Installation and Configuration Guide

NetIQ Access Gateway for Cloud 1.0

October 2012

Legal Notice

NetIQ Product Name is protected by United States Patent No(s): nnnnnnnn, nnnnnnnn, nnnnnnnn.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/.

Contents

About This Guide

This guide explains how to install and configure Access Gateway for Cloud.

Audience

This guide is intended for Active Directory administrators, Google Apps for Business administrators, and Salesforce administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

Documentation Updates

For the most recent version of the *NetIQ Access Gateway for Cloud Installation and Configuration* Guide, visit the NetIQ Access Gateway for Cloud documentation Web site (http://www.netiq.com/documentation/accessgatewaycloud/).

1 Overview of Access Gateway for Cloud

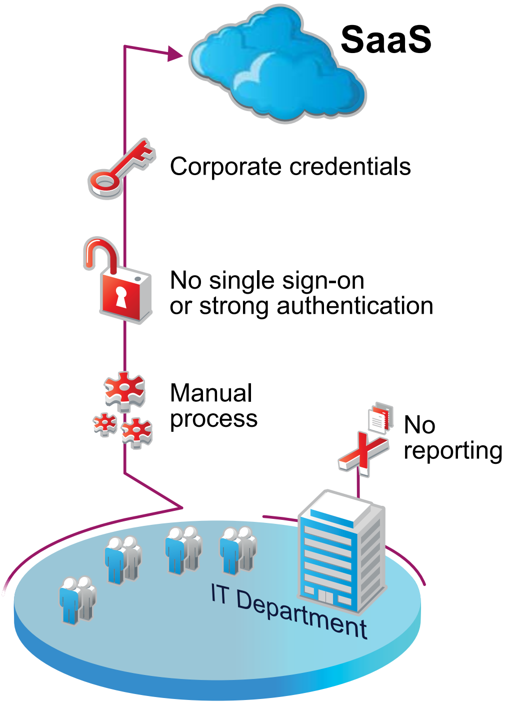
Access Gateway for Cloud is an appliance that allows you to easily and quickly provide secure access to Software-as-a-Service (SaaS) applications for your corporate users.

- Section 1.1, "Inherent Problems Using SaaS Applications," on page 7
- Section 1.2, "The Solution Access Gateway for Cloud Provides," on page 8
- Section 1.3, "How Access Gateway for Cloud Works," on page 9
- Section 1.4, "How to Manage Access Gateway for Cloud," on page 9

1.1 Inherent Problems Using SaaS Applications

A lot of users want to use SaaS applications to increase business agility. If the corporation does not provide an easy way for the users to obtain accounts for the SaaS applications, many users might by-pass the IT department and create their own accounts. Figure 1-1 depicts some of the problems that can occur.

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



Those problems include the following:

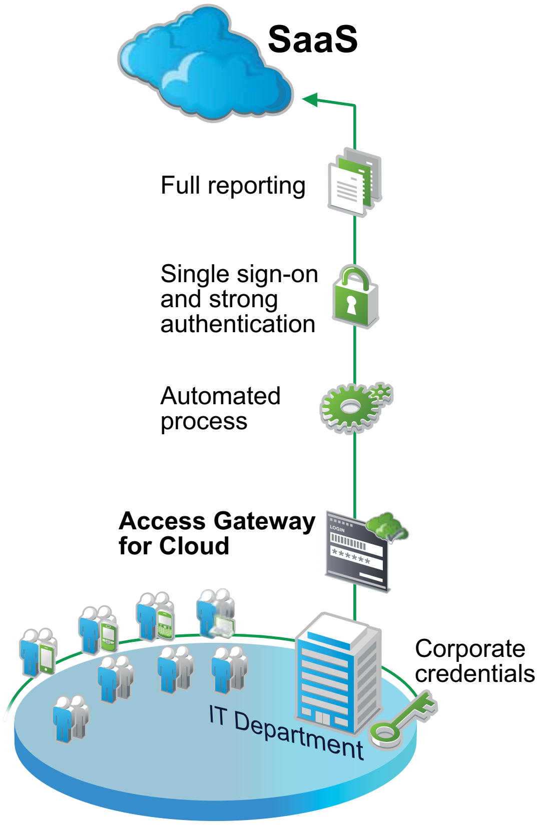
- Users by-pass the IT department and create their own accounts in the SaaS Application.

- Users must wait for the IT department to create accounts in the SaaS applications. It is a manual process, whether the IT department creates the account or if 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 Access Gateway for Cloud Provides

Access Gateway for Cloud provides a simple, secure solution to the problems presented with using SaaS applications.

Figure 1-2 *Access Gateway for Cloud Solution*



Access Gateway for Cloud provides the following:

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

1.3 How Access Gateway for Cloud Works

Access Gateway for Cloud is a virtual appliance that provides a Web service for users to access the SaaS applications securely. The appliance performs the following functions:

- **Provisioning:** Access Gateway for Cloud allows you to map account authorizations in Active Directory to account authorizations in the SaaS applications. After mapping the authorizations, by leveraging group management in Active Directory, Access Gateway for Cloud automatically creates and manages the associated user accounts in the SaaS application.
- **Secure Single Sign-on:** Access Gateway for Cloud provides single sign-on to the SaaS applications and includes Integrated Windows Authentication. Provisioned users automatically have access to the SaaS applications, if they are logged in to the Active Directory domain. The corporate credentials never leave the firewall.
- **Reporting:** Access Gateway for Cloud provides reports of the usage of the SaaS applications to enforce corporate policies and prove compliance.
- **Enabling Mobile Devices:** Access Gateway for Cloud enables mobile devices to securely access the SaaS applications.

1.4 How to Manage Access Gateway for Cloud

You manage Access Gateway for Cloud through Web pages in the following format:

```
https://dns_of_ag4c_appliance/appliance/Web_page.html
```

- **Init.html:** Initializes the appliance. For more information, see Section 2.6, “Initializing the Appliance,” on page 15.
- **Admin.html:** Configures and maintains the appliance. For more information, see Section 3.1, “Accessing the Administration Page,” on page 17.
- **PolicyMapping.html:** Maps authorizations between Active Directory and the SaaS applications. For more information, see Chapter 5, “Mapping Authorizations,” on page 29.
- **Approval.html:** Approves or denies authorizations for the SaaS applications. For more information, see Chapter 6, “Approving Requests,” on page 33.
- **Reporting.html:** Reports on the user activities to the SaaS applications. For more information, see Chapter 7, “Reporting,” on page 35.

Proceed to Chapter 2.1, “Access Gateway for Cloud Installation Worksheet,” on page 11 to gather the information required to install and configure the appliance.

2 Installing Access Gateway for Cloud

Access Gateway for Cloud is a VMware appliance that you download and deploy into your IT environment.

