Connecting Two Fabrics with MACsec Using QKD, Release 12.2.2

Table of Contents

New and Changed Information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
NDFC release 12.2.2	Support for connecting fabrics using inter-fabric links with MACsec using a QKD server or a preshared key	With this feature, you can connect two fabrics using inter-fabric links with Media Access Control Security (MACsec) using a quantum key distribution (QKD) server for secure exchange of encryption keys. Beginning with NDFC 12.2.2, NDFC added support for MACsec for inter-fabric links for the following fabric types: ▪ Data Center VXLAN EVPN ▪ Enhanced Classic LAN ▪ External Connectivity Network Prior to NDFC 12.2.2, NDFC supported MACsec for intra-fabric links for the Data Center VXLAN EVPN fabric and the BGP fabric. For more information about configuring MACsec with or without QKD, see About Connecting Two Fabrics with MACsec Using QKD.

About Connecting Two Fabrics with MACsec Using QKD

Media Access Control Security (MACsec) is the IEEE 802.1AE standard for authenticating and encrypting packets between two MACsec-capable devices.

With this feature, you can connect two fabrics using inter-fabric links with MACsec, either using a quantum key distribution (QKD) server for secure exchange of encryption keys, or by providing a preshared key. If you choose not to enable QKD, NDFC configures preshared keys supplied by the user instead of using quantum keys generated by the QKD server. You need to enable MACsec to enable the use of the QKD server for MACsec.

> NDFC does not manage the QKD server.

Beginning with NDFC 12.2.2, NDFC added support for MACsec for inter-fabric links for the following fabric types:

- Data Center VXLAN EVPN
- Enhanced Classic LAN
- External Connectivity Network

Prior to NDFC 12.2.2, NDFC supported MACsec for intra-fabric links for the Data Center VXLAN EVPN and the BGP fabrics.

The following sections provide information about connecting two fabrics with MACsec using QKD:

- Benefits of Connecting Two Fabrics with MACsec Using QKD
- Supported Switches and Cisco NX-OS Releases for Connecting Two Fabrics with MACsec Using QKD
- Supported Configurations for Connecting Two Fabrics with MACsec Using QKD
- Guidelines for Connecting Two Fabrics with MACsec Using QKD
- Limitations for Connecting Two Fabrics with MACsec Using QKD
- Workflow for Connecting Two Fabrics with MACsec Using QKD
- Troubleshooting Connecting Two Fabrics with MACsec Using QKD

Benefits of Connecting Two Fabrics with MACsec Using QKD

- Supports generation of quantum keys for encryption using a QKD server for protecting the privacy and authenticity of data.
- Instead of using preshared keys between the endpoints, NDFC uses the keys from the QKD server that are difficult to break.
- Helps to ensure data confidentiality by providing strong encryption at Layer 2 for VRF-Lite inter-fabric links. For more information, see the section "Create a VRF-Lite Inter-Fabric Link" in VRF Lite.

- Provides a secure connectivity association between fabrics.

Supported Switches and Cisco NX-OS Releases for Connecting Two Fabrics with MACsec Using QKD

For more information about MACsec configuration, which includes supported platforms and releases, see the Configuring MACsec chapter in the *Cisco Nexus 9000 Series NX-OS Security Configuration Guide*.

Supported Configurations for Connecting Two Fabrics with MACsec Using QKD

You can connect two fabrics with MACsec using QKD for the following use cases:

Fabric Type	Fabric Type
Data Center VXLAN EVPN	Data Center VXLAN EVPN
Data Center VXLAN EVPN	External Connectivity Network
Data Center VXLAN EVPN	Enhanced Classic LAN
Enhanced Classic LAN	Enhanced Classic LAN
Enhanced Classic LAN	External Connectivity Network

Guidelines for Connecting Two Fabrics with MACsec Using QKD

- You can change MACsec global parameters in the fabric settings at any time.
- MACsec and CloudSec can coexist on a border gateway (BGW) device.
- MACsec status of a link with MACsec enabled is displayed on the **Links** page.
- Brownfield migration of devices with MACsec configured is supported using switch and interface freeform configurations.

Limitations for Connecting Two Fabrics with MACsec Using QKD

This feature does not support the following fabric types:

- BGP
- Campus VXLAN EVPN
- VXLAN EVPN Multi-Site

This feature does not support inter-fabric links between two External Connectivity Network fabrics.

