old master node, then click **Remove from cluster**. For more information, see "Removing a Node from the Cluster" on page 37.

9 Remove the shutdown master node from the L4 or DNS round-robin.

The cluster now consists of one 2.0 master node and the remaining 1.5 nodes. In this state, existing user traffic should be functional through the remaining 1.5 nodes, but the capacity is lowered because one less node is available to share the load.

10 Add the next 2.0 node to the cluster.

11 Wait for all spinners to stop and all health indicators to turn green. This process may take several minutes.

12 Shut down the 1.5 node that you are replacing.

13 In the administration console, click the shutdown 1.5 node, then click **Remove from cluster**.

14 Remove the shutdown node from the L4 or DNS round-robin.

15 Repeat Step 10 through Step 14 until each 1.5 node has been replaced and shut down.

IMPORTANT: At this point, the cluster is no longer available for end-user authentications until you perform Step 16 through Step 18.

---

16 Reset and map appmarks for the SaaS connectors. For more information, see Section 2.6.3, "Upgrading SaaS Connectors," on page 26.

17 (Conditional) Import the new 2.0-compatible, custom branding files.

18 Add all 2.0 nodes back into the L4 or DNS round-robin.

19 Register the new 2.0 nodes. For more information, see Section 3.2, "Registering CloudAccess," on page 30.

2.6.3 Upgrading SaaS Connectors

If you are upgrading your environment from CloudAccess 1.5 to CloudAccess 2.0, you must map new appmarks for the SaaS connectors (Google Apps, Salesforce, and Office 365) you configured in CloudAccess 1.5. Following an upgrade, existing users will not see their expected auth cards on the OSP Welcome page until you perform the following steps:

IMPORTANT: Before you perform these steps, ensure that you have already upgraded all 1.5 nodes in the cluster to 2.0. Do not perform any configuration changes while the cluster consists of 1.5 and 2.0 nodes. For more information, see Section 2.6.2, "Manually Upgrading the Cluster," on page 25.

---

1 Create the default appmarks for each connector as follows:

1a Click the configured connector on the blue bar and click **Configure**.

1b Click the **Appmarks** tab and click the **Reset** button.

1c Click **OK**.

2 Map the appmarks. On the Policy Mapping page, drag and drop the new appmarks to the appropriate identity source roles, then click **OK**. For more information, see Section 8.5, "Mapping Authorizations," on page 95.

3 Click **Apply** and wait for your configuration changes to be applied.

2.7 Configuring the Appliance Without a DHCP Server

To configure the appliance, the appliance must obtain an IP address through DHCP or have a static IP address assigned through the VMware settings. Perform these steps *only* if there is no DHCP server in your environment. If a DCHP server exists in your environment, you can assign a static IP address after the initial boot without editing the VMware settings.

Edit the VMX file and add the following lines with the appropriate values for your environment:

```
#These settings are related to date/time/timezone and NTP server
#Configures /etc/sysconfig/clock and /etc/ntp.conf
guestinfo.prop1="CLONE_DATE="
guestinfo.prop2="CLONE_timezone="
guestinfo.prop3="CLONE_NTP_SERVER="
guestinfo.prop4="CLONE_HWCLOCK="
guestinfo.prop5="CLONE_SYSTOHC="

#
#Network related settings
#CLONE_DO_DHCP=false, only configure static settings
#CLONE_DO_DHCP=true,  tries DHCP and if it fails configure with static settings
guestinfo.prop6="CLONE_DHCP=true"
guestinfo.prop7="CLONE_DNS_NAME_SERVER1="
guestinfo.prop8="CLONE_DNS_NAME_SERVER2="
guestinfo.prop9="CLONE_DNS_NAME_SERVER3="
guestinfo.prop10="CLONE_DNS_SEARCH1="
guestinfo.prop11="CLONE_DNS_SEARCH2="
guestinfo.prop12="CLONE_DNS_SEARCH3="
guestinfo.prop13="CLONE_NETMASK="
guestinfo.prop14="CLONE_DEFAULT_GATEWAY="
guestinfo.prop15="CLONE_IP="
guestinfo.prop16="CLONE_DNS_NAME="
```

If you do not need a setting, either leave the value blank, or leave the setting out of the VMX file altogether. Power on the appliance, then proceed to Section 2.8, “Initializing the Appliance,” on page 27.

2.8 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 20.
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.

   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.

   Step 1 - Network

   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 have a static IP address obtained through the VMware settings. For more information, see Section 2.7, "Configuring the Appliance Without a DHCP Server," on page 27. Once you enter the static IP address, the appliance populates the Default gateway and DNS server fields for you to verify.

Step 2 - Identity Source

Select eDirectory or Active Directory as the identity source you plan to use.

Username and **Password** - Specify the fully distinguished LDAP format name of a user in the identity source that 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`.

Specify whether you want to **Enable LDAP SSL** for communication with the LDAP 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 LDAP source, but you can add more replicas later if needed.

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 that 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.

Step 4 - Appliance Password

New password / Confirm password - If you lose the connection to the LDAP source for any reason, you can run through these initialization steps again using the appliance password specified here. You would then specify a different LDAP 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://`*`dns_of_appliance`*`/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 LDAP identity source.

6 Proceed with Chapter 3, "Configuring the Appliance," on page 29.

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. Once 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 Pages

After you properly initialize the appliance using the information in Section 2.8, “Initializing the Appliance,” on page 27, the browser automatically redirects to the administration pages at `https://dns_of_appliance/appliance/index.html`.

If the initialization does not automatically redirect or you need access to the administration pages, use the following steps:

1. In a supported browser, enter `https://dns_of_appliance/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 LDAP user password.
3. The first time you log in, the appliance displays the Admin page and may display user count activity on the user bar as users in the search contexts from the identity source are imported and activated. Ensure that this process completes before configuring 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 11.2, “Configuring Session Timeouts,” on page 103.

For a list of the different administration pages, see Section 1.6, “Getting Started,” on page 16.

3.2 Registering CloudAccess

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 Novell Customer Center (NCC) 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 11.5, "Updating the Appliance," on page 104.

To register your appliance:

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

3.3 Configuring Network Options

CloudAccess contains a manual routing table and supports two Network Interface Cards (NICs).

- Section 3.3.1, "Configuring the Second NIC," on page 30
- Section 3.3.2, "Configuring the Routing Table," on page 31
- Section 3.3.3, "A Sample Network Configuration," on page 31

3.3.1 Configuring the Second NIC

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

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

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

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

To configure the second NIC on a node:

1. Log in with an appliance administrator account to the Admin page at `https://`*`appliance_dns`*`/appliance/index.html`.
2. Click a node icon, then select **Configure**.
3. Click the **Public Interface** tab.
4. Select **Enable Separate Public Interface**.
5. Configure the network settings for your public network.
6. Click **Apply** to save the changes.
7. Click **Close**.
8. Repeat Step 2 through Step 7 for each node in the cluster.

3.3.2 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.

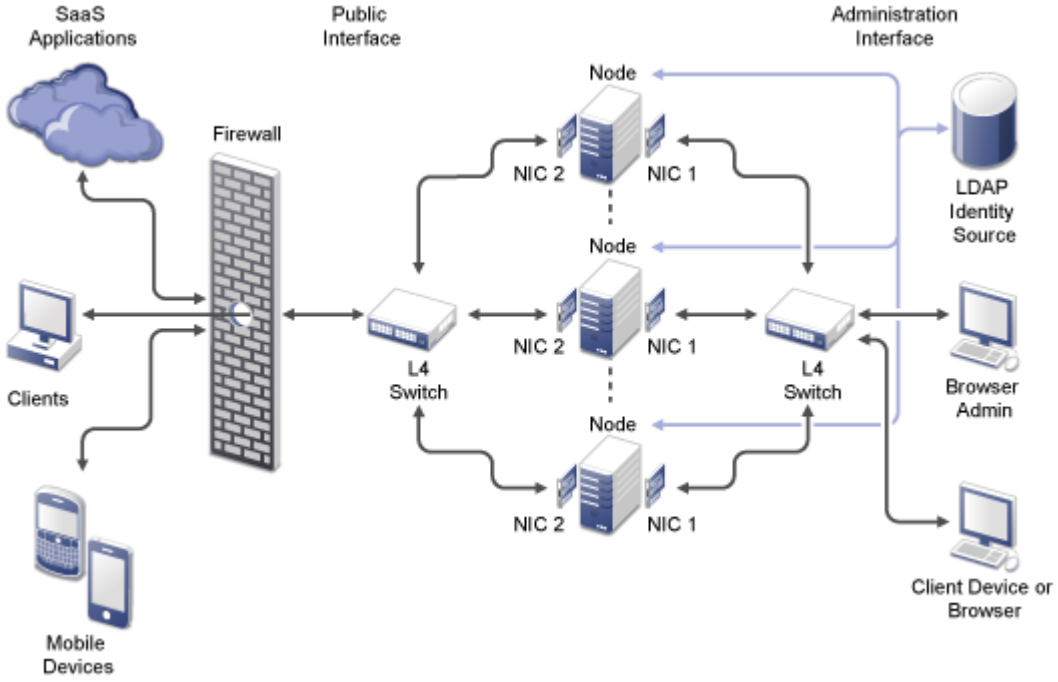
To configure the routing table for each node:

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

3.3.3 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.

3.4 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`*`/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. On 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.

3.5 Verifying the Identity Source User Attributes

CloudAccess supports the use of one or more identity sources to authenticate users and as a source 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 contains certain attributes. The attributes for each identity source are different. For more information, see Section 2.3, "Identity Source Requirements," on page 22.

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 12.4, "Provisioning Behavior," on page 112.

3.6 Configuring Additional Identity Sources

CloudAccess currently supports two different types of identity sources: Active Directory and eDirectory. You can have one or more of each type of identity source configured in your appliance.

To change the initial identity source configuration information, on the Admin page, click the identity source, then click **Configure**.

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.
- CloudAccess does not prevent you from configuring multiple eDirectory or Active Directory connectors that point to the same identity source. However, in order for the appliance to behave as expected and present accurate data, each identity source connector must point to a unique identity source.

To add another identity source:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns/appliance/index.html`.
2. Drag and drop an identity source icon from the Identity palette to the bar in the middle of the page.
3. Click the identity source icon, then click **Configure**.
4. Fill in the fields to configure the new identity source, then click **OK** to save the configuration information.
5. Click **Apply** to commit the changes to the appliance.

3.7 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.

- Section 3.7.1, "Defining the Role Types," on page 34
- Section 3.7.2, "Assigning Roles to Users," on page 34

3.7.1 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 that 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 that 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).

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.

3.7.2 Assigning Roles to Users

To assign roles to users:

1. Log in to the Admin page at `https://appliance_dns/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.

3.8 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.

3.8.1 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.

3.8.2 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 12.3, "Troubleshooting Different States," on page 109.
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 24.

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 2.8, “Initializing the Appliance,” on page 27.

4 When initialization is complete, the browser will be redirected to `index.html` and a login page will appear.

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 3.2, “Registering CloudAccess,” on page 30.

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 12.3, “Troubleshooting Different States,” on page 109.

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 11.5, “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 9.2, “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 36.
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.

3.8.3 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://ip_address_of_appliance/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.

Persistence increases the performance of the appliance for the end users, by removing 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.

3.8.4 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 38
- "Configuring the POP Protocol Handler" on page 38
- "Configuring the IMAP Protocol Handler" on page 39

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.

3.9 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.

3.9.1 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.

3.9.2 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/appliance/index.html`.
2. Click the **Active Directory** icon in the Identity Sources palette, then click **Configure**. (Do not drag the icon to the bar 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 40.
5. Click **OK** to save the changes.
6. Click **Apply** to apply the changes to the appliance.

3.9.3 Configuring End User Browsers

To complete the Kerberos configuration for Active Directory, configure the end user browser. For more information, see Section 10.2, "Configuring End User Browsers for Kerberos Authentication," on page 100.

3.10 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/appliance/index.html`.
2. Drag and drop the Syslog tool from the Tools palette to the middle of the page.
3. 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**.

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 20.

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.

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 19
- Chapter 3, "Configuring the Appliance," on page 29

Once 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 44.

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/appliance/index.html`.
2. Drag the MobileAccess icon from the **Tools** palette on the left to the blue bar.
3. Click the MobileAccess icon on the bar and then click **Configure**.
4. 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. (Optional) If you want to require users to set a PIN for the MobileAccess app on their mobile devices, select **Require PIN**. You can set or remove this requirement at any time. For more information, see Section 4.7, "Understanding the MobileAccess PIN," on page 47.
6. Click **OK**.
7. Click the **Apply** button on the Admin page.
8. Wait for the apply operation to finish. (The gear stops spinning on the appliance when the operation has finished.)
9. Continue with Section 4.4, "Replacing the Default Certificate on the Appliance," on page 44.

