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/.
## Contents

**About This Book and the Library**  
5

### 1 Understanding SaaS Account Management  
7  
Benefits of Using SaaS Account Management ............................................. 7  
Understanding Terminology ...................................................................... 7  
Typical SAM Deployment ........................................................................ 8  
How SaaS Account Management Works .................................................. 8  
Example: Provisioning a New User Account to Salesforce ......................... 9  
Locating the SaaS Account Management Connectors .................................. 11

### 2 Installing SaaS Account Management  
13  
Product Requirements ............................................................................ 13  
Deploying SaaS Account Management .................................................... 14  
Obtaining SaaS Account Management ..................................................... 14  
Deploying the Appliance ........................................................................ 14

### 3 Provisioning Users to SaaS Providers  
17  
Understanding SAM Provisioning and Authorizations .............................. 17  
Minimum User Store Requirements ....................................................... 17  
Understanding Attribute Account Matching ............................................. 18  
Preventing Accidental Account Claiming at SaaS Providers ...................... 20  
Configuring Successful Single Sign-On to Google .................................... 21  
Understanding Local Login Behavior When Enabling SAM ...................... 21  
Understanding Authorizations .................................................................. 22  
Understanding Google Apps Authorization Mappings ............................... 23  
Configuring SAML/Account Management Connectors and Provisioning Users 24  
Mapping Authorizations for Provisioned Users ......................................... 26

### 4 Managing the SAM Appliance  
27  
Accessing the Appliance Management Console ....................................... 28  
Enabling Account Management ............................................................... 28  
Setting Administrative Passwords ............................................................ 29  
Configuring Network Settings ................................................................ 30  
Adding Additional Hosts to the Hosts File .............................................. 31  
Configuring Time Settings ..................................................................... 31  
Accessing System Services ..................................................................... 31  
Managing Appliance Certificates ............................................................ 32  
Using the Digital Certificates Page ......................................................... 32  
Using an Existing Certificate and Key Pair ............................................. 34  
Activating the Certificate ....................................................................... 34  
Viewing Firewall Settings ...................................................................... 34  
Configuring Remote Logging ................................................................. 35
About This Book and the Library


Intended Audience

This guide provides information for individuals responsible for installing and maintaining the SaaS Account Management (SAM) appliance in a NetIQ Access Manager environment. You must have a good understanding of Access Manager, networking concepts, and virtual environments.

Other Information in the Library

The library provides the following information resources:

Connectors Guide
- Provides setup instructions for each of the connectors provided by NetIQ SaaS Account Management.

Help
- Provides context-sensitive information and step-by-step guidance for common tasks.

Release Notes
- Provide information specific to this release of the SaaS Account Management product, such as known issues.
About This Book and the Library
Understanding SaaS Account Management

SaaS Account Management (SAM) addresses several common problems with SaaS accounts in corporate environments, namely the proliferation of SaaS accounts, the need to have a user account in each of the SaaS systems to enable user access, and the need to deprovision accounts when user roles change or users leave the company.

Benefits of Using SaaS Account Management

Working with your existing LDAP user stores in NetIQ Access Manager, SaaS Account Management (SAM) enables you to easily provision and manage SaaS accounts. SAM not only automatically provisions user accounts to your SaaS providers, but also synchronizes changes you make in your user store. When user responsibilities change and a provisioned user no longer needs access to an application, or a user leaves the company, you do not have to manually update user accounts for the appropriate applications. SAM automatically deprovisions accounts for connected applications based on changes made in your user store.

Understanding Terminology

It is important to understand differences between various terms used in this documentation and in the product.

**Connector** A term used generically for all connectors in the NetIQ public connector catalog. A connector is essentially a starting point or template used for creating an application. For example, you import a connector from the catalog and configure its settings. When you save it, you now have an application. Depending on the connector, the application will be either a SAML application or a SAML2/Account Management application.

**SAML connector** A connector that has the capability of providing single sign-on (SSO) for existing user accounts, but does not actually provision user accounts to the SaaS providers.

**SAML/Account Management connector** A connector that you can configure either for SAML only (to provide SSO for existing user accounts), or for SAML with Account Management to get the additional benefits of user provisioning.

**SAML application** An application that you have configured in Access Manager and provides single sign-on for existing user accounts, but does not have other account management capabilities.

**SAML2/Account Management application** An application that you have configured in Access Manager either for SAML only, or for SAML with Account Management to get the additional benefit of user provisioning.
Typical SAM Deployment

You deploy the SaaS Account Management appliance as a single node in your Access Manager environment. Clustering is not currently supported.

You must deploy the appliance behind the firewall to enable it to communicate with your LDAP server. You must also open the firewall to the SaaS applications to allow user account provisioning and authentications.

The following diagram illustrates one possible scenario for deploying SaaS Account Management in your Access Manager environment. For additional information about deployment options, refer to the Access Manager documentation on the NetIQ documentation website (https://www.netiq.com/documentation/).

Figure 1-1 Typical SAM Deployment

How SaaS Account Management Works

SaaS Account Management (SAM) is an appliance that integrates seamlessly with NetIQ Access Manager. To use the account management functions in SaaS Account Management, you must have an Access Manager setup, a SAM appliance, and SaaS-specific SAML/Account Management connectors that are downloaded from the NetIQ public connector catalog.

The difference between SaaS Account Management connectors and SAML connectors is that the SaaS Account Management connectors automatically provision mapped users from the user store into the SaaS application (either by creating new users if necessary or claiming existing accounts), whereas SAML connectors require administrators to manually create the same user accounts in the user store of the application (for example, Salesforce).

NOTE: The connectors in the connector catalog that are capable of account management can be configured either for SAML only (to provide single sign-on for existing user accounts) or for SAML with Account Management to get the additional benefits of user provisioning.
SaaS Account Management currently supports only SAML2 applications.

The following graphic illustrates the SaaS Account Management architecture within the NetIQ Access Manager environment.

**Figure 1-2  SAM Architecture**

Once you have deployed SaaS Account Management in your Access Manager environment, you must provide information for each of your SAML applications to enable the service to provision user accounts to the SaaS providers. You map groups selected from your LDAP user stores in Access Manager to determine which users will be provisioned, and you can also map specific SaaS authorizations to those user groups.

The LDAP persistent search module (Psearchservice) handles provisioning, deprovisioning, and LDAP account changes for SaaS Account Management. After you configure a SAML2/Account Management application and save your configuration, the first time Psearchservice runs, it reads the LDAP directory and imports the mapped users from the user store into the specified SaaS application. Psearchservice then runs periodically (at a polling interval that you specify) to check for any changes in the LDAP directory.

**Example: Provisioning a New User Account to Salesforce**

The following example illustrates the provisioning of a new user account to Salesforce using the SAML2/Account Management application for Salesforce.

