QUANTUM

22 April 2025

CENTRAL DEPLOYMENT TOOL (CDT)

Administration Guide

CHECK POINT™

Check Point Copyright Notice

Important Information

Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.

Certifications

For third party independent certification of Check Point products, see the Check Point Certifications page.

Central Deployment Tool (CDT) Administration Guide

For more information about this tool, see sk111158.

Latest Version of this Document in English

Open the latest version of this document in a Web browser.
Download the latest version of this document in PDF format.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.
Please help us by sending your comments.

Revision History

Date	Description
22 April 2025	Release of CDT v2.1 Updated: ■ *"What's New" on page 15*
31 August 2024	Updated: ■ *"Requirements" on page 17*
22 August 2024	Updated (improved CLI syntax explanations): ■ *"Basic Mode" on page 26* ■ *"Advanced Mode" on page 37* ■ *"RMA Mode" on page 50* ■ *"CLI Syntax Quick Reference in the Expert mode" on page 110* ■ *"CDT in Gaia Clish" on page 120*
15 August 2024	Updated:
03 June 2024	Release of CDT v2.0 Updated: ■ *"What's New" on page 15* ■ *"Requirements" on page 17*
21 February 2024	Updated: ■ *"Deployment Plan File" on page 79* - the "`execute_script`" action
18 January 2024	Updated: ■ *"Introduction to CDT" on page 10*
31 October 2023	Release of CDT v1.9.8 Added *"What's New" on page 15*
20 June 2023	Updated: ■ *"CDT in Gaia Clish" on page 120* - in the "`start cdt execute`" command, added the missing "`filter`" syntax

Date	Description
13 June 2023	Updated: ■ Release of CDT v1.9.7 ■ *"Supported Actions" on page 80* - added the explanation about the "`iscritical`" attribute
12 June 2023	This unified Administration Guide replaces all Administration Guides for CDT versions 1.9.0 - 1.9.6
16 April 2023	Release of CDT v1.9.6
24 September 2022	Added *"Glossary" on page 140*
24 May 2022	Release of CDT v1.9.5
17 January 2022	Release of CDT v1.9.4
30 June 2021	Updated: ■ *"Installation Candidates List File" on page 77* ■ *"Deployment Plan File" on page 79* ■ *"Package Installation in Clusters" on page 94*
03 March 2021	Release of CDT v1.9.3
23 May 2021	Updated: ■ *"Installation Candidates List File" on page 77* ■ *"Deployment Plan File" on page 79* ■ *"Package Installation in Clusters" on page 94*
23 March 2021	Release of CDT v1.9.2
09 May 2021	Updated: ■ *"Installation Candidates List File" on page 77* ■ *"Deployment Plan File" on page 79* ■ *"Package Installation in Clusters" on page 94*
03 March 2021	Release of CDT v1.9.1

Date	Description
13 February 2021	Updated the description of the attribute "`connectivityupgrade`" in: ■ *"Elements of the CDT Primary Configuration File" on page 66* ■ *"Plan Settings" on page 80*
01 February 2021	Removed the `.tgz` extension from the CLI syntax (it is necessary to specify only the name of the CPUSE package file) in: ■ *"Specifying a CPUSE Clean Install Package when you Restore the RMA Backup Information" on page 63* ■ *"Package Installation in Clusters" on page 94* ■ *"CLI Syntax Quick Reference in the Expert mode" on page 110*
07 January 2021	Updated: ■ *"CDT Primary Configuration File" on page 66* - updated a note in the description of the element "`MailNotification`"
20 December 2020	Updated: ■ *"CDT Primary Configuration File" on page 66* - description and examples of the element "`MailNotification`" ■ *"Example 5 - Run a Script, Uninstall a Hotfix, Upgrade, Install a Hotfix, Log and Send Email, Pull a File" on page 92*
21 October 2020	Updated: ■ *"CDT in Gaia Clish" on page 120* - Installation Instructions for R80.30
29 September 2020	Release of CDT v1.9.0

Table of Contents

Introduction to CDT

Overview

Central Deployment Tool (CDT) is a tool that runs on Gaia Security Management Servers and Gaia Multi-Domain Security Management Servers.

With this tool you manage the installation of software packages from your Management Server to multiple Security Gateways and Cluster Members at the same time:

- Install and uninstall software packages.
- Do different actions - take snapshots, run shell scripts, push or pull files, and so on.
- Automate the RMA backup and restore procedure.

CDT handles cluster upgrades automatically - see *"Package Installation in Clusters" on page 94*.

CDT Installation Package

See sk111158 > section "**Downloads and Documentation**".

To see the installed CDT version and build, run in the Expert mode:

```
$CDTDIR/CentralDeploymentTool -v
```

CDT Limitations

See sk111158 > section **Known Limitations**.

CDT Workflows

Below are different workflows to use the Central Deployment Tool (CDT):

Basic workflow for an administrator

Generate an Installation Candidates List File	=>	Select Candidates	=>	Execute
Create a list if candidate Security Gateways and Cluster Members, on which to install a package		Select the applicable candidates from the Installation Candidates List File		Run the required operation on all selected candidates

CDT workflow to upgrade a single Security Gateway

When an administrator uses the CDT to install an Upgrade Package on a single Security Gateway, the CDT follows these steps:

1. CDT makes sure that the state of the Security Gateway is correct (all required processes are up and running)
2. CDT prepares Access Control Policy for the Security Gateway:
    a. Changes the version in the Security Gateway object.
    b. Changes the applicable configuration settings and Access Control Policy.
3. CDT executes the Deployment Plan File on the Security Gateway:
    a. Runs Pre-Script(s).
    b. Updates the CPUSE version.
    c. Pushes the CPUSE package(s) to the Security Gateway.
    d. Imports the CPUSE package(s) on the Security Gateway.
    e. Installs the CPUSE package(s) on the Security Gateway.
    f. Makes sure the Access Control Policy is installed on the Security Gateway.
    g. CDT v1.9.7 and higher: Makes sure the Threat Prevention Policy is installed on the Security Gateway.
    h. Runs Post-Script(s).
4. CDT makes sure that the state of the Security Gateway is correct (all required processes are up and running).

Important - You must manually install all other applicable Security Policies:

- If you used CDT v1.9.7 and higher: install QoS, Desktop policies.
- If you used CDT v1.9.6 and lower: install Threat Prevention, QoS, Desktop policies.

CDT workflow to upgrade Cluster Members in High Availability mode

When an administrator uses the CDT to install an Upgrade Package on a ClusterXL in High Availability mode, the CDT follows these steps:

1. CDT makes sure that the states of the Cluster Members are correct (**Active** and **Standby**).
2. CDT prepares Access Control Policy for the Cluster:
    a. Changes the version in the Cluster object.
    b. Changes the applicable configuration settings and Access Control Policy.
3. CDT executes the Deployment Plan File on the Standby Cluster Members.
    a. Runs Pre-Script(s).
    b. Updates the CPUSE version.
    c. Pushes the CPUSE package(s) to the Cluster Members.
    d. Imports the CPUSE package(s) on the Cluster Members.
    e. Installs the CPUSE package(s) on the Cluster Members.
    f. Makes sure the Access Control Policy is installed on the Cluster Members.
    g. CDT v1.9.7 and higher: Makes sure the Threat Prevention Policy is installed on the Cluster Members.
    h. Runs Post-Script(s).
4. CDT runs a ClusterXL Upgrade:
    a. Makes sure the upgraded Cluster Member is in the **Standby** or **Ready** state.
    b. Performs cluster failover to one of the upgraded Cluster Members.

    Note - The CDT uses the:
    - Multi-Version Cluster (MVC) Upgrade when you upgrade to R80.40 or higher.
    - Full Connectivity Upgrade (FCU) when you upgrade to R80.30 or lower.
5. CDT executes the Deployment Plan File on the former **Active** Cluster Member.
6. CDT makes sure that the states of the Cluster Members are correct (Active and Standby).

Important - You must manually install all other applicable Security Policies:

- If you used CDT v1.9.7 and higher: install QoS, Desktop policies.
- If you used CDT v1.9.6 and lower: install Threat Prevention, QoS, Desktop policies.

CDT workflow to install a Hotfix on a Security Gateway or Cluster

When an administrator uses the CDT to install a Hotfix on a single Security Gateway or Cluster, the CDT follows these steps:

1. CDT makes sure that the state:
   - CDT makes sure that the state of the Security Gateway is correct (all required processes are up and running)
   - CDT makes sure that the states of the Cluster Members are correct (**Active** and **Standby**)
2. CDT executes the Deployment Plan File:
   a. Runs Pre-Script(s).
   b. Updates the CPUSE version.
   c. Pushes the CPUSE package(s) to the Security Gateway / Cluster Members.
   d. Imports the CPUSE package(s) on the Security Gateway / Cluster Members.
   e. Installs the CPUSE package(s) on the Security Gateway / Cluster Members.
   f. Makes sure the Access Control Policy is installed on the Security Gateway / Cluster Members.
   g. CDT v1.9.7 and higher: Makes sure the Threat Prevention Policy is installed on the Security Gateway / Cluster Members.
   h. Runs Post-Script(s).
3. CDT makes sure that the state is correct:
   - On the Security Gateway all required processes are up and running
   - Cluster Members are in the states **Active** and **Standby**

Important - You must manually install all other applicable Security Policies:

- If you used CDT v1.9.7 and higher: install QoS, Desktop policies.
- If you used CDT v1.9.6 and lower: install Threat Prevention, QoS, Desktop policies.

What's New

Below is the summary of the CDT improvements.

CDT Version	CDT Release Date	What's New
2.1	22 April 2025	■ Added support for the R82.10 Security Gateways. ■ Improved error handling and reporting. ■ Fixed various issues.
2.0	03 June 2024	■ Resolved a limitation to allow the CDT management commands when a non-default port is used. ■ Fixed an issue with the Basic Mode in CDT v1.9.8.
1.9.8	31 October 2023	■ Support for a cluster installed in a Public Cloud (Amazon Web Services, Microsoft Azure, and Google Cloud Platform). ■ New CLI parameter to run several different CDT sessions at the same time: • "`-session=<Name of Management Session without Spaces>`" in the Expert mode syntax "`$CDTDIR/CentralDeploymentTool`" ◦ *"Advanced Mode" on page 37* ◦ *"RMA Mode" on page 50* ◦ *"CLI Syntax Quick Reference in the Expert mode" on page 110* • "`session <Name of Management Session without Spaces>`" in the Gaia Clish syntax "`set cdt candidates`" and "`start cdt`" ◦ *"CDT in Gaia Clish" on page 120* Note - Without this CLI parameter: • On a Security Management Server, you can run only one CDT session at a time. • On a Multi-Domain Security Management Server, you can run different CDT sessions on different Domain Management Servers (only one CDT session at a time in each Domain Management Server).
1.9.7	13 June 2023	■ Improved cluster failover during an upgrade. ■ CDT now installs Threat Prevention policy at the end of a package installation.

CDT Version	CDT Release Date	What's New
1.9.6	16 April 2023	■ Performance improvement during the generation of an Installation Candidates List File in a large management database. ■ Performance improvement in VRRP Cluster handling. ■ General code improvements and fixes.
1.9.5	24 May 2022	■ Performance improvement - CDT does not split packages while transferring them to the Security Gateways(saves the time of the split and join operations). ■ New CLI parameter "`-filter=<Filter File>`" in the RMA backup syntax "`$CDTDIR/CentralDeploymentTool -rma -generate`" (*"RMA Mode" on page 50*). ■ Before the upgrade, CDT transfers policy files to the Security Gateways and Cluster Members. ■ General code improvements and fixes.
1.9.4	17 January 2022	■ General code improvements and fixes.
1.9.3	04 July 2021	■ Ability to install the CDT tool with CPUSE. ■ General code improvements and fixes.
1.9.2	23 March 2021	■ Ability to open SmartConsole while the CDT tool runs. ■ General code improvements and fixes.
1.9.1	03 March 2021	■ Support for Gaia Fast Deployment (Blink) images in the RMA restore operation (*"Restoring RMA Backup Information" on page 56*). ■ General code improvements and fixes.
1.9.0	29 September 2020	■ Ability to run the CDT commands from Gaia Clish with the help of the Gaia Dynamic CLI (*"CDT in Gaia Clish" on page 120*). ■ General code improvements and fixes.

Note - Versions earlier than v1.9.0 are considered obsolete.

Requirements

To see the installed CDT version and build, run in the Expert mode on your Management Server:

```
$CDTDIR/CentralDeploymentTool -v
```

Example output:

```
[Expert@MyMgmt:0]# $CDTDIR/CentralDeploymentTool -v
Central Deployment Tool (version 1.9.5 build #990180640)
[Expert@MyMgmt:0]#
```

Notes - CDT versions earlier than v1.9.0 are considered obsolete.

