NetIQ CloudAccess and NetIQ MobileAccess 2.2 Release Notes

March 2015

NetIQ CloudAccess 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.

NetIQ MobileAccess is an appliance that enables user access to protected resources from mobile devices. It provides convenient access for users, as well as the ability for administrators to customize viewing options and remotely manage registered devices.

This version includes new features, improves usability, and resolves several previous issues. Many of these improvements 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 that our products meet all your needs. You can post feedback in the CloudAccess forum (https://forums.netiq.com/forumdisplay.php?118-CloudAccess) on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the NetIQ CloudAccess Documentation (https://www.netiq.com/documentation/cloudaccess/) page. To download this product, see the NetIQ Downloads (https://dl.netiq.com/) website.

1 What’s New?

The following sections outline the key features and functions provided by this version, as well as issues resolved in this release:

1.1 Supported Operating Systems

For information about the supported operating systems for the appliance, identity sources, mobile apps, and web browsers, see “Product Requirements” in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

1.2 Improved Connector for NetIQ Access Manager

NetIQ has enhanced the integration between CloudAccess and NetIQ Access Manager 4.1.*x* to simplify the configuration. If you are using an older version of Access Manager, you must use the generic connector for NetIQ Access Manager. For more information about the enhanced connector for NetIQ Access Manager, see “Connector for NetIQ Access Manager” in the *NetIQ® CloudAccess Connectors Guide*.

1.3 New Connector for Google Apps

CloudAccess 2.2 includes a new connector for Google Apps that contains the same functionality as the previous connector for Google Apps. However, in CloudAccess 2.2 the deprecated Google Apps Admin API has been replaced by the new Google Admin SDK API for Google Apps.

NOTE: The updated connector for Google Apps contains additional fields that you must configure before the connector can run again. For more information, see “The Connector for Google Apps Is Red and Stopped” on page 11.

1.4 New Basic SSO Application Catalog

CloudAccess now provides access to the NetIQ Application Catalog that contains Basic SSO connectors. You can access the catalog from the Applications palette in the administration console to import them to the appliance. For more information, see “Importing and Configuring a Connector for Basic SSO” in the *NetIQ® CloudAccess Connectors Guide*.

1.5 Connectors for Basic SSO and the NetIQ Basic SSO Extension

CloudAccess now includes additional connectors for Basic SSO in the Application Catalog. These connectors work with the NetIQ Basic SSO Extension and with MobileAccess to securely save, retrieve, store, and replay login credentials for websites.

CloudAccess includes updates for the NetIQ Basic SSO Extension for the Chrome web browser. CloudAccess now also includes the NetIQ Basic SSO Extension for the Firefox web browser.

The MobileAccess app now supports the secure retrieval and replay of previously stored credentials for the destination websites of connectors for Basic SSO. Users can access the websites through the landing page on supported iOS and Android mobile devices.

For more information, see “Connectors for Basic SSO” in the *NetIQ® CloudAccess Connectors Guide*.

1.6 Basic SSO Template Improvements in the Access Connector Toolkit

The Access Connector Toolkit now provides automatic import of the desktop browser login form information that you use to create custom connectors for Basic SSO. You can also manually add form information for the websites' login pages for iOS mobile devices and Android mobile devices. For more information, see "Creating a Basic SSO Connector Template" in the *NetIQ® CloudAccess Connectors Guide*.

1.7 Mobile Device Appmarks for Connectors for Basic SSO

CloudAccess now provides appmarks for iOS and Android mobile devices in connectors for Basic SSO. This capability enables mobile users to enjoy the replay of previously stored credentials when they access the destination website from their mobile devices.

For more information, see "Configuring Appmarks for Connectors" in the *NetIQ® CloudAccess Connectors Guide*.

