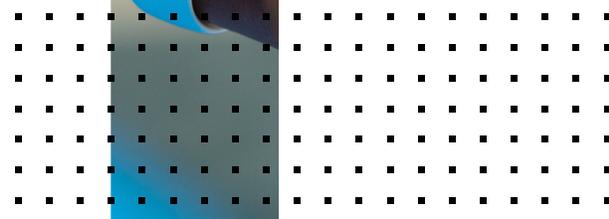
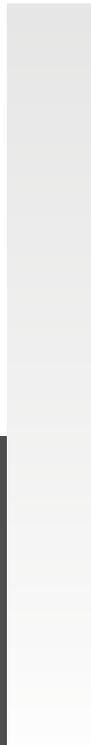
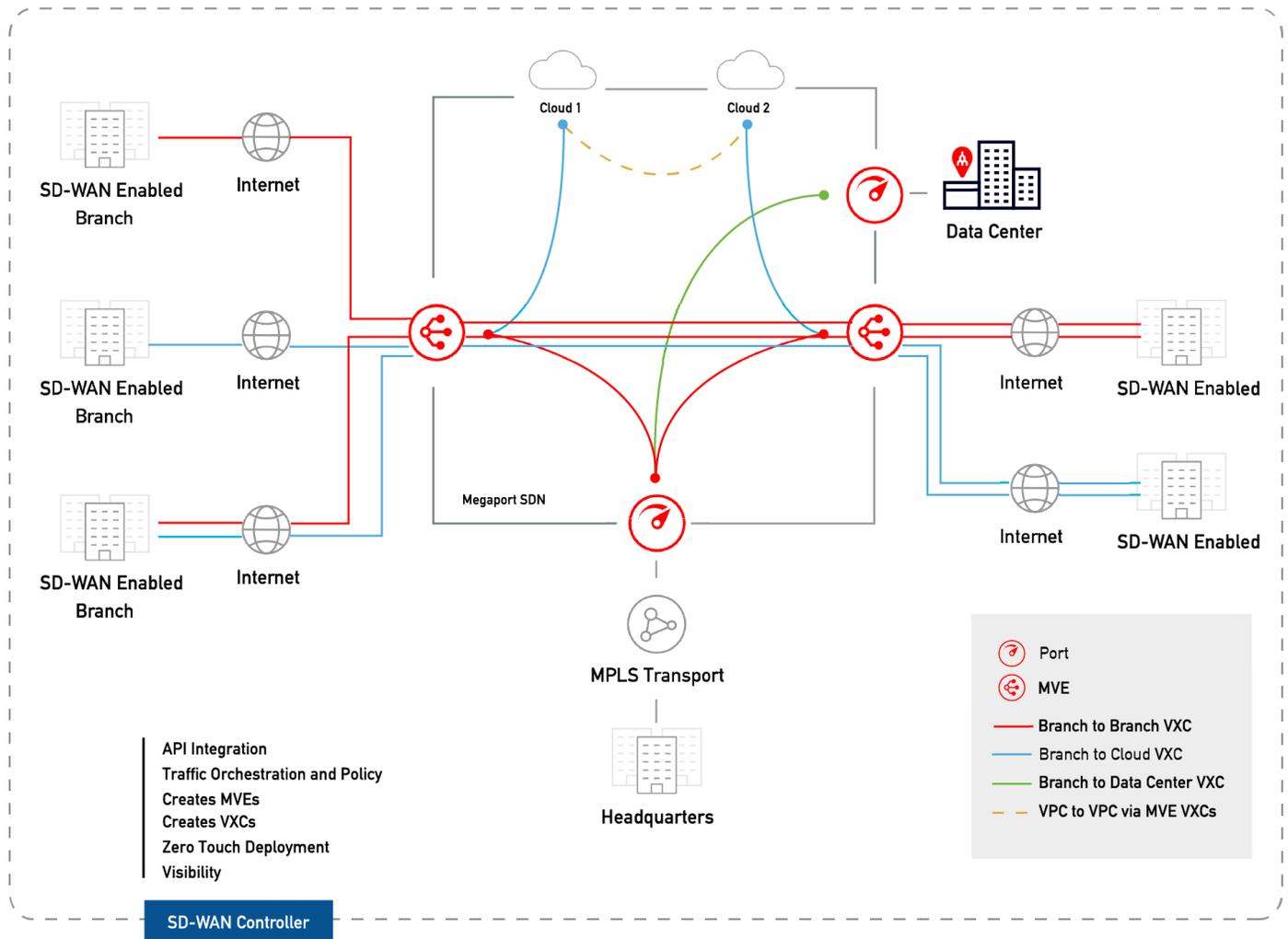


DEPLOYMENT GUIDE

Connecting MVEs Integrated With Fortinet Secure SD-WAN



This topic describes how to connect a Megaport Virtual Edge (MVE) integrated with Fortinet Secure SD-WAN to another MVE. This deployment uses the Megaport private software-defined network (SDN) to reduce reliance on the internet and connect enterprise branch locations.



