NetIQ SocialAccess 2.1 Release Notes

October 2014

NetIQ SocialAccess 2.1 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 SocialAccess forum (https://forums.netiq.com/forumdisplay.php?124-SocialAccess) 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 SocialAccess NetIQ Documentation (https://www.netiq.com/documentation/socialaccess/) page. To download this product, see the NetIQ Downloads (https://dl.netiq.com/) website.

1 What’s New?

The following section outlines the key features and functions provided by this version, as well as issues resolved in this release:

1.1 Security Improvements

SocialAccess improves security by upgrading to OpenSSL 1.0.1i.

SocialAccess improves security by addressing the GNU Bourne-Again Shell (Bash) Shellshock Vulnerability. It includes fixes for the following Common Vulnerabilities and Exposures (CVEs):

- CVE-2014-7187
- CVE-2014-7186
- CVE-2014-7169
- CVE-2014-6278 (This issue is already mitigated (fixed) by the function hardening patch introduced in the update for CVE-2014-7169.)

- CVE-2014-6277 (This issue is already mitigated by the function hardening patch introduced in the update for CVE-2014-7169.)
- CVE-2014-6271

1.2 Connector for OAuth2 Resources

SocialAccess now includes a connector for OAuth2 Resources. This connector provides simple authenticated access to a web service through SocialAccess. For more information, see "Configuring the Connector for OAuth2 Resources" in the *NetIQ® SocialAccess Installation and Configuration Guide*.

1.3 Connector for Simple Proxy

SocialAccess now includes a connector for Simple Proxy. This connector provides reverse proxy access to your enterprise web service through SocialAccess. For more information, see "Configuring the Connector for Simple Proxy"in the *NetIQ® SocialAccess Installation and Configuration Guide*.

1.4 Authentication Filter Tool

SocialAccess now provides an Authentication Filter tool. This tool allows you to create scripts that apply extended functions to add, remove, or manage a user's identity information for the session. For more information, see "Configuring the Authentication Filter to Set Session-Based Identity Information for a User" in the *NetIQ® SocialAccess Installation and Configuration Guide*.

1.5 Enhancements and Software Fixes

SocialAccess includes software fixes that resolve several previous issues.

1.5.1 Updated Connector for NetIQ Access Manager

The connector for NetIQ Access Manager has been updated to support appmarks configuration. For more information, see "Configuring the Connector for NetIQ Access Manager" in the *NetIQ® SocialAccess Installation and Configuration Guide*.

1.5.2 Updated SAML 2.0 Connector for ADFS

The SAML 2.0 connector for ADFS has been updated to support appmarks configuration. For more information, see "Configuring the SAML 2.0 Connector for ADFS" in the *NetIQ® SocialAccess Installation and Configuration Guide*.

1.5.3 Access Connector Toolkit Enhancements

The Access Connector Toolkit has been enhanced. You can now use the Access Connector Toolkit to create custom connectors for identity-aware web services or applications that use WS-Federation and SAML 2.0 Inbound (SAML-In) authentication methods for single sign-on. For more information, see "Creating Custom Connectors with the Access Connector Toolkit" in the *NetIQ® SocialAccess Installation and Configuration Guide*.

1.5.4 Appmarks for Connectors

All application connectors in SocialAccess now provide the ability to configure appmarks to enable users to access SSO applications in different ways. After users log in to SocialAccess, they see the appmarks that they are entitled to see on the landing page. For more information, see "Configuring Appmarks for Connectors" in the *NetIQ® SocialAccess Installation and Configuration Guide*.

1.5.5 Improved Administrator Console

SocialAccess now includes an improved administration console:

- **Palettes:** The Admin page displays palettes for identity sources, applications, and tools that you can add to the appliance.
- **Panels:** The Admin page displays panels for configured identity sources, applications, and tools. Icon overlays indicate their health and configuration status.
- **Health:** The Admin page includes summary health information for the identity sources, applications, tools, and users. It also includes health information for nodes in the cluster.

1.5.6 User Landing Page

SocialAccess now provides a landing page that displays the appmarks for applications the user is entitled to use. For more information about setting up appmarks for application connectors, see "Configuring Appmarks for Connectors" in the *NetIQ® SocialAccess Installation and Configuration Guide*.

1.5.7 Ability to Have a User-Selectable Language on the Login Page

SocialAccess administrators are now able to customize the login page so users can select the language they want to use for their browser session. Performing advanced branding customization requires advanced JavaServer Pages (JSP) knowledge. For more information about custom branding, see the *NetIQ® SocialAccess Installation and Configuration Guide*.

2 System Requirements

To upgrade to SocialAccess 2.1, you must have an existing installation of SocialAccess 2.0. You can update an appliance from version 2.0 to 2.1 only through the update channel. Other upgrades are not supported. For more information, see "Updating the Appliance"in the *NetIQ® SocialAccess Installation and Configuration Guide*.

For detailed information on hardware requirements and supported operating systems and browsers, see "Installing SocialAccess"in the *NetIQ® SocialAccess Installation and Configuration Guide*.

[Return to Top]

3 Installing SocialAccess

To install SocialAccess, see "Installing SocialAccess" in the *NetIQ® SocialAccess Installation and Configuration Guide*.

[Return to Top]

4 Verifying the Installation

Perform the following steps to verify that the installation was successful.

To check the installed version:

1. Access the administration console at `https://appliance_dns_name/appliance/index.html`, then log in with the password specified during the initialization process.
2. Click the appliance, then click **About**. Verify that the version listed in the window is `2.1-build number`.

[Return to Top]

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 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.

5.2 Changing from DHCP to Static IP During Initialization Causes Errors

Issue: During the appliance initialization process, changing the IP address from dynamic (DHCP) to static can cause an error stating that services are unavailable.

Workaround: This message can be ignored. Refresh your browser and the message disappears.

5.3 User Authentication Fails, but Health of the Appliance Is Green

Issue: Appliance health might be green while user authentications fail. Basic network connectivity is working, but the identity source is not available. (Bug 798835)

Workaround: If user authentications fail, verify that you can access the social networking site outside of SocialAccess. If you cannot, the social networking site is down, and user authentications will continue to fail until the social networking site is available.

5.4 Email Must Be Specified to Enable Persistent Logins

Issue: The connector definition fields in the Access Connector Toolkit include an **Email** check box for the persistent email attribute. You cannot currently change the persistent attribute to a different format, and SocialAccess does not attempt to map the persistent attribute unless you select the **Email** check box.

Workaround: To enable persistent logins, ensure that you select the **Email** check box in the connector definition.

5.5 Re-running Initialization Resets Custom Branding to Default

Issue: If you implement custom branding in your SocialAccess 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 SocialAccess. Before you re-run the initialization process on an existing SocialAccess cluster, ensure that you back up your customized branding files so that you can reuse them.

5.6 Upgrade Issues

5.6.1 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.

5.6.2 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.

5.6.3 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.

[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 Web site (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate Web site (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

PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

For information about NetIQ trademarks, see http://www.netiq.com/company/legal/ (http://www.netiq.com/company/legal/).

[Return to Top]