CloudAccess 3.0 SP2 Release Notes

February 2017

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 New Connector for ServiceNow

CloudAccess now includes a connector for ServiceNow that provides automated provisioning of user accounts from the identity sources to ServiceNow. The connector also provides federated single sign-on access to ServiceNow with SAML 2.0 through CloudAccess. The connector allows CloudAccess to authenticate a user against your identity sources and to share this authentication with ServiceNow to establish the user's session. For more information, see "Connector for ServiceNow" in the *CloudAccess Connectors Guide*.

1.2 New Option for Self-Registered Users to Delete Their Own Account

CloudAccess administrators now have the option to allow self-registered users in the Self-Service User Store to delete their own accounts. For more information, see "Configuring Self-Service Registration and Password Management" in the *CloudAccess Installation and Configuration Guide*.

1.3 OpenSSL Update

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

1.4 Software Fixes

This version includes the following software fixes.

- Section 1.4.1, "ECP Logins Fail When Office 365 Accounts Are Named Using firstname.lastname Format," on page 2
- Section 1.4.2, "Logins Fail With Outlook App on Android Phones," on page 2

1.4.1 ECP Logins Fail When Office 365 Accounts Are Named Using firstname.lastname Format

Issue: ECP logins fail when the naming policy for the provisioned Office 365 accounts is set to firstname.lastname, but the samAccountName is different. (Bug 1025288)

Fix: CloudAccess now honors the ECP requested username, and uses the whole name for matching in the identity vault.

NOTE: The mail attribute in the identity source must match the Office 365 account, otherwise authentication still fails.

1.4.2 Logins Fail With Outlook App on Android Phones

Logins using the Outlook app now work properly on Android phones. (Bug 1025287)

2 System Requirements

You can install this version in a new environment, or you can update an existing system from CloudAccess 3.0 or 3.0 SP1 through the update channel. Updates from versions prior to CloudAccess 3.0 through the update channel are not supported.

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

3 Installing or Updating CloudAccess

To install CloudAccess in a new environment, see "Installing the Appliance" in the *CloudAccess Installation and Configuration Guide*.

You can update a CloudAccess 3.0 or 3.0 SP1 appliance to this version only through the update channel. For more information, see "Updating the Appliance" in the *CloudAccess Installation and Configuration Guide*.

4 Verifying the Installation or Update

Perform the following steps to verify that the installation or 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 3.0.2-21.

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).

- Section 5.1, "Changes to the Preferred DNS Server During Initialization Result in a Static IP Address," on page 3
- Section 5.2, "Provisioning Is Not Supported for Users in an Unmanaged SAML2 In Identity Source," on page 3
- Section 5.3, "User Email Address Changes in Active Directory Are Not Provisioned to Salesforce," on page 4
- Section 5.4, "Re-enabled User Has Role That Was Previously Assigned," on page 4
- Section 5.5, "Reports Display Information from Deleted Connectors," on page 4
- Section 5.6, "Mapping Report Displays Numeric Values Appended to Data in the Authorization Name Column," on page 4
- Section 5.7, "Cannot Authenticate to Advanced Authentication Framework 5.4," on page 4
- Section 5.8, "CloudAccess Limits Number of Basic SSO Credentials Per User," on page 5
- Section 5.9, "Authentication Activity Report Shows Zero Events," on page 5

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/.

Copyright © 2017 NetIQ Corporation, a Micro Focus company. All Rights Reserved.