SM Enrollment Authentication

To provide a layer of security regarding which devices are able to enroll in a Systems Manager (SM) network, authentication using either Active Directory (AD) or Meraki users/owners can be used. This article will cover how to implement each potential option.

There are multiple methods which can be used for performing device enrollment authentication:

- **Managed: Use Meraki hosted accounts**: Use Meraki user/owner accounts managed in the Owners page. This is a good option for smaller deployments that do not require integrating with a larger third-party directory system.
- **Active Directory: Use your own Active Directory Server**: Authenticate against an Active Directory Server not located in the cloud
  - **AD via MX Security Appliance**: Authentication requests are proxied through an MX security appliance configured for AD integration.
  - **AD via SM Agent**: Authentication requests are proxied through a Windows PC/Server or macOS client with the SM Agent installed.
- **Google: Sign in with Google**: Authenticate against Google's native Oauth endpoint for use in conjunction with G Suite
- **Microsoft: Authenticate with Microsoft Azure Active Directory**: Authenticate against Microsoft's Azure Cloud-Hosed Active Directory Solution
- **OpenID Connect: Use your own OpenID Connect server**: Authenticate against any 3rd-party device or service which supports the OpenID Standard

For an additional security, you may want to enable enrollment auto-quarantine to manually approve devices before they can receive your Systems Manager profiles and apps.

iOS and macOS devices enrolling through DEP currently do not support enrolling with Azure AD, OpenID, and Google Oauth enrollment authentication. They will fall back to Meraki managed authentication and require Meraki owner accounts to authenticate if your Systems Manager network is configured with one of these methods. Note that these three methods will also not provide any group tag metadata like local Active Directory integration will.

If you are using a Google Account Bind in conjunction with Android For Work (configured on the Organization > MDM page), Google authentication is not available as it is already being used as part of the AFW enrollment process, and any selection made here would be for use in conjunction with this mechanism.

For each option, begin by navigating to Systems manager > Configure > General > User authentication settings. Then, refer to the appropriate section below to complete the configuration.
Managed Authentication with Meraki Users/ Owners

This option utilizes the list of users/owners on the Configure > Owners page in a Systems Manager network. This is best for smaller deployments, or cases where a list of owners is already actively maintained. See the Owners article for more info.

1. Set Authentication settings to "Managed".
2. Click Save Changes.

![User authentication settings]

In order to change/add/delete users, use the Configure > Owners page.

Note: Meraki Users need to use the email address of their user as their username when authenticating.

Enabling Multi-user authentication feature allows all the email addresses in the Owners list to be able to authenticate on the same device. The screenshot below shows that after enabling this feature, the option to “Switch User” becomes available on the end devices. This feature is only available on iOS and Android devices.
Active Directory Integration

AD integration allows you to use your existing directory service as a line of defense, limiting who can enroll into your Systems Manager network, but also allows you to use your existing AD groups as user tags to scope profiles and apps. For more information on AD user tags, see the Owners article, and Tags article.

You can link your Cisco Meraki MX security appliance for directory services, or enroll your Windows machine hosting the server into Systems Manager to configure AD authentication. Note that these options will not be available to configure unless you have an MX in your Dashboard organization, or a Windows machine enrolled into your SM network, respectively.

Active Directory via MX Appliance

With this option, any enrollment authentication requests will be proxied through an MX security appliance that is configured for AD integration. This works well when an MX in this configuration is already deployed, or one is available where AD authentication can be enabled.

Note: All communication between an MX security appliance and an Active Directory server will be encrypted using TLS. If AD integration has not yet
To configure Active Directory via MX appliance:

1. Set **Authentication settings** to "Active Directory".
2. Set **AD gateway type** to "Meraki".
3. Select the desired MX appliance as the **Gateway network**.
4. Click **Save Changes**.

Users attempting to enroll devices will now be required to authenticate using their Active Directory username and password. The username should be specified as the user's Active Directory name, *not* including the domain name (e.g. "testuser," not "domain/testuser")

Active Directory via SM Agent

With this option, any enrollment authentication requests will be proxied to an Active Directory server through a Windows device with the Systems Manager agent installed. This Windows device can be a user desktop, or an AD server. However, it must be enrolled in the Systems Manager network, have the SM agent installed (Systems Manager > Manage > Add Devices > Windows), and not have any firewall settings preventing it from communicating with the AD server.

