NetIQ CloudAccess and NetIQ MobileAccess 2.1.1 Release Notes

November 2014

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.

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/index.jsp) 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 Security Improvements

In this version, CloudAccess and MobileAccess include OpenSSL 1.0.1j, thereby addressing the vulnerability to potential POODLE (Padding Oracle On Downgraded Legacy Encryption) attacks. For more information, see CVE-2014-3566 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-3566). (Bugs 901709 and 903125)

IMPORTANT: This service pack fixes the POODLE vulnerability for all ports except 993 and 995. If you enable mail proxy, those ports will be vulnerable. (Bug 903146)

1.2 Enhancements and Software Fixes

CloudAccess and MobileAccess include the following enhancements and software fixes that resolve several previous issues:

1.2.1 Hyper-V Support

CloudAccess now offers an appliance image that can be deployed in a Microsoft Hyper-V environment. This image is available on an early access basis at https://dl.netiq.com/patch/finder/ (https://dl.netiq.com/patch/finder/). Select **CloudAccess** from the product list and click the link to download the image. You must log in to download the image.

1.2.2 Localization Improvements

CloudAccess and MobileAccess provide improved localization of end user pages. Users can set their browsers to any of the following languages: English, Portuguese, French, Italian, German, or Spanish. The OTP (One-Time Password) registration process also works as expected in non-English browsers. Note, however, that the administration console does not currently provide support for languages other than English. (Bugs 901977, 902539, and 901484)

1.2.3 Update Replaces Custom Certificate with New Self-Signed Certificate

Issue: When re-initializing the appliance after an update, if the custom certificate on the appliance contained a wildcard, it did not match the DNS name, so the certificate was replaced with a self-signed certificate. As a result, users were unable to register mobile devices against the appliance. (Bug 900139)

Fix: CloudAccess now matches wildcard certificates, so they are not replaced with self-signed certificates after an update.

1.2.4 Usability Improvements and Cosmetic Fixes

CloudAccess and MobileAccess include various usability improvements, as well as fixes for cosmetic issues that did not affect product functionality.

[Return to Top]

2 System Requirements

To update to CloudAccess or MobileAccess 2.1.1, you must have an existing installation of CloudAccess or MobileAccess 2.0 or 2.1. You can update an appliance to version 2.1.1 only through the update channel. Other upgrades are not supported. 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*.

[Return to Top]

3 Installing or Updating CloudAccess or MobileAccess

The steps for installing 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 appliance from CloudAccess or MobileAccess 2.0 or 2.1 to version 2.1.1 through the update channel, see “Updating the Appliance” in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

[Return to Top]

4 Verifying the Installation or Update

Complete the following steps to verify that the installation or update 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**. Verify that the version listed in the window is `2.1.1-build number`.

[Return to Top]

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 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 Re-running Initialization Resets Custom Branding to Default

Issue: If you implement custom branding in your CloudAccess or MobileAccess environment and then re-run the initialization process to modify the DNS server or make other changes to an existing cluster, branding is reset to the default settings. (Bug 852663)

Workaround: This is the intended behavior in CloudAccess and MobileAccess. Before you re-run the initialization process on an existing CloudAccess or MobileAccess cluster, ensure that you back up your customized branding files so that you can reuse them.

[Return to Top]

5.2 Performance Issue

5.2.1 Other High-Use VMs Can Affect Appliance Performance

Issue: The appliance can be a heavy consumer of CPU, disk I/O, and network bandwidth. Performance can be adversely affected by other virtual machines with similar operational requirements deployed on the same VMware host server.

Workaround: As a best practice, ensure that you group or separate virtual machines on hosts and data stores to avoid resource conflicts for CPU, disk I/O, and network bandwidth. You can do this manually as you deploy virtual machines, or use affinity and anti-affinity rules if they are available in your VMware environment.

[Return to Top]

5.3 Administration Issues

5.3.1 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 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.

5.3.2 Deleting a Node from the Cluster Removes the Node from the Console, but the VMware Image Still Runs

When you delete a node from the cluster, the appliance deletes the node from the interface, but the VMware image still exists and continues to run. Leaving the VMware image running allows users to authenticate to a node that does not exist on the Admin page. (Bug 755006)

To delete a node from a cluster:

1. Remove the node from the L4 switch.
2. Delete the node from the cluster on the Admin page.
3. Stop the VMware image on the ESX server.
4. Delete the VMware image on the ESX server.