Requirements for Security Management Servers and Multi-Domain Security Management Servers

1. Below is the summary of the CDT versions and the supported Management Server versions.

CDT Version	CDT Release Date	Supported Versions
2.0	03 June 2024	from R80.10 to R81.20
1.9.8	31 October 2023	from R80.10 to R81.20
1.9.7	13 June 2023	from R80.10 to R81.20
1.9.6	16 April 2023	from R80.10 to R81.20
1.9.5	24 May 2022	from R80.10 to R81.20
1.9.4	17 January 2022	from R77.00 Gaia to R81.10
1.9.3	04 July 2021	from R77.00 Gaia to R81.10
1.9.2	23 March 2021	from R77.00 Gaia to R81.10
1.9.1	03 March 2021	from R77.00 Gaia to R81.10
1.9.0	29 September 2020	from R77.00 Gaia to R81.10

2. You must install the recommended version of the CPUSE Deployment Agent (sk92449) on your Management Server.

   This is required to install packages from the Management Server on the Security Gateways / Cluster Members.

3. To install the CDT tool of a higher version than the current CDT tool version on your Management Server, follow one of these procedures:

CDT Package	Installation Instructions
CPUSE Offline package (TAR)	See sk92449. **Workflow in Gaia Portal** a. Import the package. b. Install the package. **Workflow in Gaia Clish** a. Transfer the package to the Management Server. b. Import the package. c. Install the package.

CDT package (TGZ)	Install it manually.
	Procedure
	a. Transfer the TGZ package to the Management Server.
	b. Connect to the command line on the Management Server.
	c. Log in to the Expert mode.
	d. Extract the RPM package from the TGZ archive:
	`tar xvfz /<Path To>/<CDT Package>.tgz`
	e. Upgrade the current RPM package:
	`rpm -Uhv --force CPcdt-00-00.i386.rpm`
	f. Examine the installed version:
	`$CDTDIR/CentralDeploymentTool -v`

Requirements for Security Gateways and Cluster Members

- Supported versions for an installation of a Hotfix package:

CDT Version on the Management Server	CDT Release Date	Supported Versions of Security Gateways, Clusters, Security Groups
2.0	03 June 2024	from R80.10 to R81.20 from R80.20SP to R81.20
1.9.8	31 October 2023	from R80.10 to R81.20
1.9.7	13 June 2023	from R80.20 to R81.20
1.9.6	16 April 2023	from R80.20 to R81.20
1.9.5	24 May 2022	from R80.20 to R81.20
1.9.4	17 January 2022	from R77.30 Gaia to R81.10
1.9.3	04 July 2021	from R77.30 Gaia to R81.10
1.9.2	23 March 2021	from R77.30 Gaia to R81.10
1.9.1	03 March 2021	from R77.30 Gaia to R81.10
1.9.0	29 September 2020	from R77.30 Gaia to R81.10

- Supported versions for an installation of an upgrade package:

CDT Version on the Management Server	CDT Release Date	Supported Versions of Security Gateways, Clusters, Security Groups
2.0	03 June 2024	from R80.10 to R81.20 from R80.20SP to R81.20
1.9.8	31 October 2023	from R80.10 to R81.20
1.9.7	13 June 2023	from R80.20 to R81.20
1.9.6	16 April 2023	from R80.20 to R81.20
1.9.5	24 May 2022	from R80.20 to R81.20
1.9.4	17 January 2022	from R75.40 Gaia to R81.10
1.9.3	04 July 2021	from R75.40 Gaia to R81.10
1.9.2	23 March 2021	from R75.40 Gaia to R81.10
1.9.1	03 March 2021	from R75.40 Gaia to R81.10
1.9.0	29 September 2020	from R75.40 Gaia to R81.10

- Supported versions for the RMA Mode (*"RMA Mode" on page 50*):

  Notes:

  - This summary table does not include Security Gateways, on which you performed a minor upgrade.
  - The RMA Mode does not support Quantum Maestro Security Groups.

CDT Version on the Management Server	CDT Release Date	Supported Versions of Security Gateways, Clusters
2.0	03 June 2024	from R80.10 to R81.20
1.9.8	31 October 2023	from R80.10 to R81.20
1.9.7	13 June 2023	from R80.20 to R81.20
1.9.6	16 April 2023	from R80.20 to R81.20
1.9.5	24 May 2022	from R80.20 to R81.20
1.9.4	17 January 2022	from R77.30 Gaia to R81.10
1.9.3	04 July 2021	from R77.30 Gaia to R81.10
1.9.2	23 March 2021	from R77.30 Gaia to R81.10
1.9.1	03 March 2021	from R77.30 Gaia to R81.10
1.9.0	29 September 2020	from R77.30 Gaia to R81.10

  Requirements for the RMA Backup and RMA Restore to work correctly:

  - For the Security Gateway to connect to its Management Server, on the Security Gateway you must use the interface configured as the Management Interface in Gaia OS.
  - The communication between the Security Gateway and the Management Server must rely on the Security Gateway's default gateway and not on static routes.

- Before you can install a package with CDT on a Security Gateway / Cluster Member, you **must**:

  1. Configure the Security Gateway / Cluster Member with the Gaia First Time Configuration Wizard.

     Note - This requirement does **not** apply to the **RMA Restore mode**.

  2. Configure the Secure Internal Communication (SIC) in SmartConsole with the Security Gateway / Cluster Member.

     Note - This requirement does **not** apply to the **RMA Restore mode**.

  3. Install the Access Control policy at least one time on the Security Gateway / Cluster Member.

     Note - This requirement does **not** apply to the **RMA Restore mode**.

Operation Modes

Central Deployment Tool (CDT) can run in these operation modes:

Mode	Description
"Basic Mode" on page 26	Installs a package and run Pre-Installation and Post-Installation scripts on the specified Security Gateways and Cluster Members.
"Advanced Mode" on page 37	Runs a Deployment Plan File (see *"Deployment Plan File" on page 79*) - a list of configured actions (such as a major upgrade, a Hotfix installation, run a post-installation script, and so on) on the specified Security Gateways and Cluster Members. **Best Practice** - We recommend this mode to install more than one package in the same CDT execution. For example: Major Upgrade and Jumbo Hotfix Accumulator.
"RMA Mode" on page 50	Automates the RMA backup and RMA restore process.

Basic Mode

In This Section:

In CDT **Basic Mode** you:

- Install one Hotfix or upgrade package, and run: user Pre-Installation scripts, user Post-Installation scripts, or the two of types of scripts.
- Run the CDT in the **preparations** and **extended preparations** modes.

Workflow

Step	Description
1	Connect to the command line on your Management Server you use to install software packages.
2	Log in to the Expert mode.
3	Install the CDT RPM package (if it is not already installed on your Management Server) from sk111158.

Step	Description
4	Edit the `$CDTDIR/CentralDeploymentTool.xml` file to change the settings. See *"CDT Primary Configuration File" on page 66*. ■ Add / configure the "**<PackageToInstall>**" element: You must specify the absolute path (with the file name) to the CPUSE Offline package you wish to install. For cluster upgrades, you can add an optional attribute to *prevent* a Connectivity Upgrade. ■ Add / configure the "**<CPUSE>**" element to specify the absolute path to the CPUSE RPM package. ■ **Optional:** Add / configure the "**<PreInstallationScript>**" and "**<PostInstallationScript>**" elements to run the Pre-Installation and Post-Installation user scripts. See *"Elements of the CDT Primary Configuration File" on page 66*.
5	Generate the Installation Candidates List File (see below) to get a full list of the Security Gateways and Cluster Members connected to your Management Server. See *"Generating an Installation Candidates List File" on the next page*. **Note** - You can edit the Installation Candidates List File to make sure the specified Security Gateways are not included (see *"Installation Candidates List File" on page 77*).
6	**Optional:** Run preparations or extended preparations before the installation itself, to decrease the total time it takes to install the packages during maintenance windows. See *"Preparations (Pre-Installations)" on the next page* and *"Extended Preparations (Extended Pre-Installations)" on page 29*. The CDT runs all the configured Pre-Installation scripts.
7	Install the selected package and run all Pre-Installation and Post-Installation scripts. See *"Installation" on page 31*. **Note** - If you use *preparations*, or *extended preparations* mode, the CDT does not run the Pre-Installation scripts again.

Generating an Installation Candidates List File

To generate an Installation Candidates List File (see *"Installation Candidates List File" on page 77*), run in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -generate <Path to and Desired Name of Installation Candidates List File>.csv`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -generate <Path to and Desired Name of Installation Candidates List File>.csv <IP Address or Name of Domain Management Server>`

Preparations (Pre-Installations)

If you have a narrow maintenance window, use the **preparations mode** and prepare in advance.

In this scenario, the CDT follows these steps:

1. Sends the installation package to the Security Gateways (to the `/var/log/upload/` directory).
2. Sends the CPUSE Deployment Agent package to the Security Gateways (to the `/var/log/upload/` directory).
3. Runs the user Pre-Installation scripts.
4. Does **not** update the CPUSE Deployment Agent package.
5. Does **not** start the actual package installation.

To use simple preparations on all marked candidates in the Installation Candidates List File (see *"Installation Candidates List File" on page 77*), run in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -preparations <Path to Installation Candidates List File>.csv`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -preparations <Path to Installation Candidates List File>.csv <IP Address or Name of Domain Management Server>`

Extended Preparations (Extended Pre-Installations)

You can extend the preparations flow. In this scenario, the CDT follows these steps:

1. Sends the installation package to the Security Gateways (to the `/var/log/upload/` directory).
2. Sends the CPUSE Deployment Agent package to the Security Gateways (to the `/var/log/upload/` directory).
3. Runs the user Pre-Installation scripts on the Security Gateways.
4. Updates the CPUSE Agent on the Security Gateways.

   Note - Update of the CPUSE Agent might cause short connectivity loss in rare cases.
5. Imports and verifies the installation package with CPUSE.
6. Does **not** start the actual package installation.

To use extended preparations on all marked candidates in the Installation Candidates List File (see *"Installation Candidates List File" on page 77*), run in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -extended_preparations <Path to Installation Candidates List File>.csv`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -extended_preparations <Path to Installation Candidates List File>.csv <IP Address or Name of Domain Management Server>`

Installation

1. To start a full installation on all marked candidates in the Installation Candidates List File (see *"Installation Candidates List File" on page 77*), run in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -install <Path to Installation Candidates List File>.csv`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -install <Path to Installation Candidates List File>.csv <IP Address or Name of Domain Management Server>`

2. The installation starts.

   The CDT shows the installation progress on the screen.

   Note - CDT writes the progress details at 5 seconds intervals to log files.

   Log files on a Security Management Server

File	Description

■ If you specified the parameter "`-session=<Name of Management Session without Spaces>`":
`$CDTDIR/CDT_status_<Name of Management Session without Spaces>.txt`
Example: `$CDTDIR/CDT_status_MySession.txt`
 	
■ If you did not specify the parameter "`-session`":
`$CDTDIR/CDT_status.txt`
	Full description of the last completed step and the current step of all Security Gateways and Cluster Members statuses.

■ If you specified the parameter "`-session=<Name of Management Session without Spaces>`":
`$CDTDIR/CDT_status_<Name of Management Session without Spaces>_brief.txt`
Example: `$CDTDIR/CDT_status_MySession_brief.txt`
 	
■ If you did not specify the parameter "`-session`":
`$CDTDIR/CDT_status_brief.txt`
	Brief description (current step only) of all Security Gateways and Cluster Members statuses currently in execution.
	Useful if your screen area is small.

Log files on a Multi-Domain Security Management Server

File	Description

■ If you specified the parameter "`-session=<Name of Management Session without Spaces>`":
`$CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_<Name of Management Session without Spaces>.txt`
Example: `$CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession.txt`
 	
■ If you did not specify the parameter "`-session`":
`$CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>.txt`
Example: `$CDTDIR/CDT_status_MyDomainServer_MyDomain.txt`
	Full description of the last completed step and the current step of all Security Gateways and Cluster Members statuses.

File	Description

■ If you specified the parameter "`-session=<Name of Management Session without Spaces>`":
`$CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_<Name of Management Session without Spaces>_brief.txt`
Example: `$CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession_brief.txt`
 	
■ If you did not specify the parameter "`-session`":
`$CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_brief.txt`
Example: `$CDTDIR/CDT_status_MyDomainServer_MyDomain_brief.txt`
	Brief description (current step only) of all Security Gateways and Cluster Members statuses currently in execution.
	Useful if your screen area is small.

Best Practice - We recommend to run the `watch` command to read the file continuously.
Example: `watch -d cat $CDTDIR/CDT_status.txt`

3. All failures in the installation cause an error.

   - By default, an error in each action **is** blocking.