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 3.4, "Changing the Certificates on the Appliance," on page 32.

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 45
- Section 4.4.2, "Installing a Self-Signed Certificate on the Mobile Device," on page 45

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 45 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_name*:

```
keytool -genkeypair -keystore name.p12 -storepass changeit -sigalg SHA256withRSA -
keyalg RSA -keysize 4096 -dname "CN=appliance_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_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 3.4, "Changing the Certificates on the Appliance," on page 32.

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 45) 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 44 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 44 and email it to the user that 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 46.

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 the Mobile Device with the Appliance," on page 46.

4.6 Registering the Mobile Device with the Appliance

Before users can register their mobile device with the appliance, the MobileAccess administrator must have the appliance installed with the MobileAccess tool and the certificate configured. The MobileAccess app must be installed on the mobile device.

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/
```

2 The user taps the link.

The link launches the application with the **Provider** value filled in.

3 The user taps **Register** to begin the registration process.

4 When prompted at the CloudAccess login page, the user enters his or her corporate credentials and taps **Sign in**.

5 (Conditional) If the administrator has set the **Pin Required** flag for the MobileAccess app, the user creates a PIN to be entered when the app launches.

The user's mobile device is registered. Tapping the Home icon displays the Applications page with icons for configured applications. This page is blank until the administrator configures application connectors to be accessible from mobile devices.

Users can verify that the mobile device is registered with the appliance by tapping **My Devices** at the bottom of the app window. Their device should be listed, along with the time of registration, on the My Devices window. The device name displayed is the name of the device set on the Settings > General > About window of the mobile device. Users can change this name, but it is not configurable by the MobileAccess administrator.

NOTE: If these steps do not work properly, users can try registering manually. They launch the MobileAccess app, enter the Provider URL provided by the administrator for the CloudAccess appliance, then tap **Register** to begin the registration process.

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. This PIN is unrelated to the built-in iPad passcode, which is designed to protect other resources on the iPad.

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 select or deselect the **Require PIN** option any time in the administration console. If the administrator selects the **Require PIN** option 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 deselects the **Require PIN** option after previously requiring users to set a PIN, users can remove the PIN from their device. However, MobileAccess does not notify users if a PIN is no longer required. For more information, see Section 4.7.3, "Removing the PIN from a Mobile Device," on page 48.

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 the Mobile Device with the Appliance," on page 46 and Section 4.7.1, "Setting the PIN on a Mobile Device," on page 47.

4.7.1 Setting the PIN on a Mobile Device

The MobileAccess app must be installed on the mobile device before you can set the PIN. If the administrator specifies that a PIN is required on mobile devices, the MobileAccess app prompts you to set a PIN the first time you open the app. Otherwise, you can set or reset a PIN any time.

To set the PIN on a mobile device:

1. Open the MobileAccess app and tap **Settings** at the bottom of the window.
2. Change the **Passcode Lock** setting to **On**.
3. Enter a four-digit PIN and re-enter it when prompted.

4.7.2 Changing the PIN on a Mobile Device

Users can change the PIN for the MobileAccess app as needed.

To change the PIN:

1. Open the MobileAccess app and enter your PIN when prompted.
2. Tap **Settings** at the bottom of the window.
3. Tap the **Passcode Lock** option.
4. Tap the **Change Passcode** option.
5. Enter your old PIN, then enter the new PIN twice.

4.7.3 Removing the PIN from a Mobile Device

To remove the PIN from a mobile device:

1. Open the MobileAccess app and enter your PIN when prompted.
2. Tap **Settings** at the bottom of the window.
3. Tap the **Passcode Lock** option.
4. Tap **Turn Passcode Off**.
5. Enter your PIN again.

4.8 Appmarks

Appmarks are essentially bookmarks for applications that you can configure for your users. Once you have configured a connector for an application, you configure one or more appmarks to enable users to access the application in different ways.

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 iOS 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:

4.8.1 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 4.8.6, "Creating Multiple Appmarks for an Application," on page 52.

Public: This option is available only for appmarks configured for Simple Proxy, Bookmark, and SSO-only type connectors. If this option is selected (the default setting), all users can see and use the appmark. If you deselect this 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 OSP Welcome page.

Initiate login at: Specifies whether the URL of the appmark on the OSP Welcome 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 4.8.7, "Using Appmark Variables," on page 53.

Icon: The icon that appears on the CloudAccess or MobileAccess OSP Welcome page. Within the same appmark, you can use different icons for the OSP Welcome page and for iOS devices.

iOS devices: Enables the appmark to be visible on supported 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 iOS apps. When the user opens the MobileAccess app on the mobile device and taps the appmark, MobileAccess opens the iOS 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.

4.8.2 Mobile Device Workflow using Safari or Chrome

When you select **Safari** or **Chrome** from the appmark **Launch with** list, 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 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.

4.8.3 Mobile Device Workflow with Internal Viewer

When you select **Internal viewer** from the appmark **Launch with** list, the workflow on the mobile device is as follows:

1. The end user opens the MobileAccess app on the mobile device.
2. (Conditional) If 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.

4.8.4 Mobile Device Workflow from Bookmarks

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 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.

4.8.5 Configuring an Appmark for the Desktop Browser or Mobile Device

Once 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 OSP Welcome 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`*`/appliance/index.html`.

2 (Conditional) If you have not already configured the connector for the application, drag it from the **Applications** palette to the blue bar.

3 Click the configured connector on the blue bar 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) Keep the **Public** check box selected 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 OSP Welcome page, select the **Desktop browser** check box and complete the following steps:

8a (Conditional) If 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** 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 4.8.1, "Understanding Appmark Options," on page 49

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 OSP Welcome page and mobile devices.

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

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

4.8.6 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`*`/appliance/index.html`.

2 Click the configured connector on the blue bar, 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 4.8.7, "Using Appmark Variables," on page 53.

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 4.8.1, "Understanding Appmark Options," on page 49.

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

4.8.7 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.

4.8.8 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 OSP Welcome 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 that 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 OSP Welcome page, they see the new appmark icon. Users who are not in the mapped group do not see the icon.

4.9 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:

- Section 4.9.1, "Unregistering Mobile Devices from the Administration Console," on page 54
- Section 4.9.2, "Unregistering a Mobile Device from the Device," on page 54
- Section 4.9.3, "Deleting and Reinstalling the MobileAccess App on a Device," on page 55

4.9.1 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/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/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 4.9.3, "Deleting and Reinstalling the MobileAccess App on a Device," on page 55.

4.9.2 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.

4.9.3 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 46.

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 Office 365 enable both account provisioning and single sign-on (SSO). The other available connectors, which are downloadable from the Customer Center, provide only single sign-on capability. For more information about the SSO-only connectors, see the *NetIQ CloudAccess Connectors Guide* available on the CloudAccess Documentation web page (https://www.netiq.com/documentation/cloudaccess/).

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.

5.1 Connector for Google Apps for Business

The connector for Google Apps provides automated provisioning of accounts from the identity sources to Google Apps. The connector also provides single sign-on for users from their identity source account to Google Apps.

Use the information in the following sections to configure a connector for Google Apps for Business:

5.1.1 Connector Requirements

Verify that you meet the following requirements before configuring the connector for Google Apps for Business:

- ❒ A valid Google Apps for Business account
- ❒ Provisioning APIs enabled on the account
- ❒ An administrative account and password

5.1.2 Configuring the Connector for Google Apps for Business

Each cluster can support multiple instances of the connector for Google Apps for Business. Once configured, the connector provides user account provisioning and single sign-on access to Google Apps for Business domains. After users log in to CloudAccess, SAML authentication is used to automatically authenticate (single sign-on) users to Google Apps for Business.

To configure the connector:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns/appliance/index.html`.
2. Drag and drop the connector for Google Apps for Business from the Applications palette to the blue bar.
3. Click the connector for Google Apps for Business, then click **Configure**.
4. Provide a unique display name for the connector to appear on the Admin and OSP Welcome pages, and also provide the administrator logon credentials and domain for the Google Apps for Business account.
5. (Conditional) Select the **Automatically configure SSO settings** option if you want CloudAccess to configure the single sign-on parameters at Google Apps for Business. Otherwise, you must manually configure the parameters at Google Apps for Business.
6. (Conditional) Select **Prompt users for an existing Google Apps account before provisioning** if you want to give users control of when their accounts are provisioned. For more information about account provisioning, see Section 5.4, "How CloudAccess Merges Existing Accounts," on page 70.
7. (Conditional) If you did not select the **Automatically configure SSO settings** option, click **Federation Instructions**. Read the instructions provided to configure the connector for Google Apps for Business to allow single sign-on for users, then complete the following steps:
   - **7a** Copy and paste the text of the signing certificate provided in the **Federation Instructions** into a file, then save the file.

     NOTE: Ensure that you use a text editor that does not introduce hard returns or additional white space. Otherwise, the certificate file may be improperly formatted and unusable. For example, use Notepad instead of Wordpad.

   - **7b** Log in to the Google Apps Dashboard with your administrator account.
   - **7c** Navigate to **Advanced Tools > Set up single sign-on (SSO)**.
   - **7d** Provide the following information:

     Enable Single Sign-on: Select this option.

     Sign-in page URL: Specify the value provided for the **Single Sign-on URL** in the **Federation Instructions**.

Sign-out page URL: Specify the value provided for the **Single Logout URL** in the **Federation Instructions**.

Change password URL: This is the page that the URL will redirect to when a user clicks **Change Password**. (This is not part of the federation per se, but Google requires a value for this field.)

Verification certificate: Upload the file into which you copied the signing certificate text above.

Use a domain specific issuer: Select this option. This changes the value sent in the SAML request to be `google.com/a/`*`google_apps_domain`* instead of google.com. For more information, see SSO (Single Sign-On) (http://support.google.com/a/bin/answer.py?hl=en&answer=60224) in the documentation for Google Apps for Business.

Network masks: Leave blank. This option is not applicable to SAML configuration.

7e Click **Save Changes**.

8 Click **OK**, then click **Apply** to commit the changes to the appliance.

9 (Optional) To provide users with access to Google Apps Mail from supported mobile devices, click the configured connector on the blue bar, then click **Enable email proxy**.

User accounts that have been provisioned to Google Apps for Business using CloudAccess must authenticate through CloudAccess. Direct logins to Google Apps for Business are not allowed. For more information, see the SAML SSO section of the Google Apps for Business website.

5.1.3 Configuring Appmarks for Google Apps

Once you have configured the connector for Google Apps for Business, you can configure appmarks to specify how users should access the applications. By default, the connector includes three appmarks that are configured for the Calendar, Mail, and Drive applications. You can modify these default appmarks or create new ones.

To configure appmarks:

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

2 Click the configured connector for Google Apps on the blue bar, then click **Configure**.

3 Click the **Appmarks** tab.

4 Modify each appmark as needed. For more information about configuring appmarks, see Section 4.8, “Appmarks,” on page 48.

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

Once the appliance has finished applying your changes, the appmarks appear on the OSP Welcome page or the Applications page of the MobileAccess app for users to whom you have granted access.

NOTE: If you are upgrading your environment from CloudAccess 1.5 to CloudAccess 2.0, you must map new appmarks for any connectors for Google Apps that you configured in CloudAccess 1.5. For more information, see Section 2.6, “Upgrading Your Environment,” on page 24.

5.1.4 Configuring Multiple Connectors for Google Apps for Business

CloudAccess can support Google Apps domains by using multiple instances of the connector for Google Apps for Business. Each connector instance must be configured with the unique credentials and domain information of the Google Apps domain that it serves.

NOTE: The **Enable email proxy** option is global across all instances of the Google Apps connector. (The option is either enabled or disabled for all instances.)

5.2 Connector for Office 365

The connector for Office 365 provides automated provisioning of accounts from the identity sources to Office 365. The connector also provides single sign-on for users from their identity source account to Office 365.

