# Configure the SASE Mobile Device Manager

*For supported software information, click [here](#).*

You use mobile device management (MDM) to administer mobile devices, such as smartphones, tablet computers, and laptops. To use MDM, you create an MDM profile to retrieve device information from a Microsoft Intune server using the device ID and other information, such as a user profile using a user ID.

You can associate MDM profiles with a secure access portal or a secure access gateway to verify device information during and Versa Secure Access (VSA) client registration (portal) and after registration (gateway).

After you link an MDM profile to a graph server, when a user tries to connect to a Versa gateway using a VPN client, a check verifies whether the device is enrolled with the graph server and if the device is compliant with the policies you have configured. If the device is managed and compliant, the VPN session is established, and the user is allowed to access internal resources.

Note: You must configure the following SASE rules, profiles, and settings in a specific order:

1. Configure users and groups, and then publish them to the gateway. For more information, see [Configure Users and Device Authentication](#).
2. Configure site-to-site tunnels. For more information, see [Configure SASE Site-to-Site Tunnels](#).
3. Configure secure client access profiles and rules. For more information, see [Configure SASE Secure Client Access Rules](#).
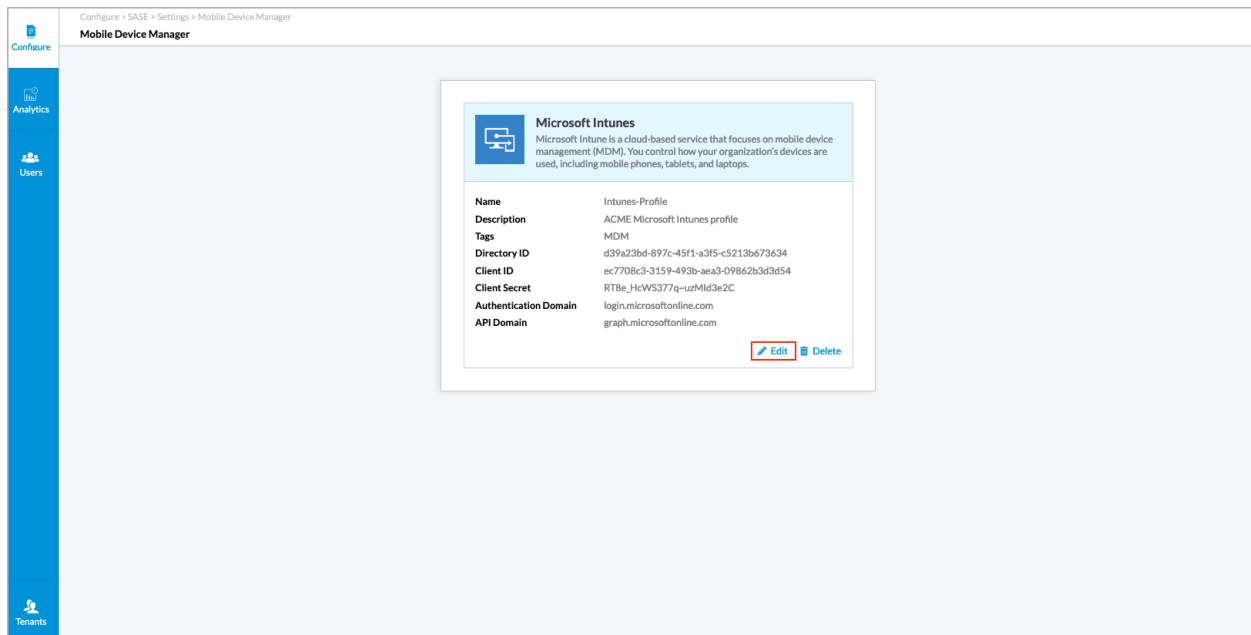
The remaining SASE rules, profiles, and settings do not need to be configured in a specific order.

To configure MDM:

1. Go to Configure > Settings > Mobile Device Manager.
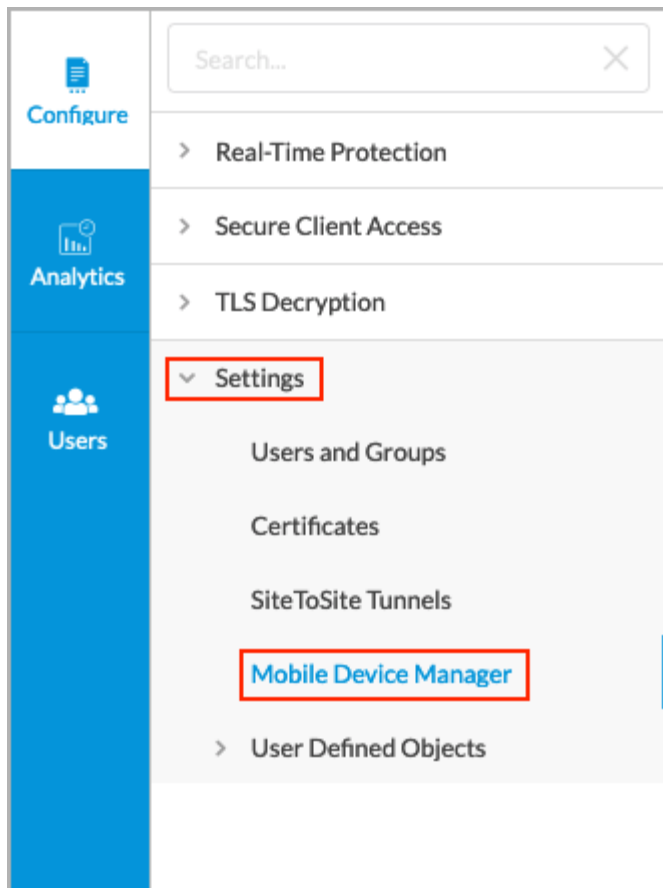
The Mobile Device Manager screen displays.

2. Click the ✏ Edit icon to edit the configuration, and then enter information for the following fields.

**Client Secret** *

**Authentication Domain** *

**API Domain** *

Cancel    Save

| Field | Description |
|---|---|
| Name | Enter a name for the MDM profile. |
| Description | Enter a text description for the MDM profile. |
| Tags | Enter tags to associate with the MDM profile. |
| Directory ID | Enter the tenant or directory ID registered on the graph (Intune) server. |
| Client ID | Enter the client identifier provided by the graph (Intune) server, in string format. |
| Client Secret | Enter the client secret provided by the graph (Intune) server, in string format. |
| Authentication Domain | Enter the domain name to use for authentication. |
| API Domain | Enter the domain name to use for APIs. |

3. Click Save.

## Supported Software Information

Releases 11.1.1 and later support all content described in this article.

# Additional Information

[Configure SASE Certificates](#)
[Configure SASE Secure Client Access Rules](#)
[Configure SASE Site-to-Site Tunnels](#)
[Configure Users and Device Authentication](#)