This service pack for SaaS Account Management (SAM) 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 Access Manager forum (https://forums.novell.com/forumdisplay.php/1314-Access-Manager) 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 SaaS Account Management Documentation (https://www.netiq.com/documentation/saas-account-management-10/) page. To download this product, see the NetIQ Downloads (https://dl.netiq.com/) website.

- Section 1, "What's New?,” on page 1
- Section 2, “System Requirements,” on page 2
- Section 3, “Updating SaaS Account Management,” on page 2
- Section 4, “Verifying the Update,” on page 2
- Section 5, “Known Issues,” on page 2
- Section 6, “Contact Information,” on page 4
- Section 7, “Legal Notice,” on page 4

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.

- Section 1.1, "Improvements to Health Information," on page 1
- Section 1.2, “Operating System and Security Updates,” on page 2

1.1 Improvements to Health Information

In this release, the appliance management console provides some additional health information and usability improvements. For example, the hover text on the landing page now informs you how old the health information is. You can still refresh the landing page using the browser’s refresh button, or open and then close the Health page for the latest information. (Bug 1130739)

In addition, if you configured a remote Syslog server with the TCP protocol, the health status shows green if the Syslog TCP port is listening for connections and yellow if the remote port is not listening, or if any other error occurs during the health check. (Bug 1131903)
NOTE: If you configured a remote Syslog server with the UDP protocol, SAM does not perform a port
check and does not provide Syslog information in the status report because of communication
limitations with the UDP protocol.

1.2 Operating System and Security Updates

This release contains operating system and security updates for the appliance.

2 System Requirements

SaaS Account Management is an appliance and it requires the following:

- NetIQ Access Manager 4.5 or later, installed and configured
- VMware vSphere and vSphere Hypervisor 6.0 or 5.5

For more information about specific requirements, see the following topics in the NetIQ SaaS Account
Management 1.0 Installation Guide on the SaaS Account Management Documentation website
(https://www.netiq.com/documentation/saas-account-management-10/):

- “Product Requirements”
- “Minimum User Store Requirements”

3 Updating SaaS Account Management

This service pack requires an existing installation of SaaS Account Management 1.0 SP1. You can
update a SAM 1.0 SP1 appliance to SAM 1.0 SP2 only through the update channel. For more
information, see “Performing an Online Update” in the NetIQ SaaS Account Management 1.0
Installation Guide on the SaaS Account Management Documentation website (https://www.netiq.com/
documentation/saas-account-management-10/).

4 Verifying the Update

To check the installed version of SaaS Account Management, log in to the appliance management
console and locate the version string at the top of the console page. The installed version of this
service pack is 1.0.2.0-346.

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).

- Section 5.1, “Changing Network Settings Requires Appliance Restart,” on page 3
- Section 5.2, “Appliance Unregistration Is Required to Stop Polling,” on page 3
- Section 5.3, “Validation of LogMeIn Settings Fails in Access Manager,” on page 3
- Section 5.4, “LogMeIn Provisioned Users Appear Suspended,” on page 3
- Section 5.5, “LogMeIn User Accounts Are Not Disabled Correctly,” on page 3
5.1 Changing Network Settings Requires Appliance Restart

In this release, if you change any network settings for the SAM appliance you must restart the appliance. When you restart the appliance, it re-registers with Access Manager using the updated information. (Bug 1117376)

5.2 Appliance Unregistration Is Required to Stop Polling

After you register a SAM appliance with Access Manager, the appliance polls Access Manager every 15 minutes to ensure that its configuration is up to date. As part of this polling process, SAM also re-registers itself automatically if Access Manager no longer has a reference to this SAM appliance. If you want to remove SAM from your Access Manager environment completely, ensure that you use the SaaS Account Management icon in the appliance management console to unregister the appliance. This removes the reference in Access Manager to the SAM appliance and also causes the appliance to stop the polling and auto registration process. (Bug 1124034)

5.3 Validation of LogMeIn Settings Fails in Access Manager

Issue: After creating an app at the LogMeIn website to get a consumer key and secret, clicking the Validate Settings button in Access Manager results in errors. (Bug 1134915)

Solution: Ensure that the administrator account you are using is capable of direct login to LogMeIn. Administrator accounts federated with LogMeIn are not valid to use for SAM to authenticate.

5.4 LogMeIn Provisioned Users Appear Suspended

Issue: After SAM provisions users to LogMeIn, the LogMeIn Admin Center shows those users’ status as Suspended. Despite this status, provisioned users are able to log in using SAML single sign-on. This issue occurs because SAM does not assign any products as part of the provisioning process. (Bug 1135800)

Workaround: You can work around this issue by using the LogMeIn Admin Center to manually assign one or more products to each user. User status then changes to Enabled.

5.5 LogMeIn User Accounts Are Not Disabled Correctly

Issue: LogMeIn user accounts that SAM has provisioned or claimed are not being disabled as expected if the user is later removed from the Psearch filtered group. The SAM log indicates that disabling a user is not supported. (Bug 1135803)

Workaround: To work around this issue, you can use the LogMeIn Admin Center to manually remove assigned products from the user. Doing so results in the user’s status being changed to Suspended.
5.6 **Local Logins at Some Applications Still Possible After SAM Claims an Existing Account**

When SAM claims a user account at a SaaS application because the LDAP user's mail attribute matches the user name of an existing user, SAM tries to randomize the user password. As a result, local login is typically unavailable after SAM has claimed the user account. However, in the case of Dropbox, Office 365, Salesforce, Tableau, and Zendesk, SAM is unable to randomize passwords for matching users, so users can still log in directly to their accounts at those applications after SAM has claimed their user accounts. Currently, no workaround is available for this issue. *(Bugs 1134244 and 1135500)*

5.7 **Automatically Send Configuration to Micro Focus Using FTP Option Does Not Work**

**Issue:** The Support widget in the appliance management console provides the option *Automatically send the configuration to Micro Focus using FTP*, but this option does not currently work. *(Bug 1138029)*

**Workaround:** You can work around this issue by selecting the other option to download and save the configuration file locally, then email it to Micro Focus manually. We will address this issue in a future release.

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. 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/](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**

© Copyright 2019 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors ("Micro Focus") are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see [http://www.microfocus.com/about/legal/](http://www.microfocus.com/about/legal/).