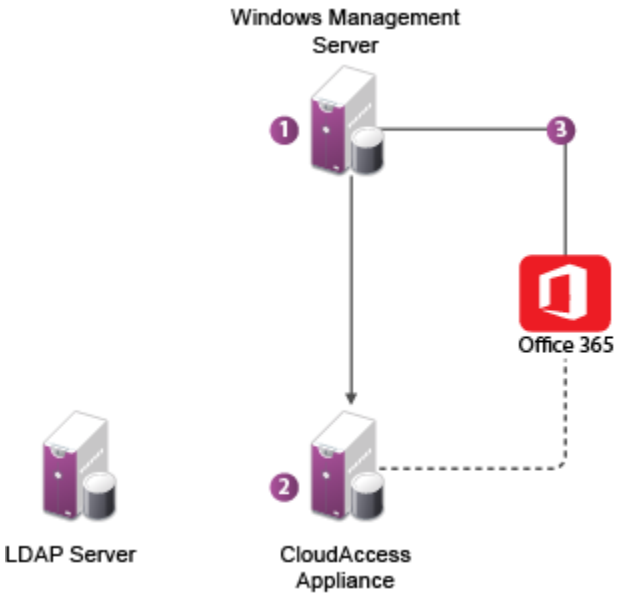
The connector for Office 365 is included with the CloudAccess appliance and appears on the Applications palette of the Admin page. However, you cannot drag and drop the connector to the blue bar as you can with other connector types. You must run the connector for Office 365 installer to connect it to your appliance.

5.2.1 How the Connector for Office 365 Works

Before you install the connector for Office 365, review the following illustrations to help you understand how the connector works with CloudAccess.

Setup and Configuration

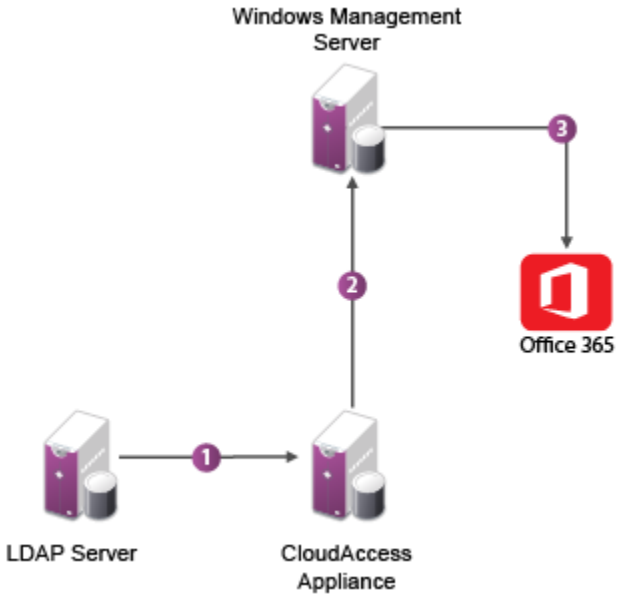
The following figure illustrates the basic setup and configuration steps.



1. Run the connector for Office 365 installation using the `.msi` file. For more information, see Section 5.2.3, "Installing the Connector for Office 365," on page 63.
2. Create a trust relationship (SAML federation) between the CloudAccess appliance and Office 365.
3. Configure user provisioning to Office 365.

User Provisioning

The following figure illustrates the workflow in provisioning users.

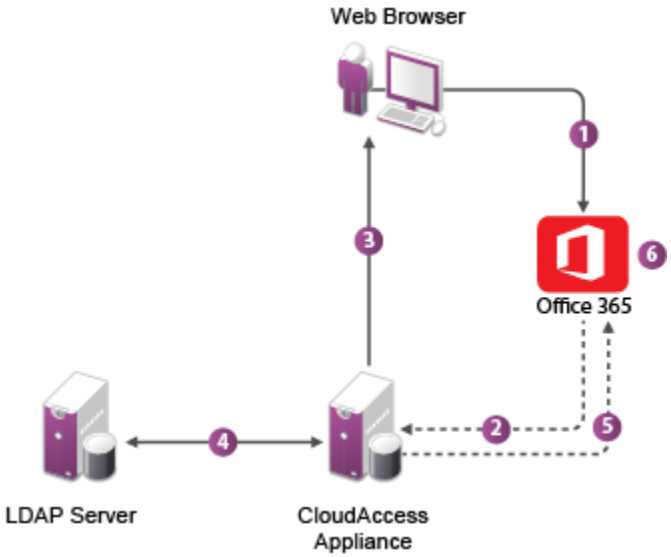


1. The administrator defines a policy to authorize access to Office 365 applications.
2. CloudAccess detects new and updated user information from the LDAP directory.

3. CloudAccess sends user creation, license assignment, update, or deletion requests to the Windows Management Server.
4. The Windows Management Server forwards requests to Office 365 using the Windows Azure Active Directory Module for Windows PowerShell cmdlets.

User Login to Office 365

The following figure illustrates the workflow for users logging in to Office 365 applications.



1. The user attempts to log in to Office 365.
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 enterprise LDAP server. Or, if Kerberos is configured, CloudAccess validates the Kerberos token.
5. CloudAccess provides a SAML assertion to Office 365.
6. Office 365 validates the SAML assertion and allows the user access to assigned Office 365 applications.

5.2.2 Connector Requirements

Complete the following steps before installing the connector for Office 365:

- ❒ Select an existing Office 365 account to use or create a new account.
- ❒ Select a federated domain name for single sign-on with CloudAccess and Office 365.
- ❒ Select a Windows server on which to install the connector. The connector does not need to be installed on a domain controller or even need to be part of the domain where the CloudAccess appliance is installed. The Windows server can be a standalone server, as long as it meets the following requirements:
  - Windows Server 2012 R2 or Windows Server 2008 R2 operating system with all available updates installed.

- Microsoft IIS 7 with the Web Server (IIS) role enabled and the ASP.NET 4.x feature added. The connector uses https between the CloudAccess appliance and the Office 365 web application in IIS.
- Microsoft .NET Framework 4.x. You can download .NET from the .NET downloads (http://www.microsoft.com/net/downloads) web page.
- Microsoft Online Services Sign-In Assistant 7.x. You can download the Microsoft Online Services Sign-In Assistant software from the following location: Microsoft Online Services Sign-In Assistant for IT Professionals BETA (http://www.microsoft.com/en-us/download/details.aspx?id=39267). Select the `msoidcli_64.msi` file.
- Windows Azure AD Module for Windows Powershell. You can download the module from the following location: Manage Windows Azure AD using Windows PowerShell (http://technet.microsoft.com/en-us/library/jj151815.aspx#bkmk_installmodule).

❒ (Conditional) If you plan to use ECP (OASIS SAML 2.0 Enhanced Client Profile), also called *http proxy authentication* in Microsoft Outlook, ensure that your CloudAccess appliance has a publicly resolvable, publicly accessible IP address. In SAML, the browser handles all the redirects and name resolution, so you can manually edit entries in the `/etc/hosts` files to work around name resolution. For ECP, however, Microsoft Office 365 actually sends a SOAP authentication request directly to the CloudAccess appliance, so it must be publicly accessible. You can use port forwarding to protect your appliance behind your corporate firewall.

In addition, ensure that the certificate for ECP support on the CloudAccess appliance meets both of the following requirements:

- Has a common name that matches the appliance hostname
- Is signed by a trusted certificate authority (CA) such as Verisign, Thawte, Symantec, or Digicert

---

NOTE: CloudAccess also supports ECP for email on mobile devices such as Android and iPhone. Users just add an Exchange account on their phone and enter their Exchange credentials. For more information, see the following web pages:

- Set up email on an Android phone or tablet (http://office.microsoft.com/en-us/office365-suite-help/set-up-email-on-an-android-phone-or-tablet-HA102823196.aspx)
- Set up email on Apple iPhone, iPad, and iPod Touch (http://office.microsoft.com/en-us/office365-suite-help/set-up-email-on-apple-iphone-ipad-and-ipod-touch-HA104106914.aspx?CTT=1)

5.2.3 Installing the Connector for Office 365

You must install the connector for Office 365 on a Windows server.

To configure the server and install the connector:

1. Obtain the credentials for an Office 365 account. For more information, see the Office 365 website (http://office.microsoft.com/en-us/support/getting-started-with-office-365-for-business-FX103993883.aspx)
2. Add the federated domain name for single sign-on with CloudAccess and Office 365 to Office 365 and validate the ownership. Use the instructions at the following web page: Add your domain to Office 365 (http://onlinehelp.microsoft.com/en-us/office365-enterprises/ff637620.aspx).

NOTE: Each CloudAccess cluster can manage only one Office 365 domain because of the Microsoft requirement that each federated domain be configured with a unique SAML issuer ID.

---

3 Verify that the Windows server where you plan to install the connector has the prerequisite software installed. For more information, see Section 5.2.2, "Connector Requirements," on page 62.

4 As an administrator on the Windows server, perform the following steps. For more information, see the IIS Manager help. Alternatively, you can use an imported server certificate. For more information, see Importing a Server Certificate (http://technet.microsoft.com/en-us/library/cc732785%28v=ws.10%29.aspx).

   4a Create a self-signed certificate in IIS Manager.

   4b Add an https binding for the Default Web Site using the certificate you created.

   4c Restart the IIS service.

5 As an administrator on the Windows server, download the connector for Office 365 `.zip` file from the Access Connectors HQ website at https://www.netiq.com/products/accessconnectorhq/index.html (https://www.netiq.com/products/accessconnectorhq/index.html). Unzip the file and run the Windows `netiq-office365-connector-1.5.1.msi` installer. You will need the following information:

   - DNS name of the CloudAccess appliance.
   - Administrator name and password of the CloudAccess appliance.
   - User name and password for the Office 365 Global administrator account.
   - The federated domain name specified in Step 2. If you get an error during installation, ensure that you selected the correct domain name.

   Alternatively, you can run the connector installer in "silent mode" from the command line as follows:

```
msiexec /i netiq-office365-connector-1.5.1.msi /qb AG4CHOSTNAME="DNS_of_appliance"
AG4CADMIN="CloudAccess_Admin_username" AG4CADMINPASS="CloudAccess_Admin_password"
O365ADMIN="Office365_Admin_username" O365ADMINPASS="Office365_Admin_password"
O365FEDDOMAIN="Office365_Federated_Domain_Name" O365USAGELOCATION="US"
```

   By default, CloudAccess does not generate an installation log when you install the connector for Office 365. If you want a log of the installation, you must launch the installer from the command line using the following command:

```
msiexec /i netiq-office365-connector-1.5.1.msi /L*V "C:\log\example.log"
```

   IMPORTANT: The connector for Office 365 installation location is `c:\NetIQ\Office365Connector`. You cannot change this location.

Once you have installed the connector, when you return to the CloudAccess administration console, the connector for Office 365 icon is automatically moved to the blue bar. No additional configuration is required, but you can configure appmarks for different Office 365 applications and map users to the appropriate applications. For more information about configuring appmarks, see Section 5.2.5, "Configuring Appmarks for Office 365 Applications," on page 65.

5.2.4 Validating the Connector for Office 365

Once you have installed the connector, perform the following steps to validate the installation:

1 Verify that the Connector for Office 365 appears on the blue bar of the Admin page of the console.

2 Verify that the Policy Mapping page displays Identity Source Groups on the left side and the Connector for Office 365 on the right side.

3 Map one of your groups to the User Authorizations, then verify that CloudAccess provisioned your users.

4 Log in to Office 365 at http://www.office365.com (http://www.office365.com) as a provisioned user.

5 Specify the user name of `user@domain` where the domain is the federated domain name specified in Step 2 on page 63.

NOTE: If you have any issues with the connector, check the Windows Event Viewer on the Windows server where the connector is installed. You can view all events for the connector to help troubleshoot those issues. In the Windows Event Viewer, expand **Windows Logs**, then click **Application**.

5.2.5 Configuring Appmarks for Office 365 Applications

By default, the connector for Office 365 includes a single appmark that is configured for the user's home page. You can modify this default appmark or create additional appmarks as needed. Appmarks that are then mapped in Policy Mapping appear on the OSP Welcome page and/or in the MobileAccess app for entitled users. For more information, see Section 4.8, "Appmarks," on page 48.

NOTE: If you configure appmarks for users to launch Office 365 applications using Safari on mobile devices, you should instruct users to set Safari to never block cookies. Alternatively, consider selecting another **Launch with** option to ensure that users do not experience logout errors. For more information, see Section 12.7.2, "Office 365 Logout Error on Mobile Devices," on page 114.

To configure appmarks:

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

2 Click the configured connector for Office 365 on the blue bar, then click **Configure**.

3 Click the **Appmarks** tab.

4 Modify appmarks as needed. For more information about configuring appmarks, see Section 4.8, "Appmarks," on page 48.

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

Once the appliance has finished applying your changes, the appmarks appear on the OSP Welcome page or in the MobileAccess app for users to whom you have granted access.

NOTE: If you are upgrading your environment from CloudAccess 1.5 to CloudAccess 2.0, you must map new appmarks for any connectors for Office 365 that you configured in CloudAccess 1.5. For more information, see Section 2.6, "Upgrading Your Environment," on page 24.

