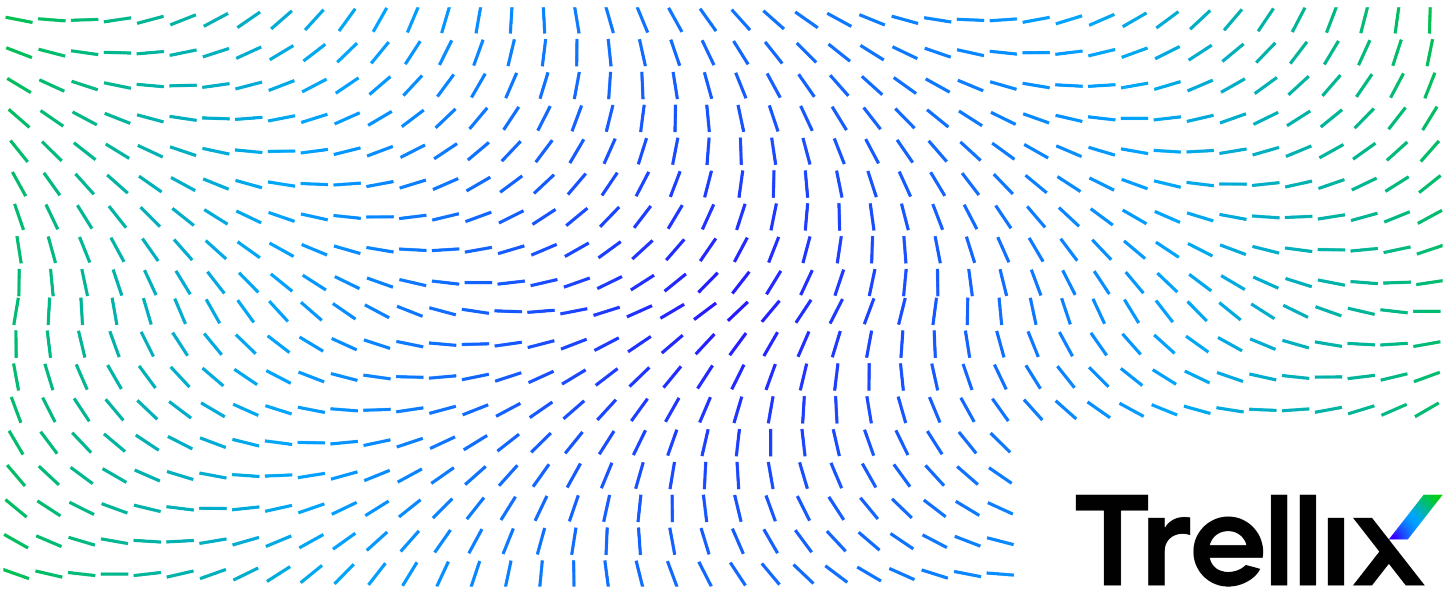
McAfee Active Response 2.4.x Installation Guide



Trellix

Contents

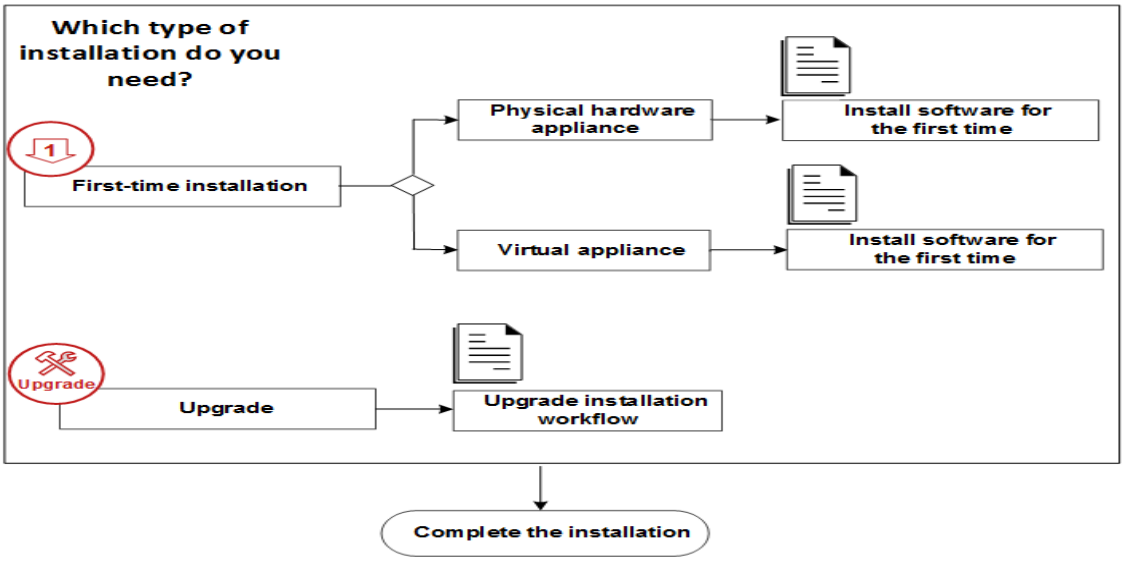
Installation overview

Which type of installation do you need?

McAfee® Active Response installation includes installing or upgrading a single appliance or multiple consolidated appliances to host services such as Active Response, McAfee® Data Exchange Layer (DXL), McAfee® Threat Intelligence Exchange (TIE).

Caution

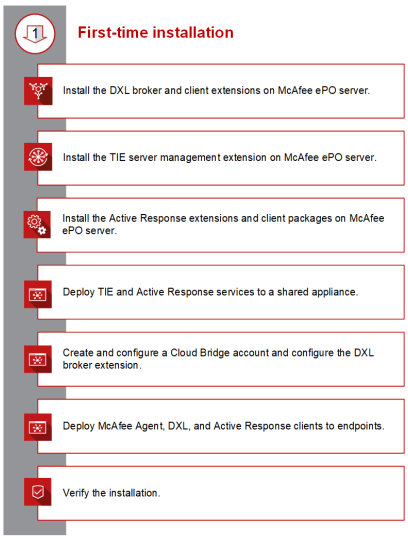
Upgrading the software requires a one-time migration of the legacy Active Response appliance. For more information, see the Upgrade Installation workflow section.



First-time installation workflow

To install Active Response, you must install the extensions, components, and client packages in a specific order.

Active Response, TIE, and DXL servers can co-exist on a single appliance, reducing server maintenance.



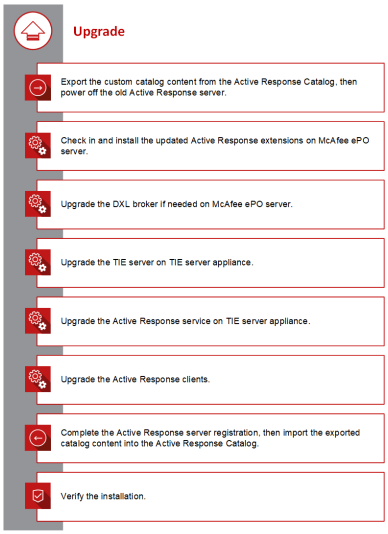
Upgrade installation workflow

When upgrading Active Response to a newer version, only those components that have updates in the package are upgraded.

Caution

Upgrading the software requires a one-time migration of the legacy Active Response appliance.

Before you upgrade, export your custom collectors, reactions, triggers, and searches from the Active Response Catalog.



System requirements

Server, hardware, and client requirements

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

Note

For a complete list of components, supported platforms, environments, and operating systems for Active Response, see KB84473.

Server minimum requirements

You can configure a single and consolidated server to host multiple services, such as Active Response, DXL, and TIE. Multiple servers can be deployed as backup servers to increase capacity.

The server can be installed on a physical server or a virtual machine. All servers can run simultaneously in a single appliance for small deployments.

Minimum requirements for McAfee® Linux Operating System (MLOS)

- Version — MLOS version 2. For more information about MLOS packages, see https://mcafeelinux.org/.
- Processor — 1 CPU with 8 cores
- Memory — 16-GB RAM
- Hard drive — 150-GB solid-state disk
- ISO — Yes
- Hardened — Yes

Note

These recommendations vary on systems with Meltdown updates, see KB90333 for the latest details.

Hardware minimum requirements based on operating system

Operating system	Version	Architecture	Processor	RAM	Free hard disk space
Windows 10 Enterprise	Base	32-bit and 64-bit	2 GHz or higher	3 GB	1 GB
Windows 8.1 Enterprise	Base, U1	32-bit and 64-bit	2 GHz or higher	3 GB	1 GB
Windows 8.0	Base	32-bit and 64-bit	2 GHz or higher	3 GB	1 GB

Operating system	Version	Architecture	Processor	RAM	Free hard disk space
Windows 7 Enterprise	Up to SP1	32-bit and 64-bit	1.4 GHz or higher	2 GB	1 GB
Windows 7 Professional	Up to SP1	32-bit and 64-bit	1.4 GHz or higher	2 GB	1 GB
Windows Server 2019	Base	64-bit only	2 GHz or higher	3 GB	1 GB
Windows Server 2016	Base	64-bit only	2 GHz or higher	3 GB	1 GB
Windows Server 2012	Base, R2, U1	64-bit only	2 GHz or higher	3 GB	1 GB
Windows Server 2008 R2 Enterprise	SP1	64-bit only	2 GHz or higher	3 GB	1 GB
Windows Server 2008 R2 Standard	SP1	64-bit only	2 GHz or higher	3 GB	1 GB
CentOS	6.6 - 8.0	64-bit only	2 GHz or higher	2 GB	1 GB
Red Hat	6.6 - 7.8, and 8.0	64-bit only	2 GHz or higher	2 GB	1 GB
macOS	Catalina 10.15 Mojave 10.14 High Sierra 10.13 Sierra 10.1 El Capitan 10.11	64-bit only	2 GHz or higher	2 GB	1 GB

Endpoint client minimum requirements

Product	Windows	Linux	macOS
McAfee ePO	5.3.1	5.3.1	5.3.1

Product	Windows	Linux	macOS
McAfee® Agent	5.0.3 (< RS2) 5.0.5 (RS2/RS3)	5.0.5.658	5.0.5.658 (El Capitan and Sierra) 5.0.6.347 (High Sierra)
Data Exchange Layer	3.0.0 + HF3 (< RS2) 3.1.0 (RS2/RS3)	3.0.0 + HF3	3.0.0 + HF3
Endpoint Security Threat Prevention with Threat Intelligence module		10.2.2**	
Endpoint Security with Adaptive Threat Protection	10.5.0 (< RS2) 10.5.1 (RS2) 10.5.3 (RS3)*		10.5.0***
Microsoft Windows 10 (version 1607) - Anniversary Update (Redstone 1 [RS1]) Microsoft Windows 10 (version 1703) - Creators Update (Redstone 2 [RS2]) Microsoft Windows 10 (version 1709) - Fall Creators Update (Redstone 3 [RS3]) Microsoft Windows 10 (version 1803) - Spring Creators Update (Redstone 4 [RS4])			

*If you have Redstone 3 endpoints, McAfee® Endpoint Security 10.5.3 must be checked in to the **Master Repository**.

**Install McAfee Endpoint Security 10.2.2 on Linux endpoints.

***Install Endpoint Security 10.5.0 for macOS.

Note

If an endpoint doesn't currently have a version of Endpoint Security or McAfee VirusScan Enterprise, the appropriate version of the Endpoint Security modules is installed automatically with the Active Response installation. If an endpoint currently has an unsupported version of Endpoint Security, upgrade the modules on the endpoint to a supported version.

Required network ports

Active Response uses specific ports to connect to McAfee Agent, Active Response clients, and Active Response server.

Caution

Make sure your network settings aren't blocking access to the Active Response server and clients through these ports.

For information about default ports used with TIE server, see the *McAfee Threat Intelligence Exchange Installation Guide*.

For details about the default ports required for each component in McAfee ePO, see KB66797.

Server ports

Port number	Open to	Incoming connections	Outgoing connections
8443	Connect the McAfee ePO extensions to the Active Response server	Yes	Yes
8883	Connect the external DXL broker and DXL client to the server	Yes	Yes
8081	Connect McAfee Agent to the McAfee ePO server	Yes	Yes
22	Connect remotely through SSH to perform maintenance tasks	Yes	Yes
123 UDP	Network Time Protocol	Yes	Yes

Client ports

Port number	Open to	Incoming connections	Outgoing connections
8081	Connect McAfee Agent to a McAfee ePO server	Yes	Yes
8883	Connect the DXL client to a DXL broker	Yes	Yes

Pre-installation tasks

Download extensions

The required extensions and packages are available on the McAfee downloads site.

Before you begin

Locate the grant number you received after purchasing the product.