You can use a freeform configuration to achieve this use case.

Workflow for Connecting Two Fabrics with MACsec Using QKD

1. Before enabling MACsec using QKD on the fabric and the associated switches, you need to do the following:

    a. Create the RSA keys.

    b. Associate the key pair to the trust point.

    c. Get the signed certificate and upload it to NDFC. For more information, see Uploading a Certificate for Connecting Two Fabrics with MACsec Using QKD.

    d. Manually add the signed certificate to the appropriate switches.

    For more information, see the section "Configuring CAs and Digital Certificates" in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

2. Create or edit one of the supported fabric types to enable MACsec and the QKD server.

    For more information, see the following sections:

    - Editing Fabric Settings for a Data Center VXLAN Fabric for Enabling MACsec Using QKD
    - Editing Fabric Settings for an Enhanced Classic LAN Fabric for Enabling MACsec Using QKD

3. Create a VRF-Lite inter-fabric link or a Layer 2 inter-fabric link.

    For more information, see the "Create a VRF-Lite Inter-Fabric Link" section or the "Create a Layer 2 DCI Link" section in VRF Lite.

Troubleshooting Connecting Two Fabrics with MACsec Using QKD

If you cannot configure MACsec with QKD on the physical interfaces of the link, an error displays when you click **Save**.

The error may occur for the following reasons:

- You are not using the minimum required release version for Cisco NX-OS. For more information, see Supported Switches and Cisco NX-OS Releases for Connecting Two Fabrics with MACsec Using QKD.
- The interface is not MACsec-capable.

Uploading a Certificate for Connecting Two Fabrics with MACsec Using QKD

1. Navigate to the **Admin > Certificate Management > CA Certificates** tab.
2. Click the **Upload Certificate** button.

   The **Upload Certificate - CA** dialog box displays.

3. Drag and drop your CA certificate file to the dialog box or browse to the location of your certificate file.

   The following are the accepted file types:

   - .pem
   - .cer
   - .key
   - .crt
4. Click **Upload**.

Editing Fabric Settings for Connecting Two Fabrics with MACsec Using QKD

Enable MACsec on the fabric and on each inter-fabric link to configure MACsec using a quantum key distribution server (QKD).

When you enable MACsec on an inter-fabric link, NDFC uses the local fabric settings for prepopulating the MACsec parameters. Switches in an External Connectivity Network fabric take MACsec settings from a Data Center VXLAN EVPN fabric or from an Enhanced Classic LAN fabric. An External Connectivity Network fabric, Data Center VXLAN EVPN fabric, or an Enhanced Classic LAN fabric can be either the source or the destination fabric.

Each MACsec-enabled inter-fabric link includes an override option to use the link’s local settings instead of from the fabric settings. The override option, **Use Link MACsec Setting**, allows switches in external fabrics to use a different QKD server from the one used in the Data Center VXLAN EVPN fabric or the Enhanced Classic LAN fabric. NDFC autopopulates MACsec parameters from the fabric settings if the **Use Link MACsec Setting** option is not enabled.

Editing Fabric Settings for an Enhanced Classic LAN Fabric for Enabling MACsec Using QKD

1. Choose **Manage > Fabrics**.
2. Choose an **Enhanced Classic LAN** fabric.
3. From the **Actions** drop-down list, choose **Create Fabric** to create a new fabric or **Edit Fabric** to edit an existing fabric.

   If you are editing an Enhanced Classic LAN fabric, you can change MACsec parameters at any time. You need to perform a **Recalculate and Deploy** operation to generate new configurations based on the updated fabric settings.

4. Click the **Security** tab.

Field	**Description**
Enable DCI MACsec	Check the check box to enable MACsec on DCI links.
Enable QKD	Check the check box to enable the QKD server for generating quantum keys for encryption. ℹ If you choose to not enable the **Enable QKD** option, NDFC uses preshared keys provided by the user instead of using the QKD server to generate the keys. If you disable the **Enable QKD** option, all the fields pertaining to QKD are grayed out.

