NetIQ Access Gateway for Cloud 1.0 Release Notes

April 2012

NetIQ Access Gateway for Cloud 1.0 is an appliance that provides a simple, secure way to manage access to Software-as-a-Service (SaaS) applications for corporate users. It provides out-of-the box security and compliance capabilities for SaaS services including full user provisioning, dynamic credentialing, privileged user management, Single Sign-On (SSO) and compliance reporting.

Many features were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure our products meet all your needs. You can post feedback in the Access Gateway for Cloud forum on Qmunity (http://community.netiq.com/forums/30.aspx), our community Web site that also includes product notifications, blogs, and product user groups.

1 System Requirements

This release requires the following:

- One VMware server
  - vSphere Hypervisor 5.0
  - vSphere 5.0
  - ESXi 4.1
  - ESX 4.1
- Minimum hardware requirements per node
  - 60 GB disk space
  - 2 cores
  - 8 GB RAM
- One browser for administration
  - Firefox 10 and 11
  - Chrome

For detailed information on system requirements, see “Requirements” in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

2 Installing Access Gateway for Cloud

Complete the following steps to install Access Gateway for Cloud:

1. 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).

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`).

For more details about the installation, see “Installing Access Gateway for Cloud” in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

3 Known Issues

For more troubleshooting information, see “Troubleshooting Access Gateway for Cloud” in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

3.1 Initialization Issues

3.1.1 Time Not Synchronized on the ESX or ESXi Server Causes Intermittent Problems

Issue: If time is not synchronized on the ESX and ESXi servers, intermittent issues can occur, such as roles not being granted to the administrative account for the appliance.

Solution: Configure NTP on the ESX or ESXi server.

3.1.2 Initialization Takes a Long Time to Display

Issue: The initialization page takes a long time to display if there is no DHCP server in your environment. The initialization page eventually displays and assigns a 192.xxx.xxx IP address to the appliance.

Workaround: Edit the VMX file for the appliance before the first boot. For more information, see "Configuring the Appliance without a DHCP Server" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

3.1.3 Changes to the Preferred DNS Server During Initialization Results in a Static IP Address

Issue: If you want to change the preferred DNS server, you must select *Use the following IP address* in Step 1 on the initialization page, which assigns a static IP address to the appliance.

Workaround: After the initialization process complete, in the Admin page, change the IP address from static to DHCP.

3.1.4 Adding a New Node to the Cluster While an Existing Node is Down Causes the Init Page to Hang

Issue: Access Gateway for Cloud assigns a number to each node as it is added to the cluster. The initialization process looks at the existing node numbers, and if a node is down, the appliance thinks that number is available and creates the new node with the existing number.

Having two nodes with the same number causes problems with the internal database and the initialization process never completes.

Workaround: Verify that all of the nodes in your cluster are healthy and communicating. For more information, see "Troubleshooting Different States" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

3.2 Admin.html Issues

3.2.1 After a Switch Master, the Active Directory Connectors are Red

Issue: After switching the master node, health displays the Active Director connector as red.

Workaround: Reboot the new master node.

3.2.2 After a Switch Master, One or More Nodes is Red

Issue: After switching the master node, health displays that one or more of the other nodes are red while the master node is green.

Workaround: Reboot the new master node. If the issue persists, reboot the red nodes.

3.2.3 Mobile Access for the Connector for Google Apps for Business Appears Disabled in the Interface, But Mobile Access Works for Users

Issue: If you delete a Connector for Google Apps for Business, the email proxy is left running on the appliance. When you add a new Connector for Google Apps for Business, the users can use the mobile access feature, even though the Admin page interface displays that the mobile access feature is disabled.

Workaround: Enable the Mobile Access feature and apply the change. Next, disable the mobile access feature and apply the change. Applying the disable again turns off the email proxy for the appliance.

3.2.4 Deleting a Node from the Cluster Removes the Node from the Interface, but the VMware Image Still Runs

Leaving the VMware image running allows users to authenticate to a node that does not exist in the Admin page. When you delete a node from the cluster, the appliance deletes the node from the interface, but the VMware image still exists and is running.

Use the following procedure to delete a node from a cluster.

1. Remove the node from the L4 switch.
2. Delete the node from the cluster in the Admin page.
3. Stop the VMware image on the ESX server.
4. Delete the VMware image on the ESX server.

3.2.5 Adding a Node Results in a Command Failure

Issue: After adding a new node to the cluster, the node is red in the Admin page. The status of the node is Command Failure.

Workaround: Reboot the new node.

3.2.6 Adding a Node Never Completes

Issue: After adding a new node to the cluster, the progress goes to 100%, but the Init page displays a message stating you must reboot the new node and try again to complete the initialization process. Rebooting the new node does not fix the problem.

