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.

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

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
- “Users Are Not Correctly Provisioned to Office 365” on page 2
- “Automatically Send Configuration to Micro Focus Using FTP Option Does Not Work” on page 2
- “Improvements to SAML/Account Management Connectors” on page 2

Operating System and Security Updates

This patch update contains operating system and security updates for the appliance.
Users Are Not Correctly Provisioned to Office 365

This patch update addresses an issue where customers using the Office 365 DEVELOPERPACK_E5 license and service plans were unable to provision users properly and received an error that the service plan was not valid. (Bug 267026)

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

This patch update addresses an issue where the Support widget option Automatically send the configuration to Micro Focus using FTP in the appliance management console did not work. (Bug 1138029)

Improvements to SAML/Account Management Connectors

This patch update contains various improvements to the SAML/Account Management connectors for Box, Docusign, Dropbox, Google Apps, LogMeIn, Office 365, Salesforce, and Tableau. These improvements include documentation updates as well as updates to behavior to ensure that the connectors work as expected.

System Requirements

SaaS Account Management 1.0 SP3 P2 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 patch update requires an existing installation of SaaS Account Management 1.0 SP1 or later. You can update a SAM appliance to SAM 1.0 SP3 P2 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 1.0.3.2-202011021255.
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 3
- “Validation of LogMeIn Settings Fails in Access Manager” on page 3
- “Local Logins at Some Applications Still Possible After SAM Claims an Existing Account” on page 3
- “Disabling Local Logins at Zendesk After SAM Claims an Existing Account Requires Additional Steps” on page 4
- “Unable to Provision Users into Locally Managed Groups in Office 365” on page 4
- “Mapping Multiple User Placement Type Authorizations Results In Unexpected Behavior” on page 4
- “Office 365 Users Are Not Provisioned to Exchange Online Plan 1 As Expected” on page 4
- “Salesforce Connector Includes Conflicting Authorization Types” on page 5
- “Changing an Email Address in the User Store Might Result in a Duplicate Account Being Created” on page 5

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.

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.

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

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. With the Connector for Google, user placement will be indeterminate if you map 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.

**Salesforce Connector Includes Conflicting Authorization Types**

**Issue:** The License type authorizations that are available in the Salesforce connector conflict with Permission Profile type authorizations. (Bug 1169358)

**Solution:** When provisioning users to Salesforce, do not map License type authorizations. Map only the Permission Profile type authorizations. In a future release of Access Manager, the License type authorizations for the Salesforce connector will no longer appear on the LDAP Groups and Authorizations page.

**IMPORTANT:** Use caution when mapping authorizations for all connectors. SaaS authorizations change frequently, so SaaS Account Management simply presents the available authorizations and does not attempt to restrict any mappings that might conflict at the SaaS application. As a best practice, we recommend that you test any mapped authorizations in a non-production environment to ensure that they work as expected before you implement them in your production environment.

**Changing an Email Address in the User Store Might Result in a Duplicate Account Being Created**

**Issue:** In Box or Tableau, changing a provisioned user’s email address in your LDAP user store might result in a duplicate account being created in the target SaaS system and the original account being orphaned. (Bugs 189407 and 288143)

**Workaround:** In Tableau, this is working as designed. Tableau does not allow an email address to be changed because the email address serves as the unique user name. If you encounter this issue, you must create a new account, transfer any content from the old account, and delete the old account. For more information, see the knowledge base article at https://kb.tableau.com/articles/howto/changing-tableau-online-user-name (https://kb.tableau.com/articles/howto/changing-tableau-online-user-name).

In Box, if you encounter this issue because a duplicate account has been created and a user notifies you that something is wrong with the Box account:

1. Delete the new duplicate account.
2. Set the email address on the old Box account to the new desired value.
3. The user gets an email at the new address and must verify the address change.
4. The user logs in to Box with the new email address and everything looks as expected.
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.

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/.