For McAfee ePO 5.10, you can use **Software Catalog** to view, download, and install the software.

Task

1. In a web browser, go to https://www.mcafee.com/us/downloads/downloads.aspx.
2. Click **Download**. Enter your grant number, then select the product and version.
3. On the **Software Downloads** tab, select and save the appropriate file.

File description	File name
Active Response extension	Active_Response_MAR_2.4.0_Build_number_(ENU-RELEASE-MAIN).zip
Server package for Active Response	ActiveResponseServer-2.4.0-Build_number.zip
Server Deployment package	ServerDeployment_2.3.0_Build_number Package #number (ENU-LICENSED-RELEASE-MAIN).zip

Increase the McAfee ePO maximum upload size

To install the Active Response server package, you must first increase the maximum upload size in McAfee ePO server properties.

Caution

This update is required only for manual check-in of the packages using remote McAfee ePO commands. The update requires restarting the McAfee ePO server. Users don't have access during the restart process.

Task

1. Log on to McAfee ePO as administrator.
2. Go to C:\Program Files (x86)\McAfee\ePolicy Orchestrator\Server\conf\orion.

3. Right-click the orion.properties file and edit with any text editor.
4. In the file, locate orion.upload.max.size, change the value to `768435456`, and save the file.
5. Restart the McAfee ePO server application on your virtual machine or physical server.
   During the restart process, McAfee ePO services aren't available to users.

Results

You can now check in the Active Response server package.

When checking in the packages via McAfee ePO console, you can edit the epo.properties file to specify `file.upload.limit` . For more information, see KB90723.

Install software for the first time

Install the Active Response extensions

To start using Active Response to detect and remediate threats, you must first install Active Response extensions and the related components on McAfee ePO.

Before you begin

- Verify that the system requirements for Active Response are met.
- Make sure you have installed McAfee Agent and that Endpoint Security is checked in to the **Master Repository** and installed on the endpoints.
- Prepare a virtual machine for Active Response, DXL broker, and TIE server. See their respective installation guides for instructions.
- For manual package check-in, increase the upload file size limit in the McAfee ePO Orion properties.

Note

Increasing the file size limit is required only for manual check-in of the packages. The update requires restarting the McAfee ePO server. Users don't have access during the restart process. But, if you are installing the extensions via Software Catalog, you don't have to restart the McAfee ePO server.

Task

1. Log on to McAfee ePO as an administrator.
2. Install the DXL broker and client extensions. See the product's installation guide for instructions.
3. Install the TIE server management extension. See the product's installation guide for instructions.
4. Install Active Response extension on McAfee ePO version 5.10:
   a. For automatic product installation, select **Menu** → **Software** → **Software Catalog**.

      Note

      If you enabled **Automatic Product Installation** when you installed McAfee ePO, the licensed products are installed automatically.

   b. Search for and select the required product packages on the **Software Catalog** page.
   c. Accept the license agreement and click **Check in** to install the package.
5. To manually check in and install the extensions on McAfee ePO:
   - Select **Menu** → **Software** → **Extensions**, select the extension and click **Install Extension**.

   For manual check-in, install the bundles in this order to avoid compatibility issues.
   a. DXL broker management extension
   b. TIE server management extension

c. Active Response extension
d. DXL client extension
e. Active Response Workspace extension
f. Active Response client extension
g. Server deployment extension

Note

The Server Deployment extension can be used if you want to configure unattended deployment on VMware.

6. To verify that the extensions are installed correctly, go to the **Active Response Health Status** page.
   The status of Active Response, DXL, and TIE appear in green.

   For installation errors, see the **Threat Event Log**.

Installing the Active Response server

Active Response server is provided as an ISO image or an OVA virtual appliance, packaging a McAfee® Linux Operating System (MLOS) version 2 instance.

The ISO package can be deployed on bare-metal servers and other virtual infrastructure. The OVA package can be deployed only on VMware.

Tip

Use the OVA package instead of the ISO package on VMware because it preconfigures resources such as CPU, RAM, and disk.

The TIE server is distributed as an OVA appliance optimized for VMware or as an ISO image used with compatible hardware or other virtualization technologies.

If you are using the ISO package, the Active Response MLOS installation, and the actual installation of the server start automatically when you turn on the VM. All base operating system packages are installed. Bash, sage, and partitioning of the disk are done without interaction with the VM. When the installation finishes, the VM turns off and you can remove the ISO. For a complex infrastructure, you can set up and deploy the package on multiple servers. For more information about deploying TIE, see the *McAfee Threat Intelligence Exchange Sizing and Performance Guide*.

Best practices when installing TIE and Active Response servers

If you are installing the TIE and Active Response servers for the first time, install the TIE server first. Run the TIE server in your environment for a few days before enabling tracing on endpoints.

- Files that don't show suspicious activity and have high prevalence because they are executed on a majority of endpoints, are eventually set to **Might be Trusted** reputation. This means you don't need to manually change occurrences of these reputations in the Active Response Workspace later.

- You can fine-tune the TIE Reputations database and decide on the reputations for your corporate-owned files and certificates before Active Response starts inspecting running processes, looking for potential threats. For more information about managing unknown threat reputations, see the Knowledge Base article KB90344.

Install the Active Response, DXL, and TIE server extensions manually

Install and configure the Active Response server, the Data Exchange Layer brokers, and the TIE server on a single appliance.

Before you begin

-

  Make sure that you have installed these extensions:

  - DXL broker management extension
  - TIE server management extension
  - Active Response extension
  - DXL client extension
  - DXL client management extension
  - Active Response Workspace extension
  - Active Response client extension

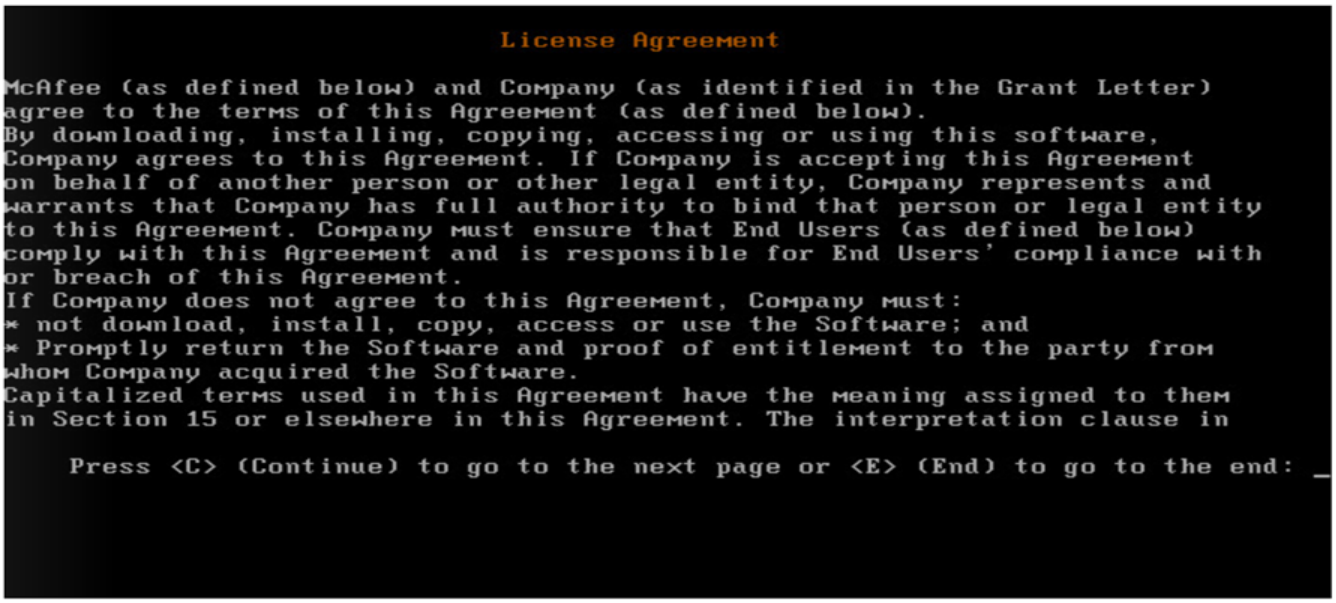
- Verify that the DXL broker server and TIE server are installed. See their respective installation guides for instructions. This is optional if you are installing DXL and TIE on the same server.

- Make sure that the server extension is installed correctly and that it matches the version of the server before you deploy the OVA appliance.
- Store your root password in a secure location.

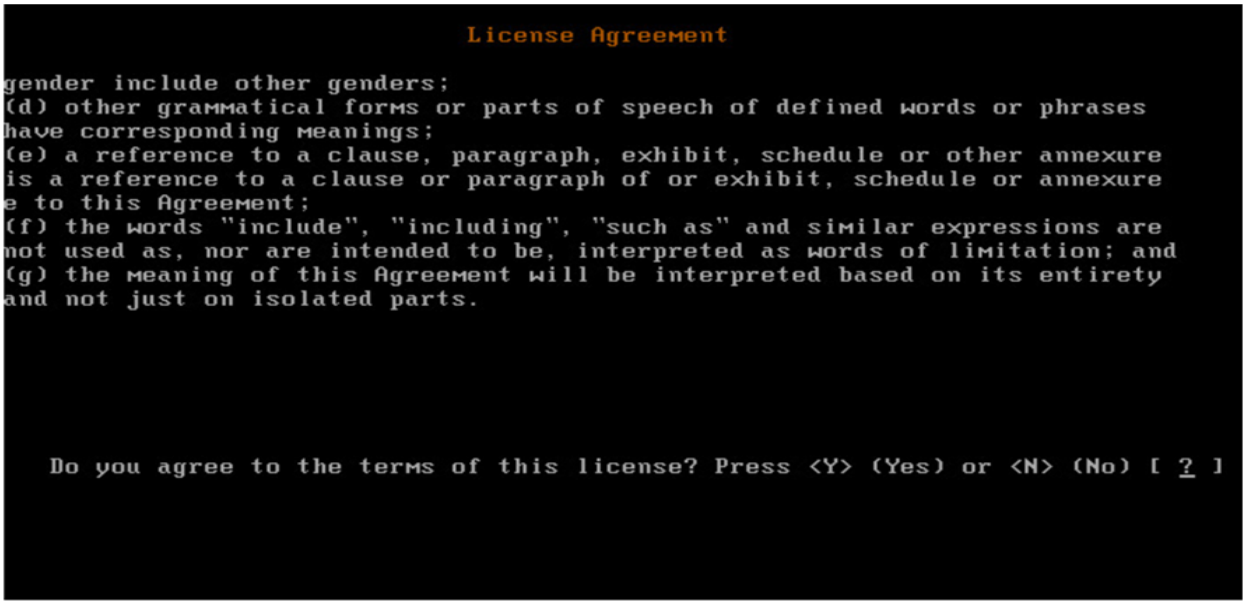
See KB84473 for details about supported platforms, environments, and operating systems.

Task

1. Download the OVA component for the server appliance from **Software Manager** (or **Software Catalog** on McAfee ePO 5.10) or from the McAfee download site, then extract.
2. Open the VMware vSphere client, then click **File** → **Deploy OVF Template**.
   a. Browse to and select the *.ova file on your computer.
   b. Click **Next** and complete the steps in the wizard.
   c. Turn on the virtual machine and open a **Console** window.



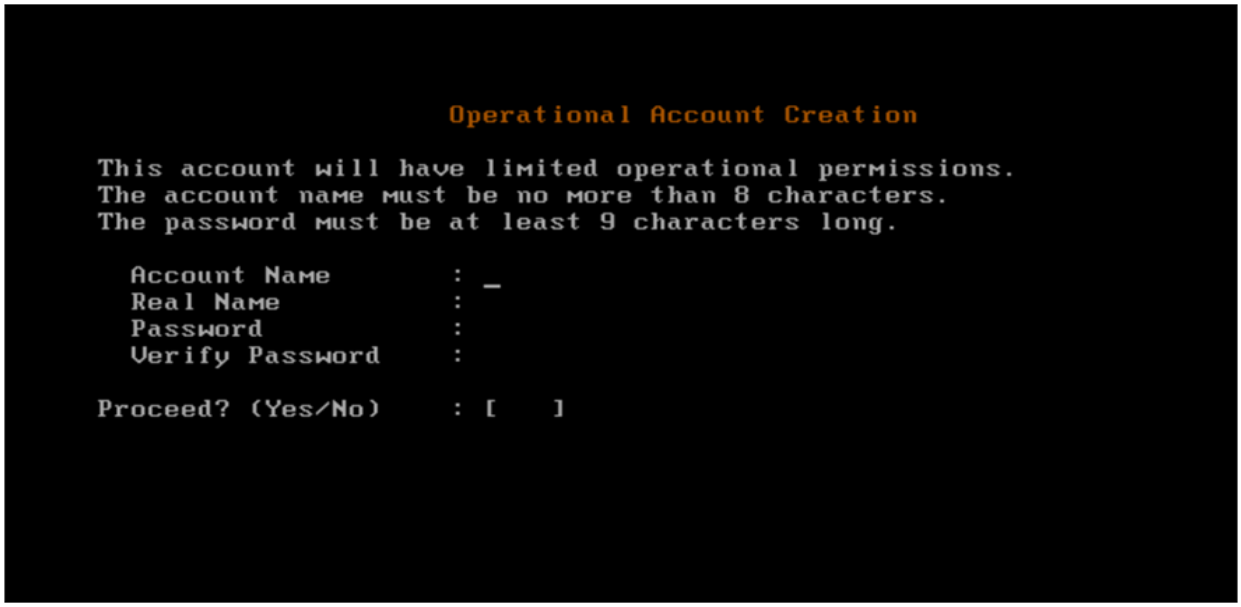
3. Read and accept the license agreement. Press **C** to view each page or **E** (End) to view the last page.



