entra-app-setup

Setting Up Microsoft Entra Enterprise Application for Intuneomator

This guide will walk you through the process of creating and configuring a Microsoft Entra Enterprise application to allow Intuneomator to connect to your tenant and manage macOS applications, scripts, and custom attributes.

Prerequisites

- Administrative access to your Microsoft Entra ID (formerly Azure AD) tenant
- Intuneomator application ready for configuration
- Decision on authentication method (client secret or certificate)

Overview

Setting up the Enterprise application involves several key steps:

1. Registering a new application in Microsoft Entra ID
2. Configuring authentication credentials (client secret or certificate)
3. Assigning required API permissions
4. Creating a client configuration for Intuneomator

Step 1: Register a New Application

1. Sign in to the Microsoft Entra admin center with an admin account
2. Navigate to **Identity** > **Applications** > **App registrations**
3. Click **+ New registration**
4. Enter the following information:
   - **Name**: Intuneomator Integration (or your preferred name)
   - **Supported account types**: Accounts in this organizational directory only (Single tenant)
   - **Redirect URI**: (Leave blank for this integration)
5. Click **Register**

Once registered, note down the following important values displayed on the Overview page:

- **Directory (tenant) ID**
- **Application (client) ID**

These values will be required when configuring Intuneomator.

Step 2: Configure Authentication Method

Option A: Using Certificate

1. Generate a self-signed certificate:

   Using Intuneomator:

- If you are viewing this in the Intuneomator Welcome Wizard, the next panel has a button that you can click **Generate Certificate Pair**.
- Enter **Common Name** in the field. (e.g., Intuneomator Cert)
- Enter **Organizarion Name** in the field. (e.g., Your Company Name)
- Enter **Country Code** in the field (e.g., US)
- If you would like to save a copy of the certificates, click **Save Certificate** and enter a **Output Name** in the field. (e.g., Intuneomator Cert without an extension)
- Click the **Path** button to select a location to save the certificate.
- Enter a **Password** for the certificate. (e.g., 12345678)
- Click **Generate Certificate** to create the certificate pair.
- The certificate pair will be saved in the location you selected in the previous step. The certificate will be saved with a .cer extension and the private key will be saved with a .key extension.
- The certificate will also automatically be setup for use in the Intuneomator application.

   Using macOS Terminal (OpenSSL):

```
# Generate private key
openssl genrsa -out intuneomator.key 2048

# Generate certificate signing request
openssl req -new -key intuneomator.key -out intuneomator.csr

# Generate self-signed certificate
openssl x509 -req -days 365 -in intuneomator.csr -signkey intuneomator.key -
out intuneomator.crt

# (Optional) Create PFX/P12 with private key and certificate
openssl pkcs12 -export -out intuneomator.pfx -inkey intuneomator.key -in
intuneomator.crt
```

2. Upload the certificate to your Entra application:

- Navigate to your application in Entra admin center
- Select **Certificates & secrets** from the left menu
- Under **Certificates**, click **Upload certificate**
- Browse to your .cer or .crt file
- Optionally provide a description
- Click **Add**

3. Note the certificate thumbprint for reference (Should match what Intuneomator will also show)

Option B: Using Client Secret

1. Navigate to your application in Entra admin center
2. Select **Certificates & secrets** from the left menu
3. Under **Client secrets**, click **+ New client secret**
4. Provide a description and select an expiration period:
   - **Description**: Intuneomator Secret
   - **Expires**: Choose according to your security policy (12 months, 24 months, etc.)
5. Click **Add**
6. **IMPORTANT**: Copy and securely store the generated secret value immediately. It will not be displayed again after you leave this page.

Step 3: Assign API Permissions

1. Navigate to your application in Entra admin center
2. Select **API permissions** from the left menu
3. Click **+ Add a permission**
4. Select **Microsoft Graph** > **Application permissions**
5. Search for and select the following permissions:
   - *DeviceManagementApps.ReadWrite.All*
   - *DeviceManagementConfiguration.ReadWrite.All*
   - *DeviceManagementManagedDevices.Read.All*
   - *Group.Read.All*
6. Click **Add permissions**
7. Click **Grant admin consent for [your organization]** and confirm when prompted

Step 4: Configure Intuneomator

Choose between Certificate and Client Secret Authentication

- In the Setup Wizard select the radio button that matches your Entra App choice.
- Click the import button that matches your choice.
- If you import a P12/PFX certificate, it will ask you for the password to open the file
- If you import a Secret Key, it will ask you for the expiration date to send a reminder

Step 5: Test the Connection

- In the next panel of the Setup Wizard, enter the Entra ID info:
- Enter the Entra Tenant ID
- Enter the Entra Application ID.
- Click the Test Connection button to confirm the connection

Troubleshooting

If you encounter issues with the connection:

1. Verify all permissions are correctly assigned and admin consent is granted
2. Ensure the client secret hasn't expired (if using client secret authentication)
3. Check that the certificate is valid and hasn't expired (if using certificate authentication)
4. Verify the tenant ID and client ID are entered correctly
5. Check Entra ID application logs or Intuneomator application logs for detailed error messages

Security Best Practices

- Rotate client secrets regularly according to your organization's security policies
- Store credentials securely
- Consider using certificate-based authentication for enhanced security
- Use the principle of least privilege - don't grant permissions the application doesn't need
- Monitor application usage through Entra ID audit logs

Additional Resources

- Microsoft Entra application documentation
- Microsoft Graph API permissions reference
- Intuneomator Wiki documentation