**Note:** The option to select "SM agent" will be grayed out until a Mac or Windows machine capable of communicating with your AD server is enrolled into Systems Manager.

To configure Active Directory via SM agent:

1. Set **Authentication settings** to "Active Directory".
2. Set **AD gateway type** to "SM agent".

**Note:** Users *may* in some AD configurations be able to successfully authenticate using the domain/testuser or `testuser@domain.tld` formats, but doing so may result in some features not functioning as expected.
3. Specify the following information regarding the AD server:
   **Short domain**: The domain users will be authenticated against.
   **Server IP**: The IP address of the AD server to use.
   **LDAP port**: Port on the AD server that will be listening for LDAP requests. Default is 3268.
   **Domain admin/Password**: Username and password of an administrator for this domain.

4. Select one or more **Gateway machines**. These are the devices that the enrollment authentication requests will be proxied through. They must have reachability to the AD server provided above.

5. Click **Save Changes**.

   ![User authentication settings](image)

If issues are encountered, ensure that the AD server used has the **Global Catalog role enabled**. Particularly if multiple domains are configured.

**Note**: Communication between the Gateway machines and the AD server is **not** encrypted. Therefore, it is strongly recommended that only the AD server being queried be used as a Gateway machine, in order to keep communication local and encrypted.

### Sign in with Google

Oauth against Google is as easy as filling in the allowed Google domain in the specified field. Note that Apple DEP enrollment does not support Google authentication, and will fall back to Meraki Authentication credentials.
Azure Active Directory Sign-In

1. Login to your Microsoft Azure portal.
2. Select "Azure Active Directory" in the side menu.
4. Under "Manage" select "App registrations".
5. Select "Add" and add a new app of type "Native". The application name will be the name displayed to your users when logging in.
6. Enter "merakismoauth://com.meraki.pcc" as a 'Public client/native' URI.
7. Enter the following as Web type URIs:
   1. "https://m.meraki.com"
   2. "https://portal.meraki.com/loginsuccess"
   3. "https://mp.meraki.com/ssp/login"

Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URIs. Learn more about adding support for web, mobile and desktop clients

<table>
<thead>
<tr>
<th>Type</th>
<th>Redirect URI</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Public client/native</td>
<td>merakismoauth://com.meraki.pcc</td>
<td></td>
</tr>
<tr>
<td>Web</td>
<td><a href="https://mp.meraki.com/ssp/login">https://mp.meraki.com/ssp/login</a></td>
<td></td>
</tr>
<tr>
<td>Web</td>
<td><a href="https://m.meraki.com/">https://m.meraki.com/</a></td>
<td></td>
</tr>
<tr>
<td>Web</td>
<td><a href="https://portal.meraki.com">https://portal.meraki.com</a></td>
<td></td>
</tr>
<tr>
<td>Web</td>
<td>e.g. <a href="https://myapp.com/auth">https://myapp.com/auth</a></td>
<td></td>
</tr>
</tbody>
</table>

8. 

9. Copy and paste your app's "Application ID" into the "Application Client ID" field below.
10. Under "Required permissions" in the newly created app make sure the following permissions are added:
   ◦ "Windows Azure Active Directory" -> "Sign in and read user profile"
   ◦ "Windows Azure Service Management API" -> "Access Azure Service Management as organization users"
   ◦ "Microsoft Graph" -> "Sign in and read user profile"
OpenID Connect

The OpenID Connect option allows you to point Dashboard/your users at your custom OAuth/OpenID endpoint. Fill the information from your endpoint into the appropriate fields, but take care to note the following:

- Whitelist the following redirect URIs for authentication requests.
  - merakismoauth://com.meraki.pcc
  - https://m.meraki.com
  - https://mp.meraki.com/ssp/login
  - https://mp.meraki.com/ssp/loginsuccess
  - https://portal.meraki.com/loginsuccess

- The token endpoint should include the ID token in the "id_token" field in its response to a valid request.
- The ID token should have an "email" claim that specifies the e-mail address of the authenticated user.
- The token endpoints should return the public key(s) used to sign ID tokens. Here are sample response formats Systems Manager expects:
  - PEM Format
  - JWK Format