With two MVEs configured, you can create a private virtual cross connect (VXC) to connect them on the Megaport network without the need for any physical infrastructure. A VXC is essentially a private point-to-point Ethernet connection between an A-End MVE and a B-End MVE.

Before You Begin

- Provision two MVEs in different locations. If you haven't already created MVEs, see [Creating an MVE in FortiManager](#) [../creating-mve/].

Creating a VXC Between Two MVEs

A private VXC deployment between two MVEs integrated with Fortinet starts in the Megaport Portal. To complete the configuration, you use the Fortinet FortiManager console.



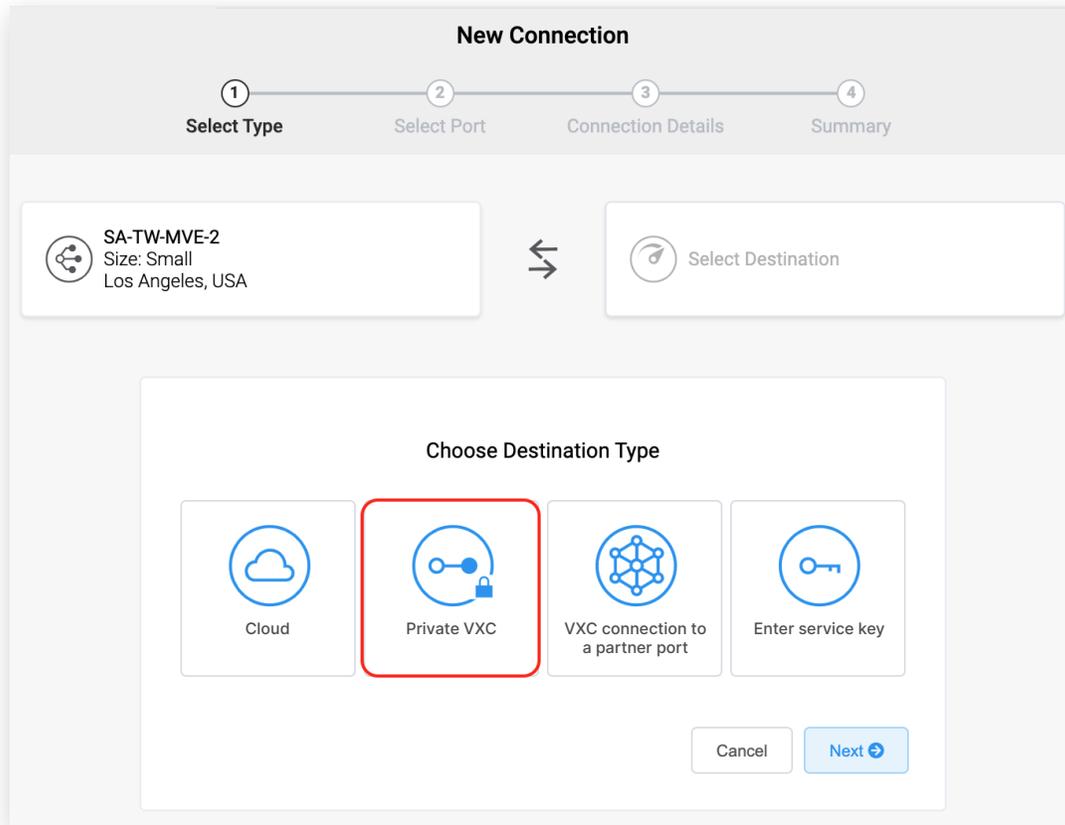
Note

FortiManager is an optional component and that FortiGate's can be deployed independently of FortiManager.



To create a VXC

1. In the [Megaport Portal](https://portal.megaport.com) [https://portal.megaport.com], go to the Services page and click +Connection next to the originating A-End MVE.
2. Select Private VXC.