2.1 Access Gateway for Cloud Installation Worksheet

Use the following worksheet to gather the required information to install and configure Access Gateway for Cloud.

- ❐ **Networking Information:** Gather your networking information:
  - ❐ Publicly resolvable DNS name for the appliance
  - ❐ NTP server
  - ❐ DNS server, subnet mask, and gateway
- ❐ **Identity Source (Active Directory):** Gather the following information or perform the following tasks to configure the identity source for Access Gateway for Cloud:
  - ❐ The IP address or DNS name of the server that contains the users
  - ❐ Context of the users
  - ❐ Name and password of a user with read rights to the users
- ❐ **Google Apps for Business:** Gather the following information to configure the Connector for Google Apps for Business:
  - ❐ Provisioning APIs enabled
  - ❐ Administrator name and password
  - ❐ Domain name
- ❐ **Salesforce:** Gather the following information to configure the Connector for Salesforce:
  - ❐ Provisioning APIs enable
  - ❐ Administrator name and password
  - ❐ Security token
  - ❐ Salesforce.com login URL

2.2 Requirements

Use the information in the following table to verify you meet the requirements for Access Gateway for Cloud before deploying the appliance.

Table 2-1 *Access Gateway for Cloud Requirements*

Components	Requirements
VMware	One of the following versions of VMware: ◆ vSphere Hypervisor 5.0 ◆ vSphere 5.0 ◆ ESXi 4.1 ◆ ESX 4.1
Node	Minimum hardware requirements for each node in the appliance: ◆ 60 GB disk space ◆ 2 Cores ◆ 8 GB RAM
Browsers	**Administration:** The supported browsers for administration tasks are: ◆ Firefox 10 and 11 ◆ Chrome **Users:** The supported browsers for users are: ◆ IE 9 on Windows 7 ◆ Firefox 10 and 11 on Windows 7
Cluster	Supported cluster configuration: ◆ Up to a five node cluster ◆ Each node must reside in the same time zone ◆ Each node must reside in the same IP subnet
Email Clients	Supported email clients for the email proxy are: ◆ Windows Live Mail 2011 ◆ Latest iPhone iOS
DNS	Access Gateway for Cloud requires that all appliance nodes, administration workstations, end user workstations, and identity sources be able to resolve the public DNS name of the appliance.
Salesforce	Obtain the following required items: ◆ A full or developer account with provisioning APIs enabled ◆ Administrative account with password ◆ Security token from Salesforce ◆ Login URL from Salesforce

Components	Requirements
Google Apps for Business	Obtain the following required items: ◆ A valid Google Apps for Business account ◆ Provisioning APIs enabled on the account ◆ An administrative account and password
Active Directory	Verify that your Active Directory meets the following requirements: ◆ Windows 2008 R2 only. ◆ A unique identity for each user account whether you have one or more domains. Access Gateway for Cloud uses the sAMAccountName as the unique identifier for the users. ◆ Populate all of the required Active Directory attributes on the Active Directory users. For more information, see Section 3.4, “Verifying the Identity Source User Attributes,” on page 18. Obtain the following required items: ◆ The password and the fully distinguished LDAP formatted name of a user in Active Directory that has read access. This user makes 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 search context of the domains. ◆ The IP address of one or more Active Directory servers that contain the users. ◆ The context of the users in Active Directory.

2.3 Merging Existing Accounts

If any of your existing Active Directory users have existing accounts in Google Apps for Business or Salesforce.com, Access Gateway for Cloud merges these accounts under the following conditions.

Google Apps for Business: If the sAMAccountName attribute in Active Directory matches the name in the email address of the Google Apps for Business account, Access Gateway for Cloud merges the existing Active Directory account and Google Apps for Business accounts. The merge process resets the password of the Google Apps for Business account to a password generated by the appliance. In order to log in, users must use the URL listed in Chapter 4, “Providing Access to the SaaS Applications for Users,” on page 27.

Salesforce: If the sAMAccountName attribute in Active Directory matches the name in the email address of the Salesforce account, Access Gateway for Cloud merges the existing Active Directory account and Salesforce accounts. The merge process resets the password of the Salesforce account to a password generated by the appliance. In order to log in, users must use the URL listed in Chapter 4, “Providing Access to the SaaS Applications for Users,” on page 27.

2.4 Deploying the Appliance

Access Gateway for Cloud is an OVF virtual appliance. For more information about virtual appliances, see What is OVF? (http://www.vmware.com/appliances/getting-started/learn/ovf.html).

You must deploy the appliance to your VMware server.

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 Access Gateway for Cloud virtual appliance.

   For more information, see Deploy Virtual Appliances (http://www.vmware.com/it/appliances/getting-started/deploy/get_started.html).

3 If you do not have a DHCP server in your environment, skip to Section 2.5, "Configuring the Appliance without a DHCP Server," on page 14.

   or

   Power on the appliance, then proceed to Section 2.6, "Initializing the Appliance," on page 15.

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

You can deploy the OVF file or convert the OVF file to a VMX file. If you use the VMX file, disable the default option of **Synchronize guest time with host** option for the image. Right-click the appliance in the VMware client, then deselect **Edit Settings** > **Options** > **VMware Tools > Synchronize guest time with host**.

2.5 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. You can assign a static IP address after the initial boot without editing the VMware settings, if a DCHP server exists in your environment.

Edit the VMX file and add the following lines with the 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 line, either leave the value blank, or leave the line out of the VMX file altogether. Power on the appliance, then proceed to Section 2.6, "Initializing the Appliance," on page 15.

2.6 Initializing the Appliance

You must now initialize the appliance.

1. Verify that you meet the requirements listed in Section 2.2, "Requirements," on page 12.
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://`*`ip_address`*`/appliance/Init.html`
3. Fill in the fields displayed to initialize the appliance.
4. Click **Finish**.

   A successfully initialized appliance automatically redirects the browser to the Access Gateway for Cloud administration login page (`https://`*`dns_of_ag4c_appliance`*`/appliance/Admin.html`).
5. Specify the admin username of the appliance and password, then proceed with Chapter 3, "Configuring the Appliance," on page 17.

3 Configuring the Appliance

After you have initialized the appliance, configure the appliance to communicate with the SaaS applications.

3.1 Accessing the Administration Page

After you properly initialize the appliance using the information in Section 2.6, “Initializing the Appliance,” on page 15, the browser automatically redirects to the administration page. If not, access the administration page as follows:

1. In a supported browser, enter `https://`*`dns_of_ag4c_appliance`*`/appliance/Admin.html`.
2. Log in as the administrator of the appliance as specified during the initialization process.

   This username is the samAccountName and Active Directory password of this user.

After you log in, the appliance activates users in the search contexts from Active Directory. Ensure this process completes before configuring any SaaS applications.