     The installation on a Security Gateway or Cluster does **not** continue.

     The CDT sends an error report to the configured email address.

     Note - The error is also blocking if you configured the "`<PreInstallationScript>`" element or "`<PostInstallationScript>`" element with the attribute `IsBlocking="true"` (see *"Elements of the CDT Primary Configuration File" on page 66*).

   - If you configured the applicable action in the Deployment Plan File with the attribute `iscritical="false"`, then an error in an action is **not** blocking.

     The installation continues, and the CDT logs and status file show a successful installation.

Retry Operation

If the installation failed on some of the Security Gateways or Cluster Members, but continues on the remaining Security Gateways:

1. Manually resolve the issue on the failed Security Gateways and Cluster Members.
2. Run one more instance of the CDT in **Retry Mode** for the failed Security Gateways and Cluster Members.

CDT tries to continue execution on failed Security Gateways and Cluster Members, starting from the last failed step.

Retry is only possible when the CDT runs.

Procedure

1. Connect to the command line on the Management Server over SSH.
2. Log in to the Expert mode.
3. Run:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -retry`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -retry <IP Address or Name of Domain Management Server>`

4. CDT detects that a different instance of the CDT runs and notifies that CDT instance to retry the same operation on all the failed Security Gateways.

Advanced Mode

In This Section:

CDT **Advanced Mode** completes a Deployment Plan File on each remote Security Gateway.

The Deployment Plan File can run a number of actions one after the other.

For the full list of actions, see *"Deployment Plan File" on page 79*.

Workflow

Step	Description
1	Connect to the command line on your Management Server you use to install software packages.
2	Log in to the Expert mode.
3	Install the CDT RPM package (if it is not already installed on your Management Server) from sk111158.
4	Edit the `$CDTDIR/CentralDeploymentTool.xml` file to change the settings. See *"CDT Primary Configuration File" on page 66*. Add / configure the **"<CPUSE>"** element to specify the absolute path to the CPUSE RPM package. See *"Elements of the CDT Primary Configuration File" on page 66*. **Important** - Make sure the elements **"<PackageToInstall>"** and **"<PreInstallationScript>"** do **not** exist in the `$CDTDIR/CentralDeploymentTool.xml` file. Otherwise, CDT runs in the Basic Mode.

Step	Description
5	Edit the Deployment Plan File with the actions sequence as described in the Deployment Plan File section. See *"Deployment Plan File" on page 79*. **Best Practice** - To decrease the total time it takes to install the packages, create a Deployment Plan File without installation actions, and run it in advance.
6	Generate the Installation Candidates List File to get a full list of the Security Gateways and Cluster Members connected to your Management Server. See *"Generating an Installation Candidates List File" on the next page*. You can do one of these: ■ Edit the Installation Candidates List File. ■ Create a Filter File to exclude the specified Security Gateways and Cluster Members (in CDT v1.9.5 and above).
7	Run the Deployment Plan File. See *"Execution of a Deployment Plan File" on page 40*.

Generating an Installation Candidates List File

To generate an Installation Candidates List File (see *"Installation Candidates List File" on page 77*), run in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -generate -candidates=<Path to and Desired Name of Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -generate -candidates=<Path to and Desired Name of Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml -server=<IP Address or Name of Domain Management Server> [-session=<Name of Management Session without Spaces>]`

Notes:

- The CDT generates an Installation Candidates List File, which is filtered only based on the first package that appears in the Deployment Plan File.
- The "`-session`" parameter is optional (available from CDT v1.9.8).
  Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Execution of a Deployment Plan File

1. To run a Deployment Plan File on Security Gateways in the in the Installation Candidates List File (see *"Installation Candidates List File" on page 77*), run in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -execute -candidates=<Path to Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -execute -candidates=<Path to Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml -server=<IP Address or Name of Domain Management Server> [-session=<Name of Management Session without Spaces>]`

Note:
The "`-session`" parameter is optional (available from CDT v1.9.8).
Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

2. Installation starts.

   The CDT shows the installation progress on the screen.

   Note - CDT writes the progress details at 5 seconds intervals to log files.

   Log files on a Security Management Server

File	Description

■ If you specified the parameter "`-session=<Name of Management Session without Spaces>`":
`$CDTDIR/CDT_status_<Name of Management Session without Spaces>.txt`
Example: `$CDTDIR/CDT_status_MySession.txt`
 	
■ If you did not specify the parameter "`-session`":
`$CDTDIR/CDT_status.txt`
	Full description of the last completed step and the current step of all Security Gateways and Cluster Members statuses.

■ If you specified the parameter "`-session=<Name of Management Session without Spaces>`":
`$CDTDIR/CDT_status_<Name of Management Session without Spaces>_brief.txt`
Example: `$CDTDIR/CDT_status_MySession_brief.txt`
 	
■ If you did not specify the parameter "`-session`":
`$CDTDIR/CDT_status_brief.txt`
	Brief description (current step only) of all Security Gateways and Cluster Members statuses currently in execution.
	Useful if your screen area is small.

Log files on a Multi-Domain Security Management Server

File	Description

■ If you specified the parameter "`-session=<Name of Management Session without Spaces>`":
`$CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_<Name of Management Session without Spaces>.txt`
Example: `$CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession.txt`
 	
■ If you did not specify the parameter "`-session`":
`$CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>.txt`
Example: `$CDTDIR/CDT_status_MyDomainServer_MyDomain.txt`
	Full description of the last completed step and the current step of all Security Gateways and Cluster Members statuses.

File	Description

■ If you specified the parameter "`-session=<Name of Management Session without Spaces>`":
`$CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_<Name of Management Session without Spaces>_brief.txt`
Example: `$CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession_brief.txt`
 	
■ If you did not specify the parameter "`-session`":
`$CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_brief.txt`
Example: `$CDTDIR/CDT_status_MyDomainServer_MyDomain_brief.txt`
	Brief description (current step only) of all Security Gateways and Cluster Members statuses currently in execution.
	Useful if your screen area is small.

Best Practice - We recommend to run the `watch` command to read the file continuously.
Example: `watch -d cat $CDTDIR/CDT_status.txt`

3. All failures in the installation cause an error.

   - By default, an error in each action **is** blocking.

     The installation on a Security Gateway or Cluster does **not** continue.

     The CDT sends an error report to the configured email address.

   - If you configured the applicable action in the Deployment Plan File with the attribute `iscritical="false"`, then an error in an action is **not** blocking.

     The installation continues, and the CDT logs and status file show a successful installation.

Limiting the Execution of a Deployment Plan File

You can use one of these ways to limit the execution of a Deployment Plan File to specified Security Gateways:

- **Preferred** - Use a Filter File.

  You can specify a list of Security Gateways and clusters (**not** Cluster Members), for which to generate the Installation Candidates List File (see *"Installation Candidates List File" on page 77*):

  Procedure

  1. Prepare a plain-text file with a list of the object names of each applicable Security Gateway and Cluster (**not** Cluster Members).

     The object names in this file must be as they are configured in SmartConsole or SmartDashboard.

     You must write each object name on a different line in this file.

     Example:

     ```
     My_Gateway_1
     My_Cluster
     My_Gateway_3
     ```

2. When you generate the Installation Candidates List File, specify the Filter File:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -generate -candidates=<Path to and Desired Name of Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml -filter=<Path to Filter File, including File Extension> [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -generate -candidates=<Path to and Desired Name of Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml -filter=<Path to Filter File, including File Extension> -server=<IP Address or Name of Domain Management Server> [-session=<Name of Management Session without Spaces>]`

Note:
The "`-session`" parameter is optional (available from CDT v1.9.8). Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

3. When you run the Deployment Plan File, specify the Filter File:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -execute -candidates=<Path to Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml -filter=<Path to Filter File, including File Extension> [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -execute -candidates=<Path to Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml -filter=<Path to Filter File, including File Extension>> -server=<IP Address or Name of Domain Management Server> [-session=<Name of Management Session without Spaces>]`

Note:
The "`-session`" parameter is optional (available from CDT v1.9.8). Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

- Use the Installation Candidates List File (see *"Installation Candidates List File" on page 77*).

Retry Operation

If the installation failed on some of the Security Gateways or Cluster Members, but continues on the remaining Security Gateways:

1. Manually resolve the issue on the failed Security Gateways and Cluster Members.
2. Run a *different* instance of the CDT in **Retry Mode** for the failed Security Gateways and Cluster Members.

CDT tries to continue execution on failed Security Gateways and Cluster Members, starting from the last failed step.

Retry is only possible when the CDT runs.

Procedure

1. Connect to the command line on the Management Server over SSH.
2. Log in to the Expert mode.
3. Run:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -retry [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -retry -server=<IP Address or Name of Domain Management Server> [-session=<Name of Management Session without Spaces>]`

Note:
The "`-session`" parameter is optional (available from CDT v1.9.8).
Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

4. CDT detects that one more instance of the CDT runs and notifies that CDT instance to retry the same operation on all the failed Security Gateways.

Resume Operation

If the installation failed on some of the Security Gateways or Cluster Members, and *later* it is necessary to continue from the action that failed:

1. Manually resolve the issue on the failed Security Gateways and Cluster Members.
2. Run the CDT in **Resume Mode** for the failed Security Gateways and Cluster Members.

CDT detects on which Security Gateways and Cluster Members the deployment failed and resumes the execution from the last failed action.

Procedure

1. Connect to the command line on the Management Server over SSH.
2. Log in to the Expert mode.
3. Run:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -resume -deploymentplan=<Path to Deployment Plan File>.xml [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -resume -deploymentplan=<Path to Deployment Plan File>.xml -server=<IP Address or Name of Domain Management Server> [-session=<Name of Management Session without Spaces>]`

Note:
The "`-session`" parameter is optional (available from CDT v1.9.8).
Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

RMA Mode

In This Section:

You can use the CDT **RMA Mode** to collect the information from the Security Gateway about the installed software and configuration.

You can use this information to reconfigure the replacement Security Gateway:

- Backup information contains installed version, list of installed Hotfixes, some Check Point configuration files, and Gaia configuration database).
- To reconfigure the replacement Security Gateway, administrator needs to provide the CPUSE package for Clean Install and the CPUSE packages of the Hotfixes.

Important:

Requirements for RMA backup and RMA restore to work correctly:

- On the Security Gateway, to connect to the Management Server, you must use the interface configured as the Gaia Management Interface.
- The communication between the Security Gateway and the Management Server must rely on the Security Gateway's default gateway and not on static routes.

For configuration instructions, see the *Gaia Administration Guide* for your version of the Security Gateway.

Warning - Do **not** edit the RMA configuration file `RmaTool.xml` installed by the CDT package.

Workflow

Step	Description
1	Connect to the command line on your Management Server you use to install software packages.
2	Log in to the Expert mode.
3	Install the CDT RPM package (if it is not already installed) from sk111158.
4	Edit the `$CDTDIR/CentralDeploymentTool.xml` file to change the settings. See *"CDT Primary Configuration File" on page 66*. ■ Add / configure the "**Repository**" element to specify the location of package files. ■ Add / configure the "**<CPUSE>**" element to specify the absolute path to the CPUSE RPM package. See *"Elements of the CDT Primary Configuration File" on page 66*.
5	When you back up Security Gateways, do it on all applicable Security Gateways. Do one of these: ■ Generate an Installation Candidates List File to back up the specified Security Gateways. You can do one of these: • Edit the Installation Candidates List File. See *"Installation Candidates List File" on page 77*. • Create a Filter File to exclude the specified Security Gateways and Cluster Members (in CDT v1.9.5 and above). See the parameter "`-filter`" in these RMA procedures: ◦ *"Generating an Installation Candidates List File for RMA Backup" on page 57* ◦ *"Collecting RMA Backup from the Specified Remote Security Gateways" on page 58* ■ Use the "`-backupall`" option to back up all the Security Gateways in one command. See *"Collecting RMA Backup Information from all Remote Security Gateways" on page 59*.
6	When you restore a Security Gateway, do it on the applicable Security Gateway.
7	Make sure the Gaia Clish configuration was restored correctly on the applicable Security Gateway.

Collecting RMA Backup Information

- The **RMA Mode** backup operation saves minimal information for these:
  - All Security Gateways in the Installation Candidates List File (see *"Installation Candidates List File" on page 77*)

    or
  - All connected Security Gateways, if you use the "`-backupall`" option

  The information saved:
  - Number and Builds of the installed Check Point version.
  - List of all installed Hotfixes.
  - Check Point and Linux configuration files:

    Table: Configuration files

File	Description
`FTW_settings.conf`	Configuration file for Automatic First Time Configuration Wizard. The CLI command "`config_system`" also uses this file to run automatic First Time Configuration Wizard (sk69701).
`machine_settings.conf`	Output of the Gaia Clish command "`save configuration`".
`SIC_settings.conf`	Configuration file to restore SIC settings in the Check Point Registry (`$CPDIR/registry/HKLM_registry.data`).
`exported_sic_cert.p12`	SIC certificate file.
`additional_settings.sh`	Backup script (for example, to restore the cluster mode, SNMP extension, and other settings).