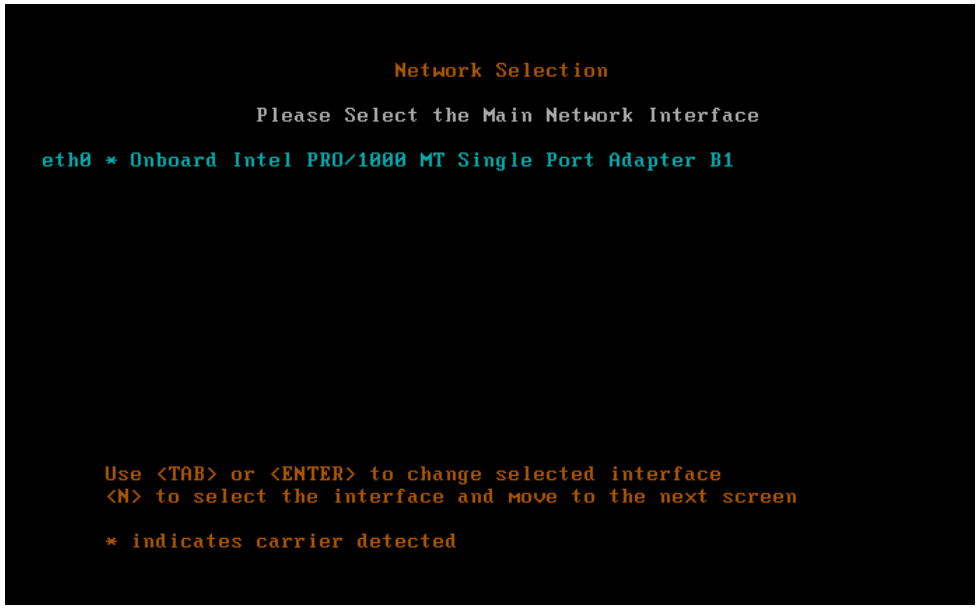
4. Press **Y** to accept the terms to continue.

5. Create a root password for the new server appliance.

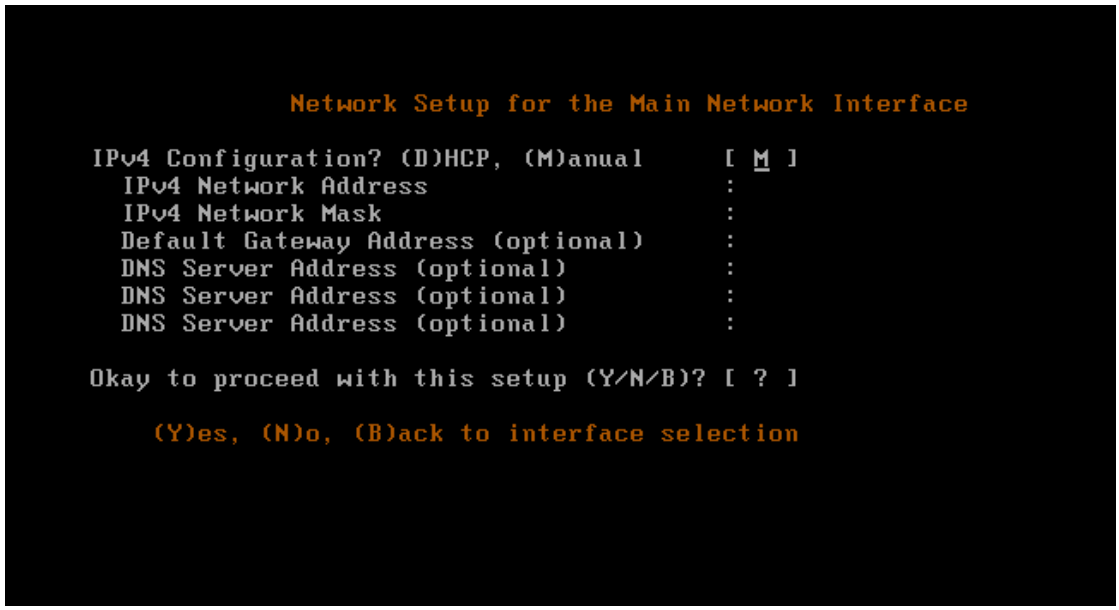
   The password must be at least nine characters. Store your password on a secure location. Press **Y** to continue.



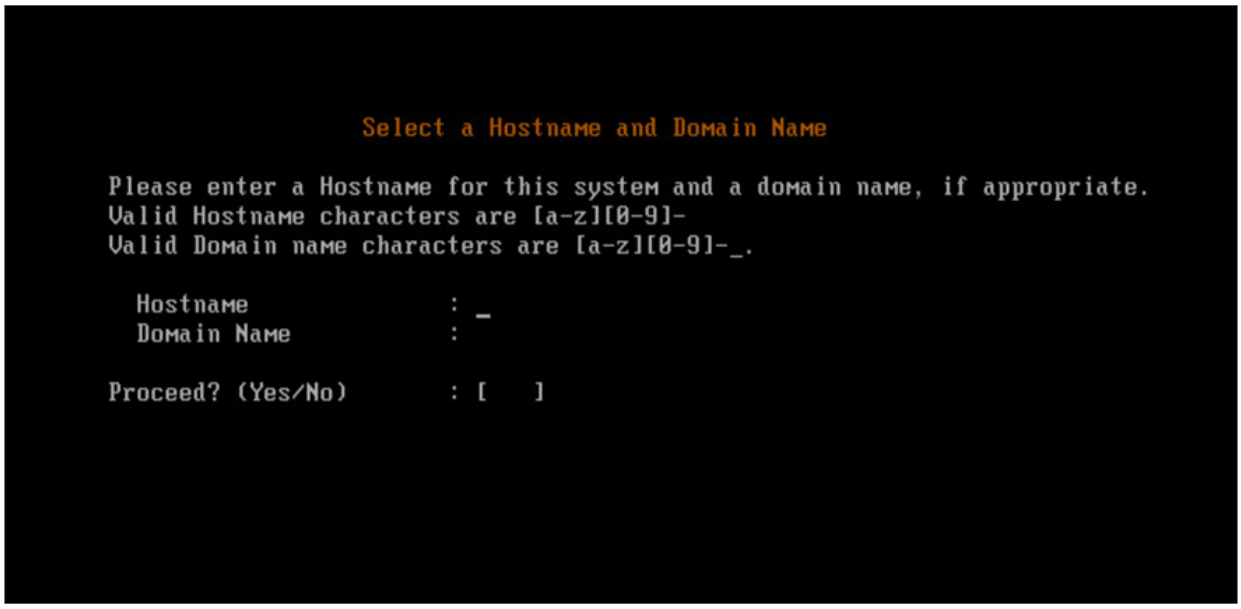
6. Enter the operational account name, real name, and password, using the **Tab** key to move to the next field. When finished, press **Y** to continue.
   The account name is typically something like `jsmith` and is used to log on to the server and to the managed services. The real name is your full name, for example, `John Smith`.



7. On the **Network Selection** page, press **N** to continue.



8. Select a configuration type, then press **Y** to continue.
    - Manual IP address — Press **M**, then enter the remaining information.
    - DHCP — Press **D**.



9. Enter the host name and domain name of the computer where you are installing the new server appliance. Press **Y** to continue.

10. Enter up to three Network Time Protocol servers to synchronize the time of the new server. Use the default servers listed, or enter the address for up to three servers.
    Verify with your networking team that you can access the URLs from your network, or you can provide internal or external NTP servers.

    Caution

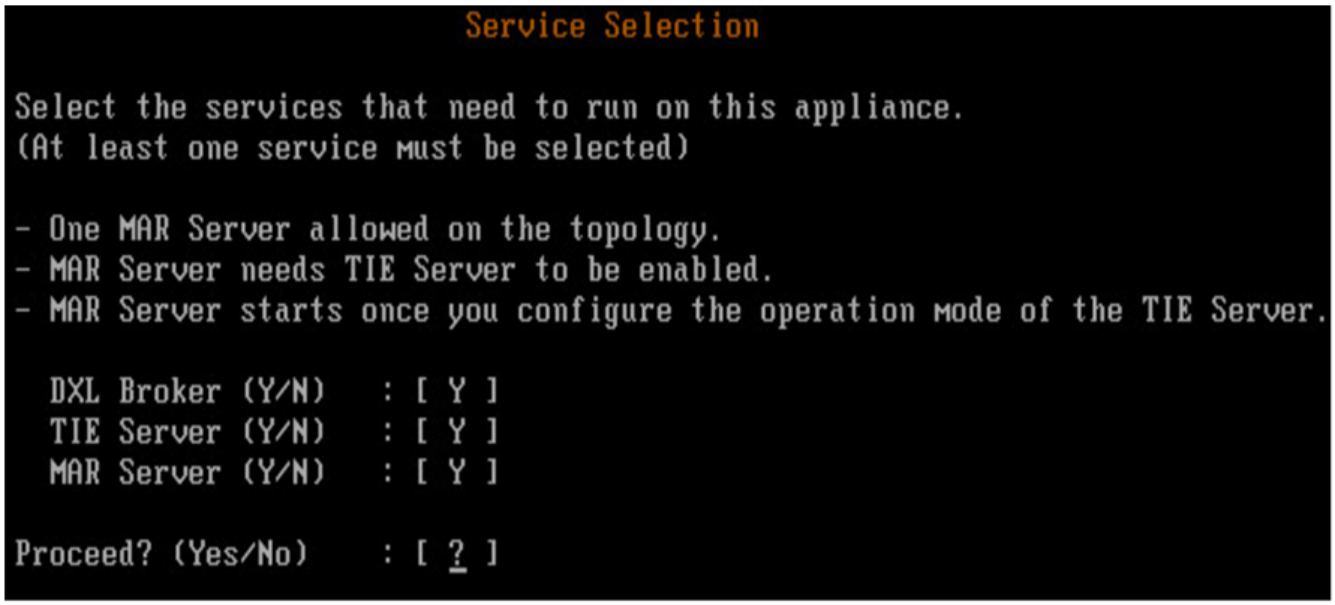
    If the NTP servers are not synchronized, DXL and TIE handshake will not be completed immediately.

    Press **Y** to continue.

11. Enter the IP address or fully qualified domain name, port, and account information for your McAfee ePO server. The user account must have administrator rights. Press **Y** to continue.
    Before proceeding, verify the authenticity of the certificate fingerprint of your McAfee ePO. In a browser navigate to McAfee ePO and verify that the fingerprint matches the one shown on the installation screen. If it does, press **Y** to continue.