1.8 Support for FIDO for Two-Factor Authentication

CloudAccess now supports FIDO (Fast IDentity Online) for two-factor authentication. FIDO requires that users enter their user name and password. The second factor authentication is a dongle that users must touch in order to authenticate. For more information, see "Configuring FIDO for Two-Factor Authentication" in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

1.9 JDBC Identity Source Support for Oracle Database 12c

CloudAccess and MobileAccess now include support for Oracle Database 12c. For more information, see "JDBC Requirements" in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

1.10 Updated Advanced Authentication Tool

CloudAccess 2.2 includes updates to the Advanced Authentication tool for two-factor authentication using the NetIQ Advanced Authentication Framework. In this release, the tool requires the NetIQ Advanced Authentication Framework 5.*x* or later appliance. For more information, see "Configuring the Advanced Authentication Tool for Two-Factor Authentication Using NetIQ Advanced Authentication Framework" in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

1.11 Software Fixes

CloudAccess 2.2 includes software fixes that resolve several previous issues.

1.11.1 Users Are Randomly Suspended for Google Apps When You Re-Activate Users in Large Batches

With the new connector for Google Apps in CloudAccess 2.2, when you re-activate users to Google Apps for Business in large batches, users are no longer randomly suspended. (Bug 894890)

1.11.2 SAML2 In Identity Source Users Cannot Be Administrators

Assigning administrator roles to users in a SAML 2.0 Inbound (SAML2 In) identity source is not supported because their credentials are not stored in the local identity store on the appliance. In this version, SAML2 In users are no longer available for selection on the Roles page. (Bug 895624)

2 System Requirements

To upgrade to CloudAccess or MobileAccess 2.2, you must have an existing installation of CloudAccess or MobileAccess 2.0 or 2.1. You can update an appliance only through the update channel. For more information, see "Updating the Appliance" in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

The prerequisites for the MobileAccess appliance are the same as those for CloudAccess. For detailed information on hardware requirements and supported operating systems and browsers, see "Installing the Appliance" in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

3 Installing CloudAccess or MobileAccess

The steps for installing and configuring the appliance are the same for CloudAccess and MobileAccess. To install CloudAccess or MobileAccess, see "Installing the Appliance" in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

To update an existing CloudAccess or MobileAccess appliance through the update channel, see "Updating the Appliance" in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

4 Verifying the Installation

Complete the following steps to verify that the installation was successful.

To check the installed version:

1. Access the Admin page at `https://dns_of_appliance/appliance/index.html`, then log in with the appliance administrator credentials.
2. Click the appliance, then click **About**. The version listed in the window should be `2.2-build number`.

5 Known Issues

NetIQ Corporation strives to ensure that our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support (http://www.netiq.com/support).

5.1 Initialization Issue

5.1.1 Changes to the Preferred DNS Server During Initialization Result 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. (Bug 754137)

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

5.2 Administration Issues

5.2.1 Modifying a Non-Public SSL Certificate on the External Filter Server Causes User Logins to Fail Until the Next Apply

Issue: If you modify a non-public SSL certificate (that is, a certificate that has not been signed by a well-known certificate authority) on the external filter server, the login service does not automatically re-read the trust store. User logins fail with a message that an external service is unavailable. However, the health status does not detect this failure and reports a healthy (green) status. This condition does not occur if you modify a certificate from a well-known certificate authority on the filter server. (Bug 895375)

Workaround: If you modify a non-public SSL certificate on a filter server, you must click **Apply** to restart the login services in the cluster, or reboot the appliance. A restart causes the login service to re-read the trust store and get the new certificate information. After the restart, users can log in again.

5.2.2 CloudAccess Cannot Set TenantName Attribute on Events Sent to Sentinel

Issue: CloudAccess cannot currently set the `TenantName` attribute on events sent to Sentinel using the Sentinel Link collector. As a result, for events received from CloudAccess, reporting and identity tracking functionality does not work properly within Sentinel. (Bug 812159)

Workaround: No workaround is available at this time.

5.2.3 Browser Errors If Kerberos Is Not Enabled in the Browser

Issue: If Integrated Windows Authentication is enabled in CloudAccess, and a user is logged in to a domain where Kerberos is configured but Kerberos is not enabled in the browser, if the user enters invalid credentials at the login prompt or clicks **Cancel**, different browsers may display errors or may not behave as expected. (Bug 802257)

Workaround: To prevent this issue, ensure that Kerberos is enabled in the browser.