3.2 Registering Access Gateway for Cloud

Access Gateway for Cloud 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. The bomb icon remains on the Admin page if there are nodes in the cluster that have not yet been registered.

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 SUES customers.

2. Under **My Products**, select **Access Gateway for Cloud**.
3. Select **License Key**, then save the license key to a location where you can access it from your Access Gateway for Cloud appliance.
4. Log on to your Access Gateway for Cloud appliance and access the Admin page.

   For more information, see Section 3.1, “Accessing the Administration Page,” on page 17.
5. Click the appliance, then click **Register Appliance**.
6. Enter the email address you used when you registered with the Customer Center.
7. Enter the license key you downloaded from the Customer Center.
8. Click **Register**.
9. Repeat Step 5 through Step 8 for each appliance in the cluster.

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

3.3 Configuring Additional Identity Sources

Access Gateway for Cloud supports one or more Active Directory domains (identity sources) to use as a source for provisioning accounts to the SaaS applications. The initial Active Directory domain is configured during the initialization of the appliance.

In the Admin page, click **Active Directory > Configure** to change the initial Active Directory configuration information.

To add another Active Directory domain as an identity source:

1. Access the Access Gateway for Cloud administration page.

   For more information, see Section 3.1, “Accessing the Administration Page,” on page 17.
2. Drag and drop an Active Directory icon from the Identity Palette to the bar in the middle of the page.
3. Click the Active Directory icon, then click **Configure**.
4. Fill in the fields to configure the new Active Directory domain, then click **OK** to save the configuration information.
5. Click **Apply** to commit the changes to the appliance.

3.4 Verifying the Identity Source User Attributes

To successfully provision Active Directory users to the SaaS applications, each Active Directory user must contain the following attributes. Access Gateway for Cloud uses these mandatory attributes to provision the accounts to Google Apps for Business and Salesforce. The mandatory attributes are as follows:

- First Name
- Last Name
- Full Name
- sAMAccountName or Logon Name (Pre-Windows 2000)
- User Principal Name (UPN)
- Email address

3.5 Configuring Clustering

You can cluster the Access Gateway for Cloud appliance. By default, it is a single node cluster. You add a node to the cluster by selecting **Join Cluster** during the initialization process. Access Gateway for Cloud supports up to a five node cluster.

- Section 3.5.1, "Advantages of Clustering," on page 19
- Section 3.5.2, "Managing Nodes in the Cluster," on page 19
- Section 3.5.3, "Configuring an L4 Switch for Clustering," on page 21
- Section 3.5.4, "Configuring an L4 Switch for Email Proxy," on page 21

3.5.1 Advantages of Clustering

Access Gateway for Cloud provides clustering for different advantages. Most of these advantages are only available 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 goes down or becomes corrupt, you can promote another node to master.

High Availability for Authentications: Access Gateway for Cloud 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 Access Gateway for Cloud. Each node in the cluster increases the number of possible simultaneous logins.

3.5.2 Managing Nodes in the Cluster

Access Gateway for Cloud supports up to five nodes in a cluster. You add nodes to the cluster through the initialization process, and perform all other initialization tasks in the Admin page.

- "Adding a Node to the Cluster" on page 19
- "Promoting a Node to Master" on page 20
- "Removing a Node from the Cluster" on page 20

Adding a Node to the Cluster

Follow the steps listed below to successfully add a node to the cluster:

1. Verify the cluster is healthy.
   - All nodes must be up and communicating.
   - All components must be in a green state.
   - All failed nodes must be removed from the cluster.

   For more information on verifying your cluster is healthy, see Section 10.3, "Troubleshooting Different States," on page 47.
2. Download and deploy a new VM machine for the new node.

   For more information, see Section 2.4, "Deploying the Appliance," on page 14.

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

   For more information, see Section 2.6, "Initializing the Appliance," on page 15.

4 Wait for the login screen for the Admin page to be displayed. A progress bar indicates how much time this take. The process completes when the login screen for the Admin page is displayed.

5 Log in to the Admin page, and wait for all spinner icons to stop processing and all components are green before performing any other tasks.

   The cluster is adding the node and there are a lot of back ground process running. This final step could take up to an hour to complete.

Promoting a Node to Master

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

1 Take a snapshot of the cluster.

2 Verify the cluster is healthy.

   For more information, see Section 10.3, "Troubleshooting Different States," on page 47.

3 Click the node to become the master node in 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.

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

When you switch the master node, the logs start again on the new master and reports start again on the new master. The historical logs are lost. The reporting data is also lost, unless you are using Sentinel Log Manager. For more information, see Section 7.2, "Integrating with Sentinel Log Manager," on page 35.

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.

Removing a Node from the Cluster

You can remove a node from the cluster if something is wrong with the node. However, after removing a node, it cannot be added 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.

2 (Conditional) If you are using an L4 switch, delete the node from the L4 switch.

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

4 Click **Remove from Cluster**.

The interface immediately reflects that the node is gone, but it takes some time for the background processes to finish.

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

3.5.3 Configuring an L4 Switch for Clustering

If you want high availability or load balancing, you must configure an L4 switch for the Access Gateway for Cloud 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://dns_ag4c_appliance/osp/h/heartbeat
```

or

