NetIQ CloudAccess and NetIQ MobileAccess 2.2.1 Release Notes

May 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 service pack 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 Operating System Updates

CloudAccess and MobileAccess 2.2.1 include various operating system updates.

1.2 Enhancements and Software Fixes

CloudAccess includes the following enhancements and software fixes:

1.2.1 Improvements for Chrome and Firefox Extensions

This version includes various improvements and minor bug fixes to the Chrome and Firefox extensions for Basic SSO connectors.

1.2.2 Updated Connector 1.6.1 for Office 365

CloudAccess 2.2.1 provides an updated connector 1.6.1 for Office 365. For information about connector requirements and installing the connector, see “Installing the Connector for Office 365” in the *NetIQ® CloudAccess Connectors Guide*.

1.2.3 Cannot Upgrade Certain Configurations From CloudAccess 2.1.0 to 2.2

All upgrades from CloudAccess 2.1.0 to 2.2.*x* now work as expected. (Bug 927798)

1.2.4 Cannot Modify Custom Login Page to Point to External SSPR Server

CloudAccess now supports the use of absolute URLs in custom links. Users can enter an absolute URL starting with either “http://” or “https://” and CloudAccess no longer assumes it is relative to the base server’s scheme, domain, and port. (Bug 927802)

2 System Requirements

This service pack requires an existing installation of CloudAccess or MobileAccess. Updates are supported from the following versions:

- 2.1.0-265
- 2.1.1-12
- 2.2.0-156

You can update the 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 `2.2.1-build number`.

5 Known Issues

NetIQ Corporation strives to ensure 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 and Administration Issues

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.

5.1.2 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.

5.1.3 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.

5.1.4 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.

5.1.5 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.

5.1.6 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.

5.1.7 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.

5.2 Provisioning Issues

5.2.1 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.

5.2.2 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.

5.2.3 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. 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.

5.2.4 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.

5.2.5 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.

5.3 Reporting Issues

5.3.1 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.

5.3.2 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.

5.4 Connector Issues

5.4.1 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.

5.4.2 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.

5.4.3 Renaming an Authorization for an 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. If you rename an authorization in Office 365, CloudAccess sees the action as a delete and create, and removes any existing policy mappings for the authorization. (Bug 811460, 815496)

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

5.4.4 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.

5.4.5 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.

5.4.6 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.

5.5 MobileAccess Issues

5.5.1 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.

5.6 Upgrade Issues

5.6.1 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*.

5.6.2 Missing Mappings for the Connector for Google Apps Groups and Users

Issue: If you update the CloudAccess appliance from version 2.1 to 2.2 when there are pending approvals for the connector for Google Apps, group and placement mappings for Google Apps are lost. (Bug 925236)

Workaround: To work around this issue:

1. Before you perform an update of the CloudAccess appliance, approve or deny any outstanding approval requests. Take note of any existing mappings for OrgUnitPlacement and Group memberships, and note whether approvals are required.
2. Perform the update from version 2.1 to 2.2.
3. In Policy Mapping, remap the user placement and group membership mappings.

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