McAfee Data Exchange Layer 6.0.x Installation Guide
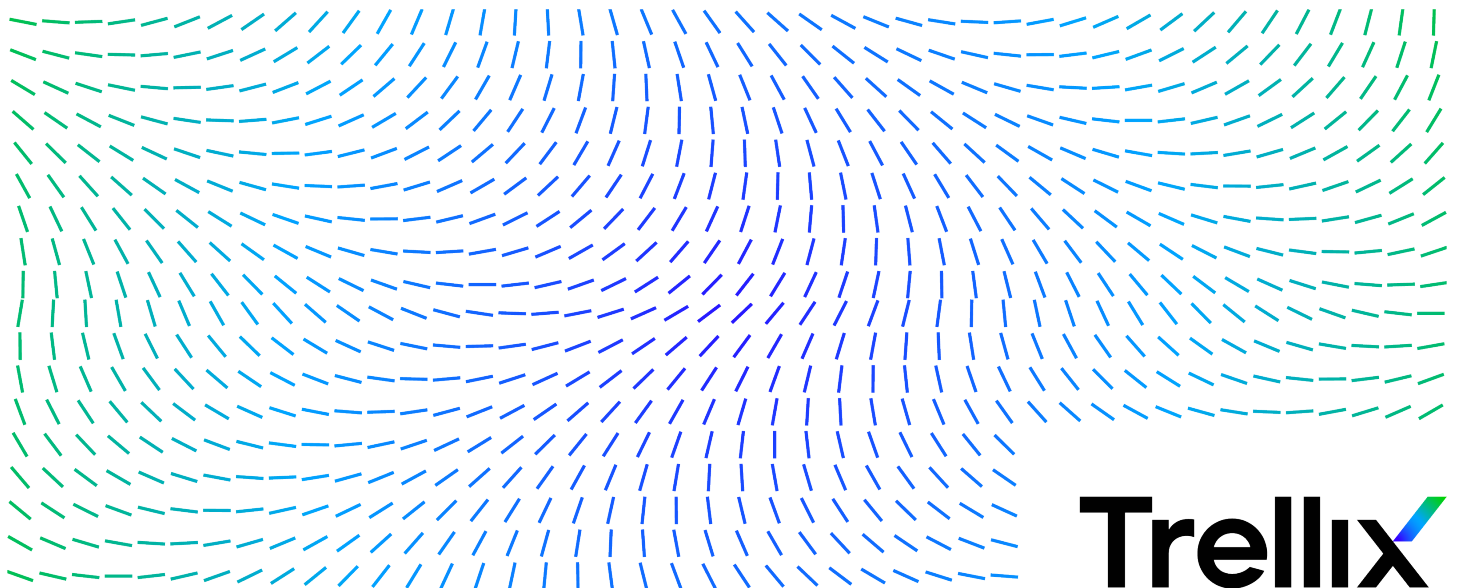
Trellix

Contents

Installation overview

Which type of installation do you need?

Determine which type of installation you need to perform: a first time installation in a new environment, or an upgrade to a newer version of McAfee® Data Exchange Layer (DXL).

Each type of installation includes a workflow of steps that must be completed in a specific order.

First-time installation workflow

DXL is installed as a McAfee ePO extension. It includes the McAfee ePO server files and DXL brokers.

When installing for the first time, you must install the components in order.
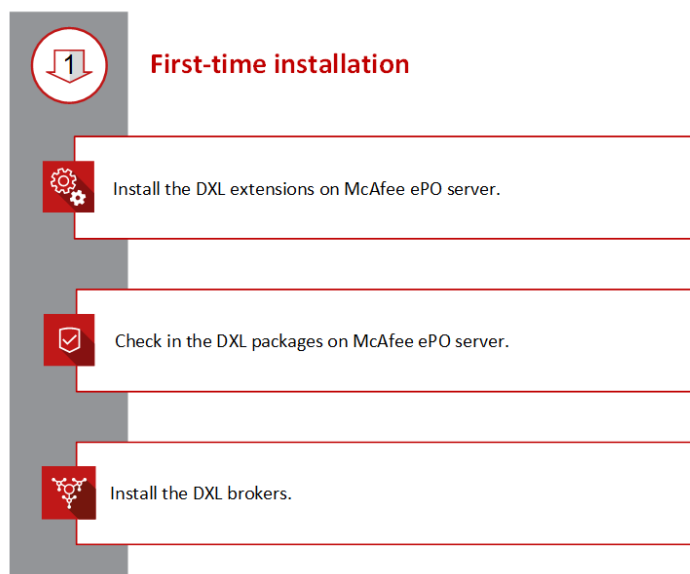
Upgrade installation workflow

To upgrade an existing installation, you install a new version of the McAfee ePO extension, server files, and DXL brokers.