Table: Configuration files (continued)

File	Description
various.tar	Contains these files: **File** / **Contents of the File** `$CPDIR/conf/cp.license` — Installed Check Point licenses `$FWDIR/boot/boot.conf` — Specific Check Point boot parameters `$FWDIR/conf/objects.C` — Applicable objects configured in SmartDashboard or SmartConsole `$FWDIR/conf/fwauth.NDB` — Users configured in SmartConsole / SmartDashboard `$FWDIR/boot/modules/fwkern.conf` — Firewall kernel parameters and their values `$PPKDIR/conf/simkern.conf` (in R80.20 and above) `$PPKDIR/boot/modules/simkern.conf` (in R80.10 and below) — SecureXL kernel parameters and their values `$PPKDIR/conf/sim_aff.conf` (in R80.20 and above) `$PPKDIR/boot/modules/sim_aff.conf` (in R80.10 and below) — SecureXL Interface Affinity configuration `$FWDIR/conf/fwaffinity.conf` — CoreXL Interface Affinity configuration

Table: Configuration files (continued)

File	Description
	<table><tr><th>File</th><th>Contents of the File</th></tr><tr><td>$FWDIR/conf/dispatcher_mode.conf</td><td>CoreXL Dynamic Dispatcher (sk105261) and Firewall Priority Queues (sk105762) internal settings</td></tr><tr><td>$FWDIR/conf/dynamic_dispatcher_mode.conf</td><td>CoreXL Dynamic Dispatcher (sk105261) internal settings</td></tr><tr><td>$FWDIR/boot/mq.conf</td><td>Multi-Queue settings</td></tr><tr><td>/etc/snmp/userDefinedSettings.conf</td><td>User-defined SNMP settings (sk90860)</td></tr><tr><td>/boot/grub/grub.conf</td><td>Linux GRUB configuration file</td></tr><tr><td>/etc/rc.d/rc.local</td><td>Linux start-up script (administrator can add the desired Linux commands to this script to run at boot)</td></tr></table>

- CDT saves the RMA backup information on the Management Server in the repository path as configured in the CDT configuration file.

  Each Security Gateway's backup is saved in a file name corresponding to the Security Gateway's object name in the management database.

The size of the RMA backup file is approximately 200kB for each backed up Security Gateway or Cluster Member.

- Each time you change the settings of a Security Gateway (in SmartConsole, or in Gaia operating system), you must collect a new backup of that Security Gateway.
- **Optional:** Add more files to the RMA Backup.

  1. Prepare a plain-text file with a list of full paths to the files it is necessary to collect.
  2. Write full path to each file on a different line.
  3. Add this parameter to the syntax:

     ```
     -additional_files=<Path to and Name of File with List of Additional Files, including File Extension>
     ```

  Notes:

  - "*<File with List of Additional Files>*" is plain-text file that contains absolute paths to the files you want to add to the RMA Backup.
  - All the files you specify must be located on all the Security Gateways and Cluster Members.
    If a specified file is not located on one of the remote targets, the RMA Backup fails on that target.
  - You cannot backup the `/var/log/` directory.

Restoring RMA Backup Information

- The RMA restore operation uses the RMA backup information to reconfigure a replaced Security Gateway.
- Requirements for the RMA restore process:
  - The replaced Security Gateway appliance must be the same model as the replaced Security Gateway appliance.
  - The replaced Security Gateway must have the default username and password (`admin/admin`).

    If you changed the default username or password, restore the Gaia to factory defaults.
  - The replaced Security Gateway must have the same physical interface configuration as the replaced Security Gateway.
  - The replaced Security Gateway must have the same networking configuration (IP address, default gateway, and so on).
  - The replaced Security Gateway must **not** be configured with the Gaia First Time Configuration Wizard.

    If the First Time Configuration Wizard was already done, you must restore the Gaia to the factory defaults before you can run the RMA restore.
  - You must have all the required packages to install in the repository configured in the primary configuration file.

    That is, you must have the CPUSE package for Clean Install of the version and the CPUSE packages of all the Hotfixes that were installed on the replaced Security Gateway.

    To see the required packages and other backup information, run in the Expert mode:

    ```
    $CDTDIR/CentralDeploymentTool -rma -info -gateway=<Name of Security Gateway or Cluster Member Object>
    ```
  - If the CDT could not recognize the CPUSE package file name of the installed version, you must explicitly specify the name of the CPUSE package for Clean Install.

    See the syntax in the procedure *"RMA Mode" on page 50*.

Note - License information is not restored on Check Point appliance, because it depends on the appliance's MAC address.

Generating an Installation Candidates List File for RMA Backup

Run these commands in the Expert mode to generate an Installation Candidates List File (see *"Installation Candidates List File" on page 77*) for RMA Backup:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -rma -generate -candidates=<Path to and Desired Name of Installation Candidates List File>.csv [-additional_files=<Path to File with List of Additional Files, including File Extension>] [-filter=<Path to Filter File, including File Extension>] [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -rma -generate -candidates=<Path to and Desired Name of Installation Candidates List File>.csv [-additional_files=<Path to File with List of Additional Files, including File Extension>] [-filter=<Path to Filter File, including File Extension>] [-session=<Name of Management Session without Spaces>] -server=<IP Address or Name of Domain Management Server>`

Notes:

- The "`-additional_files`" parameter is optional.
  Use it to collect more files for the RMA Backup.
- The "`-filter`" parameter is optional (available from CDT v1.9.5).
  Use it to exclude the specified Security Gateways and Cluster Members.
- The "`-session`" parameter is optional (available from CDT v1.9.8).
  Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Collecting RMA Backup from the Specified Remote Security Gateways

You specify the remote Security Gateways based on the Installation Candidates List File (see *"Installation Candidates List File" on page 77*).

Run these commands in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -rma -backup -candidates=<Path to Installation Candidates List File>.csv [-additional_files=<Path to File with List of Additional Files, including File Extension>] [-filter=<Path to Filter File, including File Extension>] [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -rma -backup -candidates=<Path to Installation Candidates List File>.csv [-additional_files=<Path to File with List of Additional Files, including File Extension>] [-filter=<Path to Filter File, including File Extension>] [-session=<Name of Management Session without Spaces>] -server=<IP Address or Name of Domain Management Server>`

Notes:

- The "`-additional_files`" parameter is optional.
  Use it to collect more files for the RMA Backup.
- The "`-filter`" parameter is optional (available from CDT v1.9.5).
  Use it to exclude the specified Security Gateways and Cluster Members.
- The "`-session`" parameter is optional (available from CDT v1.9.8).
  Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Collecting RMA Backup Information from all Remote Security Gateways

In this case, you do not need the Installation Candidates List File (see *"Installation Candidates List File" on page 77*).

Run these commands in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -rma -backupall [-additional_files=<Path to File with List of Additional Files, including File Extension>] [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -rma -backupall [-additional_files=<Path to File (including File Extension) with the List of Additional Files>] [-session=<Name of Management Session without Spaces>] -server=<IP Address or Name of Domain Management Server>`

Notes:

- The "`-additional_files`" parameter is optional.
  Use it to collect more files for the RMA Backup.
- The "`-session`" parameter is optional (available from CDT v1.9.8).
  Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Showing the RMA Backup Information of a Specified Remote Security Gateway

Run these commands in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -rma -info -gateway=<Name of Security Gateway or Cluster Member Object> [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -rma -info -gateway=<Name of Security Gateway or Cluster Member Object> [-session=<Name of Management Session without Spaces>] -server=<IP Address or Name of Domain Management Server>`

Note:
The "`-session`" parameter is optional (available from CDT v1.9.8).
Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Restoring the RMA Backup Information on a Remote Security Gateway

Restoring without a Gaia Fast Deployment (Blink) Image

Use these commands in the Expert mode after you performed a clean install on the appliance.

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -rma -restore -gateway=<Name of Security Gateway or Cluster Member Object> -license=<Path to License File, including File Extension> [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -rma -restore -gateway=<Name of Security Gateway or Cluster Member Object> -license=<Path to License File, including File Extension> -server=<IP Address or Name of Domain Management Server> [-session=<Name of Management Session without Spaces>]`

Notes:

- The license path must be the full path to a new license file that you get from your account in *Check Point User Center*.
- The "`-session`" parameter is optional (available from CDT v1.9.8).
  Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Restoring with a Gaia Fast Deployment (Blink) Image

Starting in CDT v1.9.1, you can use these commands in the Expert mode when you perform a clean install on the appliance with a Gaia Fast Deployment (Blink) Image (see sk120193).

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -rma -restore -gateway=<Name of Security Gateway or Cluster Member Object> -license=<Path to License File, including File Extension> -package=<Path to Blink Image, including File Extension> [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -rma -restore -gateway=<Name of Security Gateway or Cluster Member Object> -license=<Path to License File, including File Extension> -package=<Path to Blink Image, including File Extension> -server=<IP Address or Name of Domain Management Server> [-session=<Name of Management Session without Spaces>]`

Notes:

- The license path must be the full path to a new license file that you get from your account in *Check Point User Center*.
- The "`-session`" parameter is optional (available from CDT v1.9.8).
  Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).
- The CDT fails the restore operation in these cases:
  - If the major software version of the Gaia Fast Deployment (Blink) Image is different than the major software version on the appliance when you collected the RMA Backup information.
  - If the Blink Image contains software packages (for example, hotfixes) that were not installed on the appliance when you collected the RMA Backup information.
  - If the Blink Image contains only some of the software packages (for example, hotfixes) that were installed on the appliance when you collected the RMA Backup information.
    The operation fails if the missing software packages do not exist in the RMA repository on the appliance.

Specifying a CPUSE Clean Install Package when you Restore the RMA Backup Information

If the CDT could not recognize the CPUSE package file name of the installed version, **you must explicitly specify the name** of the CPUSE package for Clean Install.

You can get this CPUSE package from the Home Page for your version.

Run these commands in the Expert mode:

Management Server	Commands
Security Management Server	`$CDTDIR/CentralDeploymentTool -rma -restore -gateway=<Name of Security Gateway or Cluster Member Object> -license=<Path to License File, including File Extension> -package=<Path to CPUSE Offline Package, including File Extension> [-session=<Name of Management Session without Spaces>]`

Multi-Domain Security Management Server	`mdsenv <IP Address or Name of Domain Management Server>`
	
	`$CDTDIR/CentralDeploymentTool -rma -restore -gateway=<Name of Security Gateway or Cluster Member Object> -license=<Path to License File, including File Extension> -package=<Path to CPUSE Offline Package, including File Extension [-session=<Name of Management Session without Spaces>] -server=<IP Address or Name of Domain Management Server>`

Notes:

- The license path must be the full path to a new license file that you get from your account in *Check Point User Center*.
- The "`-session`" parameter is optional (available from CDT v1.9.8).
  Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Verification

After you run an RMA restore, we recommend to make sure the Gaia Clish configuration was restored correctly on the Security Gateway or Cluster Member, VSX Gateway or VSX Cluster Member.

Examine these log files on your Management Server from the Security Gateway or Cluster Member:

Log File	Description
`/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of Security Gateway or Cluster Member Object>_FinalClishCommand.elg`	List of Gaia Clish commands that were run to restore the Gaia Clish configuration on the Security Gateway or Cluster Member
`/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of Security Gateway or Cluster Member Object>_FinalClishLog.elg`	Outputs of the Gaia Clish commands that were run to restore the Gaia Clish configuration on the Security Gateway or Cluster Member

Examine these log files on your Management Server from the VSX Gateway or VSX Cluster Member:

Log File	Description
`/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of VSX Gateway or VSX Cluster Member Object>_FinalClishCommand.elg`	List of Gaia Clish commands that were run to restore the Gaia Clish configuration on the VSX Gateway or VSX Cluster Member
`/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of VSX Gateway or VSX Cluster Member Object>_VS0ClishCommand.elg`	List of Gaia Clish commands that were run to restore the Gaia Clish configuration in the VSX context 0 (VS0)
`/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of VSX Gateway or VSX Cluster Member Object>_FinalClishLog.elg`	Outputs of the Gaia Clish commands that were run to restore the Gaia Clish configuration on the VSX Gateway or VSX Cluster Member
`/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of VSX Gateway or VSX Cluster Member Object>_VS0ClishLog.elg`	Outputs of the Gaia Clish commands that were run to restore the Gaia Clish configuration in the VSX context 0 (VS0)

Notes:

- If these files are not found on your Management Server, most likely the CDT could not transfer them from the Security Gateway or Cluster Member.
  You can find these files on the Security Gateway or Cluster Member in the `/var/log/CPrma/` directory.
- The log file with outputs of Gaia Clish commands contains special characters.
  To see this log file on Gaia OS, use the Linux `less` command.
  To see this log file on Windows OS, use an advanced text editor, like Notepad++.

