This patch update 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 our Communities page, our online community that also includes product information, blogs, and links to helpful resources.

- 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 5
- Section 7, “Legal Notice,” on page 5

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, “Operating System and Security Updates,” on page 1
- Section 1.2, “Improvements to Connector for Docusign,” on page 1
- Section 1.3, “Improved Handling of Changes to Network Settings for the Appliance,” on page 1

1.1 Operating System and Security Updates

This patch update contains operating system and security updates for the appliance.

1.2 Improvements to Connector for Docusign

This patch update includes several bug fixes and minor improvements for the connector for Docusign.

1.3 Improved Handling of Changes to Network Settings for the Appliance

Any change to network settings requires the appliance to be rebooted before it will function normally. The network settings tool now makes it clear that a reboot is necessary and gives you the opportunity to cancel changes before they are saved. If you do save your changes, the tool offers to reboot the appliance immediately. (Bug 1117376)
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 patch update requires an existing installation of SaaS Account Management 1.0 SP2. You can update a SAM 1.0 SP2 appliance to SAM 1.0 SP2 P1 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 patch update is 1.0.2.1-201908200241.

5 Known Issues

We strive 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, “Appliance Unregistration Is Required to Stop Polling,” on page 2
- Section 5.2, “Validation of LogMeIn Settings Fails in Access Manager,” on page 3
- Section 5.3, “LogMeIn Provisioned Users Appear Suspended,” on page 3
- Section 5.4, “LogMeIn User Accounts Are Not Disabled Correctly,” on page 3
- Section 5.5, “Local Logins at Some Applications Still Possible After SAM Claims an Existing Account,” on page 3
- Section 5.6, “Disabling Local Logins at Zendesk After SAM Claims an Existing Account Requires Additional Steps,” on page 3
- Section 5.7, “Unique Tableau Behaviors After User Provisioning,” on page 4
- Section 5.8, “Automatically Send Configuration to Micro Focus Using FTP Option Does Not Work,” on page 4

5.1 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 unregister the appliance using the SaaS Account Management icon in the appliance management console. 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)

5.2 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.

5.3 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.

5.4 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.

5.5 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 Docusign, Dropbox, Salesforce, and Tableau, 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, 1135500, 1138174, and 1145784)

5.6 Disabling Local Logins at Zendesk After SAM Claims an Existing Account Requires Additional Steps

Issue: 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 to make local login unavailable to the user. However, in the case of Zendesk, the ability for administrators to change user passwords is a global security setting that is disabled by default. As a
result, when SAM tries to change the password for a claimed account, Zendesk returns an error such as "You do not have access to this page. Please contact the account owner of this help desk for further help." (Bug 1133821)

**Workaround:** To work around this issue:

1. Log in to Zendesk as an administrator.
2. Navigate to **Settings > Security**, click the **Global** tab, then click the **Admin Center** link.
3. In the Admin Center, navigate to **Advanced**.
4. Select the **Enable admins to set passwords** check box.
5. (Optional) Select the **Email Notifications** check box if you want users to receive an email that their password has been changed.
6. Click **Save**.

After you complete these steps, when SAM claims an account the password is set to a random value and local logins with the old password are no longer possible.

### 5.7 Unique Tableau Behaviors After User Provisioning

Using SAM to provision users to Tableau currently results in the following unique behaviors: (Bug 1136613)

- After SAM provisions a user to Tableau, modifying the user’s email attribute in the LDAP user store results in SAML single sign-on no longer working because SAM cannot propagate the change to Tableau. If you then restart Psearch, SAM creates a new user account in Tableau with the new email address and leaves the original account as-is.
- Newly provisioned users always get the “Viewer” Site Role.
- Claiming an existing user maintains the user’s current Site Role.
- If SAM deprovisions a user (for example, if you remove the user from the Psearch group), the Site Role changes to Unlicensed.
- If SAM reprovisions a user (for example, if you add the user back into the Psearch group), the Site Role is set to Viewer regardless of the user’s role before SAM deprovisioned the user.

Attribute mapping and synchronization are as follows:

- The LDAP email becomes the Tableau Username
- SAM does not synchronize any LDAP attributes to Tableau

### 5.8 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 (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.

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/.