1. You create an Active Directory user account in your Access Manager user store. The user is not yet a member of any group.
2. In the Applications section of Access Manager, you import the SAML/Account Management connector for Salesforce. You set the Attribute mapping as follows:
   - Remote Attribute: Salesforce ID
3 You enable **Account Management** and configure the connector settings, along with an LDAP user store and one or more mapped groups. You click **Save**.

SaaS Account Management creates a configuration file in the Psearchservice, and it begins polling the LDAP user stores. Because the user is not yet a member of any mapped group, the user is not provisioned and is not able to single sign-on to Salesforce yet.

4 In your Active Directory user store, you add the same user to the mapped group that you specified in step 3.

SAM polls the user store at the polling interval you set for the application, and sees that the user account is now a member of the mapped group.

SAM creates a new user account in Salesforce and the user is able to single sign-on to Salesforce by clicking the Salesforce appmark on the Access Manager user portal page.

SAM creates events showing these updates, and records details of the user account created in Salesforce.

5 You modify the user’s last name in your Active Directory user store.

SAM polls the user store again, and sees the update to that user account.

The change to the user’s name is reflected in the Salesforce user account, and single sign-on continues to work as expected.

6 In your Active Directory user store, you remove the user from the mapped group.

SAM polls the user store again, and sees that the user account is no longer a member of the mapped group.

SAM changes the user’s status at Salesforce from Active to Not Active, and the user is no longer able to use single sign-on to access Salesforce.

7 You add the user back into the mapped group.

SAM polls the user store again, and sees that the user account is again a member of the mapped group.

SAM changes the user’s status at Salesforce from Not Active back to Active, and the user is again able to use single sign-on to access Salesforce. No modifications to the user’s account settings occurred.

8 In your Active Directory user store, you move the user account out of the configured search context, (but the user is still a member of the mapped group).

SAM polls the user store again, and sees that the user account is no longer in the search context.

The user’s status at Salesforce changes from Active to Not Active, and the user is not able to single sign-on to Salesforce. (Actually, the user cannot log in to Access Manager either, since the user is out of the search context.)

9 In your Active Directory user store, you move the user account back into the configured search context.

SAM polls the user store again, and sees that the user account is again in the search context (and still in the mapped group).

The user’s status at Salesforce changes from Not Active to Active, and the user is able to single sign-on to Salesforce again.
Locating the SaaS Account Management Connectors

The SAM account provisioning connectors are located in the public connector catalog, along with the SAML and WSFed connectors, at https://catalog.netiq.com.

There are a couple of ways to browse and search for SAML/Account Management connectors in the public catalog. You can access the catalog directly using a web browser, and then click the Account Management tab. Or, if you open the catalog from the Applications page in the Access Manager administration console, click the filter icon to the right of the Search field and then click Account Management.

**NOTE:** If you access the public catalog directly through a browser and are browsing all connectors, you can also easily identify the SAML/Account Management connectors by the graphic ( GitHub ) that indicates they are capable of account management in addition to federated authentication.
Installing SaaS Account Management

Before you install SaaS Account Management, read the following sections to ensure that your environment meets the product requirements. In addition to prerequisites for installing the SAM appliance, your user store must meet certain requirements before you can provision users to SaaS providers. For more information, see "Minimum User Store Requirements" on page 17.

Product Requirements

SaaS Account Management is an add-on solution for NetIQ Access Manager. You must have Access Manager 4.5 SP2 or later installed and configured before you can deploy SaaS Account Management.

To be able to register for appliance updates, get appliance updates, provision SaaS accounts, and so forth, an outbound network connection is also required.

The SAM appliance opens all the ports it needs. You do not need to open or configure any additional ports. The following ports are open by default:

- 8443 and 8444 - For inbound connections from Access Manager
- 9443 - To manage the appliance using the appliance management console

If you enable SSH using the appliance management console, port 22 will also open on the appliance.

Your virtual environment must meet the following requirements before you deploy the appliance:

- One of the following supported virtual environments:
  - VMware vSphere and vSphere Hypervisor 6.0
  - VMware vSphere and vSphere Hypervisor 5.5
- The following minimum hardware:
  - 20 GB disk space
  - 2 vCPUs
  - 4 GB RAM

The appliance can be a heavy consumer of CPU, disk I/O, and network bandwidth. Performance can be adversely affected by other virtual machines with similar operational requirements deployed on the same host server.

As a best practice, ensure that you group or separate virtual machines on hosts and data stores to avoid resource conflicts for CPU, disk I/O, and network bandwidth. You can do this manually as you deploy virtual machines, or use affinity and anti-affinity rules if they are available in your virtual environment.
Deploying SaaS Account Management

The SaaS Account Management appliance is tightly integrated with NetIQ Access Manager, but installation and configuration of the appliance are essentially separate. All of the needed configuration for provisioning user accounts to SaaS providers is stored in Access Manager. When the SAM appliance starts up, it communicates with Access Manager and obtains information about all of the applications that have been configured for provisioning. The installation process sets up networking, the root password, and the time server. Access Manager provides all of the other configuration information.

After installation has completed, you must register the appliance with Access Manager. For more information, see “Enabling Account Management” on page 28. You can also set up Syslog remote logging after installation. For more information, see “Configuring Remote Logging” on page 35.

Obtaining SaaS Account Management

You must have purchased SaaS Account Management to access the product in the Customer Center. The activation code is in the Customer Center where you download the software. For more information, see Customer Center Frequently Asked Questions.

To access a full version of SaaS Account Management:

1. Log in to the Customer Center.
2. Click Software.
3. On the Entitled Software tab, click the appropriate version of SaaS Account Management for your environment to download the product.

Deploying the Appliance

The SAM appliance is an Open Virtualization Format (OVF) virtual appliance. You must deploy the appliance to your VMware server.

The appliance must either obtain an IP address through DHCP or have an assigned static IP address. A single *.ovf file is available for the SAM appliance, and the first-boot sequence prompts you to select from DHCP or a static IP address.

To deploy the appliance in a VMware environment:

1. Download the zipped OVF file from the NetIQ Downloads web page (https://dl.netiq.com/).
2. Extract or unzip the VMware image to access the OVF file.
3. Deploy the OVF into your VMware environment and power on the VM.
   1. (Conditional) If you have a DHCP server in your environment, deploy the OVF file to a specific ESXi host. For more information, see the VMware documentation.
   2. (Conditional) If you do not have a DHCP server in your environment, deploy the OVF file to a VMware vCenter Server.
4. Follow the on-screen prompts to provide the initial configuration settings for the appliance. These settings include passwords, NTP, and network settings (including whether to use DHCP or a static IP address).
   The initial boot process could take between five and twenty minutes to complete.
After the first boot process completes, the appliance console displays a screen with Help information, including the URL to access the appliance management console.

5 Using a browser and the provided URL, log in to the appliance management console and click Account Management to register the SAM appliance and pair it with your Access Manager installation. For more information, see “Enabling Account Management” on page 28.