    Note

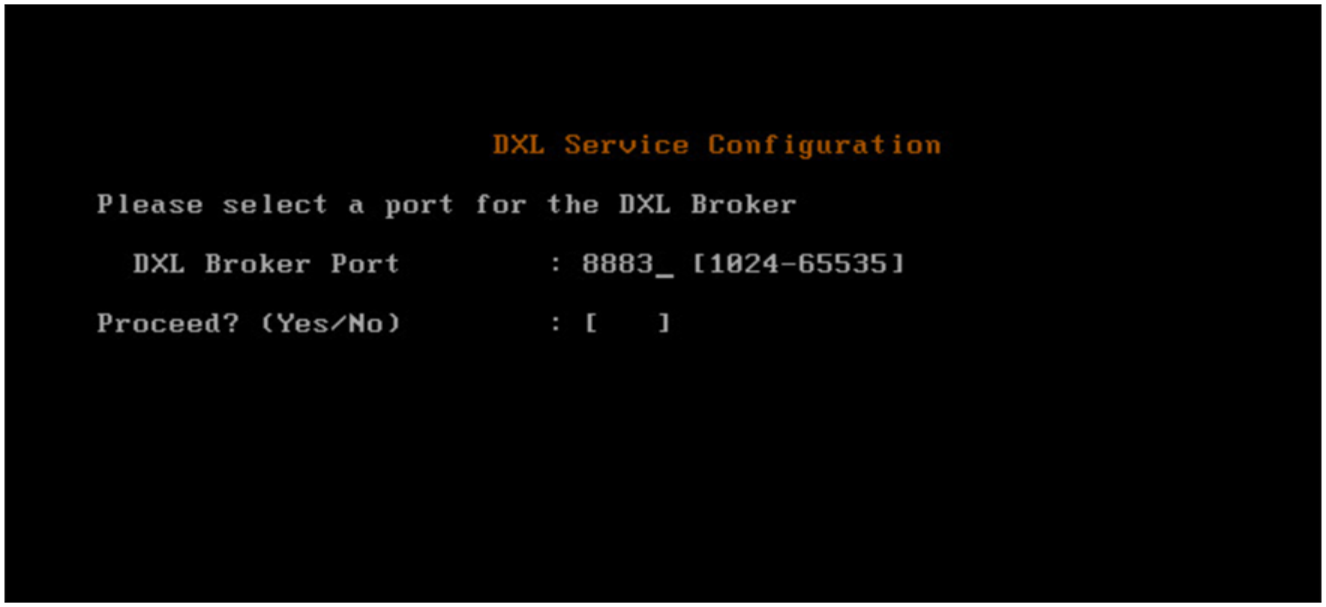
    In Windows, Internet Explorer and Chrome show the certificate information about using a built-in SHA-1 thumbprint. Firefox implements its own cross-platform and shows the certificate SHA-256 fingerprint.



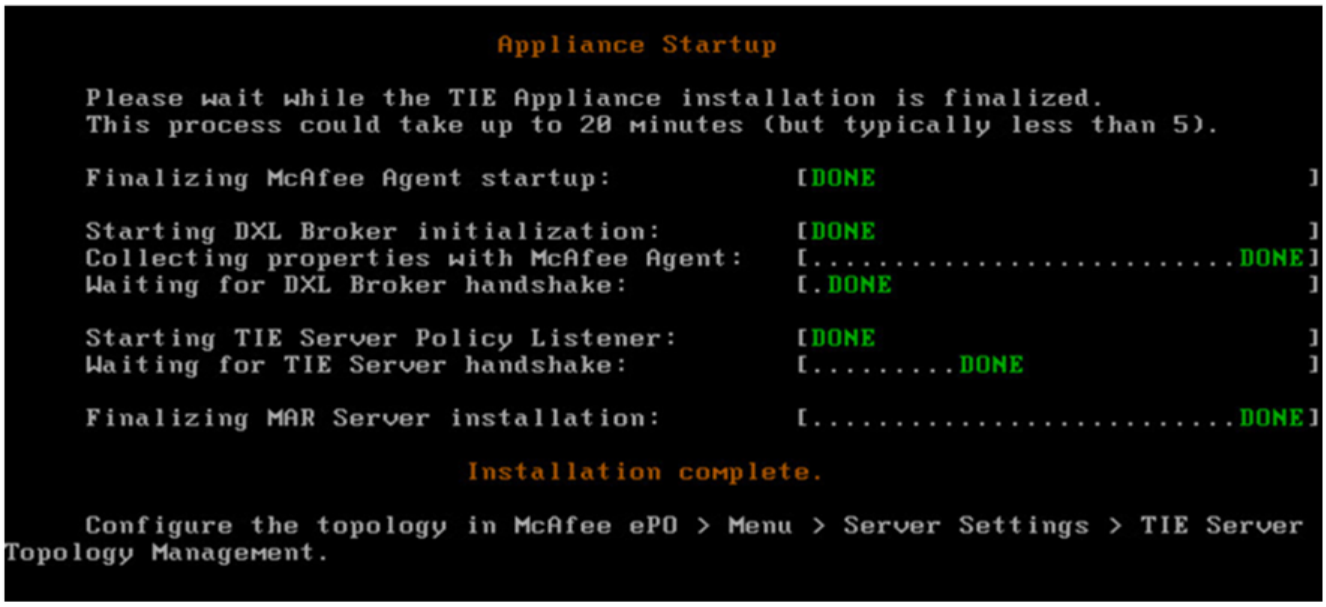
12. You can select the services that you want to run on the new server.

    You must deploy the Active Response server through McAfee ePO if you upgrade from TIE 2.2.0 or earlier versions.

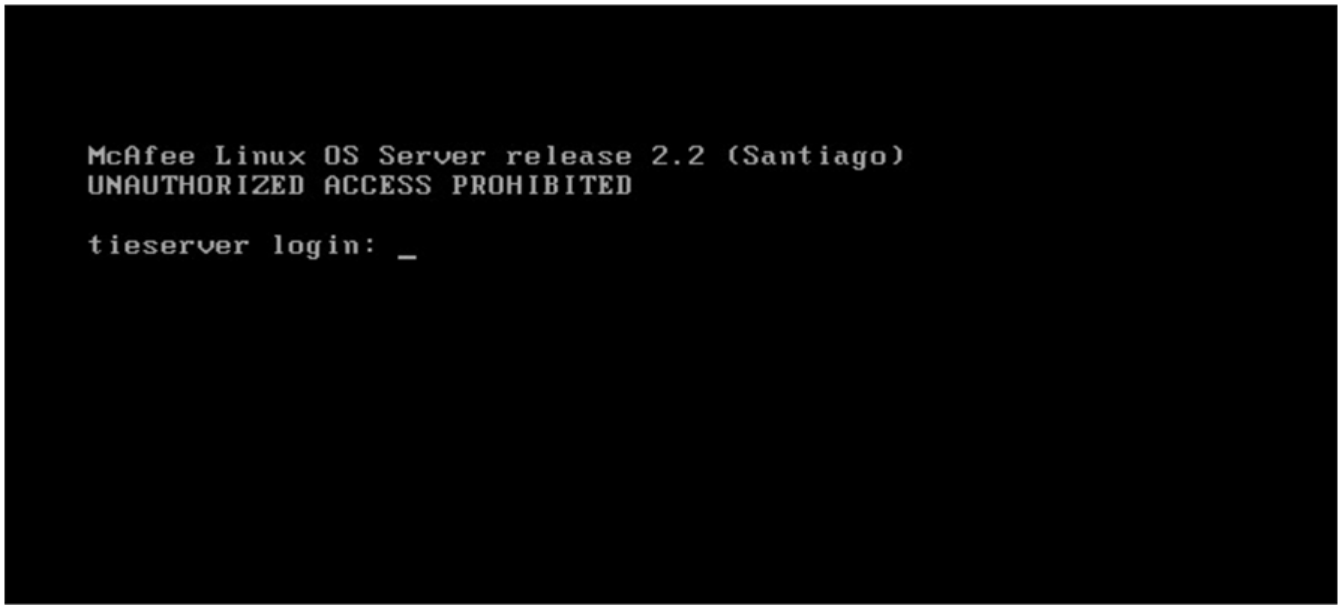
    Press **Y** to continue.



13. Configure the DXL Broker port, then press **Y** to continue.



14. Verify that the installation finishes successfully.
    All components must be in green to continue. If not, follow the suggestions to troubleshoot the issue.



15. When the logon screen appears, close it.
16. Verify that the new server is provisioned. In McAfee ePO, select **Menu** → **System Tree** → **My organization** → **Preset** → **This group and All subgroups** to look in the domain where you installed the server appliance.
17. Verify that the registered server is provisioned correctly in McAfee ePO as a managed system. Select **Menu** → **Configuration** → **Registered Servers**.
18. Verify that the Active Response server is installed and working correctly.
    a. Log on to McAfee ePO as an administrator and open the Active Response Health Status page to verify that the status of Active Response, TIE, and DXL show green.
    b. Check that the **Active Response Catalog** displays the built-in collectors. This confirms that the Active Response server is communicating with the McAfee ePO server.

Results

The appliance shows the MARSERVER, DXLBROKER or TIESERVER tag, depending on the products installed.

Deploy Active Response, DXL, and TIE server (unattended)

A single server can be used to host Active Response, TIE, and DXL services.

Before you begin

-

  Make sure that you have installed these extensions:

  - DXL broker management extension
  - TIE server management extension
  - Active Response extension
  - DXL client extension
  - DXL client management
  - Active Response Workspace extension
  - Active Response client extension
  - Server deployment extension — This extension is optional and is required only for unattended deployment.

-

  Make sure that the VMware configurations meet the required criteria:

  - VMware user must have permissions to:
    - Allocate space
    - Assign network
    - Add new disk
    - Access advanced configuration settings
    - Import
  - VMware Cluster or Host must have sufficient resources to cover the appliance requirement (8 CPU Cores, 16-GB RAM).
  - VMware Datastore must have at least 200 GB of available space.
  - VMware Network must have unassigned addresses (if there is DHCP) and doesn't require tagging.
  - VMware folder must exist.
  - VMware Virtual machine name must not exist previously and must meet VMware requirements.

-

If Active Response is deployed in a TIE server operating as a secondary server (or **Reporting Secondary**), ensure that the primary TIE server (**Write-Only Primary**) is up and running, because Active Response needs access to the TIE server primary database.

In an environment with multiple TIE servers, the Active Response server always connects to the primary database. In a complex virtual environment, deploy the Active Response server to a secondary database.

Caution

We support Active Response running with TIE servers in **Primary**, **Secondary**, and **Reporting Secondary** operation modes. We recommend deploying Active Response in TIE Reporting Secondary servers because this operation mode doesn't process reputation requests. We don't support Active Response deployed in TIE Reputation Cache operation mode.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Automation** → **Server Deployment**.
3. Provide the VMware vCenter access URL and credentials.
   a. Click **Validate Certificate** and follow the instructions to verify whether the fingerprint matches the one on the vSphere web client. This checkbox is displayed if the access URL starts with HTTPS.
   If the access URL uses HTTP, then the **Allow insecure connection (http)** option is displayed.

   Select **Allow insecure connection (http)** to connect to this IP address.

   b. Provide VMware vCenter infrastructure details such as the name of the data center, cluster, datastore, and network.
   The **Folder** and **Virtual Machine Name** fields have default values. You can change the default entries based on your requirement. But, make sure that the names are unique and that the folder exists.
   c. Provide your McAfee ePO credentials.
   The **Hostname**, **Port**, and **Wake up port** fields are automatically populated.
4. Click **Validate Certificate** and follow the instructions to verify whether the fingerprint matches the one on McAfee ePO.
5. Create a root password, user name, and password for the new server where you want to deploy the services.
6. Enter a new host name and domain name of the server network through which the services are deployed.
   The mode is set as DHCP by default. The **NTP** and **DXL port** fields are also populated. The **DXL port** field appears when the DXL service option is selected.
7. Select the checkbox next to the services that you want to deploy to the server.
   TIE and DXL checkboxes are selected by default. To deploy the Active Response services, select **MAR**.
   When you select **MAR**, both Active Response and TIE services are deployed to the server. As a result, the **TIE** option is disabled.
8. Accept the license agreement and click **Deploy**.
9. Click the **Check server health status here** link to open the Active Response Health status page and verify whether the status of Active Response, TIE, and DXL appear in green.
   The time for the status for individual services to turn green can range from 5—30 minutes.

Install the Active Response clients

The Active Response clients are installed on endpoints and they communicate potential threats on the endpoints to the Active Response server and remediate the threats based on the actions configured on the server.

Before you begin

- Verify that all Active Response endpoint client systems meet the minimum requirements.
- Remove McAfee® VirusScan® Enterprise from the endpoints otherwise the installation fails.
- Make sure that the version of McAfee® Host Intrusion Prevention on your endpoints is 8.0.0.7364 or later.
- Make sure that any endpoint compatibility issues or deployment errors are resolved (view the **Health Status** page).
- For Redstone 3 endpoints, verify that Endpoint Security 10.2.2 or 10.5.3 is checked in to the **Master Repository**.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Software** → **Product Deployment**, then click **New Deployment**.

   Note

   During deployment on Windows systems, Active Response disables Microsoft Protection Service momentarily to complete the installation. Endpoint users might see a warning that this service has been disabled. When the installation is complete, Microsoft Protection Service is restored and the warning can be ignored.

3. Select the Active Response client software package for Windows, Linux, or macOS.

   Caution

   On Linux 64-bit systems, compatible 32-bit libraries must be installed on endpoints for Active Response to work properly. See KB89991 for instructions.

4. Click **Select Systems** to select the endpoints to be managed with Active Response.
5. Select **Run Immediately** and click **Save** to start deployment.
6. Deploy the Active Response clients.