CDT Primary Configuration File

In This Section:

The `$CDTDIR/CentralDeploymentTool.xml` file is the CDT's primary configuration file.

Important:

- Names of all elements in this XML file are case-sensitive.
- String values are case-sensitive.

The Central Deployment Tool installs a sample configuration file.

Elements of the CDT Primary Configuration File

Configuring the "<PackageToInstall>" element for the CDT Basic Mode

In the CDT **Advanced Mode** (see *"Advanced Mode" on page 37*), the packages to install are configured in the Deployment Plan File (see *"Deployment Plan File" on page 79*). If you configure the element "`<PackageToInstall>`" in the CDT primary configuration file, the CDT tries to run in **Basic Mode**.

The "<PackageToInstall>" element contains these attributes:

Attribute	Default value	Description
Path	None	Holds the absolute path (with the file name) on the Management Server to the CPUSE Offline package you wish to deploy.
ConnectivityUpgrade	true	Specifies whether to keep the current connections when you upgrade a cluster. Accepted values: ■ true - The CDT keeps the current connections during the upgrade. The CDT uses the: • Multi-Version Cluster (MVC) Upgrade when you upgrade to R80.40 or higher. • Full Connectivity Upgrade (FCU) when you upgrade to R80.30 or lower. ■ false - The CDT does not keep the current connections during the upgrade.

Configuring the "<Logging>" element

The "<Logging>" element controls the CDT messages its writes to the CDT log file (/var/log/CPcdt/<*execution time*>/<*log file name*>).

- Messages that the CDT shows on the screen.
- Messages that the CDT sends to the Syslog server.

The "<Logging>" element contains these Attributes:

Attribute	Default value	Description
FileLevel	DEBUG	Holds the value of the desired priority to filter the CDT log entries that are saved in the CDT log file (order below is from highest to lowest priority): 1. DEBUG 2. NORMAL 3. ERROR 4. ALWAYS 5. NONE For example, if FileLevel is set to ERROR, then messages marked as DEBUG and NORMAL are not written to the CDT log file - only messages marked as ERROR and ALWAYS are written to the CDT log file. For example, if FileLevel is set to NONE, then no messages are written to the CDT log file.
ScreenLevel	NORMAL	Holds the value of the desired priority to filter the CDT log entries that are displayed on the screen (order below is from highest to lowest priority): 1. DEBUG 2. NORMAL 3. ERROR 4. ALWAYS 5. NONE For example, if ScreenLevel is set to ERROR, then messages marked as DEBUG and NORMAL are not shown on the screen - only messages marked as ERROR and ALWAYS are shown on the screen. For example, if ScreenLevel is set to NONE, then no messages are shown on the screen.

Attribute	Default value	Description
`SyslogLevel`	`NONE`	Holds the value of the desired priority to filter the CDT log entries that are sent to a Syslog server. All CDT messages are sent to the *local 0* facility with the prefix `CDT` (order below is from highest to lowest priority): 1. `DEBUG` 2. `NORMAL` 3. `ERROR` 4. `ALWAYS` 5. `NONE` For example, if `SyslogLevel` is set to `ERROR`, then messages marked as `DEBUG` and `NORMAL` are not sent to a Syslog server - only messages marked as `ERROR` and `ALWAYS` are sent to a Syslog server. For example, if `SyslogLevel` is set to `NONE`, then no messages are sent to a Syslog server. Mapping between the CDT Log Level priority in the `SyslogLevel` element and the Syslog Severity: ■ `DEBUG` - `debug` ■ `NORMAL` - `normal` ■ `ERROR` - `err` ■ `ALWAYS` - `info` ■ `NONE` - Not sent to Syslog server
`Colors`	`false`	Configures if the CDT shows log messages on the screen in color. Accepted values: ■ `false` - The CDT uses your default terminal settings ■ `true` - The CDT uses color

Configuring the "<CPUSE>" element

The "<CPUSE>" element contains this attribute:

Attribute	Default value	Description
RPMPath	/sysimg/CPwrapper/linux/CPda/CPda-00-00.i386.rpm	Holds the absolute path (with the file name) on the Management Server to the CPUSE Agent's RPM package: CPda-00-00.i386.rpm

Configuring the "<Batch>" element

The "<Batch>" element contains these attributes:

Attribute	Default value	Description
MaxMachinesCount	UNLIMITED	Configures the maximal integer number of Security Gateways to put in one batch, when generating the Installation Candidates List File.
LatestAllowedDate	31/12/2099	The latest date, on which a new batch is permitted to start. Format is: DD/MM/YYYY.
LatestAllowedTime	23:59	The latest time, on which a new batch is permitted to start. Format is: HH:MM.

Configuring the "<PreInstallationScript>" element for the CDT Basic Mode

The "`<PreInstallationScript>`" element contains these attributes:

Attribute	Default value	Description
`Path`	`None`	Holds the absolute path (with the script name) on the Management Server to the user Pre-Installation shell script.
`IsBlocking`	`true`	Configures if the CDT stops or continues the package installation, if the user Pre-Installation script returns an error during its execution. Accepted values: ■ `true` - The CDT stops ■ `false` - The CDT continues

Configuring the "<PostInstallationScript>" element for the CDT Basic Mode

The "`<PostInstallationScript>`" element contains these attributes:

Attribute	Default value	Description
`Path`	`None`	Holds the absolute path (with the script name) on the Management Server to the user Post-Installation shell script.
`IsBlocking`	`true`	Configures if the CDT stop or continues the package installation, if the user Post-Installation script returns an error during its execution. Accepted values: ■ `true` - The CDT stops ■ `false` - The CDT continues

Duplicate the `<PreInstallationScript>` and `<PostInstallationScript>` elements based on the number of user shell scripts that the CDT needs to run on the Security Gateway.

The CDT runs these shell scripts in the order they are configured in the CDT primary configuration file.

Configuring the "<MailNotification>" element

Important - This step applies only if you configured a valid mail server on the Security Management Server or Multi-Domain Security Management Server. Otherwise, delete this element.

The "`<MailNotification>`" element contains this attribute:

Attribute	Default value	Description
`SendTo`	`aa@xyz.com`	Holds one valid e-mail address.

Notes:

- Add the "`<MailNotification>`" element for each e-mail address.
- CDT sends the email only to the default SMTP TCP port 25.

You must first configure a mail notification server on the Gaia OS of the Management Server (see the *Gaia Administration Guide* for your version):

Where	Instructions
In Gaia Portal	Perform these steps: 1. In the left navigation tree, click **System Management > Mail Notification**. 2. In the **Mail Server** field, enter the IP address or hostname of the Mail Server that receives the e-mails. For example: `mail.example.com` 3. In the **User Name** field, enter the username on the Mail Server that receives the e-mails. For example: `user@mail.example.com` 4. Click **Apply**.

Where	Instructions

In Gaia Clish	Perform these steps:
	1. Connect to the command line.
	2. Log in to the Gaia Clish.
	3. Configure the IP address or hostname of the Mail Server that receives the e-mails (for example, `mail.example.com`):
	`set mail-notification server <IP Address or HostName of Mail Server>`
	For example: `mail.example.com`
	4. Configure the username on the Mail Server that receives the e-mails (for example, `user@mail.example.com`):
	`set mail-notification username <UserName on Mail Server>@<Domain Name>`
	For example: `user@mail.example.com`
	5. Save the changes:
	`save config`
	6. Examine the configuration:
	`show mail-notification server`
	`show mail-notification username`

The Gaia OS sends an email notification in these events:

- Batch installation is completed.

  The e-mail message is the installation results for each Security Gateway and Cluster selected for the installation batch.

- Installation error.

  An installation error for a Security Gateway and Cluster generates an e-mail notification with the error details and applicable error logs.

Configuring the "<Repository>" element for RMA Mode

The "`<Repository>`" element contains this attribute:

Attribute	Default value	Description
`path`	`/home/admin/`	Holds the location of package files on the Management Server for the **RMA Mode** (see *"RMA Mode" on page 50*).

Example CDT Configuration File

These are basic examples of the primary configuration file `$CDTDIR/CentralDeploymentTool.xml`:

Example for the CDT Basic Mode

```
<?xml version="1.0" encoding="UTF-8" ?>
<CentralDeploymentTool>
  <PackageToInstall
Path="/home/admin/toInstall.tgz" ConnectivityUpgrade="true"/>
  <Logging
FileLevel
="DEBUG" ScreenLevel="NORMAL" SyslogLevel="DEBUG" Colors="false"/>
  <CPUSE RPMPath="/sysimg/CPwrapper/linux/CPda/CPda-00-00.i386.rpm"
/>
  <Batch MaxMachinesCount="UNLIMITED" />
  <PreInstallationScript
Path="/home/admin/PreScript.sh" IsBlocking="true"/>
  <PostInstallationScript
Path="/home/admin/PostScript.sh" IsBlocking="true"/>
  <MailNotification SendTo="abc@example.com"/>
  <MailNotification SendTo="xyz@example.com"/>
</CentralDeploymentTool>
```

Example for the CDT Advanced Mode

```
<?xml version="1.0" encoding="UTF-8" ?>
<CentralDeploymentTool>
 <Logging
FileLevel
="DEBUG" ScreenLevel="NORMAL" SyslogLevel="NONE" Colors="false"/>
 <CPUSE RPMPath="/sysimg/CPwrapper/linux/CPda/CPda-00-00.i386.rpm"/>
  <Batch
MaxMachinesCount
="UNLIMITED"
 LatestAllowedDate="31/12/2099" LatestAllowedTime="23:59"/>
  <MailNotification SendTo="abc@example.com"/>
  <MailNotification SendTo="xyz@example.com"/>
</CentralDeploymentTool>
```

Example for the CDT RMA Mode

```
<?xml version="1.0" encoding="UTF-8" ?>
<CentralDeploymentTool>
  <Logging
FileLevel
="DEBUG" ScreenLevel="NORMAL" SyslogLevel="NONE" Colors="false"/>
  <CPUSE RPMPath="/sysimg/CPwrapper/linux/CPda/CPda-00-
00.i386.rpm"/>
  <MailNotification SendTo="abc@example.com"/>
  <MailNotification SendTo="xyz@example.com"/>
  <Repository path="/home/admin/"/>
</CentralDeploymentTool>
```

User Scripts

The CDT can run multiple user shell scripts on the remote Security Gateways during the package installation.

User scripts must return one of these values:

Returned Value	CDT Behavior
0	The script was run successfully. If this was a Pre-installation script, the package installation continues.
222	Reboot the remote Security Gateway. After the reboot, package installation continues. **Note** - To reboot the Security Gateway, the script must exit with a return code 222.
All values other than 0 or 222	The script failed to run. If "`IsBlocking=true`" was set for this script, the package installation on the Security Gateway is stopped.

If you configured a user shell script as blocking in the CDT configuration file, the package installation on Security Gateway stops with an error.

In the CDT **Basic Mode** (see *"Basic Mode" on page 26*), user shell scripts run in the order you configured them in the CDT primary configuration file.

In the CDT **Advanced Mode** (see *"Advanced Mode" on page 37*), user shell scripts run based on the Deployment Plan File.

Notes:

- All user scripts configured for the CDT to run, must contain full paths for each instance of a script file.
- If you wish to run a Check Point command, then use this syntax in your script (see sk90441):

```
source /etc/profile.d/CP.sh ; <command>
```

Installation Candidates List File

The Installation Candidates List File is a CSV (comma-separated values) file the CDT generates.

This list contains the supported Security Gateways and Cluster Members in the Security Management Server or Domain Management Server database.

In this Installation Candidates List File you select the Security Gateways and Cluster Members, on which to install the CPUSE packages.

How it Works

The CDT generates the Installation Candidates List File for the package to install:

- In **Basic Mode** - based on the CDT configuration file (see *"CDT Primary Configuration File" on page 66*).
- In **Advanced Mode** - based on the first package that appears in the Deployment Plan File (see *"Deployment Plan File" on page 79*).