**IMPORTANT:** You must register your SAM appliance before you can provision users. Access Manager does not display any Account Management features until you have registered your SAM appliance.

Once the registration process has completed, the appliance retrieves any application configuration details. You can then configure SAML2/Account Management applications that are capable of provisioning user accounts to supported SaaS providers.
To use SaaS Account Management to provision users to SaaS providers, you must:

- Have the appropriate accounts for the SaaS applications.
- Ensure that certain minimum attributes are populated in your user store. For more information, see “Minimum User Store Requirements” on page 17.
- Configure a SAML/Account Management connector for the SaaS application. For more information, see “Configuring SAML/Account Management Connectors and Provisioning Users” on page 24 and “Mapping Authorizations for Provisioned Users” on page 26.

Understanding SAM Provisioning and Authorizations

Before you configure SAML/Account Management connectors and begin provisioning users to SaaS applications, read the following sections to ensure that you understand SAM provisioning behavior:

- “Minimum User Store Requirements” on page 17
- “Understanding Attribute Account Matching” on page 18
- “Preventing Accidental Account Claiming at SaaS Providers” on page 20
- “Configuring Successful Single Sign-On to Google” on page 21
- “Understanding Local Login Behavior When Enabling SAM” on page 22
- “Understanding Authorizations” on page 23
- “Understanding Google Apps Authorization Mappings” on page 23

Minimum User Store Requirements

SaaS Account Management supports provisioning of users from the LDAP user stores that you have implemented in your Access Manager environment. To provision users using SAM connectors, certain minimum attributes must be populated in your user store.

<table>
<thead>
<tr>
<th>User Store</th>
<th>Attributes</th>
</tr>
</thead>
</table>
| eDirectory | - First name and last name (a GUID attribute is automatically created and populated)  
- For SAM to take any action on users, the mail attribute must also be populated with an email address |
Once the mail attribute is populated in the user store, if the user is in the search context configured for the Access Manager user store, the Psearch service in SAM starts processing the user. If the user is also a member of one or more mapped groups, SAM provisions the user to the SaaS application.

**Understanding Attribute Account Matching**

For all of the SAML/Account Management connectors, the user store email attribute is the preferred naming value when searching for and creating new accounts in the target SaaS systems. In some cases, the SAM provisioning process does not find the existing user SaaS account based on email address when doing a GET call to see if the account already exists in the target system. If the GET call returns a “Not Found” error, the SAM process then issues a POST request and tries to create a new account in the target SaaS system.

In some cases, even though the GET request returned a “Not Found” error, the POST process, because of connector API logic, may match on the existing user account based on another attribute (such as immutableID in Office 365 or UserName in ServiceNow). In these cases, it is possible that the SaaS account login name may change to match the POSTed email address from the SAM provisioning service. If this happens, you must inform your end users that their loginName (UserName) in the target SaaS system has changed to match their email address in your LDAP user store.

The following tables explain how attribute account matching works for each of the SAML2/Account Management applications.

### Table 3-2  Box

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (case-insensitive)</td>
<td>Email</td>
</tr>
</tbody>
</table>

If SAM detects a matching user, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in Box. After SAM claims and synchronizes the account, the Box user’s username remains the same.
Table 3-3  Dropbox

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (case-insensitive)</td>
<td>Email</td>
</tr>
</tbody>
</table>

If SAM detects a matching user, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in Dropbox.

Table 3-4  Docusign

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (case-insensitive)</td>
<td>Email</td>
</tr>
</tbody>
</table>

If SAM detects a matching user, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in Docusign.

Table 3-5  Google Apps

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (name part only, case-insensitive)</td>
<td>Email</td>
</tr>
</tbody>
</table>

If SAM detects a matching user, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in Google.

Table 3-6  LogMeIn Apps

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (case-insensitive)</td>
<td>Email</td>
</tr>
</tbody>
</table>

If SAM detects a matching user, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in LogMeIn.

Table 3-7  Office 365

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test 1: Email (name part only, case-sensitive)</td>
<td>UserPrincipalName (name part only)</td>
</tr>
<tr>
<td>Test 2: Email (name part only, case-insensitive)</td>
<td>UserPrincipalName (name part only)</td>
</tr>
<tr>
<td>Test 3: GUID</td>
<td>ImmutableId</td>
</tr>
</tbody>
</table>

If SAM detects a matching user with any of the three tests, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in Office 365. After SAM claims and synchronizes the account, the Office 365 user’s UniversalPrincipalName is \(<\text{ldapEmailNamePart}>@<\text{o365DomainName}>\).
Preventing Accidental Account Claiming at SaaS Providers

For each SAML2/Account Management application, SAM attempts to match *qualified users* from the Access Manager LDAP user stores to existing user accounts, if any, at the respective SaaS provider. To determine whether an Access Manager user is the same user as or a different user than an existing SaaS user, SAM compares one or more attributes between the LDAP and SaaS user. If SAM finds a match, SAM **claims** and manages the account at the SaaS provider. If SAM does not find a match, SAM provisions a new user account at the SaaS provider.

---

### Table 3-8  Salesforce

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test 1: Email (name part only, case-insensitive)</td>
<td>Email</td>
</tr>
<tr>
<td>Test 2: Email (name part only, case-insensitive)</td>
<td>Username</td>
</tr>
</tbody>
</table>

If SAM detects a matching user with either test, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in Salesforce. After SAM claims the account, the Salesforce user’s Email and Username are the value of the user’s LDAP email.

### Table 3-9  ServiceNow

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test 1: Email (name part only, case-insensitive)</td>
<td>Email</td>
</tr>
<tr>
<td>Test 2: Email (name part only, case-insensitive)</td>
<td>User ID</td>
</tr>
</tbody>
</table>

If SAM detects a matching user with either test, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in ServiceNow. After SAM claims and synchronizes the account, the ServiceNow user’s Email and User ID are the value of the user’s LDAP email.

### Table 3-10  Tableau

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (case-insensitive)</td>
<td>Email</td>
</tr>
</tbody>
</table>

If SAM detects a matching user, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in Tableau.

### Table 3-11  Zendesk

<table>
<thead>
<tr>
<th>LDAP user attribute used for matching</th>
<th>SaaS user attribute tested for match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email (case-insensitive)</td>
<td>Email</td>
</tr>
</tbody>
</table>

If SAM detects a matching user, SAM “claims” the user account and synchronizes a subset of attributes from the LDAP user store to the user account in Zendesk.
WARNING: To prevent unwanted account claiming, you must ensure that the values for the user’s email address are unique across all user stores for all active, disabled, and deleted users, and must not match existing SaaS user accounts except when those users are the same user.

*Qualified users* are those who:

1. Reside within the search contexts of the eDirectory or Active Directory user stores configured in Access Manager.
2. Have at least the following attributes populated: firstname, lastname, and email address.
3. Are members of one or more groups that are mapped in the SAML2/Account Management applications.