3. Select the destination B-End MVE and location. Use the Country filter to narrow the selection.
4. Click **Next**.
5. Specify the VXC details:
 - **Connection Name** – Specify a name for the VXC that is easily identifiable. For example, LA MVE 2 to Dallas MVE 4. You can change the name later, if you like.
 - **Invoice Reference** (optional) – Specify an identifying number for the VXC to be used for billing purposes, such as a purchase order or cost center number.
 - **Rate Limit** – Specify a rate limit, in Mbps. The maximum speed available is limited to the smallest of the originating or destination MVE. The maximum speed is displayed.
 - **Preferred VLAN** – Specify the 802.1q VLAN tag for this connection. Each VXC is delivered as a separate VLAN on the MVE. The VLAN ID must be unique on this MVE and can range from 2 to 4093. If you specify a VLAN ID that is already in use, the system displays the next available VLAN number. The VLAN ID must be unique to proceed with the order. If you don't specify a value, Megaport will assign one.
6. Click **Next** to view the Summary screen.
7. Confirm the configuration and click **Add VXC**.
8. Click **Order** to proceed through the checkout process.



Once the VXC is deployed, you can view it in the Megaport Portal Services page. The Services page displays the VXC under the A-End MVE and the B-End MVE. Note that the service identifier number is the same for the VXC at both ends of the connection. The next step is to configure the A-End and B-End MVEs in FortiManager.

**Note**

The next procedure configures IP connectivity with BGP, providing just one solution out of many. Consult your SD-WAN vendor documentation for specific network design and configuration options before configuring interfaces for the MVEs.

Configuring the A-End MVE in FortiManager

1. Log in to your FortiManager Cloud instance at [Fortinet Support](https://support.fortinet.com) [https://support.fortinet.com].
2. Choose Services > FortiManager.
3. Select the A-End MVE.
4. Go to the System menu and choose Interface.
5. Click **+Create New > Interface**.

The screenshot shows the FortiManager web interface for configuring an interface. The breadcrumb trail is: Home > SA-TW-MVE-2 > System > Interface > Router > Display Options. The 'Edit Interface' form is displayed with the following fields and values:

- Interface Name: VLAN2500
- Alias Name: mve-2 to mve-4
- Type: VLAN
- Interface: port1
- VRF ID: 0
- VLAN ID: 2500
- Role: Undefined
- Addressing Mode: Manual (selected), DHCP, One-Arm Sniffer, PPPoE
- IP/Netmask: 10.254.253.1/255.255.255.252
- Shaping Profile: OFF
- Restrict Access: OFF
- Override Default MTU Value: OFF
- Administrative Access: HTTPS, PING, SSH, SNMP, HTTP, TELNET, FMG-Access, RADIUS Accounting, Probe Response, FTM, Security Fabric Connection
- DHCP Server: OFF (selected), Server, Relay
- VRRP: >
- Security Mode: None
- Device Management: Device Detection (OFF), Broadcast Discovery Messages (OFF), Explicit Web Proxy (OFF), Explicit FTP Proxy (OFF), Secondary IP Address (OFF)
- Map to Normalized Interface: None
- Description: (empty text area)
- Administrative Status: ON (selected)
- Scan Outgoing Connections to Botnet Sites: (dropdown menu)
- Advanced Options: >

At the bottom right of the form are 'OK' and 'Cancel' buttons.

6. Provide these details:

- **Interface Name** – Enter a name for the interface, for example, VLAN2500.
- **Alias Name** (optional) – Provide an alternate name, for example, MVE-2 to MVE-4.
- **Type** – Select VLAN.
- **Interface** – Select the parent interface: port1.
- **VLAN ID** – Enter the A-End inner VLAN.
- **Role** – Select Undefined.
- **Addressing Mode** – Select Manual.
- **IP/Netmask** – Enter the customer side IP address and netmask from the VXC details in the Megaport Portal.
- **Administrative Access** – Select how you want to access this interface, such as HTTPS, PING, and SSH.
- **DHCP Server** – Choose **OFF**.

7. Click **OK**.

The new VLAN interface appears with your port1 physical interface.

You can run an `execute ping` command from FortiOS to verify the connection.

At this point, the interface is created. The next step is to optionally create the Border Gateway Protocol (BGP) session.