Example of an Installation Candidates List File

```
         Object Name ,         Cluster Name ,      IP Address ,  Version/JHF Take ,
      State , Upgrade Order

================================================================================================
============================
          MEM-68.146 ,     ClusterXL-68.148 ,  192.168.68.146 ,        R80.20/205 ,
     active ,             -
          MEM-68.147 ,     ClusterXL-68.148 ,  192.168.68.147 ,        R80.20/205 ,
    standby ,             1

          MEM-68.149 ,     ClusterXL-68.151 ,  192.168.68.149 ,        R80.30/237 ,
     active ,             -
          MEM-68.150 ,     ClusterXL-68.151 ,  192.168.68.150 ,        R80.30/237 ,
    standby ,             1

          MEM-68.162 ,     ClusterXL-68.164 ,  192.168.68.162 ,        R80.10/290 ,
     active ,             -
          MEM-68.163 ,     ClusterXL-68.164 ,  192.168.68.163 ,        R80.10/290 ,
    standby ,             1
           GW-68.152 ,                  N/A ,  192.168.68.152 ,        R80.20/205 ,
    gateway ,             -
           GW-68.153 ,                  N/A ,  192.168.68.153 ,        R80.30/237 ,
    gateway ,             -
```

The CDT assigns:

- A batch number to Security Gateways and Cluster Members that are eligible for package installation.
- A value of **N/A** to Security Gateways and that are not eligible for package installation. Do **not** change this value.
- A value of **Installed** to Security Gateways and Cluster Members, on which the requested package is already installed. Do **not** change this value.

To make sure the CDT does not install a package on the specified Security Gateways:

- You can change the candidates in the Installation Candidates List File after you generate this list.

  Edit the Installation Candidates List File with a plain-text editor. Make sure to save the file as a simple CSV file.
- In the Installation Candidates List File, you can change the values only in the "**Upgrade Order**" column.
- To exclude a Security Gateway or Cluster Member from a package installation, replace its batch number with "-" (minus character).
- Security Gateways and Cluster Members that are not eligible for package installation, have a value of **N/A**. Do **not** change this value.
- Security Gateways and Cluster Members that already have the requested package installed, have a value of **Installed**. Do **not** change this value.

For information about clusters, see *"Package Installation in Clusters" on page 94*.

Installation Batches

An installation batch is a set of one or more Security Gateways or Cluster Members.

CDT installs the packages in parallel on all batch members that have the same batch number.

When the installations on all candidates in a batch completes, the next batch is run.

The installation completes when all the batches are completed.

A new batch does not start, if it is after the date and time you specified in the configuration file.

Important - All Cluster Members of the same Cluster must be in the same batch.

Deployment Plan File

In This Section:

In the CDT **Advanced Mode** (see *"Advanced Mode" on page 37*), you can configure a sequence of actions for remote Security Gateways and Cluster Members in a user-define XML file called "Deployment Plan File". This is an XML file, which you create in a desired location with a desired name.

The XML structure of a Deployment Plan File:

```
<?xml version="1.0" encoding="UTF-8"?>
 <CDT_Deployment_Plan>
  <plan_settings>
    <name value="YOUR NAME" />
    <description value="YOUR DESCRIPTION" />
    <update_cpuse value="true" />
    <connectivityupgrade value="true" />
  </plan_settings>

  <!-- YOUR COMMENT FOR THIS ACTION -->
  <ACTION ATTRIBUTE="VALUE" />

  <!-- YOUR COMMENT FOR THIS ACTION -->
  <ACTION ATTRIBUTE="VALUE" />

  ....

 </CDT_Deployment_Plan>
```

Plan Settings

The "<plan_settings>" section in a Deployment Plan File contains:

Attribute	Default value	Description
name	None	Holds the name of the Deployment Plan File.
description	None	Holds the description of the Deployment Plan File.
update_cpuse	true	Specifies whether to update the CPUSE Agent on a remote Security Gateway before CDT does other actions.
connectivityupgrade	true	Specifies whether to keep the current connections when you upgrade a cluster. If the value of this attribute is "true", CDT uses the: ■ Multi-Version Cluster (MVC) Upgrade when you upgrade to R80.40 or higher. ■ Full Connectivity Upgrade (FCU) when you upgrade to R80.30 or lower.

Supported Actions

You can configure actions in a Deployment Plan File.

Important - By default, each action has a blocking behavior (has the implied attribute iscritical="true").
If an action fails, then the CDT stops the entire deployment.
You can configure the applicable actions as non-blocking.
If do so, and the action fails, the CDT continues to the next specified action.
To configure an action as non-blocking, at the end of the action syntax add this attribute: iscritical="false"
Example:

```
<execute_script path="/home/admin/cdt/preScript.sh"
iscritical="false" />
```

Table: Supported actions

Supported Action	Description and Attributes
`create_snapshot`	Creates a Gaia snapshot. **Attributes:** ■ `name` - The name of the snapshot to create. ■ `description` - The description of the snapshot. **Example:** `<create_snapshot name="Backup_JHA" description="Backup snapshot before Jumbo Hotfix Accumulator installation" />`
`download_from_cloud`	Downloads a package from the Check Point Cloud with CPUSE. **Attributes:** ■ `path` - Path to the package file on the Management Server (you must provide the package on the Management Server, even if the Security Gateways download it directly from the Check Point Cloud). **Example:** `<download_from_cloud path="/var/log/Check_Point_R81_JUMBO_HF_Bundle_T10_sk170114_FULL.tar" />`
`execute_command`	Runs a command on the Security Gateway in Bash shell (Expert mode). **Note** - Do not use special characters in your command (">", "|", "*", or other Bash-specific characters). **Attributes:** ■ `command` - The command you run. **Example:** `<execute_command command="cphaconf mvc on" />`

Table: Supported actions (continued)

Supported Action	Description and Attributes
`execute_script`	Runs a user shell script on the Security Gateway. **Notes:** ■ All user scripts configured for the CDT to run, must contain full paths for each instance of a file. ■ Reboot is not allowed in the user script. The script must exit with a return code. To reboot the Security Gateway, use exit code 222. **Attributes:** ■ `path` - The full local path to the user script file on the Management Server. ■ `execute_always` - Optional. If the value is set to "`true`", always runs the specified script. The default value is "`false`". **Example:** `<execute_script path="/home/admin/GetInformation.sh" execute_always="true" iscritical="false" />`
`import_package`	Sends a package to the remote Security Gateway (to the `/var/log/upload/` directory) and imports it with CPUSE. If you already sent the package with the "`send_package`" action, this action only imports the package on the remote Security Gateway. Required before you install the package. **Attributes:** ■ `path` - The full path on the Management Server to the package file you send. **Example:** `<import_package path="/var/log/Check_Point_R81_JUMBO_HF_Bundle_T10_sk170114_FULL.tar" />`

Table: Supported actions (continued)

Supported Action	Description and Attributes
`install_package`	Installs a package with CPUSE and validates that security policy is installed. When you upgrade one Security Gateway, runs the *Prepare New Policy* test before the package installation to make sure there is an updated policy for the Security Gateway to fetch. When you install a Hotfix on a cluster, runs the *Cluster Validation* test after policy validation. **Attributes:** ■ `path` - The full path on the Management Server to the package file you install. **Example:** `<install_package path="/var/log/Check_Point_R81_JUMBO_HF_Bundle_T10_sk170114_FULL.tar" />`
`log`	Generates a log message. **Attributes:** ■ `level` - The logging level of this message (`DEBUG`, `NORMAL`, `ERROR`, `ALWAYS`). ■ `value` - The message text. **Example:** `<log level="NORMAL" value="Finished installing a major upgrade." />`

Table: Supported actions (continued)

Supported Action	Description and Attributes
`pull_file`	Downloads a file from the remote Security Gateway to the Management Server. The file is saved with a prefix of the Security Gateway's object name (for example, `cluster01a_myfile.txt`). **Attributes:** ■ `remote_path` - The full remote path and filename you download on the remote Security Gateway. Use a full path with a file name, not only a directory. ■ `local_dir` - The full path on the Management Server to the directory, where you save the downloaded file. **Limitations:** ■ The size of the file must be less than 1 GB. **Example:** `<pull_file remote_path="/var/log/MyFile.txt" local_dir="/var/log/" />`
`push_file`	Uploads a file from the Management Server to the remote Security Gateway. **Attributes:** ■ `local_path` - The full local path and filename on the Management Server to the file you upload. ■ `remote_path` - The full remote path and filename on the remote Security Gateway, where you upload the file. **Example:** `<push_file local_path="/var/log/MyFile_for_GW1.txt" remote_path="/var/log/MyFile.txt" />`
`reboot`	Reboots the remote Security Gateway. **Attributes:** ■ None. **Example:** `<reboot/>`

Table: Supported actions (continued)

Supported Action	Description and Attributes
`send_email`	Sends an email message. **Attributes:** ■ `to` - The email recipient. ■ `subject` - The email subject. ■ `body` - The email body. **Example:** `<send_email to="admin@example.com" subject="Major upgrade was completed" body="Finished the installation of R81 major upgrade, preparing to install the R81 JHA" />`
`send_package`	Sends a package to the remote Security Gateway (to the `/var/log/upload/` directory) and does not import it with CPUSE. Required before you install the package. **Attributes:** ■ `path` - The full path on the Management Server to the package file you send. **Example:** `<send_package path="/var/log/Check_Point_R81_JUMBO_HF_Bundle_T10_sk170114_FULL.tar" />`
`uninstall_cpuse_package`	Uninstalls a package with CPUSE. **Attributes:** ■ `filename` - The file name (not the full path) of the package file you uninstall. **Example:** `<uninstall_cpuse_package filename="Check_Point_R81_JUMBO_HF_Bundle_T10_sk170114_FULL.tar" />`

Table: Supported actions (continued)

Supported Action	Description and Attributes
`uninstall_legacy_package`	**Important** - This action is deprecated in CDT v1.9.4 and higher. Uninstalls a legacy package (a package that was installed with the Legacy Installation procedure in Expert mode CLI). **Attributes:** ▪ `filename` - The Hotfix name you uninstall. **Example:** `<uninstall_legacy_package filename="R77_30_JHF_HF1.tgz" />`
`verify_package`	Examines an imported package with CPUSE if it is possible to install it on the remote Security Gateway. You must import the package on the remote Security Gateway. **Attributes:** ▪ `path` - The full path on the Management Server to the package file you examine. **Example:** `<verify_package path="/var/log/Check_Point_R81_JUMBO_HF_Bundle_T10_sk170114_FULL.tar" />`

Example Deployment Plan Files

This section provides example Deployment Plan Files.

Example 1 - Replace a File

This example Deployment Plan File does these actions on all applicable Security Gateways:

1. Backs up the file `/opt/productname/conf.txt` on the remote Security Gateway to the `/opt/CPcdt/ConfigurationBackupFiles/` directory on the Management Server.
2. Sends a file `/opt/CPcdt/conf.txt` from the Management Server to the remote Security Gateway as the `/opt/productname/conf.txt` file.

Example Deployment Plan File:

```
<?xml version="1.0" encoding="UTF-8"?>
 <CDT_Deployment_Plan>
  <plan_settings>
    <name value="Change configuration file" >
    <description value="Example Deployment Plan file - replace a
file" />
    <update_cpuse value="true" />
  </plan_settings>

  <!-- Backup the configuration file -->
  <pull_file remote_path="/opt/productname/conf.txt" local_
dir="/opt/CPcdt/ConfigurationBackupFiles/" />

  <!-- Push the new configuration file -->
  <push_file local_path="/opt/CPcdt/conf.txt" remote_
path="/opt/productname/conf.txt" />
 <CDT_Deployment_Plan>
```

Example 2 - Run a Script to Get Information

This example Deployment Plan File does these actions on all applicable Security Gateways:

1. Runs the script `getInformation.sh`, found on the Management Server in the `/home/admin/` directory.

   This script:

   a. Collects the desired information on the remote Security Gateway (such as the installed policy, the installed license, and so on)

   b. Saves its log to the `/home/admin/log.txt` file on the remote Security Gateway

   Example script:

   ```
   #!/bin/bash
   LOG_FILE="/home/admin/log.txt"
   cpstat -f policy >> $LOG_FILE
   cplic print -x >> $LOG_FILE
   exit 0
   ```

2. Pulls the file `/home/admin/log.txt` from the remote Security Gateway and saves it in the `/opt/CPcdt/information/` directory on the Management Server.

Example Deployment Plan File:

```
<?xml version="1.0" encoding="UTF-8"?>
 <CDT_Deployment_Plan>
  <plan_settings>
    <name value="Get information from the " />
    <description value="Example Deployment Plan file - run a script
to get information" />
    <update_cpuse value="true" />
  </plan_settings>

  <!-- The script 'getInformation.sh' redirects its output to the
'/home/admin/log.txt' -->
  <execute_script path="/home/admin/getInformation.sh" />

  <pull_file remote_path="/home/admin/log.txt" local_
dir="/opt/CPcdt/information/" />
 </CDT_Deployment_Plan>
```

Example 3 - Take Gaia Snapshot and Install a Package

This example Deployment Plan File does these actions on all applicable Security Gateways:

1. Takes the Gaia snapshot on the remote Security Gateway.
2. Downloads the CPUSE package of the R80.10 Jumbo Hotfix Accumulator from the Check Point Cloud on the remote Security Gateway.

