

Set up an Azure IoT Hub for Azure Sphere

- Article
- 04/13/2023
- 11 contributors

To use your Azure Sphere devices with [Azure IoT Hub](#), you need to create a hub and set it up to work with your Azure Sphere tenant, then configure x509 certificate authentication for each device.

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.

Important

Although you can create an Azure subscription for no charge, the sign-up process requires you to enter a credit card number. Azure provides several levels of subscription service. By default, the Standard tier, which requires a monthly service charge, is selected when you create an Azure IoT Hub instance. To avoid a monthly charge, select the Free tier. The Free tier includes the services required to use your device with Azure IoT Hub, including the [Device Twin](#). If you don't have an Azure subscription, create a [free account](#) before you begin.

Step 1. Create an IoT hub

Go to [Create an IoT hub using the Azure portal](#).

Important

In "Create an IoT hub using the Azure portal," only follow the directions in the first section, "Create an IoT hub," then return to this topic.

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 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 and prove possession of the tenant CA certificate

Upload your tenant certification authority (CA) certificate to Azure IoT Hub, then automatically or manually prove that you own the certificate.

1. In the [Azure Portal](#), navigate to the IoT hub you created.
2. Select **Certificates** in the **Security settings** section.
3. Select **Add** to add a new certificate.
4. In **Certificate name**, enter a display name for the certificate.
5. In **Certificate .pem or .cer file**, select the folder icon to choose the certificate file you downloaded in the previous step.
6. Prove possession of a CA certificate using one of the following methods:
 - [Verify certificate automatically](#)
 - [Verify certificate manually](#)

Verify certificate automatically

To add a certificate and automatically verify it (prove possession of the tenant CA certificate):

1. In the **Add certificate** box, check the box for **Set certificate status to verified on upload**.
2. After verification, the status of your certificate changes to **Verified** in the **Certificates** list view. Select **Refresh** if the status does not update automatically.

Add certificate ×

Certificate name * ⓘ
CAcertificate ✓

Certificate .pem or .cer file. ⓘ
"CAcertificate.cer" 📁

Set certificate status to verified on upload ⓘ

ⓘ We'll verify this certificate automatically, with no manual verification steps required. [Learn more](#)

Next, proceed to [Step 4. Create an X.509 device in your IoT hub for your Azure Sphere device.](#)

Verify certificate manually

To add a certificate and manually verify it (prove possession of the tenant CA certificate):

1. [Get a unique verification code from the Azure portal.](#)
2. [Download the proof-of-possession certificate that proves you own the tenant CA certificate](#) from the Azure Sphere CLI.
3. [Upload the signed verification certificate on the Azure portal.](#) The service validates the verification certificate using the public portion of the CA certificate to be verified, thus proving that you are in possession of the CA certificate's private key.

Get a unique verification code from the Azure portal

1. After you have selected a certificate in the **Add certificate** blade, leave the box **Set certificate status to verified on upload** unchecked. Select **Save**.
2. The **Certificates** list view shows your certificates. The **Status** of the certificate you created is **Unverified**.

Name	Created	Expires	Subject	Thumbprint	Status
CACertificate	01/01/2001	22/05/2022	Microsoft Azure Sphere 143adbcb9-a5c4-4be...	378A258F3B92977CBF4480602FC1C5F261FF...	Unverified

3. Select the name of your certificate to display its details. In the **Certificates** blade, select **Generate verification code**. Copy the verification code to your clipboard for use in the next step. (Do not select **Verify** yet.)

Download a proof-of-possession certificate that proves you own the tenant CA certificate

Return to the Azure Sphere CLI and download a proof-of-possession certificate for your Azure Sphere tenant. Use the verification code to generate the certificate as an X.509 .cer file.

- [Azure Sphere CLI](#)
- [Azure Sphere classic CLI](#)

Azure Sphere CLICopy

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

Upload the signed verification certificate

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

1. From **Certificates** on the Azure Portal, in the **Verification certificate .pem or .cer file** field, browse to select and upload the signed verification certificate. The certificate is located in the directory in which you invoked the download command.
2. When the certificate is successfully uploaded, select **Verify**.

Certificate Details

AzureSphereTest



Delete

Subject ⓘ

CN=Microsoft Codename 4x4 d343c...



Expiry ⓘ

Mon Jun 01 2020 10:17:01 GMT-060...



Thumbprint ⓘ

[Redacted]



Created ⓘ

Fri Jul 27 2018 11:34:46 GMT-0600 (...)



Updated ⓘ

Fri Jul 27 2018 11:34:46 GMT-0600 (...)



Verification Code ⓘ

[Redacted]



[Generate Verification Code](#)

* Verification Certificate .pem or .cer file. ⓘ

"ValidationCertification.cer"



[Verify](#)

3. After verification, the status of your certificate changes to **Verified** in the **Certificates** list view. Select **Refresh** if the status does not update automatically.

Note



Perform Steps 1-3 only once per Azure Sphere tenant.


Step 4. Create an X.509 device in your IoT hub for your Azure Sphere device


1. In the Azure portal, navigate to your IoT hub. In the **Device management** section, select **Devices > Add Device**.
2. Select **New** to add a new device.
3. In **Device ID**, provide the Device ID. Note that the Device ID must be in lowercase characters. (You can run `azsphere device show-attached` in the Azure Sphere CLI to obtain the Device ID.)
4. For **Authentication type**, choose **X.509 CA Signed**, then select **Save**.


Home > [iot-hub-contoso-one - IoT devices](#) > Create a device


Create a device

 Find Certified for Azure IoT devices in the Device Catalog 

* Device ID 

Authentication type 
 Symmetric key X.509 Self-Signed X.509 CA Signed

Connect this device to an IoT hub 
 Enable Disable

Parent device 
No parent device
[Set a parent device](#)

Next steps

You can now run the [Azure IoT sample](#) or build your own application that uses your Azure IoT Hub.

Additional information

To use Device Provisioning Service instead of direct authentication, see [Set up an IoT hub for Azure Sphere with DPS](#).

To add an Azure IoT Edge device that provides a filtering and data processing layer between your Azure Sphere device and Azure IoT Hub, see [Set up Azure IoT Edge for Azure Sphere](#).