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 Box 7

2 DocuSign 11

3 Dropbox 13

4 Google Apps 15

5 LogMeIn Apps 17

6 Office 365 19

7 Salesforce 21

8 ServiceNow 23
   Table Permissions for Provisioning API ................................................................. 23
   OAuth Authentication for Provisioning API ........................................................... 24
   Creating a New OAuth Application Registry ......................................................... 24
   Finding the Client ID and Client Secret for an Existing Application Registry .......... 24

9 Tableau 27

10 Zendesk 29
About This Book and the Library

The *NetIQ SaaS Account Management Connectors Guide* provides setup instructions for each of the connectors provided by NetIQ SaaS Account Management (SAM).

**Intended Audience**

This guide provides information for administrators implementing provisioning connectors using SaaS Account Management.

**Other Information in the Library**

The library provides the following information resources:

**Installation Guide**

Provides detailed planning, installation, and administration information for the SaaS Account Management appliance.

**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.
Complete the following steps to configure Box to allow user provisioning from Access Manager using SAM.

1 Log in to your Box developer account at https://developer.box.com.

2 On the My Apps page:
   2a Click Create New App, select Enterprise Integration, then click Next.
   2b Select OAuth 2.0 with JWT (Server Authentication), then click Next.

3 Give your app a unique name, then click Create app.

4 Click View Your App and do the following:
   4a Set Application Access to Enterprise.
   4b Verify that Application Scopes includes Manage users and Manage groups.
   4c Click Generate a Public/Private Keypair, then follow the prompts to download the JSON file and securely save it for later use when you configure Access Manager.
      In addition to the private key, this file contains values for the key passphrase, Client ID, Client Secret, Public Key ID, and enterprise ID. These values will be used later when you configure Access Manager.
   4d In the OAuth 2.0 Credentials section of the page, click Copy to save the value of the Client ID to the clipboard. You will use this value in Step 5d.
   4e Click Save Changes to save the app, then click My Apps in the left navigation bar.

5 Authorize access for the app created above using the following steps:
   5a In the left navigation bar of the My Apps page, click Admin Console to access your Box admin console.
   5b Navigate to Apps > Custom Apps.
   5c Click Authorize using client ID (the + icon on the top right of the page).
   5d In the App Authorization prompt for Client ID, paste the value of the Client ID that you saved in Step 4d.
   5e Click Next > Authorize.

When you have completed the above steps at Box, the downloaded JSON file will contain all values required for configuring the Box application’s Account Management settings in Access Manager. You can open the file using a text editor to view the values for enterpriseID, clientID, clientSecret, publicKeyID, privateKey, passphrase, and enterpriseID, which will be used when configuring Access Manager.

6 The last step before configuring the Access Manager settings is to extract and reformat the private key:
   6a Open the JSON file in a text editor.
   6b Copy the private key to the clipboard, then paste it into a new editor window. The content should look similar to the following:
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBAbgkghiG9w0BBQowMzAbBgkghiG9w0BBQowDqIWzhaNTHqDx0CAggA
MBQGCCgGSIb3DQMHAhBqPeQY/K9JwSCBiM4W9e8nUw/o14ceA1QiK/tez
MBQGCCgGSIb3DQMHAhBqPeQY/K9JwSCBiM4W9e8nUw/o14ceA1QiK/tezM

-----END ENCRYPTED PRIVATE KEY-----

6c Replace all new line (\n) characters with Line Feed (LF) characters.

6d Save the edited key to a separate text file with a .key extension. The file content should look similar to the following:

-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFDjBAbgkghiG9w0BBQowMzAbBgkghiG9w0BBQowDqIWzhaNTHqDx0CAggA
MBQGCCgGSIb3DQMHAhBqPeQY/K9JwSCBiM4W9e8nUw/o14ceA1QiK/tezM

-----END ENCRYPTED PRIVATE KEY-----
This will be the file used for the Private Key setting when configuring Access Manager.

You are now ready to complete the application settings in Access Manager.
Complete the following steps to configure Docusign to allow user provisioning from Access Manager using SAM.