5.2.6 Changing the Configuration of the Connector

If you change the federated domain name, you must reinstall the connector for Office 365. The installation changes the configuration information in the connector. Delete the existing connector, then run through the installation again using the new federated domain name.

5.2.7 Uninstalling the Connector for Office 365

The connector for Office 365 consists of multiple components. To correctly uninstall the connector, log in to the Windows server as an administrator and use the uninstall function in Windows Control Panel.

Using the Control Panel to uninstall the connector deletes the connector from the CloudAccess Admin page. If you just delete the Connector for Office 365 icon from the Admin page, all of the components on the Windows server still exist and run. This causes issues in CloudAccess if you need to reinstall the connector, unless you run the connector uninstall from the Windows server before attempting to reinstall a new connector.

Alternatively, you can uninstall the connector by running the following command on the Windows server:

```
msiexec /x netiq-office365-connector-1.5.1.msi /qb
```

5.2.8 Installing Multiple Connectors for Office 365

CloudAccess supports multiple connectors for Office 365. However, each connector must connect to a unique Office 365 domain, and you must install each connector on a separate Windows server.

5.3 Connector for Salesforce

Use the information in the following sections to configure a connector for Salesforce:

5.3.1 Connector Requirements

Verify that you meet the following requirements before configuring the connector for Salesforce:

- ❒ A full or developer account with provisioning APIs enabled
- ❒ An administrative account with password
- ❒ The metadata file from Salesforce
- ❒ (Conditional) A security token from Salesforce

5.3.2 Configuring Salesforce to Trust CloudAccess

NetIQ recommends that you configure Salesforce to trust the IP address of the CloudAccess appliance.

To add the CloudAccess IP address as a trusted source to Salesforce:

1. Log in to the Salesforce Admin tools web page.
2. Click **Administration Setup** > **Security Controls** > **Network Access**.
3. Specify the IP address of the CloudAccess appliance.

   or

   If you are in a clustered environment, specify the IP address of the L4 switch.

If you do not configure Salesforce to trust the IP address of the CloudAccess appliance, you must obtain a security token from Salesforce and append the security token to the administrator password specified when you configure the connector for Salesforce.

For example, if your Salesforce administrator account password is `Test1234` and the Salesforce security token is `XyZ`, the **Password** field must contain `Test1234XyZ`.

5.3.3 Configuring the Connector for Salesforce

Each cluster supports multiple connectors for Salesforce.

The connector for Salesforce provides automated provisioning of user accounts from the identity sources to Salesforce. The connector also provides single sign-on for users from their identity source account to Salesforce.

The phone icon that CloudAccess displays on all the Salesforce connectors indicates that Delegated Authentication can be used with Salesforce. All of the configuration required for using Delegated Authentication with CloudAccess is done at Salesforce.

You must go back and forth between the CloudAccess Admin page and the Salesforce administration page to configure the connector.

1. Log in with an appliance administrator account to the Admin page at `https://`*`appliance_dns`*`/appliance/index.html`.
2. Drag and drop the connector for Salesforce from the Applications palette to the blue bar.
3. Click the Connector for Salesforce, then click **Configure**.
4. Provide a unique display name for the connector to appear on the Admin page, and administrator logon credentials for Salesforce.
5. In the **Environment** field, specify whether you have a Production, Development, or Sandbox Salesforce environment. The login URL that is used to verify your Salesforce credentials can be different for each of these environments.
6. Select **Prompt users for an existing Salesforce account before provisioning** if you want to give users control of when their accounts are provisioned. Note that if you want to use Delegated Authentication, you cannot use Prompt before Provisioning. These are mutually exclusive options. For more information about account provisioning, see Section 5.4, “How CloudAccess Merges Existing Accounts,” on page 70.
7. Click **Federation Instructions** and read the instructions provided to configure the connector for Salesforce to allow single sign-on for users.
8. Copy and paste the text of the signing certificate provided in the **Federation Instructions** into a file, then save the file.

NOTE: Ensure that you use a text editor that does not introduce hard returns or additional white space. Otherwise, the certificate file may be improperly formatted and unusable. For example, use Notepad instead of Wordpad.

9 Log in to Salesforce as an administrator and complete the following steps:

9a Select **Administration Setup** from the drop-down menu.

9b Click **Security Controls** under **Administration Setup** in the left pane.

9c Click **Single Sign On Settings**.

9d Click **Edit**, then use the following information to configure single sign-on:

SAML Enabled: Check this option.

SAML Version: Specify 2.0.

Issuer: Copy and paste the value of the **Entity ID** provided in the **Federation Instructions**.

Identity Provider Certificate: Click **Browse**, then browse to and select the file to which you copied and pasted the signing certificate in Step 8.

Identity Provider Login URL: Copy and paste the value of the **Single Sign-on URL** provided in the **Federation Instructions**.

Custom Error URL: Leave this blank.

SAML User ID Type: Select **Assertion Contains the Federation ID from the User Object**. This option is not selected by default.

SAML User ID Location: Select **User ID is in the NameIdentifier element of the Subject statement**.

Identity Provider Logout URL: Copy and paste the value of the **Single Logout URL** in the **Federation Instructions**.

10 Download the Salesforce metadata file after the configuration is complete.

11 On the CloudAccess Admin page, edit the Connector for Salesforce.

12 Upload the metadata file generated in Step 10 into the connector for Salesforce.

13 Click **OK**, then click **Apply** to commit the changes to the appliance.

Once you have configured the connector for Salesforce, you can configure one or more appmarks to enable user access. For more information, see Section 5.3.4, "Configuring Appmarks for Salesforce," on page 68.

5.3.4 Configuring Appmarks for Salesforce

By default, the connector for Salesforce includes a single appmark that is configured for the user's home page. You can modify this default appmark or create additional appmarks as needed. Appmarks that are then mapped in Policy Mapping appear on the OSP Welcome page and/or in the MobileAccess app for entitled users. For more information, see Section 4.8, "Appmarks," on page 48.

To configure appmarks:

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

2 Click the configured connector for Salesforce on the blue bar, then click **Configure**.

3 Click the **Appmarks** tab.

4 Modify the default appmark or create new appmarks as needed. For more information about configuring appmarks, see Section 4.8, “Appmarks,” on page 48.

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

Once the appliance has finished applying your changes, the appmarks appear on the OSP Welcome page or in the MobileAccess app for users to whom you have granted access.

NOTE: If you are upgrading your environment from CloudAccess 1.5 to CloudAccess 2.0, you must map new appmarks for any connectors for Salesforce that you configured in CloudAccess 1.5. For more information, see Section 2.6, “Upgrading Your Environment,” on page 24.

5.3.5 Configuring Multiple Connectors for Salesforce

If you want to configure more than one connector for Salesforce, each Salesforce account must be configured with a unique URL. Configuring the URL requires Salesforce assistance and it often takes at least a day to complete.

To configure the Salesforce URL:

1 Log in to the Salesforce administration web page.

2 Click **Administration Setup** > **Company Profile** > **My Domain**.

3 Provide a unique subdomain name for your organization and click **Check Availability**.

4 If the subdomain you specified is available, select the check box to indicate that you agree to the terms and conditions, then click **Register Domain**.

5 Wait for Salesforce to register your domains. This process takes time.

After the registration is complete, Salesforce provides you with a URL that supports SP-initiated logins and is similar to the following:

`https://<custom name>.mysalesforce.com`

5.3.6 Configuring Delegated Authentication

Salesforce allows two different types of authentication methods: SAML and delegated authentication. By default, Salesforce activates only the SAML authentication. SAML is available only for browser-based authentication and does not work for applications that use the Salesforce Web Service API. For example, smart phones use the Salesforce Web Service API.

Delegated authentication must be activated on a per-Salesforce organization basis. This allows CloudAccess to support users authenticating with smart phones as well as users authenticating with browsers.

For delegated authentication to work properly with CloudAccess, the DNS name of the CloudAccess cluster must be publicly resolvable and the SSL certificate must be signed by a well-known certificate authority (CA).

To configure Salesforce for delegated authentication:

1 Follow the instructions in the Salesforce documentation to enable delegated authentication single sign-on for your organization.

For more information, see Configuring Salesforce for Delegated Authentication (https://login.salesforce.com/help/doc/en/sso_delauthentication_configuring.htm).

2 Once delegated authentication has been enabled at Salesforce, complete the following configuration steps:

   2a Log in to the Salesforce administration page.

   2b Click **Your Name** > **Setup** > **Security Controls** > **Single Sign-On Settings** > **Edit**.

   2c In the **Delegated Gateway URL** field, specify a value similar to the following: `https://cloudaccess_public_dns/osp/a/t1/auth/external/sfda`.

   2d Do not select **Force Delegated Authentication Callout**.

   This option affects the performance of user logins.

   2e Enable the **Is Single Sign-On Enabled** permission. Note that if you want to prompt users to validate their accounts, you must disable this option instead. For more information about the prompt before provisioning option, see Section 5.4, "How CloudAccess Merges Existing Accounts," on page 70.

3 Configure a connector for Salesforce in CloudAccess as described in section Section 5.3.3, "Configuring the Connector for Salesforce," on page 67, but deselect the **Delegated authentication single sign-on is disabled in Salesforce** option.

When end users authenticate to Salesforce through their smart phones, they will authenticate entering identity source credentials, where the user name is specified in email format to match the user name in the Salesforce account.

For example, if Active Directory user `Ted` with password `password` has been provisioned to Salesforce domain `mydomain-dev-ed.my.salesforce.com`, the user name for login from a smart phone application such as Salesforce Chatter would be `Ted@mydomain-dev-ed.my.salesforce.com` and the password would be `password`.

5.4 How CloudAccess Merges Existing Accounts

CloudAccess creates a new account or merges an existing account in the SaaS applications for users that are members of mapped groups in the identity sources. This is called *provisioning*.

Provisioning occurs in two ways:

- If approval is not required when policy mapping is configured, automatic provisioning occurs when you map authorizations for the SaaS applications to the identity source roles. If approval is required, the account is not provisioned until the request is approved.
- You can configure the SaaS connectors to allow users control of when their accounts are provisioned. A configuration option is available on the connector for Google Apps and the connector for Salesforce to **Prompt users for an existing account before provisioning**.

  When you select this option, users have two choices: create a new account or specify an existing SaaS application account during their initial attempt to access the SaaS application using single sign-on through CloudAccess.

When provisioning a new account, CloudAccess determines if a matching user account already exists in the SaaS application. If a match is found, CloudAccess merges the user with the existing SaaS application account. If no match is found, CloudAccess creates a new account. For more information, see the following sections:

- Section 5.4.1, "CloudAccess Matching Criteria," on page 71
- Section 5.4.2, "CloudAccess Naming Convention," on page 72
- Section 5.4.3, "Samples of Account Creations," on page 72

5.4.1 CloudAccess Matching Criteria

The following sections define the matching criteria of the connectors that provision users:

- "Matching Criteria for the Connector for Google Apps" on page 71
- "Matching Criteria for the Connector for Office 365" on page 71
- "Matching Criteria for the Connector for Salesforce" on page 71

Matching Criteria for the Connector for Google Apps

Table 5-1 contains the matching criteria for the connector for Google Apps. CloudAccess compares the Google Apps email attribute value to the listed identity source attribute value. If there is a match, CloudAccess merges the accounts. If there is no match, CloudAccess creates a new account in Google Apps.

Table 5-1 *Google Apps Matching Criteria*

	Google Apps Attribute	Identity Source: Active Directory Attribute	Identity Source: eDirectory Attribute
Attribute Name	UserName	sAMAccountName	CN
Display Name	Email	User logon name	Username

Matching Criteria for the Connector for Office 365

Table 5-2 contains the matching criteria for the connector for Office 365. CloudAccess compares the Office 365 userPrincipalName attribute value with the value in the identity source attribute plus the @ sign plus the Office 365 federated domain name. If the values match, CloudAccess merges the accounts. If there is no match, CloudAccess creates a new account in Office 365.

Table 5-2 *Office 365 Matching Criteria*

	Office 365 Attribute	Identity Source: Active Directory Attribute	Identity Source: eDirectory Attribute
Attribute Name	userPrincipalName (upn)	sAMAccountName@*Federated Domain Name*	CN@*Federated Domain Name*
Display Name	User name	User logon name@*Federated Domain Name*	Username@*Federated Domain Name*

Matching Criteria for the Connector for Salesforce

Table 5-3 contains the matching criteria for the connector for Salesforce. CloudAccess matches on three different attributes in a priority order. If CloudAccess does not find a match for the value in the first attribute, it performs a search in the value of the second attribute, and if it does not find a match, it performs the search for the value in the third attribute.