**Claiming** a user account means that the Access Manager user with the matching account is able to log in to that account and sees the expected content of the existing SaaS user. For example, if the SaaS application is an email service, the matching Access Manager user sees whatever email exists for that user in the SaaS when the account is claimed. SAM then synchronizes certain user attributes from the Access Manager user store to the SaaS user account.

## Configuring Successful Single Sign-On to Google

When SAM provisions users to Google, SAM creates the login name at Google from the name part of the LDAP user’s mail attribute prepended to the Google domain name. For example, if the LDAP user’s mail attribute is jdoe@novell.com and the Google domain is mygoogledomain.info, the resulting user account at Google would be jdoe@mygoogledomain.info. For SAML single sign-on between Access Manager and Google to be successful for this user, the value of NameID in the assertion must be jdoe. You must perform this “mapping” of a local attribute into the SAML assertion using the Access Manager administration console.

In the Access Manager administration console, go to Applications > Google > Attributes. From the Mapped to System Attribute list, select an attribute that contains the same value as the username portion of the user’s email address. Often, the LDAP attributes cn, uid, or LDAP User Name [Credential Profile] are populated with this value. If so, you can choose any of these attributes from the list. In cases where the user objects do not have an attribute with the same value as the username part of the email address, you can create a virtual attribute that extracts the username from the mail attribute. For example, you could create a virtual attribute similar to the following:

**Name:** extractName

**Input parameters:**

- **Name:** P1
- **Parameter value:** mail

**Modification function:**

- **Function:** Regex Replace
- **Regex:** /@(.*)$/
- **Replace with:** <empty>
After you create the virtual attribute, that attribute will be available for selection in the Mapped to System Attribute list of the Google application. For more information about virtual attributes, see the NetIQ Access Manager 4.5 Administration Guide (https://www.netiq.com/documentation/access-manager-45/admin/data/bookinfo.html).

Understanding Local Login Behavior When Enabling SAM

Before you use SaaS Account Management to provision users, it is important to understand how SAM interacts with SaaS providers and how user logins change for existing SAML accounts. For the purposes of this section, ServiceNow is the SaaS provider.

1. After configuring Account Management, you add a user into the mapped group in the LDAP user store, and Psearchservice recognizes that the account is now “in scope” for provisioning.
2. Psearchservice uses the LDAP email address to try to match the account in ServiceNow, first checking the user name in ServiceNow, then the email in ServiceNow.
3. If Psearchservice finds a match on either attribute in ServiceNow, Psearchservice claims the account, sends a PATCH, and sets the ServiceNow SaaS account’s user name and email to the LDAP user store email value.
4. If Psearchservice does not find a match, Psearchservice sends a POST, and SAM creates a new account in ServiceNow.

ServiceNow Example 1

You have manually created accounts in ServiceNow, and users are logging in with their user names and passwords, referred to as local login. You then decide to use Access Manager and SAM for account management. For the purposes of this example, the user’s email and user name are the same in the LDAP user store and in the SaaS system.

Psearchservice performs its standard workflow and claims the account. In doing so, SAM updates the password in ServiceNow, and local logins no longer work.

IMPORTANT: Once you enable SAM for Account Management, all users log in using SAML, and local logins using user name and password are no longer valid.

ServiceNow Example 2

The user is using a local login in ServiceNow. His ServiceNow user name is bob@servicenow.com and his ServiceNow email is robert@servicenow.com (which is acceptable in ServiceNow). His LDAP user store email is robert@servicenow.com.

You then decide to use Access Manager and SAM for account management, and put the user "in scope" for account management. Psearchservice performs its standard workflow and claims the account.

Once Psearchservice has claimed the account, the PATCH from SAM sets both the ServiceNow user name and ServiceNow email to robert@servicenow.com. This means that the ServiceNow user name has changed to the same value as the email address.

As in Example 1, local logins no longer work, because both the password and ServiceNow user name have changed. Federated SAML2 authentication does work.
Understanding Authorizations

Most companies define their business policies through authorization assignments. When you configure SAML2/Account Management applications, SaaS Account Management allows you to map groups in your Access Manager user stores to specific authorizations in the SaaS applications. You can map authorizations for all SAML2/Account Management applications that provision users, such as Office 365, Google Apps, Salesforce, and ServiceNow.

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 basic accounts.

Each user store can contain different groups that appear on the LDAP Groups and Authorizations page in Access Manager. Active Directory user stores can contain groups, local groups, and global groups. eDirectory user stores can contain groups.

**NOTE:** SAM supports mapping authorizations to LDAP user groups, but not to Access Manager roles. Certain SaaS applications might include authorizations for roles, but these are not the same thing as roles in Access Manager.

Each SAML2/Account Management application contains different authorizations that appear on the LDAP Groups and Authorizations page in Access Manager. For example, Office 365 has account, group, and license authorizations.

If a user is a member of multiple selected groups, the authorizations are cumulative. If you map any authorization to a user store group and later remove that authorization, members of that user store group lose that authorization, unless they are also members of another user store group that still has that authorization mapping.

**IMPORTANT:** Use caution when mapping authorizations. 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. For example, Google allows a user to exist in only one Organizational Unit or User Placement, but you can map multiple user placements to the same LDAP group or to several LDAP groups where the same user might be a member.

We assume that you are familiar with and understand the authorizations available for each SaaS application to which you are provisioning users. 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.

For additional information about authorization mapping behavior that is specific to Google Apps, see “Understanding Google Apps Authorization Mappings” on page 23.

Understanding Google Apps Authorization Mappings

Mapped placement of newly provisioned users to a sub-organization overrides the default placement in the top-level organization.
IMPORTANT: Pay careful attention when mapping User Placement authorization values to user store groups to ensure that you place users in the intended Google Apps organizations. Google Apps allows each user to be placed in only one organization at a time. If you grant a User Placement authorization to a user, and then grant another User Placement authorization to the same user, the first value is overwritten when the user is moved in the Google Apps organizational unit structure.

In addition, if you revoke a User Placement authorization for a user, even if that user has multiple User Placement authorizations, that user is moved to the default organization specified in the Google Apps connector configuration. (Because Google Apps allows a user to be placed into only one organization at a time, when a User Placement authorization value is overwritten, there is only one value that is removed, which moves the user back to the default placement.) If you want to move that user from the default location back into a new Google Apps sub-organization, you must add the user back to the appropriate user store group and perform authorization mappings again.

If you revoke a User Account authorization for a user after the user has been provisioned into Google Apps and one or more User Placement authorizations have been granted to the user, that user is placed in suspended mode in Google Apps. No placement activity takes place as long as the user account is suspended; the user simply remains in the Google Apps organization that the user was in before the suspension. When you re-grant the User Account authorization, the account is moved to the “active user” state. If you performed a User Placement authorization change while the user account was suspended, the user is moved to the appropriate organization after the account is reactivated.

Configuring SAML/Account Management Connectors and Provisioning Users

The following procedure provides the steps required to configure a SAML/Account Management connector and provision basic user accounts to the SaaS application.