Workaround: You must completely remove the new node and try again.

1. Log in to the Admin page.
2. Delete the new node that is red.
3. Remove the VMware image for the failed node from your VMware server.
4. Deploy the image to the VMware server again.

For more information on how to deploy the image, see "Deploying the Appliance" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

5 From the Init page, add the new node to the cluster.

For more information on how to add a new node, see "Adding a Node to the Cluster" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

3.3 Provisioning Issues

3.3.1 User Email Address Changes in Active Directory Are Not Provisioned to Salesforce

Issue: User email address changes in Active Directory are not provisioned to Salesforce.

Workaround: No workaround at this time.

3.3.2 The Appliance Fails to Provision all Users in Overlapping Active Directory Groups

Issue: The appliance fails to provision all users in two Active Directory groups with overlapping users to one Salesforce group.

Workaround: No workaround at this time.

3.3.3 Provisioning Continues Despite Removing the User from a Mapped Group

Issue: Removing a user from a mapped group when there is an outstanding approval request, causes the deleted user to be provisioned to the SaaS application when the administrator grants the approval.

Workaround: Verify that the user is a member of the group before granting approval or deny the request after removing the user from the group.

3.3.4 Recreated a Previously Deleted User Allows the User to Log In to Access Gateway for Cloud

Issues: If you delete a user, then recreate a user with the same sAMAccount name, the new user can log in to Access Gateway for Cloud.

Workaround: Every user must have a unique sAMAccount name. Do not recreate a new user with a deleted user sAMAccount name.

3.3.5 Multiple Domains with Duplicate sAMAccount Names Causes Authentication Issues

Issue: If you have multiple domains, and two users with the same sAMAccount name, the users can authenticate to the other user's account.

Workaround: Access Gateway for Cloud requires that all users, even in different domains, have a unique sAMAccount name.

3.4 PolicyMapping.html Issues

- Section 3.4.1, "No Connectors Displayed in PolicyMapping.html," on page 6
- Section 3.4.2, "Login Loop Occurs when Accessing the Admin and PolicyMapping Pages from the Same Session," on page 6
- Section 3.4.3, "Problem Applying Changes Error Displays in the PolicyMapping Page," on page 6
- Section 3.4.4, "The PolicyMapping Page Returns a 500 Internal Server Error," on page 6

3.4.1 No Connectors Displayed in PolicyMapping.html

Issue: The `https://`*`dns_of_ag4c_appliance`*`/appliance/PolicyMapping.html` page does not display the connectors for the SaaS applications.

Solution: There are two possible solutions:

- Verify that the connectors are configured properly and enabled. For more information, see "Configuring the Connector for Google Apps for Business" and "Configuring the Connector for Salesforce" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.
- Click the *Refresh List* icon in the upper-right corner of the PolicyMapping.html page.

3.4.2 Login Loop Occurs when Accessing the Admin and PolicyMapping Pages from the Same Session

Issue: After working in the Admin page, you access the PolicyMapping page in the Web page or open a second tab to access the PolicyMapping page. The PolicyMapping page never displays.

Workaround: Clear your browser's cache and cookies, then close the browser.

3.4.3 Problem Applying Changes Error Displays in the PolicyMapping Page

Issue: Modifying a mapping without checking the approval box causes a Problem Applying Changes error to appear.

Workaround: Ignore the error. Access Gateway for Cloud saves the changes but displays the message.

3.4.4 The PolicyMapping Page Returns a 500 Internal Server Error

Issue: If the master node is down, the PolicyMapping page returns a 500 Internal Server Error.

Workaround: Solve the problem that caused the master to node to be down. The PolicyMapping page is dependent on the master node.

3.5 Approval.html Issues

- Section 3.5.1, “The Approval Page Is Blank,” on page 7
- Section 3.5.2, “Cannot Access the Approval Page after Creating Large Numbers of Approvals Simultaneously,” on page 7

3.5.1 The Approval Page Is Blank

Issue: If the master node is down, the Approval page is blank.

Workaround: Solve the problem that caused the master to node to be down. The Approval page is dependant on the master node.

3.5.2 Cannot Access the Approval Page after Creating Large Numbers of Approvals Simultaneously

Issue: Adding 5,000 users to two mapped roles that require approvals, generates 10,000 approvals simultaneously. The Approval page displays the new approvals being added for a short while, but then you do not see new approvals added and you can no longer access the Approval page.

Rebooting the node does not fix the issue.

Workaround: Add only smaller amounts of users simultaneously. NetIQ recommends adding 2,000 users simultaneously as a maximum number of users to add.