   The package download action on the remote Security Gateway is not marked as critical.
3. If the package download on the remote Security Gateway fails, the CDT sends the package from the Management Server to the remote Security Gateway and imports it with CPUSE.

   If the package download on the remote Security Gateway succeeds, the CDT does not send the package from the Management Server to the remote Security Gateway.
4. Installs the package on the remote Security Gateway.

Example Deployment Plan File:

```
<?xml version="1.0" encoding="UTF-8"?>
 <CDT_Deployment_Plan>
  <plan_settings>
    <name value="Example Deployment Plan file - take snapshot and
install a package" />
    <description value="Create snapshot and then install HF on the
remote machines" />
    <update_cpuse value="true" />
  </plan_settings>

  <!-- Create a snapshot on remote machine -->
  <create_snapshot name="backup" description=" backup snapshot
before Jumbo installation" />

  <!-- Install Jumbo for - XXX
  If the download from the CP Cloud fails, use the CDT import and
install actions -->

  <!-- (1) Download this package (not critical) -->
  <download_from_cloud path="/home/admin/Check_Point_R80_10_JUMBO_
HF_Bundle_T97_FULL.tgz" iscritical="false" />

  <!-- (2) If download from CP Cloud failed, use the CDT import and
install actions -->
  <import_package path="/home/admin/Check_Point_R80_10_JUMBO_HF_
Bundle_T97_FULL.tgz" />
```

```
  <install_package path="/home/admin/Check_Point_R80_10_JUMBO_HF_
Bundle_T97_FULL.tgz" />
 </CDT_Deployment_Plan>
```

Example 4 - Update CPUSE, Send, Import, and Verify the Package

This example Deployment Plan File does these actions on all applicable Security Gateways:

1. Sends the package from the Management Server (`/home/admin/Check_Point_R80_10_JUMBO_HF_Bundle_T97_FULL.tgz`) to the remote Security Gateway and imports it with CPUSE.
2. Verifies the package with CPUSE on the remote Security Gateway to make sure it can be installed.

Example Deployment Plan File:

```
<?xml version="1.0" encoding="UTF-8"?>
 <CDT_Deployment_Plan>
  <plan_settings>
    <name value="Example Deployment Plan file - update, send,
import, and verify the package" />
    <description value="Update , import and verify the package on
the remote machines" />
    <update_cpuse value="true" />
  </plan_settings>

  <!-- Use the CDT import and verify actions -->
  <import_package path="/home/admin/Check_Point_R80_10_JUMBO_HF_
Bundle_T97_FULL.tgz" />
  <verify_package path="/home/admin/Check_Point_R80_10_JUMBO_HF_
Bundle_T97_FULL.tgz" />
 </CDT_Deployment_Plan>
```

Example 5 - Run a Script, Uninstall a Hotfix, Upgrade, Install a Hotfix, Log and Send Email, Pull a File

This example Deployment Plan File does these actions on all applicable Security Gateways:

1. Runs the script `preScript.sh`, found on the Security Management Server or Multi-Domain Security Management Server in the `/home/admin/cdt/` directory. This script is not marked as critical.
2. Uninstalls the CPUSE package of the R80.40 Jumbo Hotfix Accumulator (`Check_Point_R80_40_JUMBO_HF_Bundle_T89_sk165456_FULL.tgz`).
3. Imports and installs the CPUSE package for the R81 Major Upgrade (`/home/admin/Check_Point_R81_T392_Fresh_Install_and_Upgrade.tgz`).
4. Adds a log entry and sends an email message noting that the installation completed.
5. Imports and installs the package for the R81 Jumbo Hotfix Accumulator (`/home/admin/Check_Point_R81_JUMBO_HF_Bundle_T10_sk170114_FULL.tar`).
6. Pulls the file `/home/admin/file_to_pull.txt` from the Security Gateways and saves it in the `/home/admin/` directory on the Security Management Server or Multi-Domain Security Management Server.

Example Deployment Plan File:

```
<?xml version="1.0" encoding="UTF-8"?>
  <CDT_Deployment_Plan>
    <!--
    The plan_settings element contains the name and the description
of the deployment plan
    and additional configuration.
    -->
      <plan_settings>
        <name value="Example deployment plan" />
        <description value="Example deployment plan" />
        <update_cpuse value="true" />
        <connectivityupgrade value="true" />
      </plan_settings>

    <!-- Execute script -->
    <execute_script
path="/home/admin/cdt/preScript.sh" iscritical="false" />

    <!-- Remove R80.40 Jumbo HF -->
```

```
    <uninstall_cpuse_package filename="Check_Point_R80_40_JUMBO_HF_
Bundle_T89_sk165456_FULL.tgz" />

    <!-- Major upgrade to R81 -->
    <import_package path="/home/admin/Check_Point_R81_T392_Fresh_
Install_and_Upgrade.tgz" />
    <install_package path="/home/admin/Check_Point_R81_T392_Fresh_
Install_and_Upgrade.tgz" />

    <!-- Notifications during execution -->
    <log level="NORMAL" value="Finished installing major upgrade."
/>
    <send_email to="admin@example.com" subject="Major upgrade
completed" body="Finished installation of R81 major upgrade,
preparing to install R81 JHF." />

    <!-- Install R81 Jumbo HF on top of R81 -->
    <import_package path="/home/admin/Check_Point_R81_JUMBO_HF_
Bundle_T10_sk170114_FULL.tar" />
    <install_package path="/home/admin/Check_Point_R81_JUMBO_HF_
Bundle_T10_sk170114_FULL.tar" />

    <!-- Get a file from the Security Gateway to /home/admin/ -->
    <pull_file remote_path="/home/admin/file_to_pull.txt" local_
dir="/home/admin/" />
</CDT_Deployment_Plan>
```

Package Installation in Clusters

When all Cluster Members are marked for installation in the Installation Candidates List File, the CDT upgrades all Cluster Members automatically:

- In ClusterXL High Availability mode - the CDT first upgrades the Standby members, and then the CDT upgrades the former Active member.
- In VRRP Cluster - the CDT first upgrades the VRRP Backup member, and then the CDT upgrades the former VRRP Master member.
- In VSX Virtual System Load Sharing (VSLS) cluster - the CDT first upgrades all the members listed as **VSLS member** in the Installation Candidates List File, and then the CDT upgrades the member listed as the **VSLS active member** in the Installation Candidates List File.

CDT and the cluster Connectivity Upgrade:

For version upgrades (not installation of Hotfixes), the CDT runs the cluster Connectivity Upgrade (CU) by default. Meaning that the connections are synchronized between the Cluster Members.

If you wish to disable this behavior, follow the instructions below:

To use the Basic Mode

In the CDT primary configuration file (see *"CDT Primary Configuration File" on page 66*), add the "`<PackageToInstall>`" element, with both the attribute "`Path="..."`" and the attribute "`ConnectivityUpgrade="false"`":

```
<PackageToInstall Path="/<Your_Path_To>/<File_Name_of_CPUSE_
Offline_Package>.<File_Extension>" ConnectivityUpgrade="false"
/>
```

To use the Advanced Mode

In the Deployment Plan File (see *"Deployment Plan File" on page 79*), in the element "`<plan_settings>`", add the attribute "`<ConnectivityUpgrade value="false" />`" (see *"Example 5 - Run a Script, Uninstall a Hotfix, Upgrade, Install a Hotfix, Log and Send Email, Pull a File" on page 92*).

Cluster Upgrade	Workflow
Automatic cluster upgrade	1. Upgrade these Cluster Members: ▪ In ClusterXL High Availability mode - the Standby members. ▪ In VRRP Cluster - the VRRP Backup member. ▪ In VSX VSLS cluster - the members listed as **VSLS member** in the Installation Candidates List File. 2. Run the Connectivity Upgrade (if it is enabled in the Deployment Plan File). The Connectivity Upgrade performs the cluster failover. 3. Upgrade these Cluster Members: ▪ In ClusterXL High Availability mode - the former Active member. ▪ In VRRP Cluster - the former VRRP Master member. ▪ In VSX VSLS cluster - the member listed as **VSLS active member** in the Installation Candidates List File. **Note** - Cluster health checks make sure that the cluster is upgraded successfully.

Cluster Upgrade	Workflow

Semi-automatic cluster upgrade	1. Exclude this Cluster Member from the upgrade in the Installation Candidates List File:
	■ In ClusterXL High Availability mode - the member listed as "**active**" in the Installation Candidates List File.
	■ In VRRP Cluster - the member listed as "**master**" in the Installation Candidates List File.
	■ In VSX VSLS cluster - the member listed as "**VSLS active member**" in the Installation Candidates List File.
	To exclude a Cluster Member from a package installation, enter the "-" (minus) character in the "**Upgrade Order**" column.
	Example of an Installation Candidates List File
	`Object Name , Cluster Name , IP Address , Version/JHF Take , State , Upgrade Order`
	`==========`
	`MEM-68.146 , ClusterXL-68.148 , 192.168.68.146 , R80.20/205 , active , -`
	`MEM-68.147 , ClusterXL-68.148 , 192.168.68.147 , R80.20/205 , standby , 1`
	2. Install the upgrade package. This upgrades only these Cluster Members:
	■ In ClusterXL High Availability mode - the Standby members.
	■ In VRRP Cluster - the VRRP Backup member.
	■ In VSX VSLS cluster - the members listed as **VSLS member** in the Installation Candidates List File.
	Important - If the target version is R80.40 in a ClusterXL High Availability, you must enable the Multi Version Cluster mode on the upgraded Cluster Member with the "`cphaconf mvc on`" command.
	3. Generate the Installation Candidates List File again.
	4. The CDT marks these Cluster Members as installed:
	■ In ClusterXL High Availability mode - the Standby members.
	■ In VRRP Cluster - the VRRP Backup member.
	■ In VSX VSLS cluster - the members listed as **VSLS member** in the Installation Candidates List File.
	5. The CDT marks these Cluster Members with "1":
	■ In ClusterXL High Availability mode - the Active member.
	■ In VRRP Cluster - the VRRP Master member.
	■ In VSX VSLS cluster - the member listed as **VSLS active member** in the Installation Candidates List File.

Cluster Upgrade	Workflow
	6. Install the upgrade package again. The CDT runs the upgrade automatically. This upgrades only these Cluster Members: ■ In ClusterXL High Availability mode - the former Active member. ■ In VRRP Cluster - the former VRRP Master member. ■ In VSX VSLS cluster - the member listed as **VSLS active member** in the Installation Candidates List File.

Notes:

- Upgrade in clusters follows a specific order.
  - In ClusterXL High Availability mode - You cannot upgrade the ClusterXL Active member before you upgrade all the ClusterXL Standby members.
  - In VRRP Cluster - You cannot upgrade the VRRP Master member before you upgrade the VRRP Backup member.
  - In VSX VSLS cluster - You cannot upgrade the Cluster Members listed as "**VSLS active member**" in the Installation Candidates List File before you upgrade the Cluster Members listed as "**VSLS member**" in the Installation Candidates List File.
- Cluster installation stops in specific cases.
  - In ClusterXL High Availability mode - If the upgrade of the ClusterXL Standby members fails.
  - In VRRP Cluster - If the upgrade of the VRRP Backup member fails.
  - In VSX VSLS cluster - If the upgrade of the Cluster Members listed as "**VSLS member**" in the Installation Candidates List File fails.
- If the installation succeeds on the first Cluster Member, but fails on others, the CDT does not revert it.
  If the installation on the first Cluster Member succeeds, but the installation on the other Cluster Members fails, the CDT does **not** revert the first Cluster Member.

- The Full Connectivity Upgrade for VRRP Clusters is supported only when you upgrade to R80.10 or R80.30 versions.

  Important - This note applies only to CDT versions 1.9.4 and lower.

  More Information

  When you upgrade to R77.30 or R80.20, there are two options:

Option	Description
A	Disable the Connectivity Upgrade (otherwise, the cluster is marked as "`N/A`"). To disable the Connectivity Upgrade in the Deployment Plan File, in the element "`<plan_settings>`", add the attribute "`<ConnectivityUpgrade value="false" />` " (see *"Example 5 - Run a Script, Uninstall a Hotfix, Upgrade, Install a Hotfix, Log and Send Email, Pull a File" on page 92*).

