Revised: July 9, 2025

Enable Software Updates by a Remote Repository Server

Information about enabling software updates by a remote repository server

When applying software updates to devices in the network, Cisco SD-WAN Manager can use images hosted on a remote repository server. The updates may include Cisco IOS XE software updates, or other software, such as Protocol Pack updates.

A step is required to enable devices in the network to receive updates from a remote repository server. See Enable devices to receive software updates from a remote repository server, on page 1.

Enable devices to receive software updates from a remote repository server

On each WAN edge device in the network, in the tunnel configuration for the VPN 0 interface, enable the device to accept a software image from a remote repository server, using one of two methods.

- We recommend configuring an explicit ACL.
- An alternative method is to configure **allow-service all** on the devices.

Protocol to enable

During setup of a remote repository server, the server is configured to use FTP, HTTP, or SCP. Enabling edge devices in your network to receive software updates from the remote repository server requires enabling the protocol configured for the server.

- If you are using Cisco Cloud-delivered Catalyst SD-WAN (CDCS), the remote repository server uses the SCP protocol (TCP port 22). In this environment, the remote repository server address is:

  cloudopsremoterepo.sdwan.cisco.com

- If you are a tenant in a multitenancy environment, ask the provider which protocol the remote repository server uses.
- If you are using a self-hosted SD-WAN environment, check which protocol the remote repository server in your environment uses.

Temporarily enable devices to receive remote repository server updates

You can enable devices to accept software updates from a remote repository, complete the updates, and then remove the configuration to disable further updates. For example, you can use this temporary approach if you do not wish to keep the explicit ACL or **allow-service all** configurations on your devices.

Procedures

Approach A. Configure an explicit ACL:

- Configuration group
- Feature template
- CLI commands

Approach B. Use allow-service all:

- Configuration group
- Feature template
- CLI commands

Enable devices to receive software updates from a remote repository server, ACL method, using a configuration group

When applying software updates to devices in the network, Cisco SD-WAN Manager can use images hosted on a remote repository server. This procedure enables devices to receive such updates. See Information about enabling software updates by a remote repository server, on page 1 for information about which networks require this procedure.

See the alternative procedures in Enable devices to receive software updates from a remote repository server, on page 1.

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 In a Transport & Management Profile, define or modify an existing Transport VPN feature for VPN 0.

Step 3 Attach an Ethernet Interface feature to the Transport VPN feature.

Step 4 Define or modify an existing ACL IPV4 reference feature.

a) Add and name an ACL sequence.

b) Click **Add Match** and select **Destination Port**.

In some earlier releases: For **Condition**, select **Destination Port**.

c) For **Destination Port**, enter the destination port or ports that correspond to the protocol that the remote server is using.

This is 20 and 21 for FTP, 80 for HTTP, or 22 for SCP.

d) For **Action Type**, select **Accept**.

e) Save the sequence.

SD-WAN Manager returns to the Transport & Management Profile.

Step 5 In the Transport & Management Profile, in the Transport VPN area, locate the interface that supports VPN 0 for the device. For example, this may be an Ethernet Interface feature.

Step 6 Edit the feature for the interface noted in the previous step, and open the **ACL/QoS** section.

Step 7 In the **ACL** section, in the **ACL IPv4 ingress** field, add the ACL reference feature defined in an earlier step.

Step 8 Click **Save**.

Enable devices to receive software updates from a remote repository server, ACL method, using a feature template

When applying software updates to devices in the network, Cisco SD-WAN Manager can use images hosted on a remote repository server. This procedure enables devices to receive such updates. See Information about enabling software updates by a remote repository server, on page 1 for information about which networks require this procedure.

See the alternative procedures in Enable devices to receive software updates from a remote repository server, on page 1.

Note

This procedure describes the process as if no localized policy or Cisco VPN Interface Internet feature template have been configured. If you already have either of these defined for the devices requiring software update, adjust the procedure to edit the existing policy or feature template rather than creating new ones.