```
https://ip_address_ag4c_appliance/osp/h/heartbeat
```

The L4 switch uses the heartbeat to determine if the node in the cluster is up and working or not. The heartbeat URL returns a text message of Success and a 200 response code.

- **Persistence:** Also known as sticky sessions, allows all subsequent requests from a client to be sent to the same computer. 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.

3.5.4 Configuring an L4 Switch for Email Proxy

Access Gateway for Cloud contains an email proxy 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. Refer to your specific L4 documentation for further information.

- "Configuring the SMTP Protocol Handler" on page 21
- "Configuring the POP Protocol Handler" on page 22
- "Configuring the IMAP Protocol Handler" on page 22

Configuring the SMTP Protocol Handler

Use the following steps 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 time out 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

Use the following steps 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 time out 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

Use the following steps 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.

3.6 Configuring the Connector for Google Apps for Business

Each cluster supports only one Connector for Google Apps for Business. You must configure the Connector for Google Apps for Business to provision accounts into Google Apps for Business.

You can configure the connector to allow users single sign-on access into Google Apps for Business. When users log in to Active Directory, Access Gateway for Cloud automatically authenticates the users to Google Apps for Business. Providing single sign-on to the users increases the security of your company's information stored in Google Apps for Business.

1 Access the Access Gateway for Cloud administration page.

   For more information, see Section 3.1, "Accessing the Administration Page," on page 17.

2 Drag and drop the Connector for Google Apps for Business from the SaaS Palette to the bar.

3 Click the Connector for Google Apps for Business, then click **Configure**.

4 Fill in the fields to configure the connector, then click **OK** to save the configuration information.

   Selecting the single sign-on option allows uses to authenticate to Active Directory, then Access Gateway for Cloud automatically authenticates the user's login to Google Apps for Business.

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

After you enable single sign-on, all users must authenticate through Access Gateway for Cloud to access Google Apps for Business. For more information, see the SAML SSO section of the Google Apps for Business FAQ (http://code.google.com/googleapps/faq.html).

3.7 Configuring the Connector for Salesforce

Each cluster supports only one Connector for Salesforce.You must configure the Connector for Salesforce to provision accounts into Salesforce.

You can configure the connector to allow users single sign-on access into Salesforce. When users log in to Active Directory, Access Gateway for Cloud automatically authenticates the users to Salesforce. Providing single sign-on to the users increases the security of your company's information stored in Salesforce.

1 Access the administration page.

   For more information, see Section 3.1, "Accessing the Administration Page," on page 17.

2 Drag and drop the Connector for Salesforce from the SaaS Palette to the bar.

3 Click the Connector for Salesforce, then click **Configure**.

4 Fill in the fields to configure the connector.

5 (Conditional) Configure the Connector for Salesforce to allow single sign-on for users:

5a Generate a `.pem` file from the Connector for Salesforce.

5a1 Click **Configure** on the Connector for Salesforce in the Admin page.

5a2 Click **Single Sign-On Settings**, then click **Download Certificate**.

5a3 Follow the prompts to save the `.pem` file.

5b Log into Salesforce as an administrator.

5c Select **Setup** from the drop-down menu.

5d Click **Security Controls** under **Administration Set Up** in the left pane.

5e Click **Single Sign On Settings**.

5f Click **Edit**, then use the following information to configure single sign-on:

SAML Enabled: Check this option.

SAML Version: Specify 2.0 for the version.

Issuer: Specify the following URL:

```
https://<dns_of_ag4c_appliance>/osp/a/t1/auth/saml2/metadata
```

Identity Provider Certificate: Click **Browse**, then browse to and select the `.pem` file created in Step 5a.

Identity Provider Login URL: Specify the following URL:

```
https://<dns_of_ag4c_appliance>/osp/a/t1/auth/app/its/salesforce
```

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

User ID is in the NameIdentifier element of the Subject statement: Select this option.

Identity Provider Logout URL: Specify the following URL:

```
https://<dns_of_ag4c_appliance>/osp/a/t1/auth/app/logout
```

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

3.8 Configuring Integrated Windows Authentication with Kerberos

Access Gateway for Cloud allows user authentication with either name/password or Integrated Windows Authentication with Kerberos. If you choose to use Integrated Windows Authentication, you must configure Kerberos.

Access Gateway for Cloud only supports the use of one Kerberos realm. If there are multiple Active Directory domains used as the identity source, all of the domains must use the same realm. The initial domain created is the only domain where you can configure the Integrated Windows Authentication feature.

Use the following information to allow Kerberos authentication between Active Directory and Access Gateway for Cloud.

- Section 3.8.1, “Configuring the Kerberos User in Active Directory,” on page 25
- Section 3.8.2, “Configuring the Appliance to Use Integrated Windows Authentication with Kerberos,” on page 26
- Section 3.8.3, “Configuring the End User Browsers,” on page 26

3.8.1 Configuring the Kerberos User in Active Directory

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.ag4c.com and the context that has been enabled for cloud is ou=acme corporation,dc=ag4c,dc=com, use the following information to create the user.

First name: serv1

User login name: HTTP/serv1.ag4c.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:

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

For example: `setspn -A HTTP/serv1.ag4c.com@AG4C.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:

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

For example: `ktpass /out nidp.keytab /princ HTTP/serv1.ag4c.com@AG4C.COM / mapuser serv1@AG4C.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.

3.8.2 Configuring the Appliance to Use Integrated Windows Authentication with Kerberos

The following steps enable the appliance to use Kerberos.

1. Log in to the administration page.

   For more information, see Section 3.1, "Accessing the Administration Page," on page 17.
2. Click the primary Active Directory connection, then click **Configure**.
3. Click **Authentication**, then check **Integrated Windows Authentication**.
4. In 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 25.
5. Click **OK** to save the changes.
6. Click **Apply** to apply the changes to the appliance.

3.8.3 Configuring the End User Browsers

To complete the Kerberos configuration, configure the end user browser. For more information, see Section 8.3, "Configuring the End User Browsers for Kerberos Authentication," on page 38. For more information about users' authentication experience, see Section 10.7, "Typical Use Cases for Authentication to the SaaS Applications," on page 50.

4 Providing Access to the SaaS Applications for Users

After the Access Gateway for Cloud and the SaaS applications are configured, you must provide a way for users to access the SaaS applications.

Access Gateway for Cloud includes a sample landing page that contains the links for accessing the SaaS applications. You can use this page or create your own page. Access the sample landing page through the following URL:

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

After entering valid credentials, the sample landing page displays. If you access the sample landing page before configuring the SaaS connectors, the links for the SaaS applications are not displayed. The sample landing page displays the links for the SaaS applications only after they are configured properly.

On the sample landing page, the links for SaaS applications are:

- **Google Apps for Business:** `https://`*`dns_of_ag4c_appliance`*`/osp/a/t1/auth/app/its/google?target=https://mail.google.com/a/`*`your_google_domain`*
- **Salesforce:** `https://`*`dns_or_ip_of_appliance`*`/osp/a/t1/auth/app/its/salesforce`

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

If you are creating your own landing page, there are two methods to connect to the SaaS applications. You can use either method for your own landing page.

Method 1: 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 (Active Directory), 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.

Method 2: Identity Provider (IDP) Initiated Logins

1. The user clicks the link `https://`*`dns_of_ag4c_appliance`*`/osp/a/t1/auth/app/its/google?target=https://mail.google.com/a/`*`your_google_domain`* for an identity provider initiated login.
2. The browser sends a request to the appliance login URL.
3. The browser displays the Access Gateway for Cloud login form.
4. The user enters the identity source (Active Directory) 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.

Examples

The following are examples of the different logins:

IDP Initiated Login for Google Apps for Business: `https://<`*`dns_of_ag4c_appliance`*`>/osp/a/t1/auth/app/its/google?target=https://mail.google.com/a/<`*`google domain`*`>`

IDP Initiated Login for Salesforce: `https://<`*`dns_of_ag4c_appliance`*`>/osp/a/t1/auth/app/its/salesforce`

SP Initiated Login for Google Apps for Business: There are two options:

`https://mail.google.com/a/<`*`google domain`*`>`

`https://docs.google.com/a/<`*`google domain`*`>`

SP Initiated Login for Salesforce: The setup page for this feature at Salesforce is under **Setup** > **Company Profile** > **My Domain**. After Salesforce registers the domain, your URL is similar to the following that allows an SP initiated login:

`https://<`*`custom name`*`>.my.salesforce.com`

5 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 5.1, “Authorizations,” on page 29.

Authorizations give users access to resources. Access Gateway for Cloud provides a simple solution that allows you to map your Active Directory groups to the SaaS application authorizations and approve or deny access to these authorizations.

The PolicyMapping page maps the authorizations between Active Directory and the SaaS applications and allows you to select whether the authorization requires an approval or not. The Approval page allows you to accept or deny the authorization request.

5.1 Authorizations

The following table defines the authorizations in the SaaS applications.

Table 5-1 *Authorizations*

SaaS Application	Authorizations
Active Directory	groups, local groups, and global groups
Google	groups
Salesforce	groups, profiles, and roles

5.2 Prerequisites

Verify you meet the prerequisites listed before mapping SaaS application authorizations to the Active Directory groups:

- ❒ Configure SaaS Connectors. For more information, see Section 3.6, “Configuring the Connector for Google Apps for Business,” on page 23 and Section 3.7, “Configuring the Connector for Salesforce,” on page 23.

□ Ensure groups in Active Directory exist.

□ Populate the required attributes on the users in Active Directory. For more information, see Section 3.4, “Verifying the Identity Source User Attributes,” on page 18.

5.3 Loading Google Apps for Business Authorizations

1 Verify you have configured the Connector for Google Apps for Business.

For more information, see Section 3.6, “Configuring the Connector for Google Apps for Business,” on page 23.

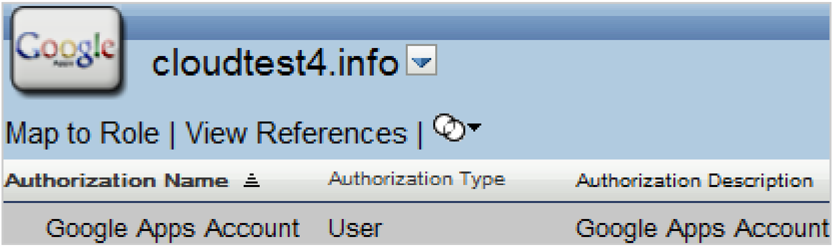
2 Access the policy mapping page in your browser by specifying:

```
https://dns_of_ag4c_appliance/appliance/PolicyMapping.html
```

3 (Conditional) Log in as the application administrator specified when you created the Connector for Google Apps for Business.

If you are currently logged into the Admin page, Access Gateway for Cloud automatically logs you in to the Policy page. No login page is displayed.

4 In the right pane, click the drop-down arrow by the Google domain, then select your Google domain name.



Authorization Name	Authorization Type	Authorization Description
Google Apps Account	User	Google Apps Account

If the Connector for Google Apps for Business is not displayed, the connector is not configured properly. For more information, see Section 3.6, “Configuring the Connector for Google Apps for Business,” on page 23.

5 Select **Group Membership** and **User**, then click **Load** to populate the PolicyMapping page with the Google Apps for Business authorizations.

5.4 Loading Salesforce Authorizations

1 Verify you have configured the Connector for Salesforce.

For more information, see Section 3.7, “Configuring the Connector for Salesforce,” on page 23.

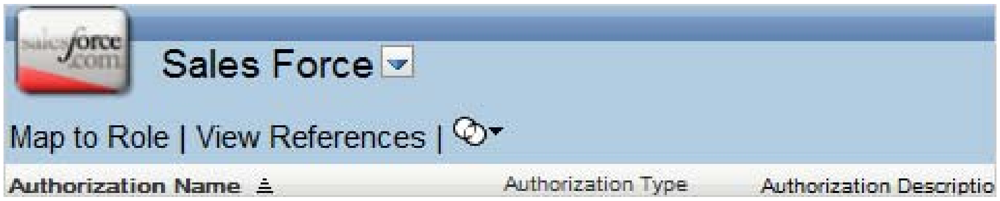
2 Access the policy mapping page in your browser by specifying:

```
https://dns_of_ag4c_appliance/appliance/PolicyMapping.html
```

3 (Conditional) Log in as the application administrator specified when you created the Connector for Salesforce.

If you are currently logged into the Admin page, Access Gateway for Cloud automatically logs you in to the Policy page. No login page is displayed.

4 In the right pane, click the drop-down arrow by the your Salesforce account name, then select your Salesforce account name.



If the Connector for Salesforce is not displayed, the connector is not configured properly. For more information, see Section 3.7, "Configuring the Connector for Salesforce," on page 23.

5 Select **Group**, **Role,** and **User**, then click **Load** to populate the PolicyMapping page with the Salesforce authorizations.

Chatter Free accounts support only one profile in Salesforce. Adding multiple authorizations to users functions as long as it is not a Chatter Free account.

5.5 Refreshing Authorizations

When performing a switch Master with the cluster nodes, or authorizations change in Active Directory or in the SaaS applications, you must refresh the authorizations in the PolicyMapping page.

1. To refresh authorizations from Active Directory, click the **Refresh List** icon in the upper right corner of the Identity Source panel.
2. To refresh authorizations from the SaaS applications, click the Refresh List icon in the upper right corner of the Authorizations panel.

5.6 Mapping Authorizations

After the authorizations load, map the SaaS application authorizations to the Active Directory groups.

1. In the right pane of the PolicyMapping page, click the drop-down arrow, then select the desired SaaS connector.
2. In the **Role Name** column on the left, select the group from Active Directory you want to map to an authorization from the selected SaaS connector, in the right pane.
3. Drag and drop the desired authorization from the SaaS connector, in the right pane, to the center mapping pane.
4. (Optional) Select **Approval**, if an approval is required to grant access.

   NetIQ recommends a maximum of 2,000 simultaneous approvals. For more information about approvals, see Chapter 6, "Approving Requests," on page 33.
5. Click **Apply**, then **OK** to map the SaaS authorization to the Active Directory group.

The mapping grants any users of the existing group authorization to the SaaS application resource. Add new users to the mapped group, and they automatically receive the authorization for the SaaS application as long as they have a user account authorization.

5.7 A Mapping Example

Use the following example steps to see how mapping works.

1 In Active Directory:

   1a Create a group named GoogleAppsUsers in Active Directory.

   1b Add users to the GoogleAppsUsers group.

2 In Google Apps for Business, create a Google Apps Account group.

3 On the PolicyMapping page:

   3a Load the authorizations for the Connector for Google Apps for Business.

   3b In the **Role Name** column, select the GoogleAppsUsers group.

   3c In the right pane, select the Google Apps Account.

   3d Drag and drop the Google Apps Account into the center pane.

   3e Click **Apply**, then **OK**.

   The appliance automatically adds all users in the GoogleAppsUsers group to the Google Apps Account group.

4 In Active Directory, create a new user, then add them to the GoogleAppsUsers group.

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

6 Approving Requests

Access Gateway for Cloud 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.

By default, Access Gateway for Cloud automatically provisions users according to mapping authorizations. To enable approvals:

1. Select **Approval** when you map the authorizations from Active Directory to the SaaS applications on the PolicyMapping page.
2. Access the Approval page at:

`https://`*`dns_of_ag4c_appliance`*`/appliance/Approval.html`

3. Select the desired authorization, then click **Approve** or **Deny**.

NetIQ recommends a maximum of 2,000 simultaneous approvals.

7 Reporting

Access Gateway for Cloud provides reports of users' activity through the appliance.

- Section 7.1, "Running a Report," on page 35
- Section 7.2, "Integrating with Sentinel Log Manager," on page 35

7.1 Running a Report

Access Gateway for Cloud contains predefined reports you run to gather information about users' activity.

To run a report:

1 In a supported browser, access the reporting page at

`https://`*`dns_of_ag4c_appliance`*`/appliance/Reporting.hmtl`

2 Log in as the administrator of Access Gateway for Cloud.

3 If you want to see the description of the report before you run it, select the **Show Descriptions** option.

4 Click the desired report, then click **Run**.

5 Click the report name to download and save the report.

After the report finishes, the report name becomes a hyperlink to view or download the report.

7.2 Integrating with Sentinel Log Manager

The 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 In the Admin page in the appliance, drag and drop the Sentinel icon 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 appliance appears as another event source in Sentinel Log Manager.

8 End User Configuration

Access Gateway for Cloud 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 the users authenticate with the 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 appliance. The appliance acts as a proxy, so when users access the SaaS applications, the appliance automatically logs the users in to the SaaS application.

- Section 8.1, "Configuring Email Clients," on page 37
- Section 8.2, "Configuring Mobile Devices," on page 38
- Section 8.3, "Configuring the End User Browsers for Kerberos Authentication," on page 38

8.1 Configuring Email Clients

You can configure any email clients to point to Access Gateway for Cloud. 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 12.

1 Access your email client.

2 Create a new email account using the following information to configure Access Gateway for Cloud as your email source:

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

   Incoming email server username: Specify the your Active Directory enterprise logon name for the account name.

   Incoming email server password: Specify your Active Directory password.

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

   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 Windows Mail: Setting up an account from start to finish (http://windows.microsoft.com/en-US/windows-vista/Windows-Mail-setting-up-an-account-from-start-to-finish).

8.2 Configuring Mobile Devices

You can also configure your mobile device to receive email from the SaaS applications through Access Gateway for Cloud. For a list of supported mobile devices, see Table 2-1 on page 12.

On your mobile device:

1 Set up a new email account using the following information:

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

Incoming Mail User Name: Specify your Active Directory enterprise logon name for the account name.

Incoming Mail Password: Specify your Active Directory password.

Incoming Mail > Advanced Options: Select **Use SSL**, then specify 993 as the IMAP port or 995 as the POP port.

Outgoing Mail Server (SMTP): Specify the IP address or hostname of your appliance.

Outgoing Mail User Name: Specify your Active Directory enterprise logon name for the account name.

Outgoing Mail Password: Specify your Active Directory password.

Outgoing Mail > Advanced Options: Select **Use SSL**, then specify 25 as the SMTP port.

For more information, see iOS: Setting up an email account (http://support.apple.com/kb/HT4810).

8.3 Configuring the End User Browsers for Kerberos Authentication

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

1 Add the computers of the users 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 If you are using Internet Explorer, configure the Web 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.ag4c.com`.

3c Click **Close > 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 If you are using Firefox, configure the Web 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.ag4c.com` to the list.

4d Click **OK**, then restart your Firefox browser.

9 Maintenance Tasks

Access Gateway for Cloud allows you to change the configuration settings. For example, moving your appliance from a staging configuration to a production environment requires changes to the networking components.

- Section 9.1, "Changing the IP Address," on page 41
- Section 9.2, "Changing Public DNS Name, NTP Server Settings, or Uploading New Certificates," on page 41
- Section 9.3, "Reloading Authorizations," on page 42
- Section 9.4, "Updating the Appliance," on page 42
- Section 9.5, "Recovering from a Disaster," on page 43

9.1 Changing the IP Address

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

1. Log in to the administration page.

   For more information, see Section 3.1, "Accessing the Administration Page," on page 17.
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.

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

The appliance contains self-generated certificates. You can upload custom certificates through this interface.

1. Log in to the administration page.

   For more information, see Section 3.1, "Accessing the Administration Page," on page 17.
2. Click the cluster icon, then click **Configure**.
3. Change the key pairs, NTP server, or public DNS name, then click **OK**.
4. Click **Apply** to apply the changes to the appliance.

Expired key pair certificates prohibit changes from being made to this page and makes the key pair field red.

9.3 Reloading Authorizations

When you load the authorization into the PolicyMapping page, you are loading what was in the SaaS applications at that specific point in time. You must reload the authorizations into the PolicyMapping page if there are changes in the SaaS applications.

1 Access the policy mapping page in your browser by specifying:

