Release Notes

NetIQ SaaS Account Management
1.0 SP3 Release Notes

March 2020

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 our Communities page, 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.

- “What’s New?” on page 1
- “System Requirements” on page 2
- “Updating SaaS Account Management” on page 2
- “Verifying the Update” on page 2
- “Upgrading Your Installation to Implement SaaS Authorizations” on page 2
- “Known Issues” on page 3
- “Contact Information” on page 6
- “Legal Notice” on page 7

What’s New?

The following sections outline the key features and functions provided by this version, as well as issues resolved in this release.

- “Operating System and Security Updates” on page 1
- “Ability to Assign Authorizations for Supported SaaS Applications” on page 2

Operating System and Security Updates

This service pack contains operating system and security updates for the appliance.
**Ability to Assign Authorizations for Supported SaaS Applications**

When you configure a SAML2/Account Management application in Access Manager, SaaS Account Management now allows you to map authorizations returned by a SaaS application (for example, Office 365), such as licenses, service plans, roles, and groups to the local LDAP groups in the Access Manager user stores. While provisioning qualified users from the LDAP user stores to a SaaS application, SAM creates these users with the authorizations as mapped on the LDAP Groups and Authorizations page. For more information, see 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/).

**System Requirements**

SaaS Account Management 1.0 SP3 is an appliance and it requires the following:

- NetIQ Access Manager 4.5 SP2 or later, installed and configured
- VMware vSphere and vSphere Hypervisor 6.0 or 5.5

To assign authorizations to SaaS applications using SaaS Account Management, you must use Chromium-based Edge (which provides backward-compatibility with Internet Explorer 11) or another browser, such as Chrome or Firefox. The authorizations feature does not work in Microsoft Internet Explorer and Microsoft Edge 18 or earlier.

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”

**Updating SaaS Account Management**

This service pack requires an existing installation of SaaS Account Management 1.0 SP1 or later. You can update a SAM appliance to SAM 1.0 SP3 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/).

**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 1.0.3.0-202003301507.

**Upgrading Your Installation to Implement SaaS Authorizations**

If you have an existing SaaS Account Management installation and provisioned users to SaaS applications, you must complete the following steps to enable the Psearch service to reprocess users.
To upgrade your installation and implement SaaS authorizations:

1 Upgrade your SAM installation to SAM 1.0 SP3. 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/).


3 Configure the appropriate SAML2/Account Management connectors on the Account Management page in the Access Manager admin console. For more information, see 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/).

For provisioning to occur, you must select at least one LDAP group on the LDAP Groups and Authorizations page. For authorizations to be assigned, you must map them to the LDAP groups you have selected. SAM then processes and provisions to the SaaS applications the LDAP users who are members of the mapped groups and who have the required firstname, lastname, and email attributes. If you do not specifically assign SaaS authorizations, the LDAP users get only accounts.

IMPORTANT: Be careful when mapping new authorizations, because SAM reprocesses users that you previously provisioned. If you assign new authorizations and they do not match authorizations that you previously configured manually, SAM removes from the user’s SaaS account any authorizations that are not mapped on the new LDAP Users and Authorizations page.

If you manually assigned authorizations to SaaS applications in a previous version of SaaS Account Management, those manual assignments remain in place until you make changes and click Save on the new LDAP Users and Authorizations page and click Save again on the Account Management page.

4 Verify that authorizations are correctly assigned at the SaaS applications.

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).

- “Appliance Unregistration Is Required to Stop Polling” on page 4
- “Validation of LogMeIn Settings Fails in Access Manager” on page 4
- “LogMeIn Provisioned Users Appear Suspended” on page 4
- “LogMeIn User Accounts Are Not Disabled Correctly” on page 4
- “Local Logins at Some Applications Still Possible After SAM Claims an Existing Account” on page 4
- “Disabling Local Logins at Zendesk After SAM Claims an Existing Account Requires Additional Steps” on page 5
- “Unique Tableau Behaviors After User Provisioning” on page 5
- “Unable to Provision Users into Locally Managed Groups in Office 365” on page 5
- “Automatically Send Configuration to Micro Focus Using FTP Option Does Not Work” on page 6
- “Mapping Multiple User Placement Type Authorizations Results In Unexpected Behavior” on page 6
- “Office 365 Users Are Not Provisioned to Exchange Online Plan 1 As Expected” on page 6
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)

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.

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.

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.

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)
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.

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

Unable to Provision Users into Locally Managed Groups in Office 365

**Issue:** When you provision LDAP users to Office 365, SaaS Account Management cannot provision locally managed, on-premise groups created in Azure. Psearch is currently unable to filter out these groups from the list that appears in the LDAP Groups and Authorizations window. (Bug 1165320)

**Workaround:** In the LDAP Groups and Authorizations page, map only groups that are not the on-premise type.
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.

Mapping Multiple User Placement Type Authorizations Results In Unexpected Behavior

**Issue:** If you map multiple *User Placement* type authorizations that exclude each other, you get different behaviors from the different connectors. The Connector for Google places the users at the root of the organization instead of in the conflicting locations. ([Bug 1165195](#))

**Workaround:** Ensure that the *User Placement* type authorizations do not conflict.

Office 365 Users Are Not Provisioned to Exchange Online Plan 1 As Expected

**Issue:** If you have two Office 365 user licenses that contain Exchange Online Plan 1 and Exchange Online Plan 2, Office 365 regards these two service plans as mutually exclusive, which means that SAM can grant only one of them to the user in Office 365.

When the Office 365 SAM connector is doing authorization provisioning for users, if both service plans are present in the list of authorizations to grant, SAM grants only Exchange Online Plan 2.

An issue might arise if you are trying to grant both authorizations (Exchange Online Plan 1 and Exchange Online Plan 2), and you exhaust all of the user licenses for Exchange Online Plan 2. Since no more licenses are available in Office 365 for this service plan, SAM grants none of its service plans either, which includes Exchange Online Plan 2. The end result is that, even though you mapped both Exchange service plans as authorizations, some users will not be granted an Exchange Online Plan as there are no licenses available to grant Exchange Online Plan 2 with, and Exchange Online Plan 1 was already removed from the provisioning event. ([Bug 1168119](#))

**Workaround:** To work around this issue, consider buying additional licenses so SAM can grant authorizations for Exchange Online Plan 2; remove Exchange Online Plan 2 from the mapped authorizations list, so SAM grants only Exchange Online Plan 1; or edit the users in the Office 365 admin portal and grant Exchange Online Plan 1 authorizations manually.

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/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

**Legal Notice**

© Copyright 2020 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/.