Step 1 Create a localized policy.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Classic** > **Policies**.
b) Select **Localized Policy**.
c) Click **Add Policy**.
d) Click **Next** multiple times to reach the **Configure Access Control Lists** step.
e) From the **Add Access Control List Policy** drop-down list, select **Add IPv4 ACL policy**.
f) Enter a name for the policy, and make note of the name for a later step where you add the policy name to a device template.
g) Add an ACL sequence.
h) For the sequence, choose **Accept** for the action, and click **Save Match and Actions**.
i) Click **Add ACL Sequence**, then **Sequence Rule**.
j) Click **Destination Port**, and enter the destination port or ports that correspond to the protocol that the remote server is using.

   This is 20 and 21 for FTP, 80 for HTTP, or 22 for SCP.

k) Click **Save Match and Actions**.
l) Click **Save Access Control List Policy**.
m) Click **Next** multiple times to reach the Policy Overview step.
n) Enter a name for the localized master policy, and make note of the name for a later step where you add the policy name to a device template.
o) Click **Save Policy**.

Step 2 Create or modify an existing Cisco VPN Interface Internet feature template for the interface that handles VPN 0.

Note If modifying an existing template, adjust the steps accordingly. First attach the policy in the Additional Template section and push the configuration to the routers. Then add the ACL name to the Ethernet interface feature template.

a) From the Cisco SD-WAN Manager menu, choose **Configuration** > **Classic** > **Templates**, then **Feature Templates**.
b) Click **Add Template**.
c) Choose a platform type.
d) Choose **Cisco VPN Interface Ethernet**.
e) In the **ACL/QoS** section, enable **Ingress ACL - IPv4**.
f) In the **Access List** field, add the name of the localized policy created in an earlier step.
g) Save the template.

Step 3 Attach the feature template for the interface, and the localized policy, to a device template.

This whole procedure is about enabling devices to get software updates from a remote repository server. So use the device template that you're pushing to those devices.

You can attach the feature template to multiple device templates if required, to address all devices for which you're enabling software updates from a remote repository server.

a) In the device template, attach the Cisco VPN Interface Internet feature template configured in an earlier step. Do this in the **Transport & Management VPN** section, in the **Cisco VPN Interface Internet** field.
b) In the device template, attach the localized policy with the ACL, created in an earlier step, in the **Additional Templates** section, in the **Policy** field.

Step 4 Push the configuration to the devices for which you are enabling updates from a remote server.

Enable devices to receive software updates from a remote repository server, explicit ACL method, using CLI commands

When applying software updates to devices in the network, Cisco SD-WAN Manager can use images hosted on a remote repository server. This procedure enables devices to receive such updates. See Information about enabling software updates by a remote repository server, on page 1 for information about which networks require this procedure.

See the alternative procedures in Enable devices to receive software updates from a remote repository server, on page 1.

Step 1 In a policy block, create an access list to allow a WAN edge device to receive remote secure copy protocol (SCP) packets.

Note This procedure does not address all details of configuring a policy.

a) Create the access list.

```
policy
  access-list access-list-name
```

b) For the access list, create a sequence for matching criteria.

Command	Value to use
source-ip	IP address of Cisco remote repository server. See the procedure prerequisites.
destination-ip	Use either 0.0.0.0 or the WAN edge device IP.
source-port	Use the destination port or ports that correspond to the protocol that the remote server is using. This is 20 and 21 for FTP, 80 for HTTP, or 22 for SCP. This configures the sequence to match SCP packets.
protocol	Use 6, for TCP.

```
sequence sequence-id
   match
    source-ip cisco-remote-repo-server-ip/32
    destination-ip {0.0.0.0 | edge-device-ip}/32
    source-port 22
    protocol 6
```

c) Accept traffic that the sequence matches.

```
action accept
```

Step 2 In an sdwan block, configure the VPN 0 interface to include the access list configured in the preceding steps.

a) Use the **sdwan** command to create an sdwan block.

```
sdwan
```

b) Use the **interface** and **tunnel-interface** commands to enter tunnel-interface configuration mode.

```
interface interface
  tunnel-interface
```

c) Use the **encapsulation ipsec** command to configure IPsec encapsulation.

```
encapsulation ipsec
```

d) Optionally, you can use the **allow-service** or **no allow-service** commands to allow or disallow services, beyond the scope of this procedure.

```
allow-service service-name
no allow-service service-name
```

e) Exit tunnel-interface configuration mode.

```
exit
```

f) Allow traffic matched by the access list created in the preceding steps. This allows SCP packets.

```
access-list access-list-name in
```

Example configuration for an explicit ACL to allow SCP packets

As described in the procedure, for the **source-ip** parameter, use the Cisco remote repository IP. This example uses a generic IP address, 10.1.1.254.