   Tip

   If an older version of Active Response is already installed, the Active Response client is updated with the newer version. Also, if deploying on an older system that takes longer for a new deployment, create a client task and increase the timeout setting to more than the default 20 minutes. This ensures the deployment doesn't time out before it is complete.

7. Verify that the deployment to endpoints is working correctly.
   The deployment events are sent back to the McAfee ePO as threat events and provides a description of deployment failures, if any.

a. Log on to McAfee ePO as an administrator.
b. Select **Systems** → **Active Response Search**, and enter `HostInfo` in the search box.

The list of deployed endpoints is displayed.

What to do next

After deploying the Active Response clients, make sure to configure the appropriate McAfee ePO policies.

Deploying on macOS endpoints

Endpoints with macOS High Sierra 10.13 and later requires user approval before allowing third-party kernel extensions.

When you deploy Active Response on macOS systems, you must approve before loading newly installed kernel extensions (KEXTs).

Active Response 2.x

When deploying Active Response on an endpoint with macOS High Sierra 10.13 and later, you must approve the FMP Kernel Extension to run Active Response service.

If the kernel extension isn't approved, Active Response service continues to run, but waits until the user approves the extension. When the kernel extension is not approved, this message appears in the /var/McAfee/Mar/data/marlog.log log file:

```
Waiting for user to accept kext.
```

Install the Active Response client manually

Install Active Response client on Windows system using the product installer

You can install Active Response client on the Windows system using the product installer.

Before you begin

- Verify that all Active Response endpoint client systems meet the minimum requirements.
- Make sure your system is managed using McAfee Agent and Data Exchange Layer.
- Remove McAfee VirusScan Enterprise from the endpoints otherwise the installation fails.
- Make sure that the version of McAfee Host Intrusion Prevention on your endpoints is 8.0.0.7364 or later.
- Make sure that any endpoint compatibility issues or deployment errors are resolved (view the Health Status page).
- For Redstone 3 endpoints, verify that Endpoint Security 10.2.2 or 10.5.3 is checked in to the Master Repository.

Task

1. Download the package from the McAfee Download site.
2. Save and open the package file MAR_client_package_<version>_<build number>.zip.
3. Extract the required installer MARSetup_ x64.exe or MARSetup_ x86.exe and run on the system.

Results

Active Response client is installed on the Windows system.

Install Active Response client on Linux system using the product installer

You can install Active Response client on the Linux system using the product installer.

Before you begin

- Verify that all Active Response endpoint client systems meet the minimum requirements.
- Make sure your system is managed using McAfee Agent and Data Exchange Layer.
- Remove McAfee VirusScan Enterprise from the endpoints otherwise the installation fails.
- Make sure that the version of McAfee Host Intrusion Prevention on your endpoints is 8.0.0.7364 or later.
- Make sure that any endpoint compatibility issues or deployment errors are resolved (view the Health Status page).
- For Redstone 3 endpoints, verify that Endpoint Security 10.2.2 or 10.5.3 is checked in to the Master Repository.

Task

1. Download the package from the McAfee Download site.
2. Run `mkdir Mar` to create a MAR folder .
3. Save the package file MAR_client_package_<version>_<build number>.zip in MAR folder.
4. Run `unzip Mar_Client_Package_<version>_<build number>.zip` to unzip the package file.
   Once the unzip command is executed, all files are displayed.
5. Run `chmod 755 /tmp/Mar/MARS_x64.run` to change permission of the installer file.
6. Run `bash /tmp/Mar/setup.sh /tmp/Mar/` as root user for the client installation.
   Once the execution starts, you see messages as `Installing McAfee Agent certificates`.
7. Verify /var/log/ MAR-Client-Install-{date}.log to see the successful installation.

Results

Active Response client is installed on the Linux system.

Upgrade to a new software version

Planning your upgrade

Before you upgrade the software, you must migrate the legacy Active Response Server from the old appliance into a consolidated one, already deployed through the latest TIE Server upgrade or a new deployment.

Caution

Before you upgrade, you must upgrade DXL and TIE to the latest versions. DXL upgrade is optional, but TIE must be upgraded to 2.3, else Active Response upgrade fails.

One-time migration

Before the upgrade, you must relocate the legacy Active Response server to a TIE appliance. If the legacy software has custom content added to the Active Response Catalog, all data must be migrated before the upgrade. For more information about data migration, see KB90915.

Reconfiguration

The legacy Active Response appliance must be powered down and removed from the **System Tree**. The Active Response registered server must be recreated, if manually customized.

Deployment

TIE server 2.3 or later must be deployed for Active Response update to work. TIE server must run in the same appliance as Active Response. This is because Active Response shares database infrastructure to replicate the Active Response Catalog.

Upgrading Active Response

A complete upgrade installs the components of the Active Response server, extensions, and client packages that have updates. Upgrading the software requires a one-time upgrade of the legacy Active Response appliance.

Caution

Before you upgrade, you must upgrade DXL and TIE to the latest versions. DXL upgrade is optional, but TIE must be upgraded to 2.3, else Active Response upgrade fails.

For information about installing DXL and TIE, see the DXL Installation Guide and TIE Installation Guide respectively.

If you are manually installing the packages, minimize downtime during the upgrade process by installing components in this order:

1. Active Response extensions: `Active_Response_MAR_{version}.zip`
2. Active Response aggregator
3. Active Response clients on managed systems

Caution

The Active Response aggregator is incompatible with the standard DXL client. For a DXL broker with Active Response aggregator installed, all DXL client updates are included in a new Active Response aggregator package.

Upgrade the Active Response extensions

Upgrading to a current version of Active Response ensures that you stay up-to-date with the latest collectors, triggers, and reactions to investigate and remediate threats on your endpoints. To upgrade, you must install the Active Response extensions on McAfee ePO server.

Before you begin

- Export custom collectors, triggers, reactions, and custom searches from the Active Response Catalog. When the upgrade is complete, import the custom content to the upgraded version.
- For servers with TIE version 2.2 and earlier, you can choose to install a new consolidated appliance or reuse an existing server by installing Active Response on it.
- Install Active Response server of the same or later version.

You can install the extensions manually or automatically. For manual method, install the bundles in this order to avoid compatibility issues:

- DXL broker management extension
- TIE server management extension
- Active Response extension/packages bundle
- DXL client package
- Active Response Workspace extension
- Active Response client package

Task

1. Log on to McAfee ePO as an administrator.
2. (Optional) Export custom collectors, reactions, and searches from McAfee ePO.
    a. On the Catalog page, from the **Collectors** tab, select your custom collectors, then select **Actions** → **Export**. When the export is complete, download the file.
    b. Go to the respective tabs and repeat this step to export your custom reactions, triggers and saved searches.
    c. Stop the Active Response server.
3. Select **Menu** → **Systems** → **System Tree**.
4. To delete the Active Response server, select your Active Response server from the **System Tree**, then go to **Actions** → **Directory Management** → **Delete**.
5. To install products automatically on McAfee ePO 5.10:
    a. Select **Menu** → **Software** → **Software Catalog**.

Note

If you enabled **Automatic Product Installation** when you installed McAfee ePO, the products for which you have licenses are installed automatically.

b. Search for the required product packages in the **Software Catalog** page.
c. Select the required product package, accept the license agreement, and click **Check in** to install the package.

6. To manually check in and install the extensions on McAfee ePO 5.10 or earlier:
   a. From the McAfee downloads site https://www.mcafee.com/enterprise/en-us/downloads.html, download the extensions and packages.
   b. Select **Menu** → **Software** → **Extensions** and click **Install Extension**.
7. Upgrade the DXL broker if needed. See *McAfee Data Exchange Layer Installation Guide* for instructions.
8. Deploy Active Response and TIE from the unified ISO/OVA package.
9. Upgrade the Active Response clients.
10. (Optional) If you have custom content:

Note

Before importing the custom content, verify whether the Active Response Health Status page displays a green indicator. This indicates all components are configured correctly.

a. Verify that the Active Response Health Status page displays a green indicator, showing that all components are configured correctly.
b. Import your custom content to the upgraded environment: go to the respective tabs on the Catalog page, click **Import**, select the file you exported, then click **OK**.

Upgrade the Active Response server

You can install and deploy the Active Response server update packages from the McAfee ePO **Software Catalog**. For Active Response 2.4, TIE and Active Response have a consolidated appliance. The existing Active Response appliance is legacy and you must do a one-time migration of all custom content before upgrading the software.

For information about exporting custom content using scripts, see KB90915.

Task

1. Log on to McAfee ePO as an administrator.
2. Use one of these methods to check in the server package:
   - Select **Menu** → **Software** → **Software Catalog** (on McAfee ePO 5.10).
   - Select **Menu** → **Software** → **Software Manager** (on McAfee ePO 5.9 or earlier).
3. Deploy the update package:
   a. Select **Menu** → **Software** → **Product Deployment**, then click **New Deployment**.
   b. In the **Package** drop-down list, select the server update package.
   c. Click **Select Systems** to select the consolidated server with Active Response and TIE in your network.

d. Select **Run Immediately** and click **Save** to start deployment.

Upgrade clients

Install a newer version of the Active Response client on managed systems to upgrade clients.

Before you begin

- Verify that all Active Response endpoint client systems meet the minimum requirements.
- Remove McAfee® VirusScan® Enterprise from the endpoints otherwise the installation fails.
- Make sure that the version of McAfee® Host Intrusion Prevention on your endpoints is 8.0.0.7364 or later.
- Make sure that any endpoint compatibility issues or deployment errors are resolved (view the **Health Status** page).
- For Redstone 3 endpoints, verify that Endpoint Security 10.2.2 or 10.5.3 is checked in to the **Master Repository**.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Software** → **Product Deployment**, then click **New Deployment**.
   During deployment to Windows systems, Active Response disables Microsoft Protection Service momentarily to complete the installation. Endpoint users might see a warning that this service has been disabled. When the installation is complete, Microsoft Protection Service is restored and the warning can be ignored.
3. Select the Active Response client software package for Windows, Linux, or macOS.

   Caution

   On Linux 64-bit systems, compatible 32-bit libraries must be installed on endpoints for Active Response to work properly. See KB89991 for instructions.

4. Click **Select Systems** to select which endpoints to manage with Active Response.
5. Select **Run Immediately** and click **Save** to start deployment.
6. Deploy the Active Response clients.

   Tip

   If an older version of Active Response is already installed, the Active Response client is updated with the newer version. Also, if deploying on an older system that takes longer for a new deployment, create a client task and increase the time out setting to greater than the default 20 minutes. This ensures the deployment doesn't time out before it completes.

7. Verify the deployment to endpoints is working correctly.
   a. Log on to McAfee ePO as an administrator.
   b. Select **Systems** → **Active Response Search**, and enter `HostInfo` in the search box.

   The list of deployed endpoints is displayed.

What to do next

You can upgrade Active Response clients while they are online. As soon as the new version is installed, clients respond to the Active Response server.

Deploying on macOS endpoints

Endpoints with macOS High Sierra 10.13 and later requires user approval before allowing third-party kernel extensions.

When you deploy Active Response on macOS systems, you must approve before loading newly installed kernel extensions (KEXTs).

Active Response 2.x

When deploying Active Response on an endpoint with macOS High Sierra 10.13 and later, you must approve the FMP Kernel Extension to run Active Response service.

If the kernel extension isn't approved, Active Response service continues to run, but waits until the user approves the extension. When the kernel extension is not approved, this message appears in the /var/McAfee/Mar/data/marlog.log log file:

```
Waiting for user to accept kext.
```

Upgrade content packages

Install content packages to get new collectors and reactions, or new versions of existing built-in collectors and reactions.

Note

New versions of collectors and reactions in the content package might make some of your saved searches and triggers unusable. This only happens if the update changes a built-in collector output field, or if the update changes built-in reaction arguments. Check the *McAfee Active Response Content Update Release Notes* for information about changes to collectors and reactions introduced by a content package.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Software** → **Software Manager** (or **Software Catalog** on McAfee ePO 5.10) to check in the Active Response content package.
   Content packages have this naming convention:
   BaseActiveResponseContent-MajorVersion.MinorVersion.PatchVersion-BuildVersion.zip

   If you have **Auto Update** enabled for deployments, after the package checks in to the **Master Repository** it is installed automatically. If not, create an update deployment task.

3. To view the version of content package, select **Menu** → **Systems** → **System Tree** → **Active Response** → **Active Response properties**, then select **Content version**.

Upgrade Trace rules

The Active Response rules content package adds, updates, and removes old Trace rules. You can automatically deploy Trace rules content updates to endpoints when a new update is available in **Software Manager** (**Software Catalog** on McAfee ePO 5.10).

