Set up Azure IoT Central to work with Azure Sphere

- Article
- 04/13/2023
- 9 contributors

This topic documents the steps to set up Azure IoT Central to work with Azure Sphere.

After you have completed the tasks in this topic, any device that is claimed into your Azure Sphere tenant is automatically authenticated when it first connects to your Azure IoT Central application. Therefore, you only need to complete these steps once.

Before you begin

The steps in this section assume that:

- Your Azure Sphere device is connected to your PC by USB.
- You have an Azure subscription.

Overview

Setting up Azure IoT Central to work with Azure Sphere devices requires a multi-step process:

1. Create an Azure IoT Central application.
2. Download the authentication CA certificate for your Azure Sphere tenant from the Azure Sphere Security Service.
3. Upload the CA certificate to Azure IoT Central to tell it that you own all devices whose certificates are signed by this CA. In return, Azure IoT Central returns a verification code.
4. Generate and download a validation certificate from the Azure Sphere Security Service, which signs the verification code.
5. Upload the validation certificate to prove to Azure IoT Central that you own the CA.

Step 1. Create an Azure IoT Central application

1. Sign in to Azure IoT Central with your Azure credentials.
2. If you do not already have an application, follow the steps in Create an Azure IoT Central application. Stop when you reach the **Register a device** section.

Important

Azure IoT Central offers a 7-day free trial application. After 7 days, applications incur charges based on the number of devices and messages. The **Azure IoT Central pricing page** provides details.

Step 2. Download the tenant authentication CA certificate

1. From the command prompt, sign in with your Azure Sphere login:

   Azure Sphere CLICopy

   ```
   azsphere login
   ```

2. Download the Certificate Authority (CA) certificate for your Azure Sphere tenant. This command downloads the certificate to a file named *CAcertificate.cer* in the current working directory. Ensure that you download the file to a directory in which you have write permission, or the download operation will fail. The output file must have a .cer extension.
   - Azure Sphere CLI
   - Azure Sphere classic CLI

   Azure Sphere CLICopy

   ```
   azsphere ca-certificate download --destination CAcertificate.cer
   ```

Step 3. Upload the tenant CA certificate to Azure IoT Central and generate a verification code

1. Open your IoT Central application. Under the **Security** section, select **Permissions**, then **Device connection groups**.

2. Select **+ New** to create an enrollment group (such as **MyX509Group**) with an attestation type of **Certificates (X.509)**. Select **Save**.
3. In the enrollment group that you created, scroll down to **Certificates (X.509)**. In **Primary**, select **Manage Primary**.
4. In the **Primary certificate** dialog, select **Add certificate**. From the **Open** dialog, select the root certificate file that you generated in the previous step. Select **Open**. At this point you can verify the certificate automatically or manually.

Verify certificate automatically

After you have selected a root certificate file in the **Primary certificate** dialog, certificates are set to be verified on upload by default. If you are using a CA certificate that you trust and know that you have full ownership of the certificate, this option allows you to self-attest that you have verified the certificate.

1. To verify the certificate automatically, leave **Set certificate status to verified on upload** set to **On**.
2. Select **Upload**. The certificate's **Subject** and **Thumbprint** appear in the **Primary certificate** dialog. The label **Verified** with a checkmark icon indicates that verification was successful. Select **Close**.
3. Select **Save** at the top of the enrollment group page to save your changes.

Verify certificate manually

After you have selected a root certificate file in the **Primary certificate** dialog, you can specify that you are verifying the certificate manually.

1. To verify the certificate manually, set **Set certificate status to verified on upload** to **Off**.
2. Select **Upload**. The certificate's **Subject** and **Thumbprint** appear in the **Primary certificate** dialog. The label **Needs verification** with an alert icon indicates that verification is needed.
3. Under **Certificate verification**, select **Generate verification code**, and copy the code that appears in **Verification code**.
4. In the command prompt, run the following command to download a validation certificate that proves that you own the tenant CA certificate. Replace `<code>` in the command with the verification code from the previous step:

    - Azure Sphere CLI
    - Azure Sphere classic CLI

    Azure Sphere CLICopy

    ```
    azsphere ca-certificate download-proof --destination
    ValidationCertification.cer --verification-code <code>
    ```

    The Azure Sphere Security Service signs the validation certificate with the verification code to prove that you own the CA.

5. Return to Azure IoT Central and select **Verify**.
6. In the **Open** dialog, select the validation certificate that you downloaded in the previous step. Select **Open**. After verification, the status of your certificate changes to **Verified** with a checkmark icon in the **Primary certificates** dialog. Select **Close**.
7. Select **Save** at the top of the enrollment group page to save your changes.

Next steps

After you complete these steps, any device that is claimed into your Azure Sphere tenant is automatically accessible to your Azure IoT Central application.

You can now run the Azure IoT sample or use Azure IoT Central to monitor and control any of your Azure Sphere devices.