```
https://dns_of_ag4c_appliance/appliance/PolicyMapping.html
```

2 Click the **Load Authorizations** icon in the upper-right corner of the right pane.

3 Select the desired authorizations from the SaaS applications, then click **OK**.

9.4 Updating the Appliance

Updating Access Gateway for Cloud to a new release is a manual process. Updating the existing appliance is not supported. The supported method of updating a node is to add a newer version node to the cluster and remove the old node.

WARNING: Always upgrade the master node last. If you delete the old master node before having a valid new master node, adding a new node to the cluster fails.

To upgrade a non-master node:

1 Take a snapshot of each node in the cluster to create a backup., including the master node.

2 Download the new version of Access Gateway for Cloud.

3 Install a new node into the cluster using the new VMware image.

   For more information, see Chapter 2, "Installing Access Gateway for Cloud," on page 11.

4 Verify all components are in a green state.

   For more information, see Section 10.3, "Troubleshooting Different States," on page 47.

5 Click the old node, then click **Remove from Cluster**.

   For more information, see "Removing a Node from the Cluster" on page 20.

6 Test the appliance to verify it is working.

7 Delete the old node from the VMware console.

8 (Conditional) Delete the old node from the L4 switch.

9 Repeat Step 3 through Step 8 for each node in the cluster except the master node.

To upgrade a master node:

1 Upgrade all of the other nodes.

2 Install a new node in to the cluster using the new VMware image.

   For more information, see Chapter 2, "Installing Access Gateway for Cloud," on page 11.

3 Promote this node to be the master node.

   For more information, see "Promoting a Node to Master" on page 20.

4 Verify all components are in a green state.

   For more information, see Section 10.3, "Troubleshooting Different States," on page 47.

5 Click the old node, then click **Remove from Cluster**.

For more information, see "Removing a Node from the Cluster" on page 20.

6 Test the appliance to verify it is working.

9.5 Recovering from a Disaster

Use snapshots of the nodes to recover from a disaster. It is important to take snapshots of each node in the cluster regularly so you do not lose information.

To recover from a disaster:

1 On a regular basis, take snapshots of the nodes in the cluster.

   1a Power off the working node, then take a snapshot.

   or

   Take a snapshot of the running node including the virtual machine's memory.

   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. Access Gateway for Cloud contains a database that is time-sensitive. Restoring one node only and not the others causes corruption in the appliance.

10 Troubleshooting Access Gateway for Cloud

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

10.1 Displaying Health

Access Gateway for Cloud displays health for each node and for the cluster in 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.**

Show Health displays the status for each component of the appliance. If the status is anything other than green (healthy), use the troubleshooting tools to determine what is wrong.

10.2 Troubleshooting Tools

Access Gateway for Cloud provides troubleshooting tools if you encounter problems. To access these tools:

1. Access the administration page.

   For more information, see Section 3.1, "Accessing the Administration Page," on page 17.
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 Access Gateway for Cloud Log Files** link to download the logs.

After you obtain the logs, turn off the troubleshooting mode by selecting **Exit Troubleshooting Mode**. Leaving the logs running affects the performance of your appliance.

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

Table 10-1 Troubleshooting Log Files

Feature	Logs
Initialization or commands	`ConfigurationReplicator.log`
	`ConfigurationReplicator_RL.log`
	`messages`
	`boot*`
	`packageoperations.log`
	`ag4c_configure.out`
	`ag4c.sh.out`
Admin.html UI	`adminui.log`
Registration	`register.log`
Updates	`zypper.log`
Identity Source Provisioning	`bis_AD_<`*xxxxx*`>.log`
	`bis_AD_<`*xxxxx*`>_RL.log`
	`ConnectorLogs.txt`
Provisioning to the SaaS Applications	`connectors_SFORCE_<`*xxxxx*`>_RL.log`
	`connectors_GOOGLEAPPS_<`*xxxxx*`>.log`
	`connectors_GOOGLEAPPS_<`*xxxxx*`>_RL.log`
	`ConnectorLogs.txt`
Mapping	`RolesandResourceServiceDriver.log`
	`UserApplicationDriver.log`
Approvals	`jboss.log`
Reporting	`ManagedSystemGatewayDriver.log`
	`DataCollectionServiceDriver.log`
Mobile Devices	`mail`
	`mail.err`
	`mail.info`

10.3 Troubleshooting Different States

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

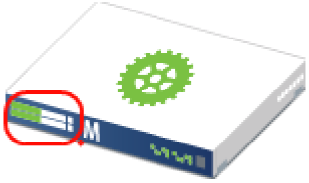
The following sections list the different components, the possible states, and troubleshooting steps you take when the state changes.

- Section 10.3.1, "Front Panel of the Node," on page 47
- Section 10.3.2, "Top of the Node," on page 47
- Section 10.3.3, "Identity Source," on page 48
- Section 10.3.4, "SaaS Applications," on page 49

10.3.1 Front Panel of the Node

The indicator is the front panel of the node.

Figure 10-1 *Front Panel*



The states are:

Green: The node is healthy.

Yellow: The node cannot communicate with the other nodes within the five minute refresh.

Red: The node cannot communicate with the other nodes within two of the five minute refresh cycles.

Clear: The node is initializing or the state of the node is unknown.

Perform the following troubleshooting steps in the order listed if the state is anything but green.

1. Wait at least five minutes for the display to refresh and display the current state.
2. Click the node, then select **Show Health**.

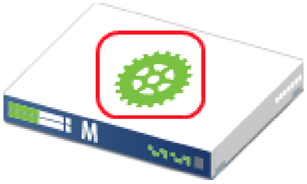
   Show Health displays which part of the appliance is having issues.
3. If Show Health displays a problem, use the troubleshooting tools to gather logs.

   For more information, see Section 10.2, "Troubleshooting Tools," on page 45.
4. Reboot the appliance, then wait at least another five minute cycle for all nodes to display the current state.

10.3.2 Top of the Node

The indicator is the top of the node.

Figure 10-2 Top of the Node



The states are:

Green: All **Apply** commands complete successfully.

Red: The **Apply** commands did not complete successfully.

Perform the following troubleshooting steps in the order listed if the state is red.

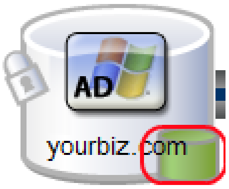
1. Mouse over the top of the node to see the status of the last **Apply** command made on the node.
2. If there is not enough information to help in the summary, click **Enter Troubleshooting Mode** on the node, then mouse over the node again.

   The troubleshooting mode displays a details summary the last **Apply** command made on the node.
3. Reboot the appliance, then wait at least another five minute cycle for all nodes to display the current state.

10.3.3 Identity Source

The indicator is the small identity source icon.

Figure 10-3 Small Identity Source



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 connector to the identity source state is unknown.

Perform the following troubleshooting steps in the order listed.

1. If the connector is green, but users are not displayed in the Access Gateway for Cloud interface, verify that the identity source servers are up and communicating.
2. Use the troubleshooting tools to gather logs, then look at the identity source provisioning logs listed in Table 10-1 on page 46 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 click **Access Gateway**.

   If this item is yellow or red, the interface displays helpful information to help troubleshoot the issue.

4. If you are using LDAPS to communicate to Active Directory, refresh the certificates. You refresh the certificates by:

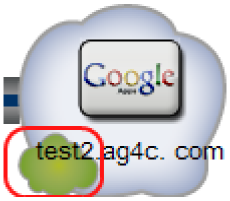
   a. Log in to the Admin.html page, then click **Configure** on the Active Directory identity source.

   b. Click the **Refresh** icon next to the Active Directory server.

10.3.4 SaaS Applications

The indicator is the small cloud on each SaaS application connector.

Figure 10-4 *SaaS Application Indicator*



The states are:

Green: The connectors to the SaaS applications are healthy.

Yellow: The connectors to the SaaS applications contain warnings.

Red: The connector to the SaaS applications contain errors or cannot communicate with the SaaS applications.

Clear: The connectors to the SaaS applications are in an unknown state.

Perform the following troubleshooting steps in the order listed.

1. Click **Show Health** on the master node, then check the status of **Provisioning**.

   If this item is yellow or red, there is helpful information displayed to help troubleshoot the issue.