5.2.4 SAML 2.0 Inbound Users See Only Public Access Appmarks

Issue: When using the SAML 2.0 Inbound connector in mode **Allow access for unknown users**, after the first login when the user has just been created, the landing page displays only the Public appmarks. (Bug 920022)

Workaround: Since these specific types of users are not stored locally on the appliance, the appliance cannot apply the proper roles until the user logs in a second time. If you have any users that see this problem, instruct them to log out and log back in to the landing page. The landing page properly displays all of the appmarks.

5.2.5 Kerberos Authentications Loop Indefinitely If External Filter Service Is Unreachable

Issue: If a filter tool is configured in CloudAccess but the external filter service becomes unreachable for any reason, users attempting to log in using Kerberos end up in a looping state where the browser flashes a blank page, then a gray background with the NetIQ logo. (Bug 923183)

Workaround: Bring the external filter service back online or disable the filter tool to allow user authentications to continue without the filter.

5.3 Provisioning Issues

5.3.1 Provisioning Is Not Supported for Users in an Unmanaged SAML2 In Identity Source

Issue: Account provisioning is not supported for the users in the SAML 2.0 Inbound unmanaged internal identity store. Because these users do not have a workforceID, they cannot be provisioned for or access the SaaS applications that depend on the workforceID attribute for authentication, such as Google Apps and Salesforce. (Bug 883446)

Workaround: To access the SaaS applications, the user must log in with the corporate identity that has a workforceID attribute.

5.3.2 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. (Bug 717153)

Workaround: No workaround is available at this time.

5.3.3 Re-enabled User Has Role That Was Previously Assigned

Issue: If you assign a user to a role in CloudAccess and then remove that user from the identity source, CloudAccess does not automatically remove the role assignment. So, if the user's context in the identity source is later restored, CloudAccess shows that user as having the same role that was previously assigned. (Bug 765609)

Workaround: To work around this issue, before you remove a user in the identity source, ensure that you have revoked all roles from that user on the Roles page in CloudAccess.

5.3.4 Relaxed User Matching Does Not Work with Active Directory or eDirectory Renamed User Objects

Issue: When you use the **Relaxed User Matching** option with an Active Directory or eDirectory identity source, renaming user objects in the identity source could present unexpected results. If you enable relaxed user matching, CloudAccess tries to match an existing account in the appliance using the CN attribute. If you rename a user object in the identity source, the CN attribute is effectively changed, so the user matching does not find the existing account, and a new account is created on the appliance. (Bug 848860)

Workaround: NetIQ recommends using relaxed user matching only when necessary to re-create users (with the same name) that have been previously deleted. If you do not enable relaxed user matching, renaming in Active Directory and eDirectory works as expected.

5.3.5 Non-Alphanumeric Characters in the Group Description Result in Users Seeing No Appmarks

Issue: If you use non-alphanumeric characters (such as !@#$%) in a group description, policy mapping may appear to be successful, but users in that group do not see the mapped appmarks. (Bug 922124)

Workaround: Remove any non-alphanumeric characters from the group description.

5.4 Policy Mapping Issue

5.4.1 Renaming Authorization for an Office 365 Account Requires Remapping Policy

Issue: CloudAccess maps policies for Office 365 based on the authorization name, and not the underlying static ID. If you rename an authorization in Office 365, CloudAccess sees the action as a delete and create. Any existing policy mappings for the authorization are removed. (Bugs 811460, 815496)

Workaround: After changing the authorization name in Office 365, you must use the Policy page to re-map entitlements for the renamed authorization, and then use the Approval page to re-approve, if necessary.

5.5 Approval Issue

5.5.1 Page Becomes Unresponsive When You Approve Requests

Issue: When you approve or deny a large number of workflow requests in a single action, the amount of memory that the browser uses can cause the page to become unresponsive and the browser to close. (Bug 815971)

Workaround: Ensure that you select less than 300 requests in a single accept or deny action.

5.6 Reporting Issues

5.6.1 Reports Display Information from Deleted Connectors

Issue: After you delete connectors, reports still contain information about the deleted connectors. (Bug 756690)

Workaround: No workaround is available at this time.

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

Issue: The numeric value in the mapping report appears after deleting and recreating mappings for connectors. (Bug 753321)

Workaround: No workaround is available at this time.