Table 5-3 Salesforce Matching Criteria

	Salesforce Attribute	Identity Source: Active Directory Attribute	Identity Source: eDirectory Attribute
First Priority			
Attribute Name	Federation Identifier	objectGUID	GUID
Second Priority			
Attribute Name	Username	sAMAccountName@*Salesforce Domain Name*	CN@*Salesforce Domain Name*
Display Name	Username	User logon name@*Salesforce Domain Name*	Username@*Salesforce Domain Name*
Third Priority			
Attribute Name	Username	mail	Internet EMail Address
Display Name	Username	E-mail	E-Mail Address

5.4.2 CloudAccess Naming Convention

CloudAccess contains a defined naming convention for creating the user accounts in the SaaS applications.

Table 5-4 CloudAccess Naming Convention

Identity Source	Connector for Google Apps	Connector for Salesforce
Active Directory	sAMAccountName	sAMAccountName@*Salesforce Domain Name*
eDirectory	CN	CN@*Salesforce Domain Name*

As shown in Table 5-4, the user name attribute in Salesforce is in the form of an email address. CloudAccess creates a unique user name based on the sAMAccountName or CN of the user object in the identity source prepended to the domain name configured in the Company Profile at the Salesforce account.

5.4.3 Samples of Account Creations

Sample experience with the **Prompt users for an existing account before provisioning** option enabled:

1. The administrator selects the **Prompt users for an existing account before provisioning** option when configuring the connector for the SaaS application.
2. The administrator maps one or more SaaS authorizations to the identity source role and grants approval, if required.
3. (Conditional) The person with the Approval role approves or denies the account creation.
4. Users log in to CloudAccess with their identity source credentials.
5. CloudAccess presents users with appmarks for the SaaS applications they are entitled to access.
6. Users click the appmark for the entitled SaaS application.

7. CloudAccess presents two options to users:
   - **I do not have an existing account. Create one for me.**
   - **I already have an existing account. These are my credentials:**
8. Users select **I do not have an existing account. Create one for me.**

   or

   Users select **I already have an existing account. These are my credentials**, then specify their credentials for the existing SaaS account.
9. Regardless of the option the user selects, CloudAccess searches for an existing, matching account.
10. (Conditional) If CloudAccess finds an existing account (for example, the user's mail attribute in the identity source matches a user name in the Salesforce domain), CloudAccess merges the existing account with the new account it creates for the user.
11. (Conditional) If CloudAccess does not find an existing account, CloudAccess creates a new account for the user in the SaaS application following the naming conventions in Table 5-4 on page 72.

Whether CloudAccess merges the user account or creates a new account, the user's SaaS application password is set to a random value that CloudAccess generates. The user's authentication to the SaaS application now uses SAML single sign-on. For information about using SAML single sign-on, see Section 5.5, "Providing Access to the SaaS Applications for Users," on page 73.

Sample experience with the automatic account creation:

1. The administrator maps one or more SaaS authorizations to the identity source role and grants approval, if required.
2. (Conditional) The person with the Approval role approves or denies the account creation.
3. CloudAccess searches for an existing, matching account.
4. (Conditional) If CloudAccess finds an existing account (for example, the user's mail attribute in the identity source matches a user name in the Salesforce domain), CloudAccess merges the existing account with the new account it creates for the user.
5. (Conditional) If CloudAccess does not find an existing account, CloudAccess creates a new account for the user in the SaaS application following the naming conventions in Table 5-4 on page 72.
6. Users log in to CloudAccess with their identity source credentials.
7. CloudAccess presents users with appmarks for the SaaS applications they are entitled to access.
8. Users click the appmark for the entitled SaaS application, then CloudAccess uses the SAML single sign-on to authenticate the users to the SaaS application.

5.5 Providing Access to the SaaS Applications for Users

Once you have configured the connectors for Google Apps, Salesforce, and Office 365, you must provide a way for users to access the SaaS applications.

CloudAccess includes an OSP Welcome page that contains the links for accessing the SaaS applications. You can use this page or create your own page. Access the OSP Welcome page through the following URL:

`https://dns_or_ip_of_appliance/osp/a/t1/auth/app`

After you enter valid credentials, the OSP Welcome page appears. This page displays the links for the SaaS applications only after they are configured properly and if you have an entitlement for that SaaS application.

On the OSP Welcome page, links for the applications are dependent on configuration. However, typical examples might be as follows:

- **Google Apps for Business:** `https://dns_of_appliance/osp/a/t1/auth/app/its?tpAuthCardId=appmarks_GOOGLEAPPS_nQZXh:zESMadesktop~browser&target=https://mail.google.com/a/google_domain`
- **Salesforce:** `https://dns_of_appliance/osp/a/t1/auth/app/its?tpAuthCardId=appmarks_SFORCE_5EC5a:pJ5W0desktop~browser&target=https://account_name-dev-ed.my.salesforce.com`
- **Office 365:** `https://dns_of_appliance/osp/a/t1/auth/app/its?tpAuthCardId=appmarks_O365_ksPh7:kQ340desktop~browser&target=https://login.microsoftonline.com/login.srf?whr=office365_domain`

If you create your own page, copy the links for the SaaS applications from the OSP Welcome page to your landing page.

If you are creating your own landing page, keep in mind that there are two methods to connect to the SaaS applications: logins can be initiated at the identity provider or at the service provider. You can use either method for your own landing page.

Method 1: Identity Provider (IDP) Initiated Logins

1. The user clicks the link `https://dns_of_appliance/osp/a/t1/auth/app/its?tpAuthCardId=appmarks_GOOGLEAPPS_nQZXh:zESMadesktop~browser&target=https://mail.google.com/a/google_domain` for an identity provider-initiated login.
2. The browser sends a request to the appliance login URL.
3. The browser displays the CloudAccess login form.
4. The user enters the identity source login credentials, then successfully authenticates to the appliance.
5. The appliance redirects the browser session back to Google Apps for Business with a SAML assertion for authentication.
6. Google Apps for Business accepts the assertion, then allows or denies access based on the content of the assertion.

Method 2: Service Provider (SP) Initiated Logins

1. The user clicks the link `https://mail.google.com/a/your_google_domain` for a service provider-initiated login.
2. The browser sends a request to Google Apps for Business.
3. Google Apps for Business redirects the browser session to the appliance for authentication.
4. The user enters login credentials.
5. After a successful authentication against the identity source, the appliance redirects the browser session back to Google Apps for Business with a SAML assertion for authentication.
6. Google Apps for Business receives the assertion, then allows or denies user access based on the content of the assertion.

Examples of IDP-Initiated Logins

The following are examples of the different IDP-initiated logins:

Google Apps (Mail): `https://dns_of_appliance/osp/a/t1/auth/app/its?tpAuthCardId=appmarks_GOOGLEAPPS_nQZXh:zESMadesktop~browser&target=https://mail.google.com/a/google_domain`

Google Apps (Calendar): `https://dns_of_appliance/osp/a/t1/auth/app/its?tpAuthCardId=appmarks_GOOGLEAPPS_nQZXh:ML0dDdesktop~browser&target=https://calendar.google.com/a/google_domain`

Google Apps (Drive): `https://dns_of_appliance/osp/a/t1/auth/app/its?tpAuthCardId=appmarks_GOOGLEAPPS_nQZXh:DzWsAdesktop~browser&target=https://drive.google.com/a/google_domain`

Salesforce: `https://dns_of_appliance/osp/a/t1/auth/app/its?tpAuthCardId=appmarks_SFORCE_5EC5a:pJ5W0desktop~browser&target=https://account_name-dev-ed.my.salesforce.com`

Office 365: `https://dns_of_appliance/osp/a/t1/auth/app/its?tpAuthCardId=appmarks_O365_ksPh7:kQ340desktop~browser&target=https://login.microsoftonline.com/login.srf?whr=office365_domain`

Examples of SP-Initiated Logins

The following are examples of the different SP-initiated logins:

Google Apps (Mail): `https://mail.google.com/a/google_domain`

Google Apps (Calendar): `https://calendar.google.com/a/google_domain`

Google Apps (Drive): `https://drive.google.com/a/google_domain`

Salesforce: `https://account_name-dev-ed.my.salesforce.com/`

Office 365: `https://login.microsoftonline.com/login.srf?whr=office365_domain`

5.6 Single Sign-On Connectors

NetIQ provides additional connectors that you can use for single sign-on to other applications or web services. These connectors are available for download from your Customer Center. For more information, see the Access Connector HQ website (https://www.netiq.com/products/accessconnectorhq/index.html).

IMPORTANT: The CloudAccess single sign-on connectors are not included in the MobileAccess-only license. For more information about product licensing, see Section 1.5, "Understanding Product Licensing," on page 16.

5.7 Importing and Configuring Custom Connectors

CloudAccess allows you to import and configure custom connectors that NetIQ partners create.

IMPORTANT: Custom connectors for CloudAccess are not included in the MobileAccess-only license. For more information about product licensing, see Section 1.5, "Understanding Product Licensing," on page 16.

To import and configure a custom connector:

1. Copy the custom connector `.zip` file to the computer where you administer CloudAccess.
2. Log in to CloudAccess as an administrator.
3. On the Admin page, click the Tools icon on the toolbar.
4. Click **Import connector definition**.
5. Browse to and select the custom connector `.zip` file, then click **Import**.
6. Drag and drop the new custom connector from the Applications palette to the blue bar.
7. Click the connector, then click **Configure**.
8. Fill in the fields and follow the **Federation Instructions** to configure your web server or application.
9. Click **OK**, then click **Apply** to save the changes.

6 Configuring Additional Embedded Connectors

CloudAccess includes additional embedded connectors that you can configure to help users access applications. These connectors include the connector for NetIQ Access Manager, the Simple Proxy connector, and the Bookmark connector. All of these connectors are included in the MobileAccess-only license as well as the CloudAccess license.

6.1 Connector for NetIQ Access Manager

When you configure the connector for NetIQ Access Manager, you must configure the connector in CloudAccess and you must also configure Access Manager to work with the connector.

6.1.1 Requirements

Verify that you meet the following requirements before you start configuring the connector:

- ❒ An Access Manager system installed and configured
- ❒ The metadata file from your Access Manager system

  `https://Access_Manager_server/nidp/saml2/metadata`
- ❒ Access Manager user accounts for each user who wants the single sign-on service

6.1.2 Configuring the Connector

To configure the connector for Access Manager:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns/appliance/index.html`.
2. Drag and drop the connector for Access Manager from the Applications palette to the blue bar, then click **Configure**.
3. Use the following information to configure the new connector for Access Manager:

   NOTE: The information from the Access Manager metadata file is case sensitive. You must enter the information exactly as it appears in the metadata file (`https://Access_Manager_server/nidp/saml2/metadata`).

Display name: Specify a display name for the connector. This name should be unique so you can identify this connector on the Admin page.

Assertion Consumer Service URL: The value in the **AssertionConsumerService** field with the HTTP-POST bindings in the Access Manager metadata file.

Destination URL: (Optional) Specify the URL where users go after initial login.

Entity ID: Specify the value in the **entityID** field in the Access Manager metadata file.

Logout Response URL: Specify the value in the **SingleLogoutService ResponseLocation** field with the HTTP-POST binding in the Access Manager metadata file.

Logout URL: Specify the value in the **SingleLogoutService Location** field with the HTTP-POST binding in the Access Manager metadata file.

Signing certificate: To secure communication to Access Manager, get the Signing Certificate from your Access Manager configuration. To get the certificate:

1. Open the Administration Console.
2. Navigate to **Identity Servers** > *Cluster Name* > **Security** > **Signing**.
3. Under **Certificates**, click the Certificate name.
4. Select **Export Public Certificate** and click **PEM File**.
5. Use this PEM file.

Assertion Attribute Mappings: Select **NameID** from the list for the LDAP attribute that contains the user name identifier in Access Manager.

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

6.1.3 Configuring Access Manager

After configuring the connector, you must configure single sign-on SAML 2.0 federation between Access Manager and CloudAccess.

1 In CloudAccess, obtain the required information to configure Access Manager:

1a On the Admin page, click the connector for Access Manager.

1b Click **Configure**.

1c Expand the Federation Instructions, then copy and paste the instructions into a text file to use during the Access Manager configuration.

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

---

2 Create a new Identity Provider for the appliance in Access Manager:

2a Log in to the Access Manager Administration Console.

2b Click **Devices** > **Identity Servers** > *Cluster Name* > **SAML 2.0**.