Before you begin provisioning users, ensure that your environment meets the requirements for provisioning to the desired SaaS applications and that you understand how provisioning works in SaaS Account Management.

IMPORTANT: If you already have a SAML application configured in your Access Manager environment that was created from a SAML connector and you want to take advantage of the additional account management benefits that SAM offers for the same SAML application, you must delete the existing application, then import the new SAML/Account Management connector and configure the application settings again.

To configure a new SAML/Account Management connector:

1. In the Access Manager administration console, access the Applications page and click the plus (+) sign next to the heading.
2. Click Add Application from Catalog.
3. On the Application Connector Catalog page, locate and select the SAML/Account Management connector that you want to configure. You can quickly locate Account Management connectors using the Account Management filter.
4. (Optional) Review the name and description of the application.
For information about using appmarks associated with applications, see the Access Manager documentation.

5 Review and configure the other sections, such as Application Connector Setup, Attributes, Access and Roles, and System Setup, for the SAML2 application. For more information, click the Help icon or refer to the Applications Configuration Guide on the Access Manager documentation website (https://www.netiq.com/documentation/access-manager/).

6 Click the arrow to expand the Account Management section, then select the Enable Account Management check box.

**NOTE:** Access Manager displays the Account Management section only after you have registered your SAM appliance. For more information, see “Enabling Account Management” on page 28.

7 Click Setup Instructions and follow the help for configuring the service account and completing other steps at the SaaS application site. The setup instructions open in a separate window so you can continue working.

8 Configure appropriate values for all required settings in the Account Management section. This information varies depending on the SaaS application type. You can click Validate Settings to verify that the values you have specified can be used successfully by SAM to authenticate to your SaaS account.

9 Under LDAP User Store Configuration, provide the required user store information:

   9a Click the plus (+) icon and select the user store that you want SAM to use for provisioning users to the SaaS application.

   9b Specify a polling interval to indicate how often you want SAM to check your LDAP user store for changes to user accounts.

   9c Repeat this step if you want to add another user store.

10 Click the Configure Groups and Authorizations icon.

11 In the LDAP Groups and Authorizations window, select the LDAP user groups you want to provision, then click Save. The LDAP Groups and Authorizations window closes.

**NOTE:** For provisioning to occur, you must map at least one LDAP group. For authorizations to be assigned, you must map them to the LDAP groups you have selected. If you do not specifically map SaaS authorizations, SAM provisions users, but they get only basic accounts. For more information about assigning authorizations, see “Mapping Authorizations for Provisioned Users” on page 26.

12 On the Account Management page, click Save.

When you click Save, SaaS Account Management begins processing and provisioning to the SaaS applications the LDAP users who are members of the mapped groups and who have the required firstname, lastname, and email attributes. Depending on the number of users and groups in your user stores, this operation may take some time.
Mapping Authorizations for Provisioned Users

Most companies define their business policies through authorization assignments. When you configure SAML2/Account Management applications, SaaS Account Management allows you to map groups in your Access Manager user stores to specific authorizations in the SaaS applications.

If you configure SAML/Account Management connectors and provision users based only on mapped groups in specified LDAP user stores, but do not assign SaaS authorizations, the provisioned users get only basic user accounts without specific licenses, groups, roles, etc. For SaaS-specific authorizations to be assigned, you must map them to the LDAP groups you have selected.

Before you map authorizations, ensure that you understand the available authorizations for the SaaS application, and plan the mappings that are appropriate for your LDAP users. For more information about how authorizations work, see “Understanding Authorizations” on page 23 and “Understanding Google Apps Authorization Mappings” on page 23.

IMPORTANT: Use caution when mapping authorizations. 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.

To map authorizations:

1. On the LDAP Groups and Authorizations page, in the LDAP Groups column, click +, then select at least one LDAP group from the list.

2. In the Authorizations column, select one or more authorizations, then click the blue arrow to map the authorizations to the LDAP groups.
   You can use the filter fields to perform simple searches for LDAP groups or authorizations. For example, to filter for jhgroup1 of an authorization, if you enter JH or jh or gro, the filter finds jhgroup1. Wildcards and regular expressions are not currently supported in these fields.

3. Click Save, then click Save again on the Account Management page.

You can unmap authorizations individually by clicking X next to the authorization in the group. You can also unmap an entire group by selecting the group and then clicking the trashcan icon.
You deploy SaaS Account Management as an appliance. You use the appliance management console to register or unregister the appliance with Access Manager and to maintain certain configuration settings for the appliance, such as administrative passwords for the vaadmin user and the root user, network settings, and certificate settings. You should perform these tasks only from the appliance management console because native Linux tools are not aware of the configuration requirements and dependencies of SaaS Account Management.

**IMPORTANT:** NetIQ delivers and updates the SaaS Account Management appliance as a single unit including the operating system, the SaaS Account Management application, and associated runtime components. NetIQ does not recommend adding any additional software components to the appliance. Any support issues that arise with customer supplied components might require removal before support issues can be resolved.

To access the appliance management console, see “Accessing the Appliance Management Console” on page 28. Use the following information to manage the appliance.

- Accessing the Appliance Management Console
- Enabling Account Management
- Setting Administrative Passwords
- Configuring Network Settings
- Adding Additional Hosts to the Hosts File
- Configuring Time Settings
- Accessing System Services
- Managing Appliance Certificates
- Viewing Firewall Settings
- Configuring Remote Logging
- Viewing Appliance Health
- Troubleshooting the Appliance
- Sending Information to Support
- Adding a Field Patch to the Appliance
- Performing an Online Update
- Performing a Product Upgrade
- Restarting or Shutting Down the Appliance
- Removing a SAM Appliance
- Logging Out
Accessing the Appliance Management Console

SaaS Account Management contains an appliance management console that allows you to configure network settings, apply field patches, apply updates, and perform many more tasks.

To access the appliance management console:

1. In a web browser, specify the DNS name or the IP address for the appliance with the port number 9443. For example:
   https://10.10.10.1:9443
   or
   https://mycompany.example.com:9443

2. Specify the administrative user name and password for the appliance, then click Sign in. The default users are vaadmin and root.

Enabling Account Management

After you deploy the SaaS Account Management appliance, you must provide some information in the appliance management console to register the SAM appliance with a specific Access Manager setup and administration console. The SAM appliance cannot be registered with more than one instance of Access Manager at a time.

1. Log in to the appliance management console as the vaadmin user.
   https://mycompany.example.com:9443

2. Under Service Configuration, click SaaS Account Management.

3. Select the Access Manager check box.

4. Provide the URL for the Access Manager administration console.
   https://admin_console_host:port

5. Provide the user name and password for the administrator account that you use to log in to the Access Manager administration console.

6. Click Register.

When you click Register, the appliance communicates with Access Manager to register the appliance with Access Manager and enable the Account Management features for the SAML/Account Management connectors in the Access Manager administration console.