5.7 Connector Issues

5.7.1 Logging Out of Identity Provider Landing Page Does Not Result in Logging Out of SaaS Accounts

Issue: Logging out of the landing page might not result in logging out of the SaaS accounts, depending on support and configuration for SAML Single Logout at the SaaS provider. Many SaaS providers do not support the SAML Single Logout service. The same issue exists with service provider-initiated logouts. (Bug 837076)

Workaround: Close the browser to allow the abandoned browser session to time out, so the session cannot be accessed again.

5.7.2 Admin Page Does Not Provide a Way to View SaaS Metadata

Issue: The Admin page in CloudAccess does not currently provide a means of viewing the critical content in an uploaded metadata file, such as when you configure the connector for Salesforce. (Bug 793495)

Workaround: No workaround is available at this time. Since metadata for connectors must be unique, ensure that the metadata file is correct before uploading it.

5.7.3 Renaming an Authorization at Office 365 Account Requires Policy Remapping in CloudAccess

Issue: If an authorization at the Office 365 account is renamed, any existing policy mappings in CloudAccess are lost, because CloudAccess uses the account name for policy mapping rather than the underlying static ID of the authorization. (Bug 811460)

Workaround: After changing the Office 365 authorization name, use Policy Mapping to re-map and Approvals to re-approve if necessary.

5.7.4 Users Who Are Provisioned to Multiple Google Domains Cannot Access Original Mailbox

Issue: If you provision a user to multiple Google Apps domains and select the **Enable email proxy** option in the administration console, the user cannot open the mailbox for any domain except the last domain to which the user was provisioned. This issue occurs because the dovecot mail proxy uses an attribute from the user object that is single-valued, so it is set with the name of the last Google domain to which the user was provisioned. (Bug 819157)

Workaround: No workaround is available at this time.

5.7.5 Connector for NetIQ Access Manager Tries to Import Certificate with the Same Name Every Time

Issue: The connector for NetIQ Access Manager tries to import the certificate to NetIQ Access Manager with the same name every time. If you remove the connector, the imported certificate to NetIQ Access Manager is not removed. So, the next time you create a connector for NetIQ Access Manager for the same Access Manager system, it fails unless the certificate is the same certificate. (Bug 923217)

Workaround: To work around this issue, before you create a new connector for NetIQ Access Manager in CloudAccess, delete the previous certificate in the Access Manager administration console.

5.7.6 Login Using Native Microsoft Office App on Mobile Device Fails

Issue: CloudAccess is currently unable to handle authentication requests from the Microsoft Office native app on supported mobile devices and displays an error. (Bug 923454)

Workaround: Contact NetIQ Technical Support for assistance with this issue.

5.8 MobileAccess Issues

5.8.1 Cannot Install MobileAccess App Using Link in Safari

Issue: Installing the MobileAccess app by clicking a link that points to the CloudAccess cluster DNS does not currently work correctly. If you click the link and then click **OK** to close the popup message, Safari displays a blank page and the smart app banner that is used to install the app from the App Store does not appear. This issue occurs in the Safari browser on iOS 7 devices, but does not occur on iOS 6 devices. (Bug 846705)

Workaround: No workaround is available at this time.

5.9 Upgrade Issues

5.9.1 Manually Configure the DNS Names and Keypairs for Dual NICs After You Update the Cluster

Issue: In a version 2.0 cluster, nodes with dual NICs can have only a single DNS name and SSL keypair. In a version 2.1 or later cluster, nodes with dual NICs must have two DNS names and matching keypairs: one for the public network and one for the administration network. However, you must not configure the additional DNS name and associated keypairs for the two NICs until after you update all nodes in the cluster. After an update, in the Cluster Configuration window for a node, the **Public Interface** section shows the cluster's old DNS name and the **Administration Interface** section is blank.

Workaround: After you update all nodes in the cluster, you must manually configure the cluster DNS names and keypairs.

To configure the Public and Administration DNS names and keypairs for the cluster:

1. Log in as administrator to the administration console.
2. Click a cluster icon, then click **Configure** to open the Configure Cluster window.
3. In the **Public Interface** section, verify the Public DNS name and keypairs, or modify them as desired.