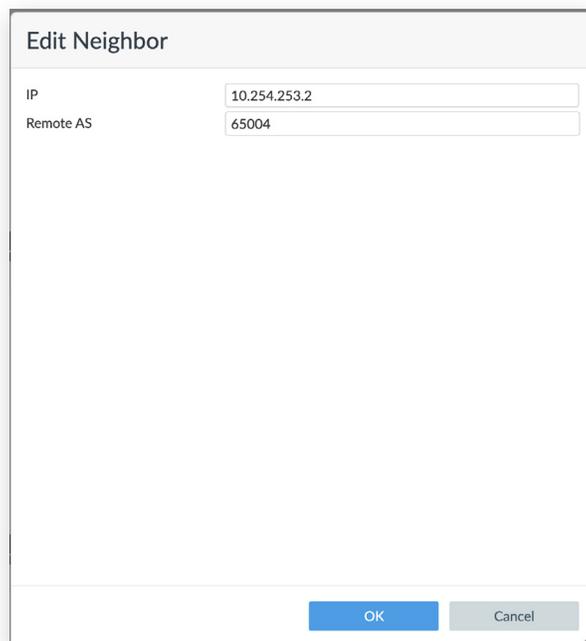
To configure a BGP neighbor

1. In FortiManager, go to **Router > BGP**.

2. Provide this information:

- **Local AS** – Enter a unique, private autonomous system number (ASN).
- **Router ID** – Enter an IP address in use on the system.

3. In Neighbors, click **+Create New**.



The screenshot shows a dialog box titled "Edit Neighbor". It contains two input fields: "IP" with the value "10.254.253.2" and "Remote AS" with the value "65004". At the bottom right, there are two buttons: "OK" (highlighted in blue) and "Cancel".

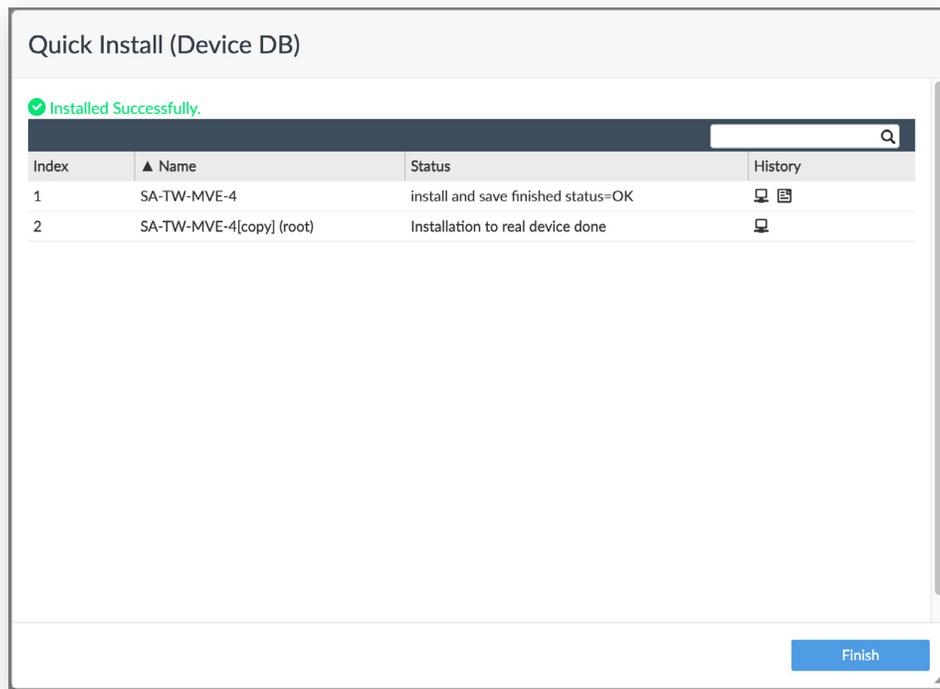
4. Enter the neighbor IP address.
5. Enter the Remote ASN.
6. Click **OK**.
7. Click **Apply**.