Install upgrades to the DXL components in this order:

Upgrade

Upgrade the DXL extensions on McAfee ePO server.

Check in the DXL packages on McAfee ePO server.

Upgrade the DXL brokers.

Planning your installation

Things to consider before installing DXL

Before installing DXL, consider the size, the number of locations, and the unique needs of your environment. The number of brokers you install depends on the number of managed endpoints and the geographical locations of those endpoints. The DXL client is automatically installed with McAfee® Agent on each managed endpoint.

At the center of DXL is the DXL broker fabric, or framework. This is the backbone that enables the communication of events and tasks throughout your environment. Each DXL client installed on a managed endpoint connects to a DXL broker, and brokers form the fabric that sends and receives information.

Broker installation questions

Consider these questions to ask when planning a DXL installation and determining the number of brokers to install.

How many systems do you manage?

The number of systems you manage determines the number of DXL brokers to install. As a rule, you need one broker per 50,000 managed endpoints, however, it's best to have at least 2 brokers so that you have a primary and a failover broker in the event the primary broker is unavailable.

How many McAfee ePO severs in your environment?

If you have multiple McAfee ePO servers or multiple data centers, two additional brokers are required to make a Root Hub, a hub that provides a communication link between all regions. These Root Hub brokers don't accept DXL client connections and aren't counted in the overall broker scaling for the number of managed endpoints.

Do you have multiple networks?

Are your systems on a single network, or do you have different geographical locations on different networks?

Do you have a DMZ?

If you have managed endpoints that are in a DMZ, you need a broker inside the DMZ that can communicate with the DXL fabric.

Question	Answer
How many McAfee ePO servers?	2
How many managed endpoints?	10,000 endpoints per server
How many data centers or regions?	1 region with 2 data centers

Question	Answer
Do clients outside the network need access (broker in a DMZ)?	Yes

Number of brokers to install

Based on the answers to the questions, the number of brokers needed is:

- One broker for the first McAfee ePO server to support its 10,000 managed endpoints.
- One broker for the second McAfee ePO server to support its 10,000 managed endpoints.
- Two brokers for a Root Hub to connect the two McAfee ePO servers. The brokers in this hub can be managed in either data center. The Root Hub doesn't service any clients and only exists for communication between the two data centers, or provides failover if a service is temporarily unavailable.
- One broker for inside the DMZ that communicates outside of the DMZ.

Data Exchange Layer protocols and ports

The Data Exchange Layer framework uses network protocols and ports for communication between the Data Exchange Layer clients and brokers throughout your environment.

Make sure these ports are open and available for use with DXL. Port 8883 is used by default, but you can assign a different port for use with DXL.
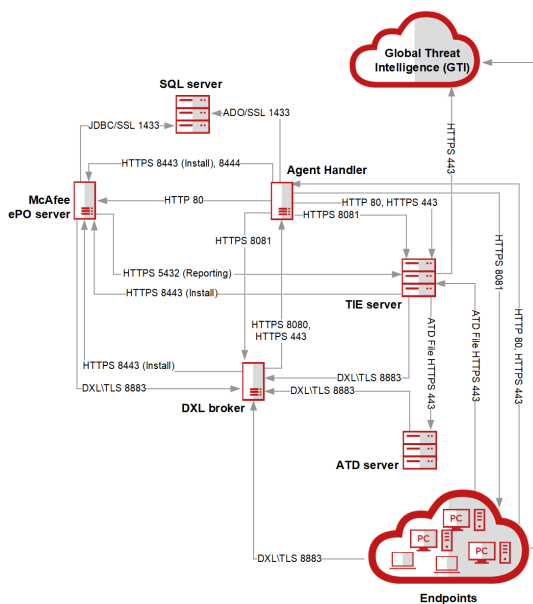
System requirements

Required software and versions

Make sure that your system environment meets all requirements and that you have administrator rights.