Trace rules determine a potential threat and its severity, and displays it in the Trace timeline. The mechanism to automatically update Trace rules content is enabled by default, with update tasks scheduled every 240 minutes (4 hours). This is an unattended task that is enabled in McAfee ePO.

If you disable this feature, you can update the rules manually.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Policy** → **Policy Catalog** , then click **My Default**.
3. On the **General** tab, select **Enable Unattended Content Updates** to disable or enable this feature.
4. To change the default time for **Unattended Content Updates Timeout (minutes)**, edit the value in the field.

Results

Updates are checked every cycle, and if there is a new update, it is deployed to the endpoints to update their Trace rules.

Create Active Response registered server

The Active Response registered server is automatically created as part of the initial hand-shake process between Active Response server and Active Response extensions running on McAfee ePO. The registered server is also updated or re-created automatically through the **Manage Active Response Servers** task or while generating Active Response certificates.

If the Active Response registered server was manually edited, it must be removed and re-created during upgrades. To re-create the registered server automatically, you must complete these steps.

⚠ Caution

Active Response registered server is not updated automatically if it was manually edited and saved.

Task

1. Log on to McAfee ePO as an administrator.
2. To delete the registered server, select **Menu** → **Configuration** → **Registered Servers**, then select **Actions** → **Delete**.
3. To generate server certificates, select **Menu** → **Configuration** → **Server Settings** → **Active Response**, then click **Edit**.

4. In the **Authentication (select this if you changed McAfee ePO certificates)** field, select **Regenerate Active Response Certificates** and click **Save**.

Results

Active Response registered server is created.

Recommendations for configuring the product

Appliance configuration

Active Response Server

Active Response does not support deployments where multiple Active Response servers are installed in the same Data Exchange Layer fabric. So, scalability is approached vertically by adding more power to an existing appliance.

Recommended configuration according to the number of endpoints

Number of endpoints	CPU	RAM	Storage
10,000–150,000	8 vCPU	16 GB	360 GB
150,000–300,000	16 vCPU	32 GB	540 GB
300,000–500,000	16 vCPU	32 GB	1 TB

Active Response aggregator

Active Response aggregators can be installed on DXL Broker appliances. They reduce the amount of DXL bandwidth and they increase the number of managed endpoints supported by the system.

The recommended specifications for an Active Response aggregator appliance are:

- CPU: 4 vCPU
- RAM: 8 GB
- Storage: 120 GB

We recommend that you install an Active Response aggregator for every 5000 endpoints.

DXL brokers and TIE server

The number of DXL brokers is also mainly driven by the number of managed endpoints in the environment. For information about DXL brokers and TIE Server, see DXL and TIE documentation.

Endpoint configuration

Active Response provides several features to achieve real-time visibility of what is happening on the endpoints during installation.

Some features might need to be modified based on the endpoint characteristics and requirements.

Feature/ Component	Description	Potential high CPU usage	Configuration to reduce CPU usage
SyntemRuntime	Executes searches and reactions through scripts or shell commands.	The script might cause high CPU usage.	
SystemInfo	Collects information processing.	No.	
Context	Collects user, network interface, and installed software information.	No.	
FileHashing	Tracks and monitors file changes.	It depends on the number of files changes.	Configure *Ignore List and Files* properly based on customer needs and applications that are being used.
WinRegistry	Searches registry keys and monitors specific changes.	If the search requires the processing of the entire registry, this might cause high CPU spikes.	
NetworkFlow	Tracks and monitors connection flows.	If the host is a server that receives thousands of connections, it might cause high CPU spikes.	You can increase the database limit to avoid the frequent shrinking of the database. Also, you can add the process to the Ignore List configuration.
Triggers	For NetworkFlow, SystemProcess, FileHashing, and WinRegistry.	CPU spikes might occur depending on the number of changes to be analyzed.	Triggers must be set temporarily during a period of time.

Feature/ Component	Description	Potential high CPU usage	Configuration to reduce CPU usage
Trace	Traces unknown reputation processes to record events that might indicate a potential threat.	TIE server needs to be properly configured to avoid false positives.	

Agent Footprint

This is a sample installation including Endpoint Security 10.5.x and Active Response 2.1.x on Windows 10 x64.

Type	MB	Notes
RAM / Memory	About 210	Includes Endpoint Security (TP, ATP), McAfee Agent, DXL, and Active Response.
Program Files Size	About 491 (decompressed with content)	
Program Data Size	About 297	Includes AMCore content and filehash database.

File Hashing

Understanding File Hashing is critical to properly configure the clients without impacting the endpoints.

The file system information is stored locally to speed up searches of hashes involved in Indicators of Compromise (IoC) or complex attribute combinations. Every file change is monitored, so triggers can be evaluated in real time.

When file hashing is enabled, this component executes the warmup process to create an initial snapshot (local database) of the entire file system. It also walks through all directories and files to get the needed attributes (such as size, hashes, and dates). It analyses every file except for those ignored by extension or path. This complete analysis might cause high CPU usage when Active Response is deployed for the first time. This could be compared to a complete antivirus scan.

When the service is restarted, the File Hashing component runs a complete analysis on the file system again. During this analysis, Active Response uses the database to scan only those files that were changed. This process usually doesn't take too long but it depends on the number of changes registered on the file system.

Active Response monitoring can cause high CPU usage under specific circumstances, for example when a ZIP file is being opened or when an installation creates numerous temporary files and then moves them to another folder location.

All changes must be analyzed. If triggers for file hashing are enabled, this process might also cause high CPU usage. Also, temporary spikes of memory are expected to hold the list of changed files until they are processed.

Active Response CPU usage closely resembles McAfee VirusScan Enterprise. For more information, see KB55145.

Warm-up process tests

The following tests have been executed in an environment with this configuration.

- Windows 7, 64 bits, 4 Logical CPU
- Memory: 8 GB
- Disk: HDD (465 GB / Used: 73 GB)

File hash stage	Performance measurement	
Warm-up	Time	1450 seconds
	CPU average usage	8.64%
	RAM usage	46.69 MB
	Maximum CPU usage	23.90%
	Write Disk (KB/s)	53.33 KB/s
Idle	CPU average usage	0.02% (it depends on HD activity)
	Average database record size	About 200 bytes

Tips for reducing high CPU usage

Adding entries to the configuration of ignored paths, extensions, folders, and file names improve the hashing process but it might pose major risks to your environment.

Having numerous ignore paths or extensions might reduce visibility if malware is downloaded to the endpoint.

Users can be impacted by default policies causing high CPU usage. This is what McAfee recommends.

- Every time an application is created, file hashing needs to track thousands of files that might be created temporarily. We recommend that you exclude extensions or create a special folder and ignore its content.

- Servers, databases, and web browsers might also create and use temporary folders to store temporary files. We recommend that you ignore those folder locations.

Performance Measurements

Active Response Server is dimensioned based on the number of endpoints in the environment and the expected response time for search queries. The goal is to get a response, for a reference query, in less than one minute.

Besides the number of endpoints, the other important aspect affecting the response time is the size of the message every endpoint responds for the query. As security analysts execute queries from the Active Response user interface, queries are not expected to have a high level of concurrency.

Test scenarios

This scenario includes a basic search where the *HostInfo* collector is used to retrieve host name from all endpoints. The expectation of the response payload is small with a low aggregation factor.

Number of endpoints	Time to complete search
100,000	9 seconds
200,000	10 seconds
300,000	13 seconds
400,000	• About 15 seconds (linear projection) • About 16 seconds (exponential projection)
500,000	• About 17 seconds (linear projection) • About 19 seconds (exponential projection)

Client network bandwidth use by built-in collectors

These queries were performed through McAfee ePO 5.9 and one DXL broker using default collector outputs.

Query	Sent bytes	Send packages	Received bytes	Received packages	Comments
Any search that generates empty result.	356	1	Depends on collector used	Depends on collector used	Size of json query is 140 bytes. The result is not compressed.
HostInfo	457	1	4425	4	Size of json query is 241 bytes. The result is not compressed.
Processes	4973	1	1283	1	78 processes running. Size of json query is 4747 bytes. The result is compressed.
Software	3263	1	1043	1	Returned 22 software. Size of json query is 3047 bytes. The result is not compressed.
CurrentFlow	1332	1	1257	1	Returned 74 entries. Size of json query is 1106 bytes. The result is compressed.
Files where Files name contains"bandwith"	1505	1	1434	1	Returned 8 entries. Size of json query is 1289 bytes. The result is not compressed.
DNSCache	485	1	1931	2	Returned 2 entries. Size of json query is 269 bytes. The result is not compressed.
DisksAndPartitions	744	1	8262	6	Returned 2 entries. Size of json query is 528 bytes. The result is not compressed.
InstalledCertificate s	2234	1	6442	4	Returned 44 entries. Size of json query is 2008 bytes. The result is compressed.

Query	Sent bytes	Send packages	Received bytes	Received packages	Comments
InstalledDrivers	9294	1	3397	2	Returned 324 entries. Size of json query is 9068 bytes. The result is compressed.
InstalledUpdates	673	1	2081	2	Returned 3 entries. Size of json query is 457 bytes. The result is not compressed.
InteractiveSessions	395	1	4874	4	Returned 1 entry. Size of json query is 179 bytes. The result is not compressed.
LocalGroups	3698	1	2728	2	Returned 18 entries. Size of json query is 3482 bytes. The result is not compressed.
LoggedInUsers	443	1	953	1	Returned 1 entry. Size of json query is 227 bytes. The result is not compressed.
NetworkInterfaces	517	1	1351	1	Returned 1 entry. Size of json query is 301 bytes. The result is not compressed.
NetworkShares	531	1	3524	1	Returned 3 entries. Size of json query is 315 bytes. The result is not compressed.
ScheduledTasks	5031	1	7961	1	Returned 159 entries. Size of json query is 4805 bytes. The result is compressed.
Services	4705	1	5624	4	Returned 223 entries. Size of json query is 4479 bytes. The result is compressed.

Query	Sent bytes	Send packages	Received bytes	Received packages	Comments
Startup	854	1	1782	2	Returned 3 entries. Size of json query is 638 bytes. The result is not compressed.
UserProfiles	1257	1	6968	5	Returned 6 entries. Size of json query result 1041 bytes. The result is not compressed.
WinRegistry where WinRegistry key path starts with "HKEY_LOCAL_MACHINE\\SOFTWARE\\McAfee\\Agent"	1708	1	1433	1	Returned 10 entries. Size of json query result 1492 bytes. The result is not compressed.

Trace size samples per event

Considerations:

- Size varies depending on dynamic factors like path names or value.
- Once the client sends that data to the cloud, there is at least 50% reduction of the entire size.

Operation	Sample count	Min (bytes)	Max (bytes)	Average (bytes)
Registry value modified	14	629	705	667
PRU	100	1114	2412	1436
Process Created	162	818	6868	1445
RegKey Enumerate	2	523	560	541
File Executed	49	1107	2080	1223
Create Key	1	539	539	539

Operation	Sample count	Min (bytes)	Max (bytes)	Average (bytes)
File Read	4	814	949	860
File Rename	1	935	935	935
Code Injection	1	1697	1697	1697
Delete Key	2	537	542	539
File Modify	6	847	871	857
Process Terminated	111	364	463	438
Network Accessed	23	663	767	703
Process Accessed	1	1040	1040	1040
RegValue Deleted	2	574	617	595
File Create	1	861	861	861
RegValue Created	3	625	762	672
File Deleted	4	862	874	868

Post-installation tasks

Verifying the Active Response Health status

The **Active Response Health Status** page displays the number of endpoints, status of endpoint deployments, incompatible and unsupported versions, and connection issues with servers and services.

This page is a central location to check the status of endpoints, servers, and cloud bridge connection.

You can view the **Active Response Health Status** page by selecting **Menu** → **Systems** → **Active Response Health Status** or by clicking the link in the **Health Status Alert** window if it appears when you open the Workspace. The **Health Status Alert** window appears if the endpoints, servers, or cloud services need attention due to critical issues.

Health status of clients

Status	Description
Total endpoints	Total number of endpoints in the environment where Active Response is deployed, is pending deployment, and is incompatible for deployment.
Active Response deployed	Indicates the number of endpoints currently running Active Response. It also displays the Trace status of the endpoints managed by McAfee ePO. If the Trace plug-in is disabled, a warning message appears and the status displays the number of endpoints affected. Click the link to see the list of endpoints affected.
Ready for Active Response deployment	Compatible endpoints pending deployment. The number of new endpoints (macOS, Windows, Linux) needing deployment and the number of endpoints needing updates are displayed.
Incompatible with Active Response	Incompatible endpoints pending deployment. An Active Response requirement on the endpoint isn't met. The status lists: • Unsupported versions of an endpoint client such as Endpoint Security or McAfee Agent and the number of endpoints affected. • Unsupported clients such as VirusScan Enterprise on the endpoint and the number of endpoints affected. • Endpoints with unsupported operating system versions and the number of endpoints affected. The Active Response installer fails on endpoints with an unsupported operating system version, so you know which endpoints need upgrading.