3.6 Reporting.html Issues

- Section 3.6.1, “Enabling Show Descriptions While Running Reports Loses the Report Status,” on page 7
- Section 3.6.2, “Reports Display Information from Deleted Connectors,” on page 7
- Section 3.6.3, “Mapping Report Displays Numeric Values Appended to Data in the Authorization Name Column,” on page 7
- Section 3.6.4, “The Reporting Page Is Blank,” on page 8

3.6.1 Enabling Show Descriptions While Running Reports Loses the Report Status

Issue: Enabling the *Show Descriptions* option while running reports causes the report status to disappear.

Workaround: Refresh the browser to display the status of the report.

3.6.2 Reports Display Information from Deleted Connectors

Issue: After deleting connectors, reports contain information about the deleted connectors.

Workaround: No workaround at this time.

3.6.3 Mapping Report Displays Numeric Values Appended to Data in the Authorization Name Column

Issue: The numeric value appears after deleting and recreating mappings for connectors.

Workaround: No workaround at this time.

3.6.4 The Reporting Page Is Blank

Issue: If the master node is down, the Reporting page is blank.

Workaround: Solve the problem that caused the master to node to be down. The Reporting page is dependent on the master node.

3.7 Browser Issue

- Section 3.7.1, "PolicyMapping.html Displays Improperly Using Chrome," on page 8

3.7.1 PolicyMapping.html Displays Improperly Using Chrome

Issue: When you use Chrome to access PolicyMapping.html, some of the icons are not rendered properly. PolicyMapping.html does not display the name of the connector in the drop-down list.

Workaround: Use Firefox when accessing PolicyMapping.html.

3.8 End User Issues

- Section 3.8.1, "Authentication to the SaaS Application Fails if Using IE 9 with Kerberos Enabled, but the User is not Authenticated to the Active Directory Domain," on page 8
- Section 3.8.2, "Google Users Can No Longer Log in After Enabling Single Sign-on," on page 8

3.8.1 Authentication to the SaaS Application Fails if Using IE 9 with Kerberos Enabled, but the User is not Authenticated to the Active Directory Domain

Issue: Login to the SaaS applications fails with Kerberos enabled, but the user is not authenticated to Active Directory.

Workaround: This issue is a bug with IE and the Microsoft incident number is 687000. The user must be authenticated to Active Directory to log in.

3.8.2 Google Users Can No Longer Log in After Enabling Single Sign-on

Issue: After implementing Access Gateway for Cloud, you might have some issues with existing Google Apps for Business accounts. Any users that either do not exist in the identity store, or are not merged with the existing Google account, can no longer log in to the Google domain.

For example:

1. User jsmith has an account in Google Apps for Business.
2. Implement Access Gateway for Cloud with single sign-on.
3. User jsmith attempts to log in to the Google domain and fails.

Google Apps for Business does not allow direct login and single sign-on to the domain.

Solution: Give users authorization to access the Google Apps for Business resource through Access Gateway for Cloud.

1. If the matching account exists in Active Directory, skip to Step 2. Otherwise, create a matching account in the identity store (Active Directory).
2. Grant the user authorization to the Google Apps for Business resource by adding the user to the proper group in Active Directory.

   or

   Map the Active Directory group to the Google Apps for Business group through the PolicyMapping page.

   For more information, see "Loading Google Apps for Business Authorizations" in the *NetIQ Access Gateway for Cloud 1.0 Installation and Configuration Guide*.

The two accounts merge when the user receives authorization for Google Apps for Business through the PolicyMapping page. Access Gateway for Cloud automatically generates a new password and resets the Google Apps for Business password.

When users access the resource after the merge occurs, they automatically log in to Google Apps for Business through single sign-on.

3.9 Time Synchronization Issues

Access Gateway for Cloud depends on timestamps to function properly. Time must be synchronized between the VMware host, each Access Gateway for Cloud node in the cluster, and the workstations administering Access Gateway for Cloud.

Issue: If time is not synchronized, provisioning fails, configurations fail, and authentication for users fail.

Solution: Use the following items to solve time synchronization issues:

- All nodes in the cluster must reside in the same time zone.
- Configure NTP on the ESX or ESXi server.
- If you convert the OVF file to a VMX file, deselect the default option of *Edit Settings* > *Options* > *VMware Tools* > *Synchronize* guest time with host.

4 Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information Web site (https://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate Web site (https://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of Qmunity, our community Web site that offers product forums, product notifications, blogs, and product user groups.

5 Legal Notices

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.

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.

Check Point, FireWall-1, VPN-1, Provider-1, and SiteManager-1 are trademarks or registered trademarks of Check Point Software Technologies Ltd.

Access Manager, ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Cloud Manager, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PlateSpin, PlateSpin Recon, Privileged User Manager, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its affiliates in the USA. All other company and product names mentioned are used only for identification purposes and may be trademarks or registered trademarks of their respective companies.

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.