CloudAccess 3.0 SP2 P1 Release Notes

April 2017

This patch update resolves specific previous issues. This document outlines why you should install this patch update.

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.

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 Security Updates

This patch update for CloudAccess includes various operating system security updates.

1.2 Enhancements and Software Fixes

This patch update includes enhancements and software fixes that resolve several previous issues.

1.2.1 OpenSSL Update

This patch update includes the OpenSSL 1.0.2k update. For more information, see the OpenSSL 1.0.2 Release Notes (https://www.openssl.org/news/openssl-1.0.2-notes.html).

1.2.2 Cipher Suites Updated to Support Microsoft Fat Clients

In this patch update, the cipher suites in CloudAccess have been updated to support Microsoft fat clients. (Bug 1032561)

1.2.3 TLS 1.0 Now Disabled by Default

Because TLS 1.0 has known vulnerabilities, it is disabled by default in this version. However, you can re-enable it if necessary to allow older mobile devices to connect. For example, Android versions prior to 5.0 and some thick clients such as Exchange might not be able to fully authenticate to Office 365 when TLS 1.0 is disabled. (Bugs 1031171, 1031201, and 1031990)

To re-enable TLS 1.0:

1. On the Admin page, click the cluster icon at the bottom of the page, then click **Configure**.
2. Select **Allow less secure TLSv1 clients**, then click **OK**.

1.2.4 ImmutableID Is Double-Base64 Encoded When Users Are Provisioned to Office 365

Issue: Customers who used a mechanism such as Azure AD Connect to replicate user objects from their local Active Directory domain to Azure AD had Office 365 provisioning issues. The issues occurred because CloudAccess would overwrite the native value set by Azure AD Connect with a base64-encoded value for the SAML assertion. (Bug 1030993)

Fix: The connector for Office 365 now includes an **ImmutableID encoding** configuration option. The default **base64** setting is appropriate for most customers. However, the connector also includes a **native** setting option. If you select the **native** option, the AD objectGUID is stored in the native format, then CloudAccess uses the same native value for provisioning and single sign-on. In the native mode, the immutableID in Office 365 always matches the objectGUID in Active Directory.

1.2.5 Office 365 Account Naming Issue

Issue: In previous versions of CloudAccess, if you set the Office 365 account naming to anything other than UserName, logins from Outlook might fail. For example, if you entered an Outlook email address such as bob.ross@mydomain.com, CloudAccess would shorten the username portion to bob.ross and then look up that user. Because the CN (and samAccountName) were most likely not bob.ross, the user would not be found and authentication would fail. (Bug 1025539)

Fix: In this version, CloudAccess honors the entire Outlook email address and looks for either the CN or the mail attribute.

NOTE: The attribute values of the Active Directory email and the Office 365 email *must* match. For example, the bross user in Active Directory must have the correct email attribute value of bob.ross@mydomain.com, otherwise authentication will fail.

1.2.6 Display Names for Provisioned Users Are Concatenated in Administration Portal

CloudAccess no longer removes the space between the first and last names of users provisioned to Office 365, so the Display Name appears correctly in the Office 365 administration portal. (Bug 1030730)

1.2.7 CloudAccess Fails to Set Licenses on Matched Users After Office 365 Provisioning

CloudAccess now matches provisioned users to Office 365 licenses as expected. (Bug 1030785)

1.2.8 RPBM Fails to Start After Changing Network Settings

If you change appliance network settings in the administration console, such as changing the IP address from DHCP to static, all required services now start as expected. (Bug 1028580)

1.2.9 Single Sign-On to Office 365 Fails After Registering Appliance With Email

CloudAccess no longer stores the registration email address for the appliance admin user in the internal user store. Therefore, single sign-on to Office 365 works as expected after registering the appliance with any email address. (Bug 1031929)

2 System Requirements

This patch update requires an existing installation of one of the following versions of CloudAccess:

- 3.0 Service Pack 1 (3.0.1-6)
- 3.0 Service Pack 2 (3.0.2-21)

You must also have an existing installation of the NetIQ Connector 1.6.3 for Office 365 to update the connector to version 1.6.4.

For detailed information about hardware requirements, and supported operating systems and browsers, see “Installing the Appliance” in the *CloudAccess Installation and Configuration Guide*.

3 Updating the Appliance and the Connector for Office 365

You can update a CloudAccess appliance with this patch update only through the update channel. For more information, see “Updating the Appliance” in the *CloudAccess Installation and Configuration Guide*.

IMPORTANT: If you are updating both the CloudAccess appliance and the connector for Office 365, we recommend that you update the connector first, then update the appliance.

4 Verifying the Update

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

To check the installed version:

1. Access the administration console at `https://dns_of_appliance/appliance/index.html`, then log in with the appliance administrator credentials.
2. Click the appliance node, then click **About**. Verify that the version listed in the window is 3.0.2-25.

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 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 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 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.

5.4 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.

5.5 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 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 Cannot Authenticate to Advanced Authentication Framework 5.4

Issue: You have configured the Advanced Authentication Framework method to work with Advanced Authentication Framework 4.2. After completing the configuration, you try to authenticate with an Advanced Authentication Framework method and it fails.

Workaround: The Advanced Authentication Framework changed with the 5.2 and later releases. You must manually enable endpoints on the Advanced Authentication Framework system to make authentications work.

To configure endpoints in the Advanced Authentication Framework administration console:

1. Log in to the administration console for Advanced Authentication Framework as an administrator.
2. From the left navigation pane, click **Endpoints**.
3. Select the **Endpoint41** endpoint.
4. Click the Pencil to edit the endpoint, then enable the endpoint.
5. Save your changes.

Authentications through the Advanced Authentication Framework methods now work.

5.8 CloudAccess Limits Number of Basic SSO Credentials Per User

Issue: CloudAccess does not currently allow a single user to save credentials for more than 25-30 Basic SSO connectors. When this maximum is reached, the browser extension still prompts to store credentials, but when the user returns to the site, the credentials are not replayed. When the user attempts to log in again manually, the extension again prompts for the credentials. Different users logging in to the same workstation can still save new credentials. In addition, users who have reached the maximum can still replay credentials that they previously saved. (Bug 994483)

Workaround: No workaround is available at this time.

5.9 Authentication Activity Report Shows Zero Events

Issue: The auditing system has been updated with a newer, industry compliant communication protocol certificate. As a result, authentication events (login, logout, failed logins) from the OSP component are no longer being processed into the reporting database. Because of this change, the CloudAccess Authentication Activity Report shows zero events. (Bug 1025746)

Workaround: The CloudAccess internal report is not working properly and Sentinel Link events are not being forwarded to Sentinel. However, Syslog and Google Analytics are still reporting the events as expected, so we recommend using those tools as a workaround for this issue.

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

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.