2c Click **New**, then select **Identity Provider**.

2d Use the following information to configure the Identity Provider:

Name: Specify the name of your appliance.

Source: Select **Metadata Text** in the list as the source, then open the Identity Broker metadata file in a browser. The URL is `https://appliance:443/osp/a/t1/auth/saml2/metadata`. Copy and paste the entry in the metadata file for Access Manager into the **Metadata Text** field.

or

Select **Metadata URL** in the list as the source, then copy the metadata URL. The URL is `https://appliance:443/osp/a/t1/auth/saml2/metadata`.

2e Click **Next**, then view the signing certificate of the Identity Broker.

2f Click **Finish** to save the configuration.

3 Configure the new Identity Provider you just created:

3a Click the new Identity Provider, then click the **Authentication Card** > **Authentication Request**.

3b Use the following information to configure the Identity Provider:

Name Identifier Format: Select **Transient**.

Options > Response protocol binders: Select **Post** from the list.

3c Click **OK** to save the changes.

4 Make any additional changes you require.

5 Import the certificate from the connector for Access Manager:

5a Click **Security** > **Trusted Roots**, then click **Import**.

5b Use the following information to import the certificate:

Name: Specify the name as *appliance_name*_signing_cert.

Certificate data file: Copy and paste the certificate information from the text file you created in the first step of this procedure.

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

5c Click **OK** to import the certificate.

6 Add the certificate to the trust store:

6a Click **Add Trusted Roots to Trust Store**.

6b In the **Trust stores** field, click **Edit**.

6c Select **Trust Store for NIDP** and **OSCP Trust Store**.

6d Click **OK** twice to save the changes.

7 Update the Identity Provider:

7a Click **Devices**, then click your Identity Provider.

7b Click **Update All**, then click **OK**.

7c Wait for Access Manager to process the new configuration.

8 Log out of Access Manager.

6.1.4 Configuring Appmarks for Protected Resources in Access Manager

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

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

For more information about configuring appmarks, see Section 4.8, “Appmarks,” on page 48.

6.2 Simple Proxy Connector

The Simple Proxy connector is essentially a simplified version of the Access Gateway component found in the Access Manager product.

If you have an application on a web server that you want to protect, but you also want users to be able to access, you can configure the Simple Proxy connector to provide access to the application. You can provide access to the root of the web server and any subdirectories on the web server, or you can provide access to a path on the web server and any subdirectories within that path.

6.2.1 Configuring the Simple Proxy Connector

To configure the Simple Proxy connector:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns/appliance/index.html`.
2. Drag the **Simple Proxy** connector from the Applications palette to the blue bar.
3. Click the new **Simple Proxy** icon and then click **Configure**.
4. On the Configuration tab, provide the following information:
   - **Display name**: The display name of the default appmark, which also appears in the user interface.
   - **Local Path**: A string that will be appended to the DNS name of the cluster for accessing the resource, and will be removed from the request before forwarding to the web server.
   - **connects to**: The URL of the web server or page on the web server that you want to protect. For example, `http://10.20.30.40:8080` or `https://10.20.30.40/path_to_protect`. You can specify either http or https, depending on requirements of the web server. If you specify a path on the web server, MobileAccess protects resources from that path down, rather than from the root of the server.
   - **Inject Identity in Query**: Causes user identity items to be added to the query string sent to the web server specified in the **connects to** field. For more information, see Section 6.2.2, "Understanding the Inject Identity in Query Setting," on page 81.
   - **Inject Identity in Headers**: Causes user identity items to be added to the headers sent to the web server specified in the **connects to** field. For more information, see Section 6.2.3, "Understanding the Inject Identity in Header Setting," on page 82.
5. Click the **Appmarks** tab.

   MobileAccess provides a default appmark for simple proxy applications, with pre-configured default settings including a globe icon. You can customize these settings as needed for your users.
6. Review and edit the default settings for the appmark. For more information about appmark options, see Section 4.8, "Appmarks," on page 48.
7. Click **OK**, then **Apply**.

Once the configuration changes have been applied on the appliance, the application is available to users. To see the application on their mobile devices, users must perform a refresh using 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.)

6.2.2 Understanding the Inject Identity in Query Setting

If you configure a proxy application to use the **Inject Identity in Query** setting, when users navigate to a configured proxy application, the web server you specified receives all of the attributes in the query string.

The attributes are mapped to various attributes in the identity source and are listed in your Identity Source connector. The attributes cannot be changed. For example, if you configure a link to your corporate intranet, when a user whose first name is Joe (as specified in the identity source) clicks the link on his mobile device, he might see "Welcome: Joe" at the top of his browser window.

You can see the default mappings that are taken from the LDAP directory. On the **Configuration** tab for the identity source, click **Advanced Options**, then scroll down and click **Default** in the **Attribute Mappings** section. For example, in eDirectory, `ID` is mapped to the `guid` attribute, `User name` is mapped to the `cn`, and so on. You can change these mappings as needed for your environment, but any changes you make are global. You cannot change them on a per proxy or app basis.

NOTE: MobileAccess cannot send a user's password for a proxy application to the back end web service. If the web server needs the user's password, you must find a workaround. For example, you could specify a static string that is accepted for all users.

The attribute values in the query string parameters sent to the web server are based on the following settings in the user interface:

ID
Email
User name
First name
Middle name
Last name
Full name
Preferred name
Generational qualifier
Gender
Phone
Birthdate
Street address
City
State
ZIP code
Country
Language

The **Attribute Mappings** section under **Advanced Options** allows additional custom attribute mappings. The X-Custom<1-5> attributes can be mapped to attributes in your LDAP directory. Note that Simple Proxy type applications will forward X-Custom1 and X-Custom2 headers to the web server, but X-Custom3-5 are not supported.

The actual names of the query string parameters sent to the web server are the following:

ID
Email
UserName

FirstName
MiddleName
LastName
FullName
PreferredName
GenerationalQualifier
Gender
Phone
BirthDate
StreetAddress
City
State
ZipCode
Country
Language
IdentityType
XCustom1
XCustom2

6.2.3 Understanding the Inject Identity in Header Setting

If you configure a proxy application to use the **Inject Identity in Header** setting, when users navigate to a configured proxy application, the web server you specified receives all of the attributes as custom headers.

The attributes are mapped to various attributes in the identity source and are listed in your Identity Source connector. The attributes cannot be changed.

You can see the default mappings that are taken from the LDAP directory. On the **Configuration** tab for the identity source, click **Advanced Options**, then scroll down and click **Default** in the **Attribute Mappings** section. For example, in eDirectory, `ID` is mapped to the `guid` attribute, `User name` is mapped to the `cn`, and so on. You can change these mappings as needed for your environment, but any changes you make are global. You cannot change them on a per proxy or app basis.

NOTE: MobileAccess cannot send a user's password for a proxy application to the back end web service. If the web server needs the user's password, you must find a workaround. For example, you could specify a static string that is accepted for all users.

The attribute values in the headers sent to the web server are based on the following settings in the user interface:

ID
Email
User name
First name
Middle name
Last name
Full name
Preferred name
Generational qualifier
Gender

Phone
Birthdate
Street address
City
State
ZIP code
Country
Language

The **Attribute Mappings** section under **Advanced Options** allows additional custom attribute mappings. The X-Custom<1-5> attributes can be mapped to attributes in your LDAP directory. Note that Simple Proxy type applications will forward X-Custom1 and X-Custom2 headers to the web server, but X-Custom3-5 are not supported.

The actual names of the headers sent to the web server are the following:

X-ID
X-Email
X-UserName
X-FirstName
X-MiddleName
X-LastName
X-FullName
X-PreferredName
X-GenerationalQualifier
X-Gender
X-Phone
X-BirthDate
X-StreetAddress
X-City
X-State
X-ZipCode
X-Country
X-Language
X-IdentityType
X-XCustom1
X-XCustom2

6.3 Bookmarks Connector

The Bookmarks connector on the Applications palette enables you to create links to web applications that are accessible from the browser landing page or directly from the MobileAccess app on users' mobile devices.

You can also create links to other iOS applications from the MobileAccess app, though there is no single sign-on for these apps. While there is no global list for these app URL schemes, you may find the following list helpful: http://wiki.akosma.com/IPhone_URL_Schemes (http://wiki.akosma.com/IPhone_URL_Schemes)

6.3.1 Configuring the Bookmarks Connector

The Bookmarks connector is intended as a container for multiple appmarks for web applications. Configure the Bookmarks connector once, then configure as many appmarks as you need within the same Bookmarks connector so you do not clutter your Admin page.

To configure a bookmark connector:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns/appliance/index.html`.
2. Drag the **Bookmark** connector from the Applications palette to the blue bar.
3. Click the new **Bookmark** icon and then click **Configure**.
4. Provide a display name for the bookmarked application. The display name appears on the Admin page of the administration console and in the MobileAccess app.
5. Click the **Appmarks** tab.
6. Click the plus (**+**) sign next to the default created appmark.
7. Rename the appmark to correspond to the bookmark URL.
8. (Conditional) Keep the **Public** check box selected if you want the appmark to appear for all users, regardless of their entitlement to the application.
9. (Conditional) If you want users to be able to access the bookmarked application from their desktop browser landing page, select **Desktop browser** and complete the following steps:
   - **9a** In the **URL** field, change the default value to the URL of the bookmarked application.
   - **9b** Click **X** next to the default icon to delete it, then browse to and select a `.png` file to represent the application on the browser landing page.
10. (Conditional) If you want users to be able to access the bookmarked application from their mobile devices, select **iOS devices** and specify the appropriate options as follows:
    - **10a** From the **Launch with** list, select the viewer in which the application should appear on mobile devices: Safari, Chrome, or an internal viewer. For more information about the available options, see Section 4.8.1, “Understanding Appmark Options,” on page 49.
    - **10b** Leave the **Launch URL** and **App installer URL** fields blank.
    - **10c** In the **URL** field, type the same URL that you provided in step 7a or type an iOS-specific URL.
    - **10d** Click **X** next to the default icon to delete it, then browse to and select a `.png` file to represent the application on the mobile device.
11. (Conditional) If you want to use the Bookmark connector to link to other iOS applications from the MobileAccess app, select **iOS devices** and specify the following options:
    - **11a** From the **Launch with** list, select **Native application**.
    - **11b** In the **Launch URL** field, enter the iOS app URL scheme. For example, `fb://profile`.
    - **11c** (Optional) In the **App installer URL** field, type the URL to install the application if it has not already been installed on the mobile device.
    - **11d** Click **X** next to the default icon to delete it, then browse to and select a `.png` file to represent the bookmarked application.
12. Click **OK**, then **Apply**.

Once the configuration changes have been applied on the appliance, the application is available to users. To see the application on their mobile devices, users must perform a refresh using 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.) How users access the bookmark appmark depends on how you configured the **Launch with** option.

7 Creating Custom Connectors with the Access Connector Toolkit

CloudAccess contains a toolkit that allows you to create SAML connectors. The Access Connector Toolkit allows you to create a connector that establishes a SAML federation between a web service and CloudAccess, enabling single sign-on and logout for users. You can create custom SAML connectors for any web service or application that uses SAML 2.0.

IMPORTANT: The Access Connector Toolkit is a CloudAccess-only feature. If you purchased MobileAccess without CloudAccess, your license entitles you to a 90-day trial of CloudAccess, including the Access Connector Toolkit. At the end of the trial period, you are expected to purchase the appropriate license for CloudAccess or discontinue use of the CloudAccess-only features. For more information, see Section 1.5, "Understanding Product Licensing," on page 16.

7.1 Meeting the Web Service or Application Requirements

In order to create a custom SAML 2.0 connector, the application or the web service that connects to CloudAccess must meet the following requirements:

- The web service supports SAML 2.0 identity federation.

  For more information about SAML, see the OASIS website (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security).
- The web service supports a SAML web browser single sign-on profile, specifically with Redirect/POST bindings for service-provider-initiated SSO, and POST binding for identity-provider-initiated SSO.
- The web service must provide a way for the tenant to configure the federation. This usually means providing a facility in the application's administration console that allows the tenant to enable and configure SAML SSO.
- The web service or application must have technical documents that describe what it requires for the following:
  - **SAML Assertions:** The document needs to describe the attributes that are required for authentication, such as the user's name or email address. It can include the attributes that are required to assign roles. If possible, obtain a SAML assertion from the application.

- **Federation Requirements:** The document needs to describe what is required for federation. It should require a CloudAccess certificate, which allows the application to set the trusted relationship with CloudAccess. The document should also include URLs for logging in and logging out.
- **SAML Metadata:** The application sends SAML metadata to CloudAccess in order to establish communication. This usually includes a login URL or a customer-specific domain name. Applications that support SAML should publish a SAML metadata document that describes their service. This document is often available from a public URL. If possible, get this document.

