

NetIQ SocialAccess 2.2 Release Notes

March 2015



NetIQ SocialAccess 2.2 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 \(https://forums.netiq.com/forumdisplay.php?124-SocialAccess\)](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 \(https://www.netiq.com/documentation/socialaccess/\)](https://www.netiq.com/documentation/socialaccess/) page. To download this product, see the [NetIQ Downloads \(https://dl.netiq.com/\)](https://dl.netiq.com/) website.

- ◆ [Section 1, "What's New?," on page 1](#)
- ◆ [Section 2, "System Requirements," on page 2](#)
- ◆ [Section 3, "Installing SocialAccess," on page 2](#)
- ◆ [Section 4, "Verifying the Installation," on page 2](#)
- ◆ [Section 5, "Known Issues," on page 2](#)
- ◆ [Section 6, "Contact Information," on page 4](#)
- ◆ [Section 7, "Legal Notice," on page 5](#)

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:

- ◆ [Section 1.1, "Supported Operating Systems," on page 1](#)
- ◆ [Section 1.2, "Improved Connector for NetIQ Access Manager," on page 2](#)

1.1 Supported Operating Systems

For information about the supported operating systems for the appliance, see "[Requirements](#)" in the *NetIQ® SocialAccess Installation and Configuration Guide*.

1.2 Improved Connector for NetIQ Access Manager

NetIQ has enhanced the integration between SocialAccess and NetIQ Access Manager 4.1.x to simplify the configuration. If you are using an older version of Access Manager, you must use the generic connector for NetIQ Access Manager. For more information about the enhanced connector for NetIQ Access Manager, see “[Configuring the Connector for NetIQ Access Manager](#)” in the *NetIQ® SocialAccess Installation and Configuration Guide*.

2 System Requirements

To upgrade to SocialAccess 2.2, you must have an existing installation of SocialAccess 2.0 or 2.1. You can update an appliance to version 2.2 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*.

3 Installing SocialAccess

To install SocialAccess, see “[Installing SocialAccess](#)” in the *NetIQ® SocialAccess Installation and Configuration Guide*.

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 *2.2-build number*.

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 \(http://www.netiq.com/support\)](http://www.netiq.com/support).

- ♦ [Section 5.1, “Changing from DHCP to Static IP During Initialization Causes Errors,”](#) on page 2
- ♦ [Section 5.2, “User Authentication Fails, but Health of the Appliance Is Green,”](#) on page 3
- ♦ [Section 5.3, “SAML 2.0 Inbound Users See Only Public Access Appmarks,”](#) on page 3
- ♦ [Section 5.4, “Upgrade Issues,”](#) on page 3

5.1 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.

5.2 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.

5.3 SAML 2.0 Inbound Users See Only Public Access Appmarks

Issue: When using the SAML 2.0 Inbound connector in mode **Allow access for unknown users**, after the first login when the user has just been created, the landing page displays only the Public appmarks. (Bug 920022)

Workaround: Since these specific types of users are not stored locally on the appliance, the appliance cannot apply the proper roles until the user logs in a second time. If you have any users that see this problem, instruct them to log out and log back in to the landing page. The landing page properly displays all of the appmarks.

5.4 Upgrade Issues

5.4.1 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 or later 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. 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, 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.

5.4.2 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 or later 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.

5.4.3 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 or later 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.

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) (<http://www.netiq.com/support/process.asp#phone>).

For general corporate and product information, see the [NetIQ Corporate Web site](http://www.netiq.com/) (<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/) (<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

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR 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.

© 2015 NetIQ Corporation. All Rights Reserved.

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