NOTE: If you need to unregister the appliance from Access Manager, deselect the Access Manager check box, then click Unregister.
Setting Administrative Passwords

Use the Administrative Passwords page to modify the passwords and SSH access permissions for the appliance administrators: the vaadmin user and the root user. You might need to modify passwords periodically in keeping with your password policy, or if you reassign responsibility for the appliance administration to another person.

**IMPORTANT:** Ensure that you make a note of your root password, because you cannot reset it. If you forget the root password, the only option is to delete the appliance from your virtual network and redeploy a new appliance.

The vaadmin user can use the Administrative Passwords page to perform the following task:

- Modify the vaadmin user password. To change a password, you must be able to provide the old password.
- The vaadmin user automatically has permissions necessary to remotely access the appliance with SSH instead of using a VMware client. The SSH service must be enabled and running to allow SSH access.

**NOTE:** By default, the SSH service is disabled and is not running. For information about how to start SSH on the appliance, see “Accessing System Services” on page 31.

The root user can use the Administrative Passwords page to perform the following tasks:

- Modify the root user password. To change a password, you must be able to provide the old password.
- Enable or disable the root user SSH access to the appliance.
  
  When this option is enabled, the root user is able to SSH to the appliance. If this option is disabled, only the vaadmin user can SSH to the appliance, and the root user cannot SSH to the appliance even if the sshd service is running.

To manage administrative access as the vaadmin user:

1. Log in to the appliance management console as the vaadmin user.
   
   https://mycompany.example.com:9443
2. Click Administrative Passwords.
3. Specify a new password for the vaadmin administrator. You must also specify the current vaadmin password.
4. Click OK.

To manage administrative access as the root user:

1. Log in to the appliance management console as the root user.
   
   https://mycompany.example.com:9443
2. Click Administrative Passwords.
3. Specify a new password for the root administrator. You must also specify the current root password.
4 (Optional) Select or deselect Allow root access to SSH.
5 Click OK.

**NOTE:** The root user can also reset the vaadmin password to a new value. The root user does not need to know the vaadmin current password.

### Configuring Network Settings

Use the Network page to configure settings for the DNS servers, search domains, gateway, and NICs for the appliance. You might need to modify these settings after the initial setup if you move the appliance VM to a new host server, or move the host server to a new domain in your network environment. You can also optionally restrict the networks that are allowed to access the appliance.

**To configure network settings for the appliance:**

1 Log in to the appliance management console as the vaadmin user.
   
   https://mycompany.example.com:9443

2 Click Network.

3 In the DNS Configuration section, you can modify the DNS name servers, search domains, and gateway settings for your appliance network.
   
   If the Search Domains field is left blank, it is auto-populated with the domain of the appliance hostname. For example, if the hostname of the appliance is ptm.mycompany.com, the domain is auto-populated with mycompany.com.

4 In the NIC Configuration section, you can modify the IP address, hostname, and network mask of any NIC associated with the appliance.
   
   4a Click the ID of the NIC.
   
   4b Edit the IP address, hostname, or network mask for the selected NIC.
   
   4c Click OK.
   
   4d Repeat these steps for each NIC that you want to configure.

5 (Optional) In the Appliance Administration UI (port 9443) Access Restrictions section, do one of the following:
   
   • Specify the IP address of each network for which you want to allow access to the appliance. Only the listed networks are allowed.
   
   • Leave this section blank to allow any network to access the appliance.

**NOTE:** After you configure the appliance, changes to your appliance network environment can impact the appliance communications.

6 Click OK.

7 Click Reboot in the top right corner of the appliance’s landing page.
Adding Additional Hosts to the Hosts File

You can add additional entries to the hosts file for the SaaS Account Management appliance. You must add the entry to the /etc/opt/novell/base/hosts.appliance file manually. Attempting to change the host entries through any other means will not work.

1. Log in to the appliance management console as the vaadmin user.
   https://mycompany.example.com:9443
2. Access the command line console of the appliance.
3. Navigate to /etc/opt/novell/base/hosts.appliance.
4. Open the file in a text editor, then add the additional entries to the hosts file.
5. Save and then close the file.
6. Reboot the appliance to have the change take effect.

Configuring Time Settings

Use the Time page to configure the Network Time Protocol (NTP) server, the geographic region, and the time zone where you have deployed the appliance.

To configure time parameters for the appliance:

1. Log in to the appliance management console as the vaadmin user.
   https://mycompany.example.com:9443
2. Click Time.
3. Change the following time configuration options as appropriate:
   - NTP Server: Specify the NTP server that you want to use for time synchronization.
   - Region: Select the geographic region where your appliance is located.
   - Time Zone: Select the time zone where your appliance is located.
4. Click OK.

Accessing System Services

Use the System Services page to view the status of services running on the appliance, or perform any of the following actions:

- Start, stop, or restart system services
- Make system services automatic or manual

System services include the following:

- SSH
- SAM Application (SaaS Account Management)
- PLDAP Application (persistent LDAP search service)
- REDIS Application (internal caching service to improve performance)
**NOTE:** For the SAM appliance to function properly, the SAM, PLDAP, and REDIS applications all need to be running. Do not stop them or set them to manual unless Technical Support instructs you to do so temporarily for the purpose of troubleshooting.

**To access and perform actions on system services:**

1. Log in to the appliance management console as the **vaadmin** user.

   https://mycompany.example.com:9443

2. Click **System Services**.

3. To start, stop, or restart a service on the appliance:
   
   3a. Select the service that you want to start, stop, or restart.
   
   3b. Click **Action**, then select **Start**, **Stop**, or **Restart**.

4. To make system services automatic or manual:
   
   4a. Select the service that you want to make automatic or manual.
   
   4b. Click **Options**, then select either **Set as Automatic** or **Set as Manual**.

5. Click **Close** to exit System Services.

**Managing Appliance Certificates**

Use the Digital Certificates page to add and activate certificates for the appliance. You can use the Digital Certificates page to create your own certificate and then have it signed by a CA, or you can use an existing certificate and key pair if you have one that you want to use.

**NOTE:** This section is primarily for managing certificates for the SaaS Account Management appliance administration console (port 9443). However, the SAM service and the Psearchservice (ports 8443 and 8444) also use the same certificate for the HTTP REST calls.

The appliance ships with a self-signed digital certificate. Instead of using this self-signed certificate, NetIQ recommends that you use a trusted server certificate that is signed by a trusted certificate authority (CA), such as VeriSign or Equifax.

