# CloudAccess 3.0 Release Notes

October 2016

CloudAccess 3.0 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 CloudAccess Includes SocialAccess and MobileAccess

The CloudAccess appliance now includes all features that were previously available in the CloudAccess, MobileAccess, and SocialAccess products. In addition to all previously supported identity sources, CloudAccess now supports many social media identity sources - such as Facebook and LinkedIn - for basic user authentication to SAML applications or web services. You can configure as many identity sources as needed, as long as each identity source meets all stated requirements. CloudAccess displays the number of social identity users on the Admin page of the administration console. For more information about identity sources, see the *CloudAccess Installation and Configuration Guide*.

## 1.2 Ability to Link Corporate and Social Accounts

Once you have enabled the Linked Logins tool in CloudAccess, corporate users that have been provisioned into the local identity vault can link their social identity to their corporate identity so they can use either identity to authenticate. For additional security, you can use a second factor authentication tool such as Fido in conjunction with social federation. For more information, see "Understanding Linked Logins in CloudAccess" in the *CloudAccess Installation and Configuration Guide*.

## 1.3 Ability to Filter Users Imported from LDAP Identity Sources

By default, the connector for Active Directory and the connector for eDirectory import all users found in the search context of the identity source. However, if you have a large number of users or groups and you want to import only a subset, you can now use a filter option to specify which users and groups to import. If users do not meet the criteria you define in the filter, CloudAccess does not import those users. For more information, see "Understanding LDAP Advanced Options" in the *CloudAccess Installation and Configuration Guide*.

## 1.4 Changes to Appliance Initialization Process

The appliance initialization process has been simplified and no longer requires you to set up an identity source and specify an administrative user account for the appliance. CloudAccess provides a default administrative user account that you use to log in to the appliance. You configure one or more identity sources after you have initialized and logged in to the appliance. For more information, see "Installing the Appliance" in the *CloudAccess Installation and Configuration Guide*.

## 1.5 Ability to Specify Naming Policy for Provisioning Connectors

Before you map users to the appropriate applications to set their entitlements, you have the option to specify the naming policy that the SaaS connectors should use for each user account when provisioning users to Office 365, Google Apps, or Salesforce. Naming policies are used for both newly provisioned accounts and matching accounts. For more information, see "Understanding Naming Policy Options" in the *CloudAccess Connectors Guide*.

## 1.6 Application Connector Catalog Includes All SSO-Only Connectors

The Application Connector Catalog now includes all SAML, WS-Fed, and Basic SSO connectors, so you no longer have to download them from the NetIQ Downloads site. For more information, see the *CloudAccess Connectors Guide*.

## 1.7 Connector for NetIQ Access Manager Removed

The connector for NetIQ Access Manager that was included in previous versions of CloudAccess has been removed in this release. The connector is obsolete now that this functionality is available in NetIQ Access Manager 4.2 and later versions. For more information, see "Enabling Mobile and Web Access" (https://www.netiq.com/documentation/access-manager-43/admin/data/mobileaccess.html) in the *Administration Guide* on the NetIQ Access Manager documentation web page (https://www.netiq.com/documentation/access-manager-43/).

## 1.8 Internal Components Updated

All internal components of CloudAccess have been updated in this release. From a user standpoint the changes are not apparent; however, these updates optimize future supportability.

## 1.9 Software Fixes

This version includes the following software fixes.



### 1.9.1 Cannot Use Case Exact Attributes with User or Group Filtering

When using the user or group filtering option with an LDAP identity source, using case exact attributes now works as expected for values containing uppercase characters. (Bug 935967)

### 1.9.2 Cannot Set Search Context to Root of Active Directory

You still cannot set the search context for the connector for Active Directory to the root of your AD identity source, but CloudAccess now validates the entry instead of displaying an exception error if you set the search context to the root. (Bug 956310)

### 1.9.3 SAML 2.0 Inbound Users Using Kerberos and TOTP Cannot Access OAuth Appmarks

Enabling Kerberos and Google TOTP on OAuth appmarks no longer causes login issues for SAML 2 Inbound users. (Bug 923207)

### 1.9.4 SAML 2.0 Inbound Users See Only Public Access Appmarks

When you configure **Allow access for unknown users** on the SAML 2.0 Inbound connector, SAML 2 Inbound users no longer have to log out and then log back in to view all available appmarks on the landing page. (Bug 920022)

# 2 System Requirements

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 Upgrading CloudAccess

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

CloudAccess 3.0 does not support in-place upgrades from previous versions. However, you can upgrade your existing CloudAccess or SocialAccess environment to CloudAccess 3.0 as follows:

1. Install a new CloudAccess 3.0 appliance.
2. Add the new appliance to your existing cluster.
3. Ensure that the health status indicators on the appliance are green and healthy.
4. Make the new appliance the master node.
5. Remove the old master node.
6. Replace the other nodes in the cluster by adding a new 3.0 node, then removing the old node.

# 4 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).



## 4.1 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.

## 4.2 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.

## 4.3 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.

## 4.4 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.

## 4.5 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.

## 4.6 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.

## 4.7 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.

## 4.8 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.

## 4.9 MSLive Authentications Fail After Upgrading SocialAccess to CloudAccess

**Issue:** If you are upgrading your SocialAccess environment to CloudAccess and you have MSLive configured as an identity source in your existing installation, MSLive authentications will start failing until you add the following URL to your existing URLs in MSLive: `https://<appliance_DNS_name>/osp/a/t1/auth/oauth2/landingpad`. (Bug 1001301)

**Workaround:** We recommend that you add this URL before you upgrade. However, after you add the URL, authentications will succeed again.

## 4.10 Only Browser-Based Logins Work With Office 365

**Issue:** The connector for Office 365 has been updated for CloudAccess 3.0. However, in this version only browser-based Office 365 logins work. Access is currently unavailable through fat or thick clients, such as Lync/Skype for Business and mobile native apps. (Bug 1007109)

**Workaround:** No workaround is available at this time.

## 4.11 Customized Branding Does Not Work After Upgrade to CloudAccess 3.0

**Issue:** Due to major JSP (JavaServer Pages) framework changes in CloudAccess 3.0, any JSP customizations made in a CloudAccess 2.3 environment are unlikely to work in CloudAccess 3.0.

**Workaround:** To apply the same customized branding changes in your 3.0 environment, you must redo the JSP files. No other workaround is available at this time.

# 5 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.

# 6 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/.