DXL broker requirements

Product	Minimum version	Installed on
VMware vSphere for use with MLOS brokers	ESXi 5.1	Virtual system
McAfee ePO	5.9.0	Virtual system or a physical system
McAfee® Agent Extension	5.5.0	McAfee ePO systems with brokers installed running CentOS, Red Hat, and Microsoft Windows
McAfee Agent	5.5.0	Each of the endpoints that you want to manage that are running CentOS, Red Hat, and Microsoft Windows

DXL operating system requirements

For a list of supported operating systems, see KB90421.

Hypervisor support for DXL

You can install DXL on a hypervisor virtual machine. See KB90421 for a complete list of supported hypervisor software.

Standalone DXL broker requirements

	Linux	Microsoft Windows
Recommended requirements		
Processor	4 cores	4 cores
Memory	8 GB	12 GB

	Linux	Microsoft Windows
Disk space	25 GB	20 GB
Minimum requirements		
Processor	2 cores	2 cores
Memory	4 GB	8 GB
Disk space	20 GB	20 GB

Install software for the first time

DXL is an extension to McAfee ePO. It has two components: the DXL extensions installed on the McAfee ePO server and the brokers that enable communication throughout your environment.

The tasks for installing DXL are:

1. Download the DXL software.
2. Install the DXL extensions on the McAfee ePO server.
3. Check in the DXL packages.
4. Install the DXL broker software.
5. Verify the installation.

Download the DXL software

The DXL software includes McAfee ePO server extensions and the DXL broker software.

Task

Download the DXL product software from one of these locations:
- The McAfee ePO **Software Catalog**
- The McAfee product download website

Install the extensions

Install the Data Exchange Layer extensions on the McAfee ePO server.

Task

1. Select **Menu → Software → Extensions**.
2. Click **Install Extension** and install the extensions in this order:
    - DXL Broker Management
    - DXL Client
    - DXL Client Management
    - Cisco pxGrid extension (if used)

Check in the DXL packages

Check in the Data Exchange Layer packages to the **Master Repository** on the McAfee ePO server.

Task

1. Select **Menu** → **Master Repository**, then click **Check In Package**.
2. Check in these DXL packages:

   • DXL Broker

   • DXL Platform, only if you are installing the DXL broker using an .iso or .ova file. If you are installing a broker on a Microsoft Windows Server system, or on a system running a supported operating system in Amazon Web Services (AWS), you do not have to check in the DXL Platform package.

   ⓘ **Important**

   > Before checking in the DXL Platform, the McAfee ePO product package upload limit must be increased. See KB90036 for details.

Installing the DXL broker software

Brokers are installed on virtual appliances or physical systems to send and receive messages between security products that are integrated with the DXL. The network of brokers tracks active clients and dynamically adjusts the message routing as needed.

Brokers can be installed on the same system as the McAfee ePO Server, SuperAgents, or Agent Handlers. Use one of these broker components to install DXL brokers:

   • .ova — Used to install on a VMware vSphere appliance
   • .iso — Used to install on virtual appliances (including VMware vSphere) or on a physical system
   • DXL broker package — Used to install on a Linux system, a Microsoft Windows Server system, or on a system running a supported operating system in Amazon Web Services (AWS)

Deploying brokers only on systems with specific operating systems

In McAfee ePO 5.x and McAfee Agent 5.x and later, when deploying a broker using a **Product Deployment** task, the deployment task does not consider the **Target platform** (operating system) option on the **Product Deployment** page. The brokers are installed on all supported systems, regardless of the operating system selection. This occurs on Microsoft Windows systems and Linux systems. There are two workarounds you can use to ensure the brokers are installed only on those systems you want. See KB 91361 for details.

Install DXL brokers on a VMware vSphere appliance

Using the .ova file, you can install the DXL brokers on a VMware vSphere virtual system.

Before you begin

Extract the downloaded .ova .zip file before starting.

Task

1. Open the VMware vSphere client, then click **File → Deploy OVF Template**.
2. Browse to and select the DXL .ova file on your computer and complete the steps in the wizard.
3. Install and configure the DXL broker appliance.
   a. Read and accept the license agreement.
   b. Create a root password for the appliance (minimum 9 characters).
   c. Enter the operational account name, real name, and password. When finished, enter **Y** to continue.
      The account name is typically something like `jsmith` and is used to log on to and administer the appliance. The real name is your full name, for example, `John Smith`.
   d. On the **Network Selection** page, enter **N** to continue.
   e. Select a configuration type, then enter **Y** to continue.