5.3.3 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.

5.3.4 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.

5.3.5 Adding a Large Number of Users Takes Time

Issue: The initial import of a large number of users (for example, 20,000 or more) from the identity source can take several hours, and the administration console does not currently provide a warning to administrators before beginning the process. During the user import process, the health status in the console might report the following warnings on and off: `Driver seems unresponsive | Provisioning | bis_AD_a4uLn | Driver seems unresponsive`. (Bug 853863)

Workaround: If you have a large number of users in your environment, ensure that you allow several hours for the provisioning process to complete. After users are added, performance of other administration tasks in the console improves considerably.

[Return to Top]

5.4 Provisioning Issues

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

Issue: When you re-activate users to Google Apps for Business in large batches, several users might be randomly suspended, even though their accounts have been created or activated properly by the connector for Google Apps for Business. (Bug 894890)

Workaround: Depending on the level of suspension, you can take the following actions to resolve the issue:

- **Users suspended by admin:** Verify that the suspended users are members of the appropriate group in the identity source. If they are not members, you can add them. If they are already members, you can remove and re-add them. The users' accounts will then appear as active.
- **Users suspended for abuse:** After a user's account for Google Apps is suspended for abuse, you cannot re-activate the account by making changes in CloudAccess or in the identity source. The administrator of your Google Apps for Business account should contact Google Apps Support and ask them to restore the affected users' accounts to an active state.

5.4.2 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.

5.4.3 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.

5.4.4 Approval-Based Provisioning Continues Despite Removing the User from a Mapped Group

Issue: If you remove a user from a mapped group when there is an outstanding approval request, CloudAccess provisions the deleted user to the SaaS application when the administrator grants the approval. (Bug 752527)

Workaround: Verify that the user is a member of the group before you grant approval, or deny the request after removing the user from the group.

5.4.5 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.

5.4.6 eDirectory User Objects with Other Name Are Created with Unpredictable CN Value

Issue: For eDirectory identity sources, CloudAccess uses the CN attribute to provision user accounts and to look up the user when the user tries to log in. eDirectory also provides the **Other name** field, which appends additional values to the underlying CN attribute. When CloudAccess queries the CN values, the order in which eDirectory returns the values is unpredictable, causing multiple issues. User objects that have values for "`Other name`" in eDirectory might be created in the identity vault with a CN that is set to one of the values in "`Other name`" rather than the original CN value. As a result, attempts to log in to the appliance or the service provider with the original user name might fail. (Bug 845116)

Workaround: NetIQ strongly discourages use of "`Other name`" in eDirectory. This issue does not occur in Active Directory because the lookup attribute (sAMAccountName) has a single value.

To restore functionality to a user account that has been renamed, but is unable to log in because of the CN mismatch,

1. Delete the user account in the eDirectory identity source.
2. Enable the **Relaxed User Matching** option on the eDirectory identity source, then click **Apply**.
3. Recreate the user account in the eDirectory identity source with the desired CN value for the login user name.
4. Update group memberships as needed.
5. Disable relaxed user matching on the eDirectory identity source connector.

5.4.7 Relaxed User Matching Does Not Work with eDirectory Renamed User Objects

Issue: When you use the **Relaxed User Matching** option with an eDirectory identity source, renaming user objects in eDirectory 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 eDirectory, 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 eDirectory works as expected.

[Return to Top]

5.5 Role Management Issue

5.5.1 SAML2 In Identity Source Users Cannot Be Administrators

Issue: Users in a SAML 2.0 Inbound (SAML2 In) identity source must not be assigned as administrators because their passwords are not stored in the local identity store on the appliance. (Bug 895624)

Workaround: Assign administrator roles to users in other types of identity sources.

[Return to Top]

5.6 Policy Mapping Issues

5.6.1 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.

5.6.2 No Connectors Appear on the Policy Mapping Page

Issue: The Policy Mapping page does not display the connectors for the SaaS applications.

Solution: There are two possible solutions:

- Verify that the connectors are configured properly and enabled. For more information, see the appropriate sections for configuring connectors in the *NetIQ CloudAccess Connectors Guide*.
- Click the **Refresh List** icon in the upper-right corner of the Policy Mapping page.

