

How to Enable Microsoft IoT Edge and Docker on a Secure Connector

<https://campus.barracuda.com/doc/91987807/>

The new enhanced container feature for LXC, Docker, and IoT Edge is currently in EA and thus free of charge until at least December 2020. Starting January 2021 we will make this new functionality available for purchase and all existing deployments will need to be licensed.

On Secure Connector version 2.0.9, you can configure container engines that allow you to easily perform Edge computing capabilities on the FSC2 such as data aggregation, normalization, and offline logic. The SC 2.0.9 container configuration supports the following options:

- **Azure IoT Edge** – Azure IoT Edge extends IoT Hub. Analyze device data locally instead of in the cloud in order to send less data to the cloud, react to events quickly, and operate offline. Installing this runtime engine on the Secure Connector allows you to manage Edge modules from your Azure portal. In addition, Microsoft provides a list of IoT Edge modules in their marketplace that you can use out of the box for various scenarios. Microsoft IoT Edge provides a cost-savings solution for your business, allowing maximum flexibility even in offline mode, as the latest state of your edge device gets automatically synchronized after reconnecting to the cloud. Barracuda SC2 running firmware version 2.0.9 is Azure IoT Edge certified.

For more Information on Azure IoT Edge, please refer to <https://docs.microsoft.com/en-us/azure/iot-edge/>

For getting started with Azure IoT Edge on the Secure Connector, please refer to <https://catalog.azureiotsolutions.com/details?title=Barracuda-FSC2&source=null>

- **Docker Engine** – Docker Engine is a client-server application designed for building and containerizing applications and managing objects such as networks, containers, images, and volumes. A built-in command line interface uses APIs to interact via scripting and commands.

Configure Azure IoT Edge

Configure Azure IoT Edge as container engine on a Secure Connector.

Before You Begin

Configuring Azure IoT Edge requires the IoT Edge Device primary connection string. To access your device on Azure IoT Edge, do the following:

1. Log into the Azure portal: <https://portal.azure.com>
2. Go to the Azure IoT Hub your Edge device should be linked to:

Microsoft Azure

Home > Resource groups > iot-Playground > CudaIoThub | IoT Edge

CudaIoThub | IoT Edge

Deploy Azure services and solution-specific code to on-premises devices. Use IoT Edge devices to perform compute and analytics tasks on data before it's sent to the cloud.

IoT Edge devices

Field: deviceid Operator: = Value: 'TestDevice'

Query devices

Device ID	Runtime Response	IoT Edge Module Count	Connected Client Count
SC-1061399	OK	3	1

3. Copy the IoT Edge Device **Primary Connection String**.

Microsoft Azure

Home > Resource groups > iot-Playground > CudaIoThub | IoT Edge > SC-1061399

SC-1061399

Device ID: SC-1061399

Primary Key: [Redacted]

Secondary Key: [Redacted]

Primary Connection String: [Redacted]

Secondary Connection String: [Redacted]

IoT Edge Runtime Response: 200 -- OK





Enable connection to IoT Hub: Enable Disable

NAME	TYPE	SPECIFIED IN DEPLOYMENT	REPORTED BY DEVICE	RUNTIME STATUS	EXIT CODE
SedgeAgent	IoT Edge System Module	✓ Yes	✓ Yes	running	0
SedgeHub	IoT Edge System Module	✓ Yes	✓ Yes	running	0
SimulatedTemperatureSensor	IoT Edge Custom Module	✓ Yes	✓ Yes	running	0

Configure the Container Engine

Configure Microsoft IoT Edge on the Secure Connector.

1. On the Control Center, go to **your cluster** > **Cluster Settings** > **Secure Connector Editor**.
2. Click **Lock**.
3. Double-click to edit the device or Secure Connector.
4. Make sure the container is enabled and a root password is set. For more information, see [Secure Connector Container](#).
5. Select **Microsoft IoT Edge** as the **Container Engine**.
6. Paste the **IoT Edge Device Connection String**.

Container Engine	
Select Container Engine	Microsoft IoTEdge 
IoTEdge Device Connection String	HostName=iothub-vpnd2.azure-devices.net;DeviceId=IoT-TempDemo;St 
Docker start Container	<input type="text"/> 
Docker Registry	<input type="text"/> 

7. Click **OK**.
8. Click **Send Changes** and **Activate**.





It will take a couple of minutes until the runtime is installed and configured.

The activity is logged on the Secure Connector in **/var/log/changevirtualizationengine.log**. To verify successful installation, log into the container via SSH and run the **iotedge check** command.

Configure Docker

Configure Microsoft Docker as container engine on a Secure Connector.

1. On the Control Center, go to **your cluster** > **Cluster Settings** > **Secure Connector Editor**.
2. Click **Lock**.
3. Double-click to edit the device or Secure Connector template.
4. Make sure the container is enabled and a root password is set. For more information, see [Secure Connector Container](#).
5. Select **Docker** as the **Container Engine**. Provide the information for start container as well as for the Docker Registry the container must be pulled from.

Container Engine	
Select Container Engine	Docker 
IoTEdge Device Connection String	HostName=iothub-vpnd2.azure-devices.net;DeviceId=IoT-TempDemo;St 
Docker start Container	hello-world 
Docker Registry	hello-world 

6. Click **OK**.

7. Click **Send Changes** and **Activate**.

It will take a couple of minutes until the runtime is installed and configured.

The activity is logged on the Secure Connector in **/var/log/changevirtualizationengine.log**. To verify successful installation, log into the container via SSH and run the **docker ps** command.

Next Step

Create a Secure Connector firewall management rule to allow SSH access into the **container** zone. For more information, see [Secure Connector Container](#).

Figures

1. container_az_01.png
2. container_az_02.png
3. container_az_03.png
4. container_doc_01.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.