Refer to the following sections to change the appliance certificate for your appliance:

- “Using the Digital Certificates Page” on page 32
- “Using an Existing Certificate and Key Pair” on page 34
- “Activating the Certificate” on page 34

**Using the Digital Certificates Page**

For more information about using the Digital Certificates page, see the following topics:

- “Creating a New Self-Signed Certificate” on page 33
- “Getting Your Certificate Officially Signed” on page 33
Creating a New Self-Signed Certificate

1. Log in to the appliance management console as the vaadmin user.
   
   https://mycompany.example.com:9443

2. Click Digital Certificates.

3. In the Key Store drop-down list, ensure that Web Application Certificates is selected.

4. Click File > New Certificate (Key Pair), then specify the following information:

   4a. General
   
   - **Alias**: Specify a name that you want to use to identify and manage this certificate.
   - **Validity (days)**: Specify how long you want the certificate to remain valid.

   4b. Algorithm Details
   
   - **Key Algorithm**: Select either RSA or DSA.
   - **Key Size**: Select the desired key size.
   - **Signature Algorithm**: Select the desired signature algorithm.

   4c. Owner Information
   
   - **Common Name (CN)**: This must match the server name in the URL in order for browsers to accept the certificate for SSL communication.
   - **Organization (O)**: (Optional) Large organization name. For example, My Company.
   - **Organizational Unit (OU)**: (Optional) Small organization name, such as a department or division. For example, Purchasing.
   - **Two-letter Country Code (C)**: (Optional) Two-letter country code. For example, US.
   - **State or Province (ST)**: (Optional) State or province name. For example, Utah.
   - **City or Locality (L)**: (Optional) City name. For example, Provo.

5. Click OK to create the certificate.

   After the certificate is created, it is self-signed.

6. Make the certificate official. For more information, see “Getting Your Certificate Officially Signed” on page 33.

Getting Your Certificate Officially Signed

1. On the Digital Certificates page, select the certificate that you just created, then click File > Certificate Requests > Generate CSR.

2. Complete the process of emailing your digital certificate to a certificate authority (CA), such as Verisign.

   The CA takes your Certificate Signing Request (CSR) and generates an official certificate based on the information in the CSR. The CA then emails the new certificate and certificate chain back to you.
Managing the SAM Appliance

3 After you have received the official certificate and certificate chain from the CA:
   3a Revisit the Digital Certificates page.
   3b Click File > Import > Trusted Certificate. Browse to the trusted certificate chain that you received from the CA, then click OK.
   3c Select the self-signed certificate, then click File > Certification Request > Import CA Reply.
   3d Browse to and upload the official certificate to be used to update the certificate information.
      On the Digital Certificates page, the name in the Issuer column for your certificate changes to the name of the CA that stamped your certificate.
4 Activate the certificate. For more information, see “Activating the Certificate” on page 34.

Using an Existing Certificate and Key Pair

When you use an existing certificate and key pair, use a .P12 key pair format.

1 Log in to the appliance management console as the vaadmin user.
   https://mycompany.example.com:9443
2 Click Digital Certificates.
3 In the Key Store drop-down menu, select JVM Certificates.
4 Click File > Import > Trusted Certificate. Browse to and select your existing certificate, then click OK.
5 Click File > Import > Trusted Certificate. Browse to and select your existing certificate chain for the certificate that you selected in Step 4, then click OK.
6 In the Key Store drop-down menu, select Web Application Certificates.
7 Click File > Import > Key Pair. Browse to and select your .P12 key pair file, specify your password if needed, then click OK.
8 Continue with “Activating the Certificate” on page 34.

Activating the Certificate

1 On the Digital Certificates page, in the Key Store drop-down menu, select Web Application Certificates.
2 Select the certificate that you want to make active, click Set as Active, then click Yes.
3 Verify that the certificate and the certificate chain were created correctly by selecting the certificate and clicking View Info.
4 When you successfully activate the certificate, click Close to exit Digital Certificates.

Viewing Firewall Settings

Use the Firewall page to view your current firewall configuration directly from the appliance. By default, all ports are blocked except those needed by the appliance. For example, the Login page for the appliance management console uses port 9443, so this port is open by default. The SAM
appliance uses port 8443 for both inbound and outbound communication, and Psearchservice uses port 8444, so those ports are also open. To have a seamless experience with the appliance, ensure that you do not block the ports with your firewall settings.

**To view firewall settings for the appliance:**

1. Log in to the appliance management console as the `vaadmin` user.

   https://mycompany.example.com:9443

2. Click **Firewall**.

   The Firewall page lists port numbers with the current status of each port number. The page is for informational purposes and is not editable.

3. Click **Close** to exit the Firewall page.

---

### Configuring Remote Logging

Use the Remote Logging page to configure logging to a remote Syslog server. Your Syslog server must be configured before you can enable remote logging in Access Manager.

**To configure remote logging:**

1. Log in to the appliance management console as the `vaadmin` user.

   https://mycompany.example.com:9443

2. Click **Remote Logging**.

3. In the **Syslog host** field, specify the IP address or DNS name of your configured Syslog server.

4. In the **Syslog port** field, specify the port that your Syslog server listens on.

   By default, Syslog uses port 514 if you select the UDP protocol, and port 601 if you select the TCP protocol. However, the port is configurable, so check with your Syslog server administrator if you are unsure which port to use.

5. (Conditional) Change the **Syslog protocol** as needed for your environment.

   **NOTE:** SaaS Account Management does not currently support encrypted remote Syslog.

6. Click **Enable**.

   When you click **Enable**, the appliance is configured to send log messages to the Syslog server. To change to a different Syslog server, follow the same steps but enter the new information. When you click **Update**, the previous Syslog configuration on the appliance is replaced with the new values.

   **NOTE:** To disable remote logging on the appliance, click **Disable**.
Viewing Appliance Health

Use the Health page to view the status of some appliance components. The page is for informational purposes only and is not editable.

**NOTE:** Appliance health information - whether the health status icon on the appliance landing page or the more detailed information on the Health page itself - is current when the page first loads but does not update itself dynamically after that. To refresh the health icon you can reload the landing page. To refresh the detailed health information on the Health page itself, use the Refresh button.

To view health for the appliance:

1. Log in to the appliance management console as the vaadmin user.

   ![https://mycompany.example.com:9443](https://mycompany.example.com:9443)

   The icon that takes you to the Health page shows an overall health status of the tested components. The health status on the icon is updated every time the page is loaded or refreshed.

2. Click Health to load the Health page and see details about the health of several individual appliance components.

   Whenever you open the Health page, it refreshes the health status so the information is current. You can click Refresh to re-fetch the current health of the components.

3. Click Close to exit the Health page.

Troubleshooting the Appliance

If you are having issues with your SAM appliance, use the following table as a starting point for troubleshooting. For additional help from NetIQ Technical Support, see “Sending Information to Support” on page 37.