  CloudAccess has the ability to create a SAML 2.0 connector that can retrieve the metadata from a specified URL. You must verify that the web service supports this type of connection if you want to use it.

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

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

7.2 Creating a Custom SAML Connector Template

A SAML connector template consists of multiple components. CloudAccess contains an interface that allows you to create the components in one place.

To create a custom connector template:

1. Verify that you have gathered the web service or application requirements. For more information, see Section 7.1, “Meeting the Web Service or Application Requirements,” on page 87.
2. Log in to the Access Connector Toolkit through the following URL:

`https://dns_of_appliance/css/toolkit`

3. Click **New** > **SAML2**.

   NOTE: CloudAccess does not currently support the **WSFed** option.

4. Create the connector template. For more information, see Section 7.2.1, “Creating the Connector Template,” on page 89.
5. Create the metadata. For more information, see Section 7.2.2, “Creating the SAML 2.0 Metadata,” on page 90.
6. Create the assertions. For more information, see Section 7.2.3, “Creating the Assertion,” on page 91.
7. (Optional) Create the provisioning definitions. For more information, see Section 7.2.4, “Creating the Provisioning Setting Definition,” on page 91.
8. Click **Save** to save the new connector template.
9. Proceed to Section 7.3, “Exporting the Connector Template,” on page 92 to finish creating the new connector.

7.2.1 Creating the Connector Template

Just as with shipping SAML connectors, you must import a connector template into CloudAccess for the connector to work. CloudAccess provides help for you to create a connector template.

Table 7-1 *Connector Template Fields*

Field	Description	Action
Type	Defines the type of connector for CloudAccess. You cannot change the value of this field. It is set when you select the type of connector to create. For example: SAML2	
Type Name	Defines the type name of the connector for CloudAccess. You cannot change the value of this field. It is set when you select the type of connector to create. For example: Generic SAML2 Connector	
Target Name	The target name is the name of the connector template file.	Specify a unique name for the connector template file.
Icon	Allows you to uses a custom graphic for your new connector.	Browse to and select a graphic that you want as the icon for the new connector.
Description for Provider	CloudAccess does not use this field.	
Description for Customer	Provide enough information so the CloudAccess administrator knows what the connector does.	Specify a description that CloudAccess displays on the Admin page.
Settings > Federation Instructions	CloudAccess displays the federation instructions when the administrator configures the connector.	Edit the default federation instructions for your connector. You must add information that is specific to your CloudAccess appliance.
Settings > New Settings	A setting provides a way for CloudAccess administrators to input data when creating the connector.	Create a setting for your connector. ◆ Customer-specific sections of the Assertion Consumer Service URL. ◆ Connector-specific setting, such as a customer domain.
Certificate required from provider	Specifies whether a signing certificate is required when the administrator configures the connector. If you do not select this check box, the Signing Certificate field will be optional. For example, the connector for NetIQ Access Manager has this flag set, but the SAML 2.0 connector for ADFS does not.	

7.2.2 Creating the SAML 2.0 Metadata

The metadata is the configuration information that the web service or application uses to communicate with CloudAccess. Some web services and applications allow you to export the required metadata to an XML file, or it is contained in a URL provided by the web service or application. You can use the provided URL, import the XML file, or enter the required information.

Table 7-2 *Metadata Fields*

Field	Description	Example
Request	Select this option to allow the connector to retrieve the metadata from a specified URL instead of manually entering the data in the fields.	
Request > Source URL	Specify the web service URL that contains the metadata. The connector retrieves the required information.	
Generate	Select this option to manually fill in the metadata fields.	
Generate > EntityID	Specify the Entity ID from the metadata or select a setting that will contain the entity ID. EntityID is a field from the metadata that uniquely identifies that particular service provider.	google.com
Generate > Login URL	Specify the Login URL from the metadata or select a setting that will contain the login URL. The login URL corresponds to the Assertion Consumer Service URL in the metadata where the Assertion is posted by the browser.	https://www.google.com/a/${customer-domain}/acs
Generate > Logout URL	(Optional) Specify a logout URL. The logout URL corresponds to the **SingleLogoutService** field from the metadata.	
Generate > Logout URL Binding	(Optional) Select a binding type for the logout URL. The options are HTTP Post or Redirect.	
Generate > Signing Certificate	(Optional) Browse to and select the Service Provider's signing certificate.	
Import from a file	Select this option to import the metadata from a file to fill out the Generate fields. You can view the values found in the metadata file and keep the existing values or replace them with the values in the file.	

Field	Description	Example
Import from URL	Select this option to import the metadata from a URL to fill out the Generate fields. You can view the values found in the URL and keep the existing values or replace them with the values in the URL.	

7.2.3 Creating the Assertion

The assertion is a package of information that supplies statements made by the identity source.

Table 7-3 *Assertion Fields*

Fields	Description	Example
Properties	Use the **Properties** tab to define the properties of the SAML assertion.	
Audience Restriction	(Optional) Audience Restriction is a field in the Assertion that defines the recipient of the Assertion. Usually this is the same value as the EntityID. If you leave the field blank, the EntityID value is used for this field.	google.com
NameID	The NameID field in the Assertion defines what attribute the service provider receives in the NameID field of the SAML2 assertion.	
Format	The NameID format is an email address or it is unspecified. It depends on the requirements of the connected system as to which format you use.	
Destination URL	(Optional) The Destination URL is where the end user ends up after the CloudAccess login with the URL provided on the connector configuration page.	
Protocol Binding	The only binding currently supported is POST.	
Attributes	Use the **Attributes** tab to define what attributes are required in the Assertion sent to the Service Provider.	

7.2.4 Creating the Provisioning Setting Definition

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

7.3 Exporting the Connector Template

After you create the connector template, you must export the connector template. The first step when creating a connector in the administration console is to import the connector template. Exporting the connector template creates a file you can use on any CloudAccess system.

To export the connector template:

1. Log in to the Access Connector Toolkit through the following URL:

`https://dns_of_appliance/css/toolkit`

2. Select the connector template you created, then click **Export**.
3. Save the `.zip` file for use on this or another CloudAccess system.

7.4 Importing and Configuring the Connector

After you create the connector template, you must import the template into CloudAccess and configure the connector. The steps to configure the connector are determined by the information you added to the connector template.

NOTE: Custom connectors created with the Access Connector Toolkit are not included in the MobileAccess-only license and should not be used after the 90-day trial period for CloudAccess has expired. At the end of the trial period, you are expected to purchase the appropriate license for CloudAccess or discontinue use of the CloudAccess-only features. For more information, see Section 1.5, "Understanding Product Licensing," on page 16.

To import a custom connector:

1. Log in with an appliance administrator account to the Admin page at `https://appliance_dns/appliance/index.html`.
2. Click the **Tools** icon on the toolbar, then select **Import connector template**.
3. Browse to and select the exported custom connector, then click **Import**. Ensure that the file you import is a `.zip` file, not a `.xml` file.
4. Drag and drop the new custom connector from the palette.
5. Click the custom connector, then click **Configure**.
6. Configure the custom connector according to the federation instructions included in the connector.
7. Configure the connecting application or web service to work with the custom connector.

7.5 Toolkit Compatibility

The toolkit contains new functionality for the CloudAccess 2.0 release. If you have any connectors that were created with the toolkit prior to CloudAccess 2.0, you can import that connector into the new toolkit and then export the connector and the connector contains the functionality. However, you cannot import a connector from CloudAccess 2.0 into a toolkit that came with a prior version of CloudAccess. The import will fail.

8 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 8.1, “Supported Roles and Authorizations,” on page 93.

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.

Authorizations are available only for the connector types that provision users (Office 365, Google Apps, and Salesforce). If you use connector types that provide only authentication, there are no authorizations. For example, the connector for WebEx and the connector for Accellion do not have authorizations.

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.

8.1 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

Each SaaS 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)

8.2 Prerequisites

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

- ❒ Configure SaaS connectors. For more information, see Chapter 5, "Configuring Connectors," on page 57.
- ❒ 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 3.5, "Verifying the Identity Source User Attributes," on page 33.

8.3 Loading Authorizations

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

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

   For more information, see Chapter 5, "Configuring Connectors," on page 57.
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.

   If the Policy Mapping page does not display the SaaS application connector, you did not configure the connector properly. For more information, see Chapter 5, "Configuring Connectors," on page 57.

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

8.4 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.

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.

8.5 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/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.
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 8.7, "Approving Requests," on page 96.
7. Click **OK** to map the SaaS authorization to the identity source group.

The mapping grants access for users that 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 OSP Welcome 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.

8.6 A Mapping Example

Use the following example steps 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. On the Policy Mapping page:
   - **3a** Load the authorizations for the connector for Google Apps for Business.
   - **3b** In the **Role Name** column, select the connector for Active Directory.
   - **3c** In the right pane, select the connector for Google Apps.
   - **3d** Drag and drop the Google Apps Account into the left pane, over the Google AppsUsers group.

3e 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 to either create an account or specify an existing account the first time they log in.

4 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.

8.7 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/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 that 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 that 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.

9 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.

9.1 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`.
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 blue bar.
7. Enter the Tracking ID (not the tracking code) that Google provided during the registration process and click **OK**.
8. Click **Apply** and wait for the appliance to update.

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

9.2 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, ssh 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 bar.

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.

10 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 welcome pages so they display your company's branding instead of the default NetIQ branding.

10.1 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 21.

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

---

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.

10.2 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.

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.

10.3 Customizing Login, Logout, and Welcome Pages

CloudAccess allows you to customize user-facing pages, such as the login, logout, and welcome pages, 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

- If you implemented custom branding in CloudAccess 1.5, that branding is not compatible with CloudAccess 2.0. You must download, customize, and import compatible 2.0 branding files after you have upgraded your cluster. For more information, see Section 2.6, “Upgrading Your Environment,” on page 24.
- Customizing the login, logout, and welcome pages 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 2.8, “Initializing the Appliance,” on

page 27.

To customize the login, logout, and welcome pages:

1. Take a snapshot of the appliance.
2. Log in with an appliance administrator account to the Admin page at `https://dns_of_appliance/appliance/index.html`.
3. On the toolbar, click the Tools icon, then click **End user branding**.
4. Click **Download Default Login Pages**.
5. Save the file to your local computer.
6. Save a backup copy of the file.
7. Unzip the downloaded file and locate the `.jsp` files in the `osp\jsp` subdirectory.
8. 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.
9. Zip up the files again, but include only the `images` and `jsp` directories.
10. Log in to the Admin page again.
11. On the toolbar, click the Tools icon, then click **End user branding**.
12. (Conditional) If you are customizing pages for the first time, click **Browse**, then browse to and select the modified file.
13. (Conditional) If you are updating previously customized pages, delete the name of the existing file that appears in the **Branding zip file** field. Click **Browse**, then browse to and select the `.zip` file that contains the newly modified `.jsp` files.
14. Wait until the file name changes to a hexadecimal value, then click **OK**.
15. Click **Apply**.

The pages now display the branding you customized in the `.jsp` files.

11 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.

11.1 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**.

11.2 Configuring Session Timeouts

The admin session timeout is set to 5 minutes and is not configurable. The user session timeout is set to 10 minutes by default and 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**.

11.3 Changing the IP Address

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

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

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

3 Select whether the appliance uses DHCP or a static IP address.

   If you select to use a static IP address, you can change the required values for the subnet mask, default gateway, and the DNS server.

4 Click **OK** to save the changes, then click **Apply** to apply the changes to the appliance.

11.4 Changing 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/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.

11.5 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 3.2, “Registering CloudAccess,” on page 30.

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. 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 12.1, "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.

11.6 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.

12 Troubleshooting CloudAccess

Use the information in the following sections to troubleshoot any issues you might encounter.

12.1 Displaying Health

CloudAccess displays health status information for each node and for the cluster on 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.

12.2 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/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 12-1 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 12-1 *Troubleshooting Log Files*

Feature	Logs
Initialization or commands	ConfigurationReplicator.log
	ConfigurationReplicator_RL.log
	messages
	boot*
	packageoperations.log
	dserv.log
	firewall
Admin.html UI	adminui.log
Registration	register.log
Updates	zypper.log
	downloadUpdate.log
	afterUpdate.log
	beforeUpdate.log
	rpmsAfterUpdate.log
	rpmsBeforeUpdate.log
	rpmsUpdateDiff.log
	300_appliance_SnapshotUconPackages.sh.log
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

Feature	Logs
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

12.3 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.