To push the configuration to the device

1. Choose Managed Devices.

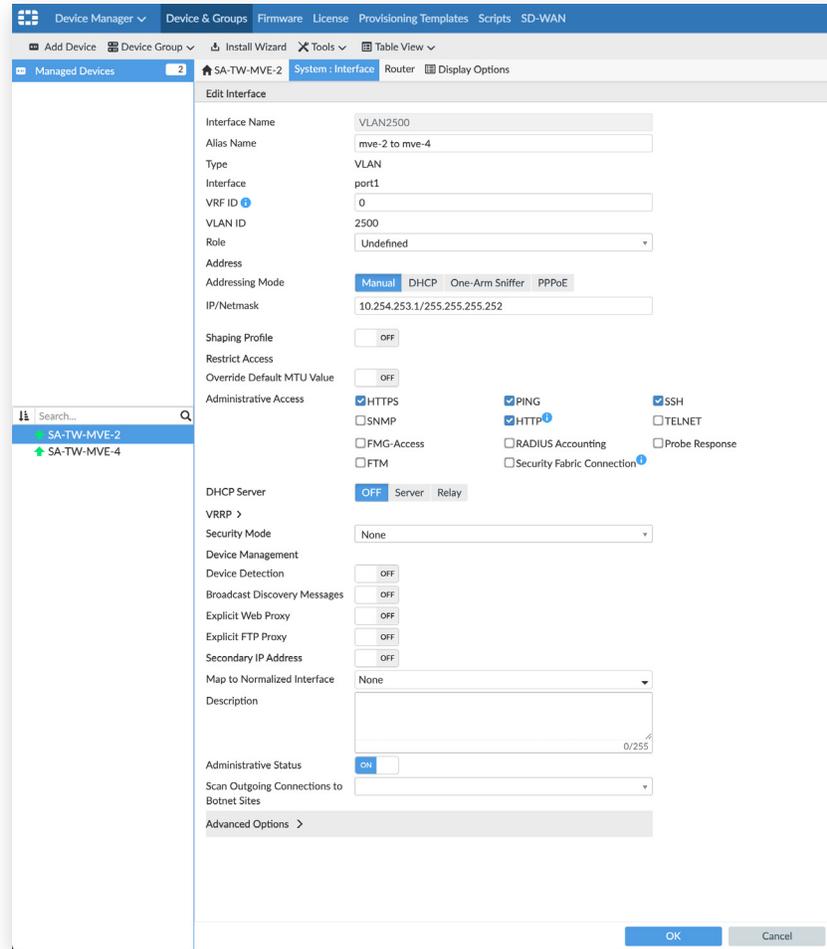
The device Config Status is Modified.

2. Select the device.
3. Choose Install > Quick Install (Device DB).
4. Click **OK**.
5. Verify a successful installation and click **Finish**.



Configuring the B-End MVE in FortiManager

1. Log in to your FortiManager Cloud instance at [Fortinet Support](https://support.fortinet.com) [https://support.fortinet.com].
2. Choose Services > FortiManager.
3. Select the B-End MVE.
4. Go to the System menu and choose Interface.
5. Click **+Create New > Interface**.



6. Provide these details:

- **Interface Name** – Enter a name for the interface, for example, VLAN2500.
- **Alias Name** (optional) – Provide an alternate name, for example, MVE-4 to MVE-2.
- **Type** – Select VLAN.
- **Interface** – Select the parent interface: port1.
- **VLAN ID** – Enter the B-End inner VLAN. Match the A-End inner VLAN.
- **Role** – Select Undefined.
- **Addressing Mode** – Select Manual.
- **IP/Netmask** – Enter the customer side IP address and netmask from the VXC details in the Megaport Portal.
- **Administrative Access** – Select how you want to access this interface, such as HTTPS, PING, and SSH.
- **DHCP Server** – Choose **OFF**.

7. Click **OK**.

The new VLAN interface appears with your port1 physical interface.

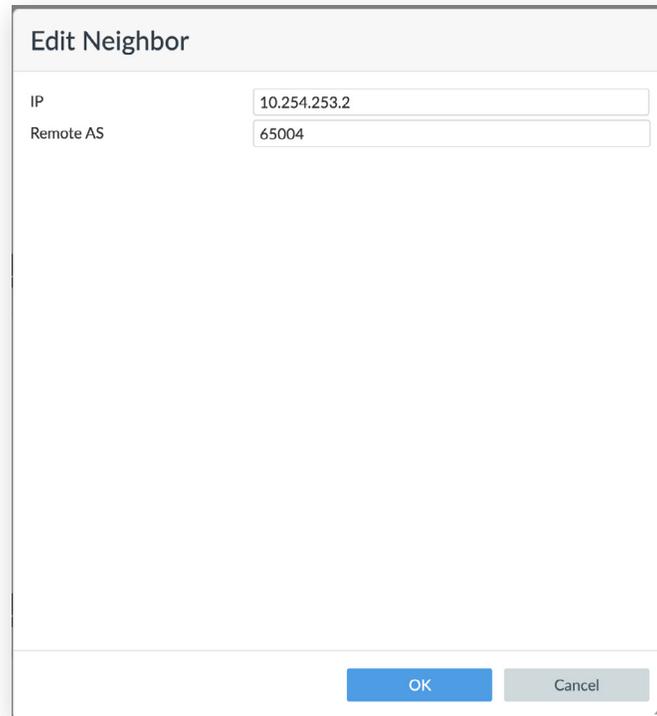
You can run an `execute ping` command from FortiOS to verify the connection.