2. Save the provided Integrator Key for later use.

When you have completed the above steps at Docusign, use the values you saved to configure the application’s Account Management settings in Access Manager.
Complete the following steps to configure Dropbox to allow user provisioning from Access Manager using SAM:

1. From a browser, log in to your Dropbox for Business account using administrator credentials.
2. In the browser address bar, enter https://www.dropbox.com/developers/apps.
3. Click Create app.
4. In Choose an API, select Scoped access.
5. In Choose the type of access you need, select Full Dropbox.
6. In the Name your app field, type a descriptive name.
7. Click Create app.
   The application’s Settings page appears.
8. On the Permissions tab under Team Scopes, select the following:
   - team_info.read
   - members.read
   - members.write
   - members.delete
   - groups.read
   - groups.write
   - team_data.member
9. Click Submit.
10. Click the Settings tab.
11. Under OAuth2 > Access token expiration, select No expiration.
12. Under OAuth2 > Generated access token, click Generate.
13. Copy the value of the access token for later use.

When you have completed the above steps at Dropbox, configure the application’s Account Management settings in Access Manager, using the value of the access token you saved.
Complete the following steps to configure Google Apps to allow user provisioning from Access Manager using SAM.

1. Go to https://console.cloud.google.com/home/ and log in as your domain administrator.
2. (Conditional) If you already have a Google Cloud project available, skip to Step 4.
3. (Conditional) Create a Google Cloud project:
   3a. Click Create project.
   3b. Enter a project name, then click Create.
   The project’s dashboard appears. Refresh the page if necessary to see your project.
4. Enable the Admin SDK API for your project:
   4a. From the list in the top menu bar, select your project to access the project Dashboard.
   4b. From the Navigation menu in the top menu bar, select APIs & Services > Library.
   4c. Search for and select the Admin SDK service.
   4d. Click Enable.
5. Create and configure a service account:
   5a. From the navigation menu in the top menu bar, select APIs & Services > Credentials.
   5b. In the Credentials menu bar, select Create credentials > Service account.
   5c. On the Create service account page:
      5c1. For Step 1, enter a value for the service account name. Click Create to go to Step 2.
      5c2. For Step 2, under Select a role, select Project > Owner. Click Continue to go to Step 3.
      5c3. For Step 3, click Done.
      The Credentials page shows your newly created service account.
   5d. Click the edit (pencil) icon for the service account.
   5e. Under Email, make note of the email address for the service account. You will need this when you configure the Google application in Access Manager.
   5f. Under Unique ID, make note of the client ID. You will need this ID later in these steps.
   5g. Click Show Domain-wide Delegation.
   5h. Select Enable G Suite Domain-wide Delegation.
   5i. In the Product name for the consent screen field, enter a name.
   5j. Under Keys, select Add Key > Create new key.
   5k. Ensure that the selected Key type is JSON, then click Create.
      Follow the prompts to download the certificate file. Make note of the name and location of the downloaded certificate for later use.
   5l. After you have downloaded the certificate, click Close.
   5m. Click Save to complete the service account setup.
Configure G Suite security:

6a Go to https://admin.google.com and log in as your domain administrator.

6b From the Main menu in the top menu bar, select Security > API controls.

6c At the bottom of the page, select Manage Domain-wide Delegation.

6d Click Add new.

6e For Client ID, paste the client ID of the service account that you created in Step 5f.

6f In OAuth scopes, paste the following comma-delimited string to grant read-only access:


6g Click Authorize.

You should now see your service account listed with Name, Client ID, and scopes as an authorized client of G Suite.

The setup at Google is now complete.

7 In the Access Manager administration console, configure the Google Apps application. Use the value for the service account email that you recorded in Step 5e and the certificate file that you downloaded in Step 5k.
To configure LogMeIn Apps to allow user provisioning from Access Manager using SAM, follow the instructions at the GoTo Developer Center website (https://goto-developer.logmeininc.com/how-create-developer-app). You might also need to go to the LogMeIn billing page (https://billing.logmeininc.com) to manage your subscriptions.

When you have completed the above steps at LogMeIn, use the values you saved to configure the application's Account Management settings in Access Manager.