Status	Description
Active Response deployment failed	Number of deployment failures on endpoints.

Health status of servers

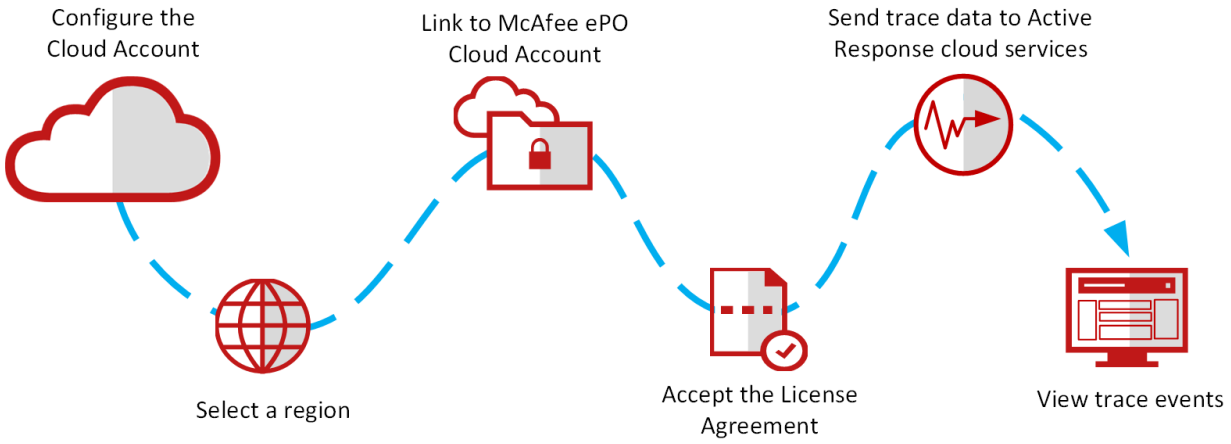
Status	Description
Active Response Server *(version #)*	Displays the version, name, IP address, and status of the Active Response server and a link to its configuration page. The status is displayed if the server is unreachable or needs to be updated. Click the link to troubleshoot the issue.
Advanced Threat Defense *(version #)*	Displays the name and IP address of the McAfee® Advanced Threat Defense server. Click the link to edit the configuration.
DXL Brokers *(version #)*	Displays the version and status of the DXL brokers that display a successful or failed connection. If a broker isn't available, click the link to troubleshoot the issue.
Threat Intelligence Exchange Servers *(version #)*	Displays the version, name, IP address, and status of the TIE servers and a link to its configuration page. If a server isn't available, click the link to troubleshoot the issue. The Active Response server and the TIE server display same IP address if they are deployed to the same server.
Cloud Storage & Services	At times, certain connection or configuration requirements aren't met. For example, the Cloud Bridge connection is disrupted or a timeout has occurred. The cloud account isn't set up or configured correctly. • Bridged McAfee ePO servers are configured with different geolocations. You can select only one geolocation for each DXL fabric. • Bridged McAfee ePO servers are linked to different cloud accounts. You can configure only one cloud account to bridged McAfee ePO servers.

Create a McAfee Cloud account

McAfee ePO Cloud Bridge is an extension that you install on your local McAfee ePO server, allowing you to link McAfee ePO Cloud Bridge to your McAfee cloud account where you store threat data.

You can register a new cloud account or configure your cloud account through the Workspace **Configuration** link.

You can view the connection status of your McAfee Cloud account by clicking **Configuration** from the Workspace bar.



Caution

Switching between different geolocations is not supported or recommended, because you might lose data. This setting is meant to be permanent.

If you unlink an existing McAfee Cloud account from the McAfee ePO Cloud Bridge settings, and link to a different McAfee Cloud account, you lose access to the threat data in the previous McAfee Cloud account.

Task

1. Log on to McAfee ePO as an administrator.
2. From the Workspace bar, click **Configuration**.
   If the cloud account is configured, the **Configuration** pane displays the geolocation and cloud account credentials.
3. To change the geolocation, create your cloud account, click the edit icon (pencil) next to **Cloud Account**.
   If you don't have a McAfee Cloud account:
   a. Click the **Create Account** link.
   b. Complete the company and contact information.

      Note

      The email address you provide is the email address used to create the McAfee Cloud account for your company.

   c. Read and accept the license agreement, then click **Submit**.

After submitting the form, you will receive an email to activate the McAfee Cloud account and set the password.

4. From the **Region** drop-down list, select the geolocation where you want to store your data.
   If you are upgrading Active Response, the geolocation from the previous version of Active Response remains the default selection.
5. Enter the email address and password for your McAfee Cloud account, accept the license agreement, and click **Save**.
6. (Optional) Select **Send trace data to Active Response cloud services** to configure the DXL Broker to send trace data to the Active Response cloud services.

   Note

   Disabling this functionality won't allow Active Response Workspace to receive any data from cloud services. We recommend enabling it to start investigations about potential threats.

7. Click **Save**. The **Save** button is enabled only after you accept the license agreement.

Changing the cloud storage geolocation

You can change the cloud storage location for your threat data in a scenario where the servers to store data are in different locations.

You can select a different geolocation by clicking **Configuration** from the Workspace and selecting a region from the **Cloud Account** drop-down list. Here are the guidelines for selecting different geolocations.

Caution

Switching between different geolocations is not supported or recommended, because you might lose data. This setting is meant to be permanent.

- The selected geolocation from the previous release of Active Response remains the default selection after upgrading.
- If you have bridged McAfee ePO servers, you must select one geolocation and one McAfee Cloud account. You can't point bridged McAfee ePO servers to different geolocations. Check the **Health Status** page for alerts. If you have multiple McAfee ePO servers that aren't
- linked, you can select different geolocations, but you must use the same McAfee Cloud bridge account.
- You are allowed one geolocation per DXL fabric.
- You must use the same McAfee Cloud bridge account for all linked McAfee ePO servers.

Caution

Switching between multiple cloud accounts is not supported or recommended, because you might lose data. We recommend using one cloud account for managing your cloud geolocation and bridged McAfee ePO servers.

- Endpoint roaming isn't supported.
- Data between the cloud geolocations can't be shared.
- New geolocations are added to the selection menu as they become available, without reinstalling or upgrading Active Response.

Caution

Only one geolocation is accessible at a time for trace information. For example, if you change from geolocation X to geolocation Y, all existing threat data that was available on geolocation X is no longer accessible. If you switch back to geolocation X, old trace information is accessible, but the new traces on geolocation Y aren't accessible. You risk losing data by switching back and forth between one geolocation to another.

Configure the DXL broker extension

Broker extensions are additional features that can be enabled on a Data Exchange Layer broker to add new functionality created by other managed products. Enable the Trace broker extension used by Active Response.

Active Response 2.1 or later requires at least one DXL broker version 3.0.0 or later. The Trace extension is not available on previous broker versions.

Task

1. Select **Menu** → **Configuration** → **Server Settings** → **DXL Topology**.
2. Click **Edit**.
3. (Optional) To create a hub, select the **Actions** drop-down list and select **Create Hub**.
    a. Select **Hub** in the topology tree and set **Broker 1** to the DXL broker.
    b. Select the **Provides trace data to the cloud for MAR Workspace** option for at least one broker.
    c. Set **Broker 2** to the Active Response server.
    d. Click **Save**.
4. Verify that the brokers are connected by selecting **Menu** → **Systems** → **Data Exchange Layer Fabric**.
   The brokers are represented as green circles with a line connecting them.

Configure McAfee ePO proxy server settings (optional)

Proxies are mainly used to monitor outgoing traffic, when a company wants to control internet usage, for example blocking malicious websites to improve security. If your company uses proxy addresses to monitor outgoing traffic, enter the proxy address in the McAfee ePO proxy settings.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Configuration** → **Server Settings** → **Proxy Settings**.
3. Click **Edit.**
4. Enter the proxy information.
5. Click **Save**.

Install aggregators (optional)

Aggregators reduce the amount of DXL bandwidth required, and increase the number of managed endpoints supported.

Install Active Response aggregators on DXL broker systems in your fabric. We recommend that you install an aggregator on each system in your fabric that runs only a DXL broker.

Caution

You can't pre-install or upgrade a DXL client from McAfee ePO on the DXL broker. Always use the Active Response Aggregator package to install the DXL client on the DXL broker. You can install the aggregator package from the **Master Repository**.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Software** → **Software Catalog** and check in the Active Response Aggregator package.
3. Select **Menu** → **Software** → **Product Deployment**, then click **New Deployment**.
4. In the **Package** drop-down list, select the Active Response aggregator.
5. Click **Select Systems** and choose the DXL broker where you want to install the aggregator.
6. Select **Run Immediately** and click **Save** to start deployment.

Configuring multiple McAfee ePO servers

In an environment with multiple McAfee ePO servers, more than one McAfee ePO server is connected to DXL brokers on bridged DXL fabrics. Bridging fabrics allows DXL brokers that are managed by different McAfee ePO servers to communicate with each other.

Note

Only one Active Response server is supported in a multiple McAfee ePO server environment.

Using a multiple McAfee ePO server environment

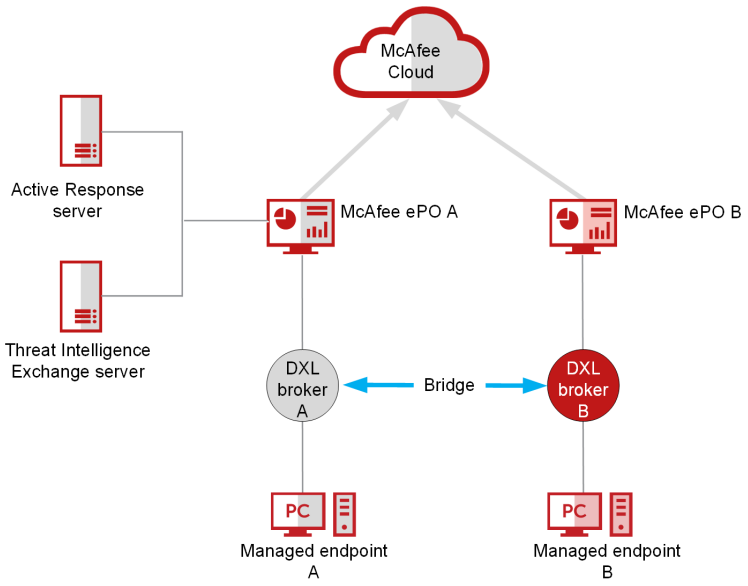
To expand your remediation and upgrade capabilities:

- Deploy Active Response client packages from one McAfee ePO server to upgrade another bridged McAfee ePO server's endpoints.
- Share saved and custom searches using collectors and reactions across bridged McAfee ePO servers with a single Active Response server.
- Manage potential threats across bridged McAfee ePO servers and store threat data in the cloud, using a single cloud storage location.

Caution

Switching between multiple cloud accounts is not supported or recommended, because you might lose data. We recommend using one cloud account for managing your cloud geolocation and bridged McAfee ePO servers.

- Investigate and remediate potential threats across McAfee ePO servers that you manage with a single TIE server.



Note

Active Response 2.1 and earlier don't support environments where two or more McAfee ePO servers have bridged DXL hubs.

Export custom catalog content

Before you bridge multiple McAfee ePO servers, you must first export the Active Response Catalog content, such as custom collectors, triggers, reactions, and custom searches from the server you are replacing.

Note

Only one Active Response server is supported per DXL fabric.

For information about exporting custom content using scripts, see KB90915.

Task

1. Log on to McAfee ePO as an administrator.
2. To export custom collectors, reactions, and searches:
   a. On the Active Response Catalog page, from the **Collectors** tab, select your custom collectors, then select **Actions** → **Export**, then download the file.
   b. Go to the respective tabs and repeat this step to export your custom reactions, triggers, and saved searches.
3. Stop the Active Response server.
4. Select **Menu** → **Systems** → **System Tree**.

5. To delete the Active Response server, select your Active Response server from the **System Tree**, then go to **Actions** → **Directory Management** → **Delete**.
6. Open the McAfee ePO server to be used after the bridging process.
7. Click **Edit**, then select **Regenerate Active Response Certificates**.
8. Import the custom collectors, reactions, triggers, and searches.

   Note

   Before importing the custom content, verify whether the Active Response Health Status page displays a green indicator. This indicates all components are configured correctly.

   a. Go to the respective tabs on the Catalog page and click **Import**.
   b. Select the file exported earlier and click **OK**.