Field	Description
DCI MACsec Cipher Suite	Choose one of the following DCI MACsec cipher suites for the DCI MACsec policy: - **GCM-AES-128** - **GCM-AES-256** - **GCM-AES-XPN-128** - **GCM-AES-XPN-256** The default value is **GCM-AES-XPN-256**.
DCI MACsec Primary Key String	Specify a Cisco Type 7 encrypted octet string that is used for establishing the primary DCI MACsec session. For **AES_256_CMAC**, the key string length must be 130 and for **AES_128_CMAC**, the key string length must be 66. If these values are not specified correctly, an error is displayed when you save the fabric. ℹ The default key lifetime is infinite.
DCI MACsec Primary Cryptographic Algorithm	Choose the cryptographic algorithm used for the primary key string. It can be **AES_128_CMAC** or **AES_256_CMAC**. The default value is **AES_128_CMAC**. You can configure a fallback key on the device to initiate a backup session if the primary session fails.
DCI MACsec Fallback Key String	Specify a Cisco Type 7 encrypted octet string that is used for establishing a fallback MACsec session. For **AES_256_CMAC**, the key string length must be 130 and for **AES_128_CMAC**, the key string length must be 66. If these values are not specified correctly, an error is displayed when you save the fabric. ℹ This parameter is mandatory if **Enable QKD** is not selected.
DCI MACsec Fallback Cryptographic Algorithm	Choose the cryptographic algorithm used for the fallback key string. It can be **AES_128_CMAC** or **AES_256_CMAC**. The default value is **AES_128_CMAC**.
QKD Profile Name	Specify the crypto profile name. The maximum size of the crypto profile is 63.
KME Server IP	Specify the IPv4 address for the Key Management Entity (KME) server.
KME Server Port Number	Specify the port number for the KME server.
Trustpoint Label	Specify the authentication type trustpoint label. The maximum size is 64.
Ignore Certificate	Enable this check box to skip verification of incoming certificates.

Field	Description
MACsec Status Report Timer	Specify the MACsec operational status periodic report timer in minutes.

5. Click **Save** to save the fabric settings.
6. From the **Actions** drop-down list, choose **Recalculate and Deploy** to apply the new MACsec settings to links that have MACsec enabled and where the **Use Link MACsec Setting** option is disabled.

Editing Fabric Settings for a Data Center VXLAN Fabric for Enabling MACsec Using QKD

1. Choose **Manage > Fabrics**.
2. Choose a **Data Center VXLAN EVPN** fabric.
3. From the **Actions** drop-down list, choose **Edit Fabric** to edit the fabric settings.
4. Click the **Security** tab.

   The DCI MACsec parameters are the same as for the **Enhanced Classic LAN** fabric type, as the Data Center VXLAN EVPN fabric type has MACsec parameters for intra-fabric links. For more information, see Editing Fabric Settings for an Enhanced Classic LAN Fabric for Enabling MACsec Using QKD.

   For more information about the remaining fields, see the section " Creating a VXLAN EVPN Fabric Using the Data Center VXLAN EVPN Template > MACsec" in Data Center VXLAN EVPN.

5. Click **Save** to configure the MACsec with QKD feature on each switch in the fabric.
6. From the **Actions** drop-down list, choose **Recalculate and Deploy**.

Editing Fabric Settings for an External Connectivity Network Fabric for Enabling MACsec Using QKD

> ℹ With this release, no MACsec parameters are added to the External Connectivity Network fabric.

Switches in an External Connectivity Network fabric take MACsec settings from a Data Center VXLAN EVPN fabric or from an Enhanced Classic LAN fabric.

For more information, see the section " Creating an External Fabric" in External Connectivity Network.

Disabling MACsec Using QKD

The process described in this section is for disabling MACsec for an inter-fabric link for the supported fabric type. For the supported fabric types, see About Connecting Two Fabrics with MACsec Using QKD.

The following operations will disable MACsec and QKD from a link:

- Disables MACsec on the inter-fabric link using QKD or a preshared key.
- If this is the last link where MACsec is enabled, NDFC deletes the switch-level MACsec configuration from the switch.

  1. Navigate to the **Fabric Overview > Links** tab.
  2. Choose the link on which you want to disable MACsec with QKD.
  3. From the **Link Management - Edit Link** page, navigate to the **Security** tab and unselect the following options:
     - **Enable MACsec**
     - **Enable QKD**
  4. Click **Save**.
  5. From the **Fabric Overview > Switches** tab, select **Actions > Deploy** to remove the MACsec configuration from the switch.

Copyright

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.