**NOTE**: The LogMeIn Apps connector works only with the GoTo* product suite. Goto uses LogMeIn Inc and the domain name logmeininc.com, not the domain name logmein.com (which is associated with the LogMeIn product).
Complete the following steps to configure Office 365 to allow user provisioning from Access Manager using SAM:

2. In the left navigation pane, select Azure Active Directory to open the Overview page for your domain.
3. At the top middle of the Overview page, the domain name appears. Copy and save it for later use.
4. In the left navigation pane for your domain, select Properties.
5. From the Properties page, copy the Tenant ID and save it for later use.
6. In the left navigation pane, select App registrations, then click All applications.
7. (Conditional) If you are creating a new application:
   7a. Select New registration.
   7b. In the provided form, enter a Name, leave the default Single tenant button selected, then for the Redirect URI (optional) select Web and type the following:
       https://www.office.com
   7c. Click Register.
       The page redirects you to the Overview page.
   7d. Copy and save the Application ID and Directory ID for later use.
8. (Conditional) If you are using an existing Native type application:
   8a. Select the application from the App registrations page.
   8b. Copy the Application ID and save it for later use.
9. On the application details page, in the left navigation pane select API permissions. Microsoft Graph is automatically added with the User.Read permission.
10. Click Microsoft Graph, then configure additional permissions as follows:
   10b. Expand Group and select Group.ReadWrite.All (Read and write all groups).
   10c. Expand User and select User.Read.All, User.ReadWrite, and User.ReadWrite.All.
11. Click Update permissions.
12. Click Grant admin consent for <Your organization>.
13. In the left navigation pane, click Authentication again.
14. Under Implicit grant, select the ID tokens check box.
15  Under Advanced settings, toggle Treat application as a public client to Yes.

16  At the top of the page, click Save.

When you have completed the above steps for Office 365, use the values you saved to configure the application's Account Management settings in Access Manager.

**NOTE:** The first time you register an application in the Azure AD portal, if the Implicit grant section does not appear in the application portal interface, you can enable it manually. Click the application's Manifest in the left navigation pane, then change oauth2AllowIdTokenImplicitFlow from false to true.
Complete the following steps to configure Salesforce to allow user provisioning from Access Manager using SAM.

1. Log in to your Salesforce account with administrator credentials.

2. Add a connected app as follows:
   
   2a. (Conditional) If you are using the Salesforce Lightning UI, go to Setup. From the left navigation pane, go to Platform Tools > Apps > App Manager and click New Connected App.

   2b. (Conditional) If you are using the Salesforce legacy UI:
   
   2b1. From the user name menu, click Setup.

   2b2. Depending on the settings available in your user interface, do one of the following:
   
   - From the left navigation pane, go to App Setup > Create > Apps > Connected Apps and click New
   - Go to Build > Create > Apps > Connected Apps and click New

   2c. Provide the required details for the new connected app as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected App Name</td>
<td>Enter the connected app’s name, which displays in the App Manager and on its App Launcher tile. The connected app name must be unique within your organization.</td>
</tr>
<tr>
<td>API Name</td>
<td>Enter the API name used when referring to your app from a program. It defaults to a version of the name without spaces.</td>
</tr>
<tr>
<td>Contact Email</td>
<td>Enter the contact email for Salesforce to use in case they want to contact you or your support team.</td>
</tr>
<tr>
<td>Enable OAuth Settings</td>
<td>Ensure that this check box is selected.</td>
</tr>
<tr>
<td>Callback URL</td>
<td>Enter <a href="https://login.salesforce.com/services/oauth2/token">https://login.salesforce.com/services/oauth2/token</a></td>
</tr>
<tr>
<td>Selected OAuth Scopes</td>
<td>From Available OAuth Scopes, select Full access (full) and click the button under Add. This provides the necessary permissions when accessing this app.</td>
</tr>
</tbody>
</table>

   2d. Click Save, then click Continue.

3. On the next screen showing app details, take note of the following information. You will need this for configuration steps in Access Manager:
   
   - Consumer Key
   - Consumer Secret
When you have completed the above steps at Salesforce, use the values you noted in Step 3 to configure the application's Account Management settings in Access Manager.
SaaS Account Management performs account provisioning to ServiceNow by calling the ServiceNow Table API. The following two sections describe how to verify that the Table API has access to the tables it needs, and how to configure OAuth authentication to the Table API.

When you have completed the required steps at ServiceNow, use the values you saved to configure the application’s Account Management settings in Access Manager.

- “Table Permissions for Provisioning API” on page 23
- “OAuth Authentication for Provisioning API” on page 24

### Table Permissions for Provisioning API

In a default ServiceNow instance that has not modified its table access, the Table API already has access to the data it needs. However, since that access is configurable in ServiceNow, we recommend completing the following steps to verify that the Table API has correct access to tables required for provisioning.