      • DHCP — Enter **D**.
      • Manual IP address — Enter **M**, then enter the remaining information.

   f. Enter the host name and domain name of the computer where you are installing the appliance, then enter **Y**.
   g. Enter up to 3 Network Time Protocol servers to synchronize the time of the appliance, then enter **Y**.
      Use the default server listed, or enter the address.
   h. Enter the IP address or fully qualified domain name, port, and account information for your McAfee ePO server, then enter **Y**.
      The user account must have administrator rights.
   i. In a web browser, navigate to McAfee ePO and verify that the McAfee ePO server certificate's Common Name (CN) and fingerprint match the information shown.
      Verifying certificates depends on your browser. For most browsers, click the Lock icon in the address bar to view certificate details.
   j. Specify the port that DXL uses, then enter **Y**.
      Use the default port or enter a port number within the range shown.
   k. When the logon screen appears, close it.
4. Log on to McAfee ePO as an administrator and verify that a DXL broker is listed in the **System Tree**.
5. Click **Wake Up Agents**, select **Force complete policy and task update**, then click **OK**. It might take a few minutes for the broker properties to be sent to the appliance.

Install DXL brokers using the .iso file

Using the .iso file, you can install the DXL brokers on several types of virtual appliances (including VMware vSphere) and physical systems.

Before you begin

Extract the downloaded .iso .zip file.

Task

1. Browse to and select the DXL .iso file.
2. Install and configure the DXL broker appliance.
   a. Read and accept the license agreement.
   b. Create a root password for the appliance (minimum 9 characters).
   c. Enter the operational account name, real name, and password. When finished, enter **Y**.
      The account name is typically something like `jsmith` and is used to log on to and administer the appliance. The real name is your full name, for example, `John Smith`.
   d. On the **Network Selection** page, enter **N**.
   e. Select a configuration type, then enter **Y**.

      • DHCP — Enter **D**.
      • Manual IP address — Enter **M**, then enter the remaining information.

   f. Enter the host name and domain name of the computer where you are installing the appliance, then enter **Y** to continue.
   g. Enter up to 3 Network Time Protocol servers to synchronize the time of the appliance, then enter **Y**.
      Use the default server listed, or enter the address.
   h. Enter the IP address or fully qualified domain name, port, and account information for your McAfee ePO server, then enter **Y**.
      The user account must have administrator rights.
   i. In a web browser, navigate to McAfee ePO and verify that the McAfee ePO server certificate's Common Name (CN) and fingerprint match the information shown.
      Verifying certificates depends on your browser. For most browsers, click the Lock icon in the address bar to view certificate details.
   j. Specify the port that DXL uses, then enter **Y**.
      Use the default port or enter a port number within the range shown.
   k. When the logon screen appears, close it.
3. Log on to McAfee ePO as an administrator and verify that a DXL broker is listed in the **System Tree**.
4. Click **Wake Up Agents**, select **Force complete policy and task update**, then click **OK**. It might take a few minutes for the broker properties to be sent to the appliance.

Install DXL brokers on a Linux system

You can install the DXL brokers on a managed Linux system using a McAfee ePO deployment task.

Task

1. In McAfee ePO, select **Menu → Software → Product Deployment**, then click **New Deployment**.
2. Complete the new deployment information, then start the deployment.
3. When the deployment task finishes, configure the broker.

a. To use a communication port other than the default 8883, update the DXL broker configuration file /opt/McAfee/dxlbroker/conf/dxlbroker.conf. Change the listenPort setting.

```
# The broker listen port
listenPort=port number
```

b. Update the firewall to allow communication on the broker port with the commands for your platform (replace <listenPort> with the correct port).

- Red Hat Enterprise Linux 6.x / CentOS 6.x

```
iptables -N DXLBROKER
iptables -I INPUT -j DXLBROKER
iptables -A DXLBROKER -p tcp -m tcp --dport <listenPort> -j ACCEPT
service iptables save

ip6tables -N DXLBROKER
ip6tables -I INPUT -j DXLBROKER
ip6tables -A DXLBROKER -p tcp -m tcp --dport <listenPort> -j ACCEPT
service ip6tables save
```

- Red Hat Enterprise Linux 7.x / CentOS 7.x

```
firewall-cmd --zone=public --permanent --add-port=<listenPort>/tcp
firewall-cmd --reload
```

c. Restart the DXL Broker service.

```
$> service dxlbroker restart
```

4. (Optional) For troubleshooting, use the log files for installing and deploying brokers on a Linux system.
   - /var/log/dxlbroker <version_number> <build_number>.log
   - /var/log/dxlbroker-uninstall.log

5. In the McAfee ePO **System Tree**, select the broker system and click **Wake Up Agents**, select **Force complete policy and task update**, then click **OK**. It might take a few minutes for the broker properties to be sent to the appliance.