4. In the **Administration Interface** section, enter the Administration DNS name, then import the SSL keypair.
5. Click **OK** to save the new settings.
6. Click **Apply** to apply the settings to the cluster.
7. Repeat Step 2 through Step 6 for each node in the cluster.

5.9.2 SAML-Based Single Sign-On Fails for Some Connectors After You Update a Cluster with Dual NICs

Issue: After you update a cluster from version 2.0 to version 2.1 or later and configure the DNS names and keypairs for the public and administration networks, users might not be able to access applications for connectors that use SAML-based single sign-on if the connector does not provide automatic configuration. Changing the Public DNS name or keypair can affect your existing connectors that provide SAML single sign-on.

Workaround: You must manually re-configure the affected SaaS applications to use the new URL and SAML certificate for the new Public DNS name and its associated keypair.

5.9.3 Simple Proxy Users See an SSL Handshake Error After You Update a Cluster with Dual NICs

Issue: After you update a cluster from version 2.0 to version 2.1 or later and configure dual NICS to use two different DNS names and certificates for the public and administration networks, users might see the following SSL Handshake error when they click an appmark for a connector for Simple Proxy:

```
Server error! Error during SSL handshake.
```

Workaround: For each configured instance of the connector for Simple Proxy, you must open its Configuration page to allow it to detect the new settings for DNS names and certificates. After you update the connectors for Simple Proxy, users should no longer encounter the SSL Handshake error when they click the related appmarks.

To update the connectors for Simple Proxy:

1. Log in as administrator to the administration console for the appliance.
2. In the **Applications** panel, click the icon for an instance of the connector for Simple Proxy, then click **Configure**.
3. In the connector's Configuration window, click **OK**.
4. Repeat Step 2 through Step 3 for each connector for Simple Proxy.
5. On the Admin page, click **Apply** to apply the changes for all connectors for Simple Proxy.
6. Wait to perform other administrative tasks until the configuration changes have been applied on each node of the cluster.

5.9.4 Users Cannot See Appmarks and Cannot Directly Access Protected Resources

Issue: After you update a cluster from version 2.0 to version 2.1 or later, users might not see the appmarks for the existing configured application connectors, and they are unable to directly access protected resources. (Bug 899434)

Workaround: Reboot each node in the cluster.

5.9.5 Appmarks Cannot Display Their Global URLs and Public Icons

Issue: After you update a cluster from version 2.0 to version 2.1 or later, the appmarks for the existing configured application connectors cannot display the global URL and Public icon. The update does not automatically re-create appmarks for existing configured applications to get the new capabilities. (Bug 897349)

Workaround: At the top of the connector's Appmarks configuration page, click **Reset** to re-create the appmarks with the new feature. Click **Save**, then click **Apply** on the Admin page. You can alternatively drag and drop a 2.1 or later version of the connector from the **Applications** palette to the **Applications** panel, remove the old 2.0 version of the connector, and then set policy mappings for the new instance of the application connector. Users must perform a refresh on their mobile devices before the re-created appmarks are displayed and the new capabilities are available.

5.9.6 Appmarks for Existing Applications Do Not Appear on Android Devices

Issue: CloudAccess and MobileAccess 2.0 did not support appmarks on the MobileAccess app for Android devices. After you update from version 2.0 to 2.1 or later, no appmarks for the existing applications appear on Android devices. (Bug 893055)

Workaround: After you update from version 2.0 to 2.1 or later, use the administration console to enable and create the Android appmarks for each of the connectors for existing applications, and then click **Apply**. Users must perform a refresh on their Android devices to get the newly created appmarks.

5.9.7 The Connector for Google Apps Is Red and Stopped

Issue: After you update the CloudAccess appliance, the connector for Google Apps stops running and turns red.

Solution: The CloudAccess appliance contains a new connector for Google Apps. The update process upgrades the connector for you, but you must perform some additional configuration to get the connector running again. For more information, see "Updating the Connector for Google Apps" in the *NetIQ® CloudAccess Connectors Guide*.

6 Contact Information

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

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

For general corporate and product information, see the NetIQ Corporate website (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

7 Legal Notice