**To verify Table API permissions:**

1. Log in to the ServiceNow home page using your administrative user account.
2. In the list of settings on the left side, expand System Definition and select Tables.
3. In the list of tables, enter `sys_user` in the search box at the top of the Name column to find the following tables:
   - `sys_user` (User)
   - `sys_user_group` (Group)
   - `sys_user_role` (Role)
   - `sys_user_grmember` (Group Member)
   - `sys_user_has_role` (User Role)
4. For each of the tables:
   4a. Click the Label name (shown in parentheses in the list above) to open its settings.
   4b. In the table settings, click the Application Access tab.
   4c. Verify that the Allow access to this table via web services check box is selected. If not, select it and then click Update.
OAuth Authentication for Provisioning API

SaaS Account Management with Access Manager uses OAuth to authenticate calls to the ServiceNow Table API when provisioning users. In the Account Management section of the application connector in Access Manager, values for Instance name, User credentials, Client ID, and Client secret are required.

The OAuth Client ID and Client Secret both come from an OAuth Application Registry. If you do not already have an Application Registry in ServiceNow, you must create a new one. Otherwise, you can find the Client ID and Client Secret associated with an existing OAuth Application Registry. For more information, see the following topics:

- “Creating a New OAuth Application Registry” on page 24
- “Finding the Client ID and Client Secret for an Existing Application Registry” on page 24

Creating a New OAuth Application Registry

Complete the following steps to create a new OAuth Application Registry.

1. Log in to the ServiceNow home page using your administrative user account.
2. In the list of settings on the left side, expand System OAuth and select Application Registry.
3. At the top of the list, select New.
4. Select Create an OAuth API endpoint for external clients.
5. Enter a name for the Application Registry, such as Account Provisioning API Authentication.
6. Either enter a string in the Client Secret field, or leave it blank to generate a secure Client Secret.
7. Verify that the Application field value is Global.
8. Verify that the Accessible from field value is All application scopes.
9. Verify that the Active check box is selected.
10. (Optional) Change or leave the default values in the other fields in the form.
11. Click Submit.

Finding the Client ID and Client Secret for an Existing Application Registry

Complete the following steps to find the Client ID and Client Secret associated with an existing OAuth Application Registry.

1. Log in to the ServiceNow home page using your administrative user account.
2. In the list of settings on the left side, expand System OAuth and select Application Registry.
3. Click the name of the Application Registry you want to use to authenticate provisioning API requests.
4. The value shown next to Client ID is the value you use for the Client ID setting in the Account Management section of the ServiceNow application in Access Manager.
5 To see the Client Secret, click the **Toggle Password Visibility** button next to the **Client Secret** field. The button's icon looks like a padlock.

6 The value shown under the Client Secret field is the value you use for the **Client Secret** setting in the Account Management section of the ServiceNow application in Access Manager.
No specific configuration steps are required at Tableau Online to enable user provisioning from Access Manager using SAM. However, you will need to record the following information from your Tableau Online account:

- The user name (in email format) and password of the site administrator user.
- The site name of your Tableau Online account that you specified when you created the account. You can find this value in the URL that you use to access the Tableau Online administration pages. For example, if your administration URL is `https://10ay.online.tableau.com/#/site/usethisname/settings`, then `usethisname` is the site name.
- The subdomain name of your Tableau Online setup. You can find this value in the URL that you use to access the Tableau Online administration pages. For example, if your administration URL is `https://10ay.online.tableau.com/#/site/usethisname/settings`, then `10ay` is the subdomain name.

Use the values you recorded to configure the Account Management settings for the Tableau Online application in Access Manager.
Complete the following steps to configure Zendesk to allow user provisioning from Access Manager using SAM. These steps assume that you have already configured a Zendesk account and subdomain.

1. Log in to your Zendesk administration console at https://your_subdomain.zendesk.com/accessible/normal with your administrator credentials.
2. In the sidebar click the Admin (gear) icon, then navigate to Channels > API.
3. Accept the license agreement, then click Get started.
4. Enable Token Access.
5. Click the plus icon (+) to create a new token.
6. From the API Token field, click Copy, then save the token for later use.
7. Click Save.

After you have completed the above steps at Zendesk, use the administrator email address, token, and subdomain to configure the Account Management settings for the Zendesk application in Access Manager.