Install DXL brokers on a Microsoft Windows Server

DXL brokers can be installed on a Microsoft Windows Server system using a McAfee ePO deployment task.

Task

1. In McAfee ePO, select **Menu → Software → Product Deployment**, then click **New Deployment**.
2. Complete the new deployment information, then start the deployment.

Install DXL brokers on a system running in AWS

DXL brokers can be installed on a system that is using any of the supported operating systems running in Amazon Web Services (AWS).

You must establish and maintain a VPN connection between the on-premise infrastructure for the DXL client and the AWS infrastructure for the DXL brokers. This VPN connection must be established full time to maintain connectivity between the brokers and the clients.

See the installation instructions for the specific operating system that you're using in AWS for details about installing brokers on that system.

Verify the DXL installation

After you install and deploy the DXL broker, verify that the installation was successful and that the brokers are connected to the DXL clients on the managed endpoints.

Task

1. On the **System Tree** main page, verify that the broker is listed and tagged as **DXLBROKER**.
   If it isn't tagged as **DXLBROKER**, run the **Manage DXL Brokers** server task.
2. In the **System Tree**, select the DXL broker name, then click the **Products** tab to verify that the DXL broker and version are listed.
   If the DXL broker and version aren't listed, click **Wake Up Agents**, select **Force complete policy and task update**, then click **OK**. It might take a few minutes for the broker properties to be sent to the appliance.

Results

When the installation is successful, the installed brokers are tagged as **DXLBROKER** and the correct DXL version is displayed in

the **Products** tab. When you click the McAfee shield icon in the Windows taskbar, the **McAfee Data Exchange Layer** heading displays the broker connection status, and the broker name, address, and port number that the DXL client is connected to.

Upgrading to a new software version

Install DXL upgrades when they are available to get the latest features, enhancements, and security protection.

Before upgrading Data Exchange Layer, if using a Hypervisor virtual machine, create a snapshot of your virtual machine. If using a Linux system, back up your system.

ⓘ **Important**

The C:\ProgramData\Package Cache\ folder and files, where the WiX installer stores its bundle and other data, must not be removed from systems running DXL. When upgrading DXL, this bundle is used to uninstall the previous version of DXL as part of the upgrade process. If the bundle isn't there, DXL upgrades will fail. Ensure that system users, administrators, or disk cleanup utilities are not deleting files in this folder to free up disk space.

The tasks for updating DXL are:

1. Download the DXL software.
2. Upgrade the DXL extensions on the McAfee ePO server.
3. Check in the DXL packages.
4. Upgrade the DXL broker software.
5. Verify the upgrade.

Upgrade the DXL extensions in McAfee ePO

Install the Data Exchange Layer extension upgrades on the McAfee ePO server.

Before you begin

Make sure that you've downloaded the latest DXL software extension.

ⓘ **Important**

If you are upgrading the DXL C++ Client on Microsoft Windows systems from a version older than DXL 2.1.0 (not including 2.1.0), you must first upgrade the C++ client. Upgrade the client to any DXL version between 2.1.0 and 4.0.0 before upgrading to a newer version.

ⓘ **Important**

The DXL extension version must be the same or newer than the DXL broker version. You can't install an older extension version with a newer broker version.

Task

1. Select **Menu → Software → Extensions**.

2. Click **Install Extension** and install the extensions in this order:

   - DXL Broker Management
   - DXL Client
   - DXL Client Management
   - Cisco pxGrid extension (if used)

Upgrade DXL brokers

The method you used to install the broker initially determines the upgrade steps.

Before you begin

Make sure that you've checked-in the latest DXL packages to the **Master Repository** on the McAfee ePO server.

- To upgrade DXL brokers that were installed using an .ova or .iso appliance, create a product deployment task in McAfee ePO to install the DXL platform and the broker.
- To upgrade brokers that were installed on CentOS, Red Hat, or on a Microsoft Windows system, create a product deployment task in McAfee ePO to install the DXL the broker only.