5.6.3 CloudAccess Does Not Reconcile Pending Approvals with Changes to Policy Mappings

Issue: CloudAccess does not reconcile pending approvals with changes to policy mappings. Users with pending approvals are granted the pending requests even if the mappings were removed after the requests were launched. (Bug 787938)

Workaround: If a policy mapping for a resource occurs by mistake, decline all the requests for that resource. If a policy mapping for a resource occurs correctly, but then the mapping is removed, simply decline all outstanding approval requests. You can often avoid this issue by ensuring that requests are approved or denied in a timely manner.

5.6.4 Using Multiple Browsers or Browser Windows Can Result in Duplicate Mappings

Issue: If you simultaneously use more than one browser or browser window to map authorizations, CloudAccess does not warn you if you inadvertently do the same mapping in two different browsers. Clicking **Refresh** displays two identical mappings on the Approvals page, but only one of them is a valid mapping. If you remove one of the mappings, CloudAccess might not actually deprovision the user until you remove the authorization that is mapped to the group. (Bug 815825)

Workaround: You can avoid this issue by using only one browser when you create policy mappings. To work around this issue, on the CloudAccess Policy page, manually remove all duplicate authorization mappings from the role, then map the desired authorizations back to the role.

5.6.5 Using Wildcards for Filtering on Roles Page Does Not Work As Expected

Issue: If you use wildcards such as an asterisk (*) or question mark (?) in the **Filter** field on the Roles page, CloudAccess does not correctly filter results. (Bug 813540)

Workaround: Filters must be full regular expressions. If you want to use wildcards, they must be regular expression wildcards. If the filter does not start with '^' and '.*', then '.*' is added to the filter. If the filter does not end with '$' and '.*', then '.*' is added to the filter. Thus, a filter for "test" would end up as the regular expression ".*test.*"

[Return to Top]

5.7 Approval Issue

5.7.1 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.

[Return to Top]

5.8 Reporting Issues

5.8.1 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.

5.8.2 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.

[Return to Top]

5.9 User Issue

5.9.1 Google Users Can No Longer Log in After Enabling Single Sign-On

Issue: After you implement CloudAccess, you might have some issues with existing Google Apps for Business accounts. Any users who either do not exist in the identity source, or are not merged with the existing Google account, can no longer log in to the Google domain. For example, if user jsmith has an account in Google Apps for Business, and you implement CloudAccess with single sign-on, user jsmith cannot log in directly to the Google domain. Google Apps for Business does not allow both direct login and single sign-on to the domain.

Solution: Give users authorization to access the Google Apps for Business resource through CloudAccess.

1. (Conditional) If the matching account exists in Active Directory, skip to Step 2. Otherwise, create a matching account in the identity source (Active Directory).

2. Grant the user authorization to the Google Apps for Business resource by adding the user to the proper group in Active Directory. Alternatively, you can map the Active Directory group to the Google Apps for Business group through the Policy Mapping page. For more information, see "Loading Authorizations" in the *NetIQ® CloudAccess and MobileAccess Installation and Configuration Guide*.

   The two accounts merge when the user receives authorization for Google Apps for Business through the Policy Mapping page. CloudAccess automatically generates a new password and resets the Google Apps for Business password. When users access the resource after the merge occurs, they automatically log in to Google Apps for Business through single sign-on.

[Return to Top]

5.10 Connector Issues

5.10.1 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.

5.10.2 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.

5.10.3 Access Connector Toolkit Does Not Provide a Logout Option

Issue: The Access Connector Toolkit does not currently provide a logout option, though the session does time out after 60 minutes of inactivity. (Bug 789303)

Workaround: Close the browser after you finish working in the Access Connector Toolkit.

5.10.4 Display Name Does Not Change in Office 365 after Changing It in an Identity Source

Issue: If you change the display name of a user in Active Directory or eDirectory, the display name in Office 365 does not change accordingly. CloudAccess constructs the display name from the first and last name and does not synchronize the display name and full name from the identity source. (Bug 794602)

Workaround: Change the user's first and last name in the identity source instead of the display name.

5.10.5 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.

5.10.6 Office Web Apps Cannot Be Assigned or Unassigned Without SharePoint Online

Issue: When you assign or unassign Office 365 subscriptions to users, if you select Office Web Apps, you must also select SharePoint Online. This is a Microsoft Office 365 dependency, and the Office 365 admin portal page displays an error if you attempt to assign or unassign subscriptions without also selecting SharePoint Online. The Policy page in CloudAccess does not actually prevent you from assigning Office Web Apps by itself, but nothing happens and the logs show `Unable to assign this license`. In addition, if you assign several subscriptions to a user, and you include Office Web Apps but do not include SharePoint Online, none of the other licenses in that operation are applied until you add SharePoint Online. This behavior occurs on the Office 365 admin portal page as well as in CloudAccess.