This example uses the WAN edge device IP for the **destination-ip** parameter.

```
policy
 access-list allow-remote-scp
  sequence 1
   match
    source-ip      10.1.1.254/32
    destination-ip 10.1.1.2/32
    source-port    22
    protocol       6
   !
   action accept
   !
  !
  default-action accept
 !
!
sdwan
 interface GigabitEthernet1
  tunnel-interface
   encapsulation ipsec
   no allow-service bgp
   no allow-service dhcp
   no allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   no allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
```

```
 access-list allow-remote-scp in
exit
```

Enable devices to receive software updates from a remote repository server, allow-service all method, using a configuration group

When applying software updates to devices in the network, Cisco SD-WAN Manager can use images hosted on a remote repository server. This procedure enables devices to receive such updates. See Information about enabling software updates by a remote repository server, on page 1 for information about which networks require this procedure.

We recommend the ACL policy method rather than the allow-service all method described here, in most scenarios. See the alternative procedures in Enable devices to receive software updates from a remote repository server, on page 1.

Use this procedure only on a device protected by a firewall.

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

Step 2 In a Transport & Management Profile, define or modify an existing Transport VPN feature for VPN 0.

Step 3 Attach an Ethernet Interface feature to the Transport VPN feature.

Step 4 In the Ethernet Interface feature, select Tunnel.

Step 5 In the **Allow Service** section, enable **All**.

What's next

We recommend that if you use this method, enable the updates, complete the updates, and then remove this configuration, which corresponds to the **allow-service all** CLI command.

Enable devices to receive software updates from a remote repository server, allow-service all method, using a feature template

When applying software updates to devices in the network, Cisco SD-WAN Manager can use images hosted on a remote repository server. This procedure enables devices to receive such updates. See Information about enabling software updates by a remote repository server, on page 1 for information about which networks require this procedure.

We recommend the ACL policy method rather than the allow-service all method described here, in most scenarios. See the alternative procedures in Enable devices to receive software updates from a remote repository server, on page 1.

Use this procedure only on a device protected by a firewall.

Step 1 From the Cisco SD-WAN Manager menu, choose **Configuration** > **Classic** > **Templates**, then **Feature Templates**.

Step 2 Create or edit a Cisco VPN Interface Internet feature template. If creating a new one...

a) Click **Add Template**.
b) Choose a platform type.
c) Choose **Cisco VPN Interface Ethernet**.

Step 3 In the **Tunnel** section, in the **Allow Service** section, choose **All**.

Step 4 Attach the feature template to a device template and push the configuration to the devices for which you are enabling updates from a remote server.

What's next

We recommend that if you use this method, enable the updates, complete the updates, and then remove this configuration, which corresponds to the **allow-service all** CLI command.

Enable devices to receive software updates from a remote repository server, using the allow-service all CLI command

When applying software updates to devices in the network, Cisco SD-WAN Manager can use images hosted on a remote repository server. This procedure enables devices to receive such updates. See Information about enabling software updates by a remote repository server, on page 1 for information about which networks require this procedure.

We recommend the ACL policy method rather than the allow-service all method described here, in most scenarios. See the alternative procedures in Enable devices to receive software updates from a remote repository server, on page 1.

Use this procedure only on a device protected by a firewall.

Get the IP address of the Cisco remote repository server. To do this, perform a DNS lookup for this Cisco server: cloudopsremoterepo.sdwan.cisco.com

Step 1 Use the **interface** and **tunnel-interface** commands to enter tunnel-interface configuration mode.

```
interface interface
  tunnel-interface
```

Step 2 Use the **encapsulation ipsec** command to configure IPsec encapsulation.

```
encapsulation ipsec
```

Step 3 On a WAN edge device, use the **allow-service all** command to enable the device to accept a software image from a remote repo server:

```
allow-service all
```

Example configuration using allow-service all

```
sdwan
interface GigabitEthernet1
  tunnel-interface
   encapsulation ipsec
   allow-service all
  exit
exit
```