💡 **Tip**

In McAfee ePO 5.x and McAfee Agent 5.x and later, when deploying a broker using a **Product Deployment** task, the deployment task does not consider the **Target platform** (operating system) option on the **Product Deployment** page. The brokers are installed on all supported systems, regardless of the operating system selection. There are two workarounds you can use to ensure the brokers are installed only on those systems you want. See KB 91361 for details.

Task

1. Select **Menu → Software → Product Deployment**.
2. Select **New Deployment**.
3. Complete the new deployment information for the DXL broker.

   Create a task for each package. If installing both packages, they must be updated in this order:

   - DXL platform
   - DXL broker

4. Save the task and run it against the DXL broker.
5. In the **System Tree**, select a DXL broker name, then on the **Properties** tab, click **Wake Up Agents** and select **Force complete policy and task update**.

   It might take a few minutes for the broker properties to be sent to the appliance.
6. (Optional) For troubleshooting, use the log files.

   /var/log/dxlbroker-<version_number>-<build_number>.log

/var/log/DXLPlatform-<version_number>-<build_number>-<timestamp>.log

/var/McAfee/dxlbroker/logs/ipe-start.log

/var/McAfee/dxlbroker/logs/ipe.log

C:\ProgramData\McAfee\dxlbroker\logs\dxlbroker.log

C:\ProgramData\McAfee\dxlbroker\logs\ipe.log

Verify the DXL broker upgrade

After you complete the DXL upgrade, verify that the upgrade was successful.

Task

In the **System Tree**, select the DXL broker name, then click the **Products** tab to verify that the DXL broker and version are listed. If the DXL broker and version aren't listed, click **Wake Up Agents**, select **Force complete policy and task update**, then click **OK**. It might take a few minutes for the broker properties to be sent to the appliance. If the **DXLBROKER** tag doesn't appear in the **System Tree**, run the **Manage DXL Brokers** server task again.

Results

When the upgrade is successful, the installed brokers are tagged as **DXLBROKER** and the correct DXL version is displayed in the

Products tab. When you click the McAfee shield icon in the Windows taskbar, the **McAfee Data Exchange Layer** heading displays the broker connection status, and the broker name, address, and port number that the DXL client is connected to.

Troubleshooting the installation

McAfee provides log files and scripts that can help you resolve common issues that might occur during installation.

Accessing log files

To troubleshoot installation problems, view the log files. Depending on your operating system, have these files available if you contact Technical Support.

/var/log/dxlbroker-<version_number>-<build_number>.log

/var/log/DXLPlatform-<version_number>-<build_number>-<timestamp>.log

/var/McAfee/dxlbroker/logs/ipe-start.log

/var/McAfee/dxlbroker/logs/ipe.log

C:\ProgramData\McAfee\dxlbroker\logs\dxlbroker.log

C:\ProgramData\McAfee\dxlbroker\logs\ipe.log

Reconfiguring the installation using scripts

You can use scripts to reconfigure the DXL brokers and McAfee Agent installed using an .ova or .iso file. The scripts are located in the /home/<username> directory. They must be executed with sudo permissions, for example:

sudo /home/myname/reconfig-dxl.

Script name	Description	Reboot?
change-hostname	Changes the host name of the current DXL broker appliance. It restarts the McAfee Agent and the broker.	Recommended
change-services	Enables or disables the DXL broker. If the broker was initially disabled during first boot, the script prompts for broker configuration information.	No
reconfig-dxl	Reconfigures the DXL port.	No
reconfig-ma	Reconfigures the McAfee Agent.	Recommended

Script name	Description	Reboot?
	The agent and DXL broker services are restarted. New keystores are generated when the service starts. ✏ **Note:** Do not run this script on a broker in a McAfee ePO environment that is in the process of migrating certificates. During the certificate regeneration process, running the script creates a new certificate chain causing connection issues. Before using this script, read KB85043 for important information.	
reconfig-network	Reconfigures the current network interface (from DHCP to manual, or from manual to DHCP).	Required
reconfig-ntp	Reconfigures the Network Time Protocol servers.	No

Remove the DXL software

Uninstall DXL brokers

You can uninstall DXL brokers that were installed on a Linux or Microsoft Windows system. You cannot uninstall brokers that were installed using an .ova or .iso file.

Task

1. Select **Menu → Software → Product Deployment → New Deployment**.
2. Complete and save the new deployment information for the uninstall.
3. In the **Product Deployment** page, from the **Action** drop-down, select **Uninstall**. Then start the deployment to uninstall DXL.

COPYRIGHT