<table>
<thead>
<tr>
<th>For the following issues ...</th>
<th>NetIQ recommends ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>I cannot register my SAM appliance with my Access Manager server.</td>
<td>If you are registering by fully qualified domain name, check the network settings on the SAM appliance to ensure that it can resolve the host name of the Access Manager administration console system.</td>
</tr>
<tr>
<td>My Access Manager application configuration keeps failing to save Account Management information. It returns an error when saving.</td>
<td>Verify that the Access Manager system has network connectivity to the SAM appliance by IP address.</td>
</tr>
<tr>
<td>When I make changes to my Access Manager user stores, the SAM appliance does not take any action.</td>
<td>Verify that the SAM appliance has LDAP network access to the configured Access Manager user stores.</td>
</tr>
</tbody>
</table>
## Sending Information to Support

Use the Support page to send configuration information to Technical Support ([https://www.netiq.com/support/](https://www.netiq.com/support/)) by uploading files directly to FTP, or by downloading the files to your management workstation and sending them by an alternative method.

### To send configuration files to Technical Support:

1. Log in to the appliance management console as the `vaadmin` user.
   
   `https://mycompany.example.com:9443`

2. Click **Support**.

3. Use one of the following methods to send the appliance's configuration files to Technical Support ([https://www.netiq.com/support/](https://www.netiq.com/support/)):
   - Select **Automatically send the configuration to Micro Focus using FTP** to initiate the FTP transfer of configuration information.
   - Select **Download and save the configuration file locally, then send it to Micro Focus manually** to download configuration information to your management workstation. You can then send the information to Technical Support ([https://www.netiq.com/support/](https://www.netiq.com/support/)) using a method of your choice.

4. Click **OK** to complete the process.

### For the following issues ...

<table>
<thead>
<tr>
<th>Issue Description</th>
<th>NetIQ recommends ...</th>
</tr>
</thead>
<tbody>
<tr>
<td>I have uploaded a new certificate, but my appliance management console still shows the older certificate.</td>
<td>Reboot the appliance to apply the new certificate.</td>
</tr>
<tr>
<td>I am unable to SSH into the SAM appliance.</td>
<td>SSH is disabled by default. Log into the appliance management console, click the <strong>System Services</strong> icon, and start SSH. (You can also enable automatic start if appropriate for your environment.)</td>
</tr>
<tr>
<td>My SAM appliance fails to register for online updates.</td>
<td>Verify that the SAM appliance has network connectivity and a valid license key.</td>
</tr>
<tr>
<td>I have updated my system, but not all of the services have restarted.</td>
<td>Reboot the appliance. (NetIQ always recommends rebooting after an online update or network change.)</td>
</tr>
<tr>
<td>I have Account Management configured, but when I put my user in the appropriate group, SAM does not provision the account.</td>
<td>Verify that the user object has an email address in the source user store. SAM requires the email address attribute to be populated for all users that you want to provision.</td>
</tr>
<tr>
<td>SAM is not provisioning users to Salesforce.</td>
<td>Verify that users in the LDAP user stores have email addresses that are unique across all Salesforce domains.</td>
</tr>
</tbody>
</table>

---

Managing the SAM Appliance 37
Adding a Field Patch to the Appliance

Use the Field Patch option to add patches provided by engineering or support. A field patch is not a full patch and should be used only until a full patch is released. When you apply a field patch, you must disable all other updates for the appliance, otherwise the field patch can be overwritten.

To manage field patches:

1. Log in to the appliance management console as the vaadmin user.

   https://mycompany.example.com:9443

2. Click Field Patch.

3. Click Browse and browse to and select the field patch file you received from engineering or technical support, then click Open.

4. Click Install and follow the prompts to install the patch.

5. (Conditional) If you need to uninstall the patch update, select the patch you want to uninstall, then click Uninstall Latest Patch and follow the prompts.

6. Download a log file that includes details about the patch update installation by clicking Download Log File for the appropriate patch update.

7. Click Close to exit the Field Test Patch page.

8. To disable online updates and automatic updates until you apply a full patch, click Online Updates, then click Schedule > Manual, then exit out of the Field Patch page.

Performing an Online Update

Use the Online Update option to register for the online update service from the Customer Center (https://www.netiq.com/customercenter). You can install updates automatically or manually to update the SaaS Account Management appliance.

You must have the license key for SaaS Account Management to activate the Update Channel. You obtain the license key from the Customer Center. If the key is not available, contact the Customer Center through an email from within the Customer Center (https://www.netiq.com/customercenter).

To register for the Online Update Service:

1. Log in to the appliance management console as the vaadmin user.

   https://mycompany.example.com:9443

2. Click Online Update.

3. If the Registration window does not open automatically, click the Register tab.

4. For the Service Type, specify Customer Center.

5. Specify the following information about the Customer Center (https://www.netiq.com/customercenter) account for this SaaS Account Management appliance:

   - Email address of the account in the Customer Center
   - Activation key (the same Full License key that you used to activate the product)
• Allow data send (select any of the following):
  • Hardware Profile
  • Optional information

6 Click Register.

   Wait while the appliance registers with the service.

7 Click OK to dismiss the confirmation.

After you have registered the appliance, you can view a list of the needed updates, or view a list of installed updates. You can use manual or automatic options to update the appliance.

To perform other actions after registration:

• **Update Now**: Click Update Now to trigger downloaded updates.
• **Schedule**: Configure the type of updates to download and whether to automatically agree to the licenses.

  **To schedule online updates**:
  1. Click the Schedule tab.
  2. Select a schedule for download updates (*Manual, Daily, Weekly, Monthly*).

• **View Info**: Click View Info to display a list of installed and downloaded software updates.
• **Refresh**: Click Refresh to reload the status of updates on the appliance.

### Performing a Product Upgrade

The difference between a product update and a product upgrade is that the product upgrades contain new features and functionality while a product update contains bug fixes. The upgrades also increase the major or minor version of the product. For example, an upgrade changes the version from 1.0 to 1.1.

SaaS Account Management provides an automated process to upgrade the appliance, but this option is not currently available. It will be available in a future release.

### Restarting or Shutting Down the Appliance

You might need to initiate a graceful shutdown or restart the appliance for maintenance purposes. Using the appliance management console options is preferable to using a Power Off/On option in the VMware management tool.

1 Log in to the appliance management console as the vaadmin user.

  https://mycompany.example.com:9443

2 In the upper right corner of the Appliance Configuration pane, click Reboot or click Shutdown.
Removing a SAM Appliance

To remove a SAM appliance from your Access Manager environment when the appliance is still functional, use the Unregister option in the appliance management console. For more information, see “Enabling Account Management” on page 28.

The Access Manager administration console does not currently provide an option to remove a SAM appliance that is no longer functional. To remove a non-functional SAM appliance from your Access Manager environment, use the DELETE API endpoint with the following syntax:

DELETE https://NAM Admin Console IP or DNS:port/amsvc/v1/accountmgmtconfig

**NOTE:** This API requires a base64-encoded basic authentication header with Access Manager administrator credentials. For example, `cn=admin,o=novell:password`.

Logging Out

For security reasons, you should log out of the appliance management console to exit your session with the appliance, then close your web browser. Your session terminates automatically when you close your web browser.

To log out of the appliance management console:

1. In the upper-right corner of the appliance management console page, next to your user name, click Logout.
2. Close the web browser.