Configure DXL brokers to connect multiple McAfee ePO servers

You can connect multiple McAfee ePO servers using DXL brokers. Connecting multiple McAfee ePO servers are helpful in a scenario when you want to manage multiple McAfee ePO servers from one location or when there is a need to use a common platform across an organization located in different geolocations.

Before you begin

- If upgrading from Active Response 2.1 to 2.2 and bridging multiple McAfee ePO servers, upgrade the DXL extensions, client, and at least one online broker to version 4.0. See KB84473 for details.
- Install DXL 4.0 broker, extensions, and client. See KB84473 for DXL requirements for multiple McAfee ePO servers.
- Deploy the Active Response client 2.2 or later to all endpoints managed by the different McAfee ePO servers.
- Verify that the DXL broker fabrics between McAfee ePO servers are bridged.

Task

1. From McAfee ePO server A, select **Menu** → **Configuration** → **Server Settings** → **DXL Topology**, then select broker A and click **Edit**.
2. From the topology tree, select the top-level hub, and from the **Actions** drop-down list, select **Create Hub**.
   a. Select the newly created hub, and from the **Actions** drop-down list, select **Create Incoming Bridge - Remote ePO Hub**.
   b. From the drop-down list, set **Broker 1** to DXL broker A, then click **Save**.
3. Download hub information for server A.
   a. Select **Incoming Bridge - Remote ePO Hub** and click **Edit**.
   b. Click **Export Local Hub Information** to download a .zip file with information about McAfee ePO server A, to import into the remote hub for McAfee ePO server B, then click **Save**.

4. From McAfee ePO server B, select **Menu** → **Configuration** → **Server Settings** → **DXL Topology**, then select DXL broker B and click **Edit**.
5. From the topology tree, select the top-level hub, and from the **Actions** drop-down list, select **Create Hub**.
    a. Select the newly created hub and from the **Actions** drop-down list, select **Create Outgoing Bridge - Remote ePO Hub**.
    b. From the drop-down list, set **Broker 1** to DXL broker B, then click **Save**.
6. Download hub information for server B.
    a. Select **Outgoing Bridge - Remote ePO Hub** and click **Edit**.
    b. Click **Export Local Hub Information** to download a .zip file with information about McAfee ePO server B, to import into the local hub for McAfee ePO server A, then click **Save**.
7. From the **DXL Topology** page on McAfee ePO server A, click **Edit**.
    a. Select **Incoming Bridge - Remote ePO Hub**, and click **Import Remote Hub Information**.
    b. Click **Choose File** and upload the .zip file for McAfee ePO server B, then click **OK**.
    c. Review the settings and click **OK**
8. From the **DXL Topology** page on McAfee ePO server B, click **Edit**.
    a. Select **Outgoing Bridge - Remote ePO Hub**, and click **Import Remote Hub Information**.
    b. Click **Choose File** and upload the .zip file for McAfee ePO server A, then click **OK**.
    c. Review the settings and click **OK**
9. Refresh the connections for McAfee ePO servers A and B.
    a. Select **Menu** → **Automation** → **Server Tasks** → **Manage DXL Brokers**, then click **Run**.
    b. From the **System Tree**, select the DXL broker and click **Wake Up Agents**.
    c. Select **Force complete policy and task update** and click **OK**.
10. Select **Menu** → **Systems** → **Data Exchange Layer Fabric** to verify the configuration.
    A line between two circles represents the bridge between DXL broker A and DXL broker B.

    Note

    If you do not see the connector between the broker icons, wait a few minutes for the DXL client to wake up and complete the configuration, or refresh the display.

11. For each McAfee ePO server, select a broker icon and click the **Bridges** tab, then the **Services** tab to verify the services are connected.

Bridged and non-bridged McAfee ePO server configuration examples

Deciding when to use bridge or non-bridge multiple McAfee ePO servers is based on whether you want to use same or different geolocations and cloud accounts.

McAfee ePO servers are bridged — A company bridges their USA and Germany McAfee ePO servers on a single DXL fabric to use their TIE database worldwide for consistent hash reputations. In this scenario, they use a single cloud account and single cloud storage geolocation.

McAfee ePO servers are not bridged — A company has not yet bridged their USA and Germany McAfee ePO servers on a single DXL fabric. They want parallel deployments for each geography because of a possible restriction where certain data can't be shared between countries. The USA and Germany sites each have separate McAfee ePO servers with separate TIE and Active Response servers. Each of them has different geolocations and uses different cloud accounts.

Endpoint roaming is not supported — A company has two non-bridged McAfee ePO servers assigned to different geolocations (USA and Germany). An employee travels to a different company site with her laptop managed by McAfee ePO server A and geolocation USA. When she connects to McAfee ePO server B in Germany, potential threats on her laptop do not appear in the Workspace managed by McAfee ePO server B.

Search in a DXL bridged environment

Create a super user account to extend the search (and reactions) to the endpoints where users do not have permission.

When executing a search where DXL brokers are managed by different McAfee ePO servers, the search applies only to managed endpoints where the user has permissions. To extend the search (and reactions) to endpoints where the user does not have permission, you can create a super user account. Searches executed from this account return results from all endpoints, regardless of permissions.

Task

1. Log on to the virtual appliance where the Active Response service is installed.
   Use the same credentials that were used when installing.
2. Use `$ su` command to open the super user file.
   File located at this location `vi /opt/McAfee/marserver/conf/users/superusers.conf` .
3. Add a line to the file that includes the McAfee ePO client user ID and the super user name separated by a colon.
   In an environment, you can add only the users who need to do a search across all the DXL bridged environment.
   On McAfee ePO, navigate to **Menu** → **Configuration** → **Server Settings** → **DXL Client for ePO** for client user ID.

   Note

   Get the client user ID in **Server Settings**, "client UID: {948617fa-6c76-4b7c-89ce-4f65a01cfb3f}" and want to make McAfee ePO login user "admin" as a super user, then open the superusers.conf file and update the user as shown below:
   {948617fa-6c76-4b7c-89ce-4f65a01cfb3f}:admin

   Once the super user file is updated, save the file and restart the Active Response server. Then, execute a HostInfo query and you will get hosts information from multiple McAfee ePO servers which have the same DXL fabric configuration.

   Note

   If the super user details are not updated in the file, Active Response search pulls information only from the respective McAfee ePO System Tree. To see the data across DXL fabric from any McAfee ePO, you should have the super user access.

Results

User with super user account can search in a DXL fabric and returns with a result from all endpoints, regardless of permissions.

Configuring McAfee Advanced Threat Defense

Configure the McAfee Advanced Threat Defense server with Active Response

You can integrate and configure McAfee® Advanced Threat Defense with Active Response to view the McAfee Advanced Threat Defense sandbox analysis reports on the Workspace. These reports can also be downloaded as a PDF file.

Before you begin

- Make sure that you have the McAfee Advanced Threat Defense URL and logon credentials.
- Verify you are running McAfee Advanced Threat Defense version 4.4 or later.

You can view the McAfee Advanced Threat Defense connection status in the **Active Response Health Status** page and reputation status in the **Sandbox Results** card. The status page can confirm if McAfee Advanced Threat Defense is active and responding to queries.

Note

Only one Advanced Threat Defense server can be configured with this version of Active Response. Advanced Threat Defense supports a standalone server or the primary server of a cluster of physical or virtual servers.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Configuration** → **Server Settings** → **Advanced Threat Defense Server**, then click **Edit**.
3. Enter the URL of the Advanced Threat Defense server.
4. Enter your user name and password.
5. Click **Validate Certificate** and save the configuration.
   An error message appears if you are configuring an unsupported version of Advanced Threat Defense.
6. To disconnect the Advanced Threat Defense server from the Active Response environment, enable **Delete Connection** and save the configuration.

Configure McAfee Advanced Threat Defense on the TIE server

Enable the Advanced Threat Defense sandboxing feature in the TIE server management policy.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Policy** → **Policy Catalog**.
3. From the **Product** drop-down list, select **McAfee Threat Intelligence Exchange Server Management**.
4. Select **My Default** policy and enable McAfee Advanced Threat Defense on the **Sandboxing** tab.
5. Configure the McAfee Advanced Threat Defense server list, connection settings, and files types available, then click **Save** when finished.

Troubleshooting installation

Roll back content rules

You can roll back a content or trace rule when a content update causes issues in the endpoints. The last update of content rules can be rolled back to a previous version by creating a client task.

Two product properties are associated with the endpoint rules content rollback.

- **Blacklisted Rules Version** — The version that is not applied when upgraded.
- **Rules Version** — The current version of the client.

View the properties, then create a task to roll back the rule.

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Policy** → **Client Task Catalog**.
3. Under Client Task Types, locate and select Active Response 2.4.0.
4. Select **Roll Back Dat Rules**.
5. Click **New Task** and click **OK**.
   a. Type in a name for the task.
   b. In the **Roll Back Rules** text box, enter the version number of the rules you want to remove or block. When you run this task, a new blocked version is sent to the client and if one of them is already applied, the version automatically rolls back to the previously installed update.

      Note

      You can only roll back one rules version.

   c. Click **Save**.
6. Select **Menu** → **Policy** → **Client Task Assignments** to assign this new task to all applicable endpoints.
7. Verify the completion of the rollback in the **Threat Events** logs to see the status.

You can reuse this client task to roll back subsequent rules updates. In the **Roll Back Rules** text box, add a comma to separate the previous version number from the new version number to blacklist.

Installation error messages

Detailed endpoint installation errors are described in the **Threat Event Log** to inform you of missing or invalid dependencies.

If an installation fails, the error messages listed in the **Server Task Log** are generic and non-specific. Select **Menu** → **Reporting** → **Threat Event Log** and use the event ID `36639` to filter and display detailed error messages caused by deployment issues.

Error messages

Error code	Error Message	Description
0	UNKNOWN	Unknown error
1	ESP_MISSING_PACKAGE_ON_EPO	Endpoint Solutions Platform package missing on McAfee ePO
2	TP_MISSING_PACKAGE_ON_EPO	Threat Prevention package missing on McAfee ePO
3	TIE_MISSING_PACKAGE_ON_EPO	Threat Intelligence Exchange package missing on McAfee ePO
4	ATP_MISSING_PACKAGE_ON_EPO	Adaptive Threat Protection package missing on McAfee ePO
5	DXL_MISSING_PACKAGE_ON_EPO	Data Exchange Layer package missing on McAfee ePO
6	VSE_INSTALLED	VirusScan Enterprise installed
7	MA_INCOMPATIBLE_VERSION	McAfee Agent incompatible version installed
8	ESP_INCOMPATIBLE_VERSION	Endpoint Solutions Platform incompatible version installed
9	TP_INCOMPATIBLE_VERSION	Threat Prevention incompatible version installed
10	HIP_INCOMPATIBLE_VERSION	Host Intrusion Prevention incompatible version installed
11	ESP_INSTALLATION_FAILED	Endpoint Solutions Platform installation failed
12	TP_INSTALLATION_FAILED	Threat Prevention installation failed
13	TIE_INSTALLATION_FAILED	Threat Intelligence Exchange installation failed
14	ATP_INSTALLATION_FAILED	Adaptive Threat Protection installation failed
15	DXL_INSTALLATION_FAILED	Data Exchange Layer installation failed
16	MAR_INSTALLATION_FAILED	Active Response installation failed

Error code	Error Message	Description
17	ENS_INCOMPATIBLE_VERSION	Endpoint Security incompatible version installed (Non-Windows only)
18	ATP_INCOMPATIBLE_VERSION	Adaptive Threat Protection incompatible version installed
19	OS_INCOMPATIBLE_VERSION	Not a supported operating system version

Remove the software

Uninstall Active Response clients

You can remove Active Response clients from endpoints when they are no longer active or when there is a need to contain threats to affected endpoints.

This procedure doesn't remove Endpoint Security Threat Intelligence module, Endpoint Security Adaptive Threat Protection, or Data Exchange Layer.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Software** → **Product Deployment** → **New Deployment**.
3. Complete and save the new deployment information for the task that uninstalls the software.
4. On the Product Deployment page, from the **Action** drop-down list, select **Uninstall**. Then start the deployment to uninstall Active Response.

Uninstall Active Response extension

To completely remove Active Response from McAfee ePO, you must uninstall the extensions, related components, and client packages in a specific order.

Task

1. Log on to McAfee ePO as an administrator.
2. Select **Menu** → **Software** → **Extensions**.
3. In the **Extensions** pane, select Active Response to display all Active Response extensions.
4. Click **Remove** to uninstall the extensions in a specific order (the components are interdependent).
    a. Active Response Workspace extension
    b. Active Response UI extension
    c. Active Response license extension
    d. Active Response server extension
    e. Active Response client extension

COPYRIGHT

Trellix