Workaround: When you assign or unassign Office Web Apps to a user, ensure that you also assign or unassign SharePoint Online.

5.10.7 Connectors for Office 365 that are Configured for Domain and Subdomains Do Not Work Correctly

Issue: If you configure a connector for Office 365 for a parent domain and then configure connectors for one or more child domains, users in the child domains do not see their assigned appmarks. Office 365 sends the same metadata for each domain, so the landing page shows only one of them. Users with policy mappings to the first connector installed can still see their appmarks. (Bug 847293)

Workaround: Microsoft does not support subdomains having different federated settings than their parent. To use a subdomain for Office 365, ensure that either you do not use Office 365 with the parent domain, or that both the parent domain and its subdomain have the identical federation settings.

5.10.8 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.

5.10.9 Service Provider-Initiated Login to Salesforce and NetIQ Access Manager Does Not Work Correctly

Issue: In Safari or Internet Explorer 9, if you attempt a service provider-initiated login from Salesforce, the Salesforce site does not send a SAML2 AuthnRequest XML document with the SAML Request. As a result, the landing page appears instead of the logged-in Salesforce page. The same behavior occurs with the connector for NetIQ Access Manager using Safari or Internet Explorer 9 or 10. (Bug 813313)

Workaround: This is application service provider behavior and cannot be addressed in the connector. This behavior does not occur in Internet Explorer 10.

5.10.10 Behavior of Service Provider-Initiated Login To Salesforce When Kerberos Is Enabled

Issue: If you have Kerberos enabled on your CloudAccess cluster, service provider-initiated login attempts to Salesforce might result in the browser staying at the landing page after authenticating to CloudAccess instead of redirecting to Salesforce. This issue occurs only if Kerberos is enabled on the CloudAccess cluster. It occurs regardless of whether users log in with Kerberos single sign-on or with another authentication (for example, when the workstation is not a member of the Active Directory domain). (Bug 817909)

Workaround: This issue occurs on workstations running Windows 7 and Internet Explorer 9, but does not occur with Firefox on Windows 7.

You can prevent or address this issue by changing an option on the Single Sign-On Settings page at Salesforce. This page includes a radio button named **Service Provider Initiated Request Binding** with two options: **HTTP POST** (selected by default) and **HTTP Redirect**. If you have Kerberos enabled on your CloudAccess cluster, select **HTTP Redirect** instead of the default **HTTP POST** option. If you do not have Kerberos enabled on the CloudAccess cluster, you do not need to change this option.

5.10.11 Single Sign-On to Box.com Fails if User Session Timeout Is Set to 75 Minutes or Longer

Issue: If you set the user session timeout for the cluster to 75 minutes or longer, the Box connector displays an error when users attempt to use single sign-on to Box. (Bug 814752)

Workaround: To ensure that single sign-on works for the Box connector, set the **User session timeout** value to 74 minutes or less. This is a cluster-level setting so it will affect behavior of user sessions not using Box as well.

[Return to Top]

5.11 MobileAccess Issues

5.11.1 Safari on Mobile Devices Cannot Access the Login Page After You Enable the MobileAccess Connector

Issue: Logins to the CloudAccess login page from the Safari browser on a mobile device no longer work after you enable the MobileAccess connector in the administration console. When you enable the MobileAccess connector, support for mobile devices requires that users install the MobileAccess app on their mobile devices. (Bug 838977)

Workaround: This is intended behavior.

5.11.2 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.

[Return to Top]

5.12 Upgrade Issues

5.12.1 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 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 to version 2.1. 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 from version 2.0 to version 2.1, 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.

5.12.2 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 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.

5.12.3 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 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.

5.12.4 Users Cannot See Appmarks and Cannot Directly Access Protected Resources

Issue: After you update from version 2.0 to version 2.1, 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.

5.12.5 Appmarks Cannot Display Their Global URLs and Public Icons

Issue: After you update from version 2.0 to version 2.1, 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 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.

5.12.6 Appmarks for Existing Applications Are Not Displayed on Android Devices

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

Workaround: After you update from 2.0 to 2.1, 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.

[Return to Top]

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.

[Return to Top]

7 Legal Notice

[Return to Top]