At this point, the interface is created. The next step is to optionally create a BGP session.



To configure a BGP neighbor

1. In FortiManager, go to **Router > BGP**.
2. Provide this information:
 - **Local AS** – Enter a unique, private autonomous system number (ASN).
 - **Router ID** – Enter an IP address in use on the system.
3. In Neighbors, click **+Create New**.

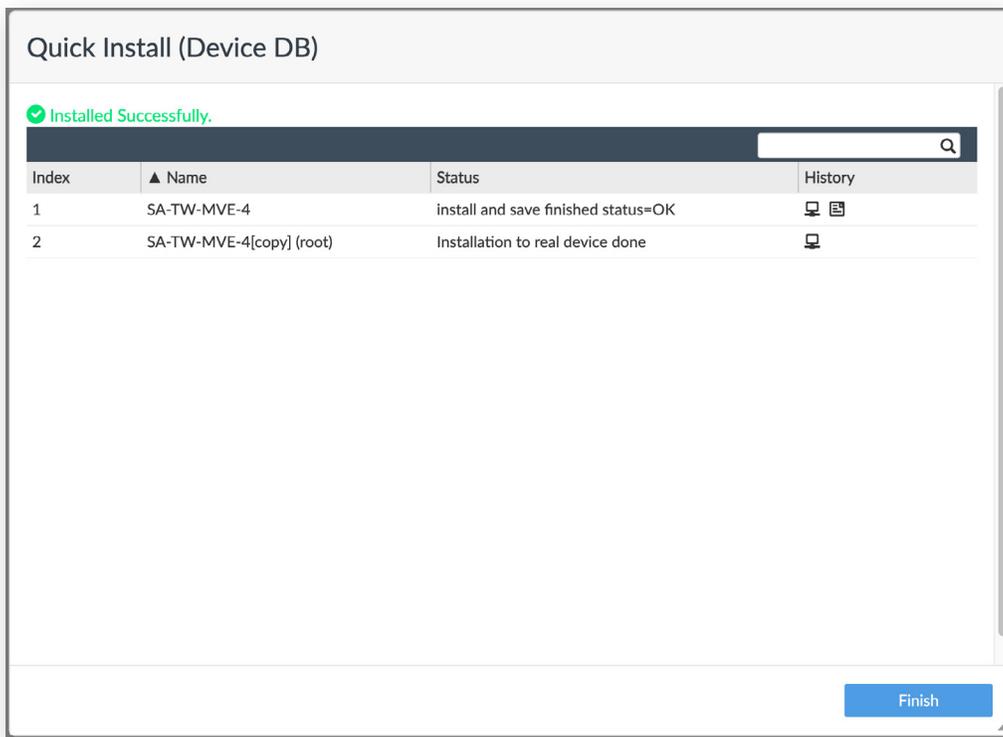


The screenshot shows a dialog box titled "Edit Neighbor". It has two input fields: "IP" with the value "10.254.253.2" and "Remote AS" with the value "65004". At the bottom right, there are two buttons: "OK" (blue) and "Cancel" (grey).

4. Enter the neighbor IP address.
5. Enter the Remote AS.
6. Click **OK**.
7. Click **Apply**.

To push the configuration to the device

1. Choose Managed Devices.
 - The device Config Status is Modified.
2. Select the device.
3. Choose Install > Quick Install (Device DB).
4. Click **OK**.
5. Verify a successful installation and click **Finish**.



Validating Your Connection

You can review connection details, including the connection state, from the CLI with these commands:

- `get system interface` – Displays configuration details and current status for the device interfaces.
- `get router info bgp neighbor <ip-address>` – Displays configuration details and current status for the BGP neighbors.