12.3.1 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.

12.3.2 Front Panel of the Node

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

Figure 12-1 *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 12.2, “Troubleshooting Tools,” on page 107.
4. Restart the appliance, then wait at least another five minute cycle for all nodes to display the current state.

12.3.3 Top of the Node

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

Figure 12-2 *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.

12.3.4 Identity Source

The health indicator for the identity source is the small identity source icon.

Figure 12-3 *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.

Clear: 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 12-1 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.

12.3.5 Applications

The health indicator is the small cloud icon on each application connector.

Figure 12-4 *Application Indicator*

The states are:

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.

Clear: 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 12-1 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.

12.4 Provisioning Behavior

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 12-2 *Provisioning Actions*

Identity Sources	SaaS Applications
Delete a user.	Disables the SaaS account.
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.

Identity Sources	SaaS Applications
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.

12.5 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.

12.6 Valid Salesforce Credentials Fail

Configuration of the connector for Salesforce may fail, even with valid credentials. One possible reason is that the Salesforce password has expired. Log in to the Salesforce site and reset your password. You receive a new password and a new security token. Use these credentials when creating the connector for Salesforce.

Even if your credentials are correct, you may occasionally be unable to log in to Salesforce, and the connector for Salesforce in CloudAccess may show an intermittent red status. Salesforce has API metering that limits the number of calls during a 24-hour period. For more information, see the following Salesforce resources:

- http://www.salesforce.com/us/developer/docs/api/Content/implementation_considerations.htm#sforce_api_rate_metering (http://www.salesforce.com/us/developer/docs/api/Content/implementation_considerations.htm#sforce_api_rate_metering)
- http://boards.developerforce.com/t5/General-Development/REQUEST-LIMIT-EXCEEDED/td-p/24901 (http://boards.developerforce.com/t5/General-Development/REQUEST-LIMIT-EXCEEDED/td-p/24901)

12.7 Troubleshooting the Connector for Office 365

Use the information in the following sections to help you troubleshoot issues with the connector for Office 365:

- Section 12.7.1, "Obtaining Installation and Provisioning Logs," on page 114
- Section 12.7.2, "Office 365 Logout Error on Mobile Devices," on page 114

12.7.1 Obtaining Installation and Provisioning Logs

By default, CloudAccess does not generate an installation log when you install the connector for Office 365. If you want a log of the installation, you must launch the installer from the command line using the appropriate command. For more information, see Section 5.2.3, "Installing the Connector for Office 365," on page 63.

The connector for Office 365 integrates with the Windows Event Log. The Windows Event Log displays the connector for Office 365 events as O365ConnectorEventLog. For more information about the Windows Event Log, see Windows Event Log (http://msdn.microsoft.com/en-us/library/windows/desktop/aa385780%28v=vs.85%29.aspx).

12.7.2 Office 365 Logout Error on Mobile Devices

If you configure Office 365 applications to launch with Safari on mobile devices, users are likely to encounter an issue when they try to log out of Office 365. When they tap the **Sign out** link at Office 365, they get the following Microsoft error: "Sorry, but we're having trouble signing you out." If they go back to the MobileAccess app and tap the Office 365 appmark again, they get another Microsoft error: "Sorry, but we're having trouble signing you in."

Once this issue has occurred, the workaround for users to be able to use the Office 365 appmark again is to manually clear the cache and cookies in the Safari browser. However, if you want users to launch Office 365 in Safari, you can avoid this issue by having them set Safari's cookie handling to "Never" block cookies. On iOS mobile devices this option is in the following location: **Settings** > **Safari** > **Privacy and Security** > **Block Cookies**.

12.8 Troubleshooting Custom Connectors

Custom connectors allow for authentication into other systems, but they do not provide provisioning of user accounts. Unlike the connector for Salesforce, CloudAccess does not create a specific log for each custom connector.

CloudAccess captures all information about custom connectors in the `catalina.out` file. To troubleshoot issues with custom connectors and capture the information in the `catalina.out` file, perform the following steps:

1. Log in with an appliance administrator account to the Admin page at `https://`*`appliance_dns`*`/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 **Authentication / Single Sign-on** to increase the logging levels.
5. Duplicate the error or condition.
6. Click **Download CloudAccess Log Files** to download the logs.
7. Extract the download file and search for `catalina.out`.
8. Open `catalina.out` in a text editor, then search for errors in association with your custom connector.

A Open Source Licenses

A.1 Documentation

The following sources provide information about CloudAccess:

- **Installation:** *NetIQ CloudAccess and MobileAccess Installation and Configuration Guide*
- **Online product documentation:** NetIQ CloudAccess and MobileAccess documentation website (http://www.netiq.com/documentation/cloudaccess/install_config/data/bookinfo.html).

A.2 Open Source Components

A.2.1 ActiveMQ-CPP Library

See Section A.3.1, “Apache 2.0 License,” on page 126.

http://www.ohloh.net/p/activemq/contributors (http://www.ohloh.net/p/activemq/contributors)

Doxygen

Oren Ben-kiki

30+

A.2.2 ActiveMQ

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright The Apache Software Foundation

A.2.3 Apache 2.2.17

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright (c) 2001-2009, The Apache Software Foundation

A.2.4 Apache Commons Logging 1.1.1

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright The Apache Software Foundation

A.2.5 Apache Portable Runtime 1.4.2

See Section A.3.1, “Apache 2.0 License,” on page 126.

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.2.6 Argo 2.21

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright 2011 Mark Slater

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.2.7 Bouncy Castle 1.5.140

See Section A.3.2, “BouncyCastle - Adaptation of the MIT X11 License,” on page 129.

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

A.2.8 dom4j 1.6.1

See Section A.3.3, “BSD Style License,” on page 130.

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

A.2.9 dovecot20-backend-pgsql-2.0.20-31.1

See Section A.3.4, “MIT,” on page 130 Dovcot - MIT.

See Section A.3.5, “LGPL V2.1,” on page 131 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.2.10 dovecot20-backend-mysql-2.0.20-31.1

See Section A.3.4, “MIT,” on page 130 Dovcot - MIT.

See Section A.3.5, “LGPL V2.1,” on page 131 Dovecot - LGPL V2.1.

See Section A.2.9, “dovecot20-backend-pgsql-2.0.20-31.1,” on page 119.

A.2.11 dovecot20-backend-sqlite-2.0.20-31.1

See Section A.3.4, “MIT,” on page 130 Dovcot - MIT.

See Section A.3.5, “LGPL V2.1,” on page 131 Dovecot - LGPL V2.1.

See Section A.2.9, “dovecot20-backend-pgsql-2.0.20-31.1,” on page 119.

A.2.12 dovecot20-2.0.20-31.1

See Section A.3.4, “MIT,” on page 130 Dovcot - MIT.

See Section A.3.5, “LGPL V2.1,” on page 131 Dovecot - LGPL V2.1.

See Section A.2.9, “dovecot20-backend-pgsql-2.0.20-31.1,” on page 119.

A.2.13 dovecot20-devel-2.0.20-31.1

See Section A.3.4, “MIT,” on page 130 Dovcot - Mit.

See Section A.3.5, “LGPL V2.1,” on page 131 Dovecot - Lgpl V2.1.

See Section A.2.9, “dovecot20-backend-pgsql-2.0.20-31.1,” on page 119.

A.2.14 GTM-OAuth2 v2

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright (c) 2011 Google Inc.

A.2.15 GWT 2.4.0

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright (c) Google, Inc. 2009. All rights reserved. All other product, service names, brands, or trademarks, are the property of their respective owners.

A.2.16 GWT Mosaic 0.4.0-rc4

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright (c) Google, Inc. 2009. All rights reserved. All other product, service names, brands, or trademarks, are the property of their respective owners.

A.2.17 gwtupload 0.6

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright 2009 Manolo Carrasco (Manuel Carrasco MoÃ±ino)

A.2.18 Hibernate 3

See Section A.3.5, “LGPL V2.1,” on page 131.

Copyright © 2007 by Red Hat, Inc. This copyrighted material is made available to anyone wishing to use, modify, copy, or redistribute it subject to the terms and conditions of the GNU Lesser General Public License, as published by the Free Software Foundation.

A.2.19 httpclient 4.1.2

See Section A.3.1, “Apache 2.0 License,” on page 126.

Apache HttpComponents Client Copyright 1999-2009 The Apache Software Foundation. This product includes software developed by The Apache Software Foundation (http://www.apache.org/).

This project contains annotations derived from JCIP-ANNOTATIONS

Copyright (c) 2005 Brian Goetz and Tim Peierls. See http://www.jcip.net

Apache HttpComponents Core – HttpCore

Copyright 2006-2009 The Apache Software Foundation

This product includes software developed by The Apache Software Foundation (http://www.apache.org /).

A.2.20 JavaMail 1.4.3

See Section A.3.6, “Javamail,” on page 137.

Sun Microsystems, Inc.

A.2.21 JavaService 2.0.10

See Section A.3.7, “JavaService,” on page 142.

See Section A.3.5, “LGPL V2.1,” on page 131.

Copyright owner John Rutter

A.2.22 Jaxb 2.2

See Section A.3.8, “COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0,” on page 143.

See Section A.3.9, “GPL V2 + classpath exception dual license.,” on page 148.

A.2.23 jersey 1.0.3

See Section A.3.8, “COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0,” on page 143.

See Section A.3.9, “GPL V2 + classpath exception dual license.,” on page 148.

A.2.24 KKPasscodeLock 0.2.2

See Section A.3.1, “Apache 2.0 License,” on page 126.

A.2.25 libvmtools 9.0.0-9.1

See Section A.3.12, “GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999,” on page 156.

See Section A.3.13, “GNU GENERAL PUBLIC LICENSE Version 2,” on page 163.

See Section A.2.32, “Open-vm-tools 9.2.3-113.1,” on page 124.

A.2.26 log4cxx 0.10.0

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright (c) 2004-2007 The Apache Software Foundation

A.2.27 log4j 1.2.15

See Section A.3.1, “Apache 2.0 License,” on page 126.

Copyright (c) The Apache Software Foundation

A.2.28 NTLM Library (TCP implementation) 2

See Section A.3.10, “Microsoft Public License MS-PL,” on page 153.

Microsoft Public License MS-PL

Could not find an explicit copyright notice. The source code headers include the following author:

Auteur : Dominique GUERIN

* dominiqueph.guerin@gmail.com

* dominique.guerin@insee.fr

* Le code est utilisable, modifiable et redistribuable à volonté sous la seule condition de ne pas supprimer ces 7 lignes.

A.2.29 OpenInChromeController

See Section A.3.14, “OpenInChromeController,” on page 167.

BSD Style License (OpenInChrome)

Copyright 2013, Google Inc. All rights reserved.

A.2.30 OpenSAML 2.0

See Section A.3.1, “Apache 2.0 License,” on page 126.

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.2.31 OpenSSL 1.0.0a

See Section A.3.11, “OpenSSL License and SSLeay License,” on page 154.

A.2.32 Open-vm-tools 9.2.3-113.1

See Section A.3.12, “GNU LESSER GENERAL PUBLIC LICENSE Version 2.1, February 1999,” on page 156.

See Section A.3.13, “GNU GENERAL PUBLIC LICENSE Version 2,” on page 163.

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.2.33 Recaptcha4j 0.0.8

See Section A.3.1, “Apache 2.0 License,” on page 126.

A.2.34 snmp4j

See Section A.3.1, “Apache 2.0 License,” on page 126.

A.2.35 Tomcat 7.7.0.27-10

See Section A.3.1, “Apache 2.0 License,” on page 126.

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.2.36 WSS4J

See Section A.3.1, “Apache 2.0 License,” on page 126.

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.2.37 Xalan 2.7.1

See Section A.3.1, “Apache 2.0 License,” on page 126.

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.2.38 Xerces 2.9.1

See Section A.3.1, “Apache 2.0 License,” on page 126.

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.2.39 XMLSec 1.3.0

See Section A.3.1, “Apache 2.0 License,” on page 126.

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.2.40 Zlib 1.2.3

See Section A.3.15, “Zlib 1.2.3,” on page 168.

A.3 Open Source Licenses

A.3.1 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.3.2 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.3.3 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.3.4 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.3.5 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.3.6 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.3.7 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.3.8 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.3.9 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.3.10 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.3.11 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.3.12 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.3.13 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.3.14 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.3.15 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.4 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, Novell, Inc., 1800 Novell Place, Provo, Utah 84606. With the request, please include the name of the product (CloudAccess) and the version of the product (1.1). There is a charge of $10.00 USD for each request to cover cost of media and shipping.