2. Use the troubleshooting tools to gather logs, then look at the provisioning logs listed in Table 10-1 on page 46 for errors.

3. Make a cosmetic change to the SaaS application connector configuration, then click **Apply**.

   By forcing an **Apply**, the appliance refreshes the SaaS application connector state and this can resolve issues.

10.4 Provisioning Behavior

Actions taken on users and groups in Active Directory might not be reflected in the SaaS applications. The following table lists the actions in Active Directory and the corresponding action in the SaaS applications.

***Table 10-2** Provisioning Actions*

Active Directory	SaaS Applications
Delete a user.	The SaaS accounts are disabled.
Remove a user from the authorized group.	The SaaS accounts are disabled.
Create a user.	Creates an account for the user in the SaaS applications, if the user is a member of group with mapped SaaS authorizations.
Move a user from out of the search context into the search context.	Creates an account for the user in the SaaS applications, if the user is a member of group with mapped SaaS authorizations.
Move a user out of the search context.	The SaaS accounts are disabled.

10.5 Troubleshooting Authentications or Single Sign-On Issues

There can be multiple reasons why authentications to the SaaS applications fail.

Time Synchronization: Access Gateway for Cloud 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 Access Gateway for Cloud 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.

10.6 Valid Salesforce Credentials Fail

Configuring the Connector for Salesforce fails with valid credentials. The reason is that the Salesforce password 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.

10.7 Typical Use Cases for Authentication to the SaaS Applications

The use cases below explain the end user experience using single sign-on with Kerberos. Use this information while troubleshooting any end user authentication issues.

- Section 10.7.1, “Use Case: Users Access the SaaS Application without Single Sign-On or Integrated Windows Authentication Configured,” on page 51
- Section 10.7.2, “Use Case: From within the Corporate Firewall, Users Access the SaaS Application with Integrated Windows Authentication Configured,” on page 51
- Section 10.7.3, “Use Case: The User Logs in to Active Directory without a Trusted Intranet Zone Defined,” on page 52

- Section 10.7.4, “Use Case: The User is within the Corporate Firewall But Not Logged in to Active Directory,” on page 53
- Section 10.7.5, “Use Case: The User is outside of the Corporate Firewall and Not Logged in to Active Directory,” on page 53

10.7.1 Use Case: Users Access the SaaS Application without Single Sign-On or Integrated Windows Authentication Configured

Preconditions

Meet the following preconditions:

- Configure the appliance.
- Do not configure Integrated Windows authentication (Kerberos).
- Do not configure single sign-on.

User Experience

1. The users access the link for the SaaS application through the basic landing page or a company landing page.
2. The appliance automatically redirects the users to a login screen on the browser.
3. When users enter their Active Directory logon names and passwords successfully, the appliance authenticates the users into the SaaS application.

This behavior is the same whether the users are inside or outside of the corporate firewall.

Exceptions

No exceptions.

10.7.2 Use Case: From within the Corporate Firewall, Users Access the SaaS Application with Integrated Windows Authentication Configured

Preconditions

Meet the following preconditions:

- Enable Integrated Windows authentication in the appliance for user authentication. For more information, see “Configuring the Appliance to Use Integrated Windows Authentication with Kerberos” in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.
- Enable Kerberos authentication in Active Directory.
- The users authenticate to Active Directory when logging on to their workstation or laptop.
- Select the default Advanced options setting of **Enable Integrated Windows Authentication** in your browser.
- Configure the user browsers to accept the Kerberos ticket. For more information, see “Configuring the End User Browsers for Kerberos Authentication” in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

User Experience

1. The user authenticates to Active Directory when logging on to their workstation or laptop.
2. The user accesses the link for the SaaS application through the basic landing page or a company landing page.
3. The browser automatically redirects to the appliance for authentication, then the user seamlessly logs in to the SaaS application using single sign-on with the Kerberos ticket.

Exceptions

No exceptions.

10.7.3 Use Case: The User Logs in to Active Directory without a Trusted Intranet Zone Defined

Preconditions

Meet the following preconditions:

- Enable Integrated Windows authentication in the appliance for user authentication. For more information, see "Configuring the Appliance to Use Integrated Windows Authentication with Kerberos" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.
- Enable Kerberos authentication in Active Directory.
- The user authenticates to Active Directory when logging on to their workstation or laptop.
- Select the default Advanced options setting of **Enable Integrated Windows Authentication** in the user's browser.
- Do not configure the user browsers to accept the Kerberos tickets. Do not perform the steps in "Configuring the End User Browsers for Kerberos Authentication" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

User Experience

1. The user authenticates to Active Directory when logging on to their workstation or laptop.
2. The user accesses the link for the SaaS application through the basic landing page or a company landing page.
3. The browser automatically redirects to the appliance for authentication to a pop-up.
4. Users enter their corporate usernames and passwords.

Exceptions: Users successfully log in after entering their corporate usernames and passwords using IE or Firefox.

10.7.4 Use Case: The User is within the Corporate Firewall But Not Logged in to Active Directory

Preconditions

Meet the following preconditions:

- Enable Integrated Windows authentication in the appliance for user authentication. For more information, see "Configuring the Appliance to Use Integrated Windows Authentication with Kerberos" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.
- The user logs on to the local computer, but not into Active Directory.
- Do not configure the user browsers to accept the Kerberos tickets. Do not perform the steps in "Configuring the End User Browsers for Kerberos Authentication" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.
- Select the default Advanced options setting of **Enable Integrated Windows Authentication** in your browser.

User Experience

1. The user logs in to the local computer, but does not log in to Active Directory.
2. The user accesses the link for the SaaS application through the basic landing page or a company landing page.
3. The browser automatically redirects to the appliance for authentication.
4. The user enters in their corporate usernames and passwords in the pop-up.

Exceptions

Users successfully log in when they enter their corporate usernames and passwords using IE or Firefox.

10.7.5 Use Case: The User is outside of the Corporate Firewall and Not Logged in to Active Directory

Preconditions

Meet the following preconditions:

- Enable Integrated Windows authentication in the appliance for user authentication. For more information, see "Configuring the Appliance to Use Integrated Windows Authentication with Kerberos" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.
- Log into your local computer, but do not log in to Active Directory.
- Do not configure the user browsers to accept the Kerberos tickets. Do not perform the steps in "Configuring the End User Browsers for Kerberos Authentication" in the Installation and Configuration Guide for Access Gateway for Cloud 1.0.0 Early Access.
- Select the default Advanced options setting of **Enable Integrated Windows Authentication** in the user browsers.

User Experience

1. The user logs in to the local computer, but does not log in to Active Directory.
2. The user accesses the link for the SaaS application through the basic landing page or a company landing page.
3. The browser automatically redirects to the appliance for authentication.
4. The user enters their corporate usernames and passwords in the pop-up.

Exceptions

Users successfully log in after they enter their corporate usernames and passwords using IE or Firefox.

A Documentation Updates

The following updates have been made to this guide:

A.1 October 2012

- Added registration information in Section 3.2, “Registering Access Gateway for Cloud,” on page 17.