B	Run the Connectivity Upgrade:
	1. In the `$CDTDIR/CentralDeploymentTool.xml` file, add this debug configuration (see *"Debug Configuration" on page 103*): `<Debug CUSyncForVRRP="true">`
	2. In the Deployment Plan File, after the installation of an upgrade package, add the installation of a Jumbo Hotfix Accumulator package:
	• For Security Gateways R77.30, you must use the Jumbo Hotfix Accumulator Take 342 or above. See sk106162.
	• For Security Gateways R80.20, you must use the Jumbo Hotfix Accumulator Take 17 or above. See Jumbo Hotfix Accumulator for R80.20.
	Example for a Security Gateway R80.20 (the instructions contain four lines):
	`<import_package path="/home/admin/Check_Point_R80.20_T101_Fresh_Install_and_Upgrade_Security_Gateway.tgz" />`
	`<install_package path="/home/admin/Check_Point_R80.20_T101_Fresh_Install_and_Upgrade_Security_Gateway.tgz" />`
	`<import_package path="/home/admin/Check_Point_R80_20_JUMBO_HF_Bundle_T17_sk137592_FULL.tgz" />`
	`<install_package path="/home/admin/Check_Point_R80_20_JUMBO_HF_Bundle_T17_sk137592_FULL.tgz" />`

CDT Log Files

This section describes the log files the Central Deployment Tool generates, the format of the log messages, and the debug configuration.

Generated Log Files

Important - These log files can contain special characters.

- To see these log files on Gaia OS, use the Linux "`less`" command.
- To see these log files on Windows OS, use an advanced text editor, like Notepad++.

CDT saves its log files in this location on the Management Server:

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/
```

The primary CDT log file is:

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/Main_log.elg
```

CDT generates a log file for each Security Gateway and Cluster marked for installation:

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/<Name of Object>_log.elg
```

Note - Logs for a cluster contain information about all the Cluster Members.

After a package installation, the CDT copies all CPUSE installation logs from the remote Security Gateway and Cluster Members:

CDT copies all CPUSE installation logs from remote Security Gateways to:

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/<Name of Security
Gateway Object>_CPUSE_Logs/
```

CDT copies all CPUSE installation logs from remote Cluster Members to:

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/<Name of Cluster
Object>_CPUSE_Logs/<Name of Cluster Member Object>_CPUSE_Logs/
```

CDT generates RMA logs in this location on the remote Security Gateways:

```
/var/log/CPrma/
```

CDT copies these RMA logs from the `/var/log/CPrma/` directory on the remote Security Gateways or Cluster Members to your Management Server:

List of Gaia Clish commands that were run to restore the Gaia Clish configuration on the Security Gateway or Cluster Member:

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of
Security Gateway or Cluster Member Object>_FinalClishCommand.elg
```

Outputs of the Gaia Clish commands that were run to restore the Gaia Clish configuration on the Security Gateway or Cluster Member:

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of
Security Gateway or Cluster Member Object>_FinalClishLog.elg
```

CDT copies these RMA logs from the `/var/log/CPrma/` directory on the remote VSX Gateways or VSX Cluster Members to your Management Server:

List of Gaia Clish commands that were run to restore the Gaia Clish configuration on the VSX Gateway or VSX Cluster Member:

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of VSX
Gateway or VSX Cluster Member Object>_FinalClishCommand.elg
```

List of Gaia Clish commands that were run to restore the Gaia Clish configuration in the VSX context 0 (VS0):

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of VSX
Gateway or VSX Cluster Member Object>_VS0ClishCommand.elg
```

Outputs of the Gaia Clish commands that were run to restore the Gaia Clish configuration on the VSX Gateway or VSX Cluster Member:

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of VSX
Gateway or VSX Cluster Member Object>_FinalClishLog.elg
```

Outputs of the Gaia Clish commands that were run to restore the Gaia Clish configuration in the VSX context 0 (VS0):

```
/var/log/CPcdt/logs_<YYYY-MM-DD-HH-mm-ss>/RmaLogs/<Name of VSX
Gateway or VSX Cluster Member Object>_VS0ClishLog.elg
```

Log Message Format

CDT prints log messages on the screen in this format:

```
<TimeStamp> *<Log_Level>* [<Name_of_Object>]: <Log_Message>
```

Example

```
Mon Jan 15 17:35:50 2018 *A* [Main]:
```

Current execution logs are in this directory:

```
/var/log/CPcdt/logs_2018-01-15-17-35-50/
```

CDT saves its log messages in the CDT log files in this format:

```
<TimeStamp> *<Log_Level>*: <Log_Message>
```

Example

```
Mon Jan 15 17:35:50 2018 *A*:
```

Current execution logs are in this directory:

```
/var/log/CPcdt/logs_2018-01-15-17-35-50/
```

CDT sends its log messages to the Syslog server in this format:

```
<TimeStamp> CDT *<Log_Level>* [<Name_of_Object>]: <Log_Message>
```

Example

```
Mon Jan 15 17:35:50 2018 CDT *A* [Main]:
```

Current execution logs are in this directory:

```
/var/log/CPcdt/logs_2018-01-15-17-35-50/
```

Debug Configuration

A number of debug configurations are available, which can control different aspects of CDT's operation.

Change the CDT primary configuration file in this way in the Expert mode:

Step	Description
1	Back up the current `$CDTDIR/CentralDeploymentTool.xml` file: `cp -v $CDTDIR/CentralDeploymentTool.xml{,_ORIGINAL}`
2	Edit the current `$CDTDIR/CentralDeploymentTool.xml` file: `vi $CDTDIR/CentralDeploymentTool.xml`
3	Go to the end of the file.

4	Add the applicable keys (see the table below) above the last tag "**</CentralDeploymentTool>**" in this way:
	`<?xml version="1.0" encoding="UTF-8" ?>`
	`<CentralDeploymentTool>`
	`... ... ...`
	`<Debug KEY1="VALUE1"/>`
	`<Debug KEY2="VALUE2"/>`
	`<Debug KEY3="VALUE3"/>`
	`... ... ...`
	`<Debug KEYn="VALUEn"/>`
	`</CentralDeploymentTool>`

5	Save the changes in the file and exit the editor.
6	Run the CDT.

Important Notes:

- If a key is not configured explicitly, then the CDT uses its default value (see the table below).
- Enclose all values in double-quotes.
- String values are case-sensitive.

Table: Debug configuration keys

Key Name	Default Value	Description
`ClusterValidationTimeout`	`1200`	How much time (in seconds) to wait for Cluster Members to synchronize.
`CollectLogsTimeout`	`600`	How much time (in seconds) to wait for CPUSE logs collection to complete.
`CreateSnapshotTimeout`	`5400`	How much time (in seconds) to wait for Gaia snapshot to complete.
`CUSyncForVRRP`	`false`	If set to "`true`", runs a cluster Connectivity Upgrade on a VRRP Cluster (for specified clients with packages that support this). For more information about the cluster Connectivity Upgrade, see sk107042.

Table: Debug configuration keys (continued)

Key Name	Default Value	Description
`CuSyncTimeout`	`900`	How much time (in seconds) to wait for a cluster synchronization to complete during a Connectivity Upgrade. For more information about the cluster Connectivity Upgrade, see sk107042.
`DbgetTimeout`	`300`	How much time (in seconds) to wait for the Gaia "`dbget`" command to complete.
`DbsetTimeout`	`300`	How much time (in seconds) to wait for the Gaia "`dbset`" command to complete.
`DownloadingFromCloud`	`3600`	How much time (in seconds) to wait for a download from Check Point Cloud to complete.
`ExecuteImportCmdTimeout`	`600`	How much time (in seconds) to wait for the CPUSE "`import`" command to complete.

Table: Debug configuration keys (continued)

Key Name	Default Value	Description
ExecuteInstallCmdTimeout	600	How much time (in seconds) to wait for the CPUSE "install" command to complete.
ExecuteUninstallCmdTimeout	600	How much time (in seconds) to wait for the CPUSE "uninstall" command to start.
FinishImportTimeout	1800	How much time (in seconds) to wait for a package import to complete.
FinishUninstallTimeout	3600	How much time (in seconds) to wait for a package uninstall to complete.
InstallationTimeout	10800	Timeout (in seconds) for a package installation.
MailNotificationSender	CDT-Do_Not_Reply@checkpoint.com	Email address of the notification sender.

Table: Debug configuration keys (continued)

Key Name	Default Value	Description
`MDSAuditing`	`false`	If set to "`true`", requires the administrator to enter the Multi-Domain Security Management Server Superuser or the Domain Management Server Superuser username and password to run installations. The CDT logs this username for auditing purposes.
`RemoteDefaultPassword`	`admin`	The default password to configure during the RMA Restore procedure.
`SkipVerifySupportedByOS`	`false`	If set to "`true`", CDT skips the verification, whether the Management Server supports an upgrade to the new target version.
`StartDATimeout`	`300`	How much time (in seconds) to wait for the CPUSE "DA" service to start.

Table: Debug configuration keys (continued)

Key Name	Default Value	Description
StopDATimeout	300	How much time (in seconds) to wait for the CPUSE "DA" service to stop.
ValidatePolicyTimeout	1200	How much time (in seconds) to wait for a Security Gateway to fetch its Security Policy.
ValidateVSXPolicyTimeout	1800	How much time (in seconds) to wait for a VSX Gateway to fetch its Security Policy.
WaitAfterReboot	300	How much time (in seconds) to wait after reboot.

CLI Syntax Quick Reference in the Expert mode

This section provides a summary of CLI command for the Central Deployment Tool operation modes in the Expert mode.

For CLI commands in Gaia Clish, see *"CDT in Gaia Clish" on page 120*.

Notes for a Multi-Domain Security Management Server:

1. **Go to the context of the applicable Domain Management Server**

   ```
   mdsenv <IP Address or Name of Domain Management Server>
   ```

2. **Specify the IP Address or Name of the applicable Domain Management Server in the syntax**

   - In the Basic Mode:

     ```
     $CDTDIR/CentralDeploymentTool <options> <IP Address or Name of Domain Management Server>
     ```

   - In the Advanced Mode and the RMA Mode:

     ```
     $CDTDIR/CentralDeploymentTool <options> -server=<IP Address or Name of Domain Management Server>
     ```

CLI Syntax Quick Reference for the Basic Mode

Viewing the built-in help

```
$CDTDIR/CentralDeploymentTool [-h | --help]
```

Generating an Installation Candidates List File

```
$CDTDIR/CentralDeploymentTool -generate <Path to and Desired Name of Installation Candidates List File>.csv [<IP Address or Name of Domain Management Server>]
```

Running only preparations on all marked candidates in the Installation Candidates List File

```
$CDTDIR/CentralDeploymentTool -preparations <Path to Installation Candidates List File>.csv [<IP Address or Name of Domain Management Server>]
```

Running extended preparations on all marked candidates

```
$CDTDIR/CentralDeploymentTool -extended_preparations <Path to Installation Candidates List File>.csv [<IP Address or Name of Domain Management Server>]
```

Running a full installation on all marked candidates

```
$CDTDIR/CentralDeploymentTool -install <Path to Installation Candidates List File>.csv [<IP Address or Name of Domain Management Server>]
```

Monitoring the installation progress

Note - The CDT writes the progress details at 5 seconds intervals to these log files in the `$CDTDIR` directory.

- Log files on a Security Management Server:
  - Full log:

    ```
    watch -d cat $CDTDIR/CDT_status.txt
    ```

  - Brief log:

    ```
    watch -d cat $CDTDIR/CDT_status_brief.txt
    ```

- Log files on a Multi-Domain Security Management Server:
  - Full log:

    ```
    watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>.txt
    ```

    Example:

    ```
    watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession.txt
    ```

  - Brief log:

    ```
    watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_brief.txt
    ```

    Example:

    ```
    watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession_brief.txt
    ```

Retrying a failed installation

Important - You must run this command in a new SSH shell.

```
$CDTDIR/CentralDeploymentTool -retry [<IP Address or Name of Domain Management Server>]
```

CLI Syntax Quick Reference for the Advanced Mode

Generating an installation Installation Candidates List File

```
$CDTDIR/CentralDeploymentTool -generate -candidates=<Path to and Desired Name of Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml [-server=<IP Address or Name of Domain Management Server>] [-session=<Name of Management Session without Spaces>]
```

Selecting Security Gateways, for which to generate the Installation Candidates List File

```
$CDTDIR/CentralDeploymentTool -generate -candidates=<Path to and Desired Name of Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml -filter=<Path to Filter File, including File Extension> [-server=<IP Address or Name of Domain Management Server>] [-session=<Name of Management Session without Spaces>]
```

Running a Deployment Plan File on Security Gateways in the Installation Candidates List File

```
$CDTDIR/CentralDeploymentTool -execute -candidates=<Path to Installation Candidates List File>.csv -deploymentplan=<Path to Deployment Plan File>.xml [-server=<IP Address or Name of Domain Management Server>] [-session=<Name of Management Session without Spaces>]
```

Monitoring the installation progress

Note - The CDT writes the progress details at 5 seconds intervals to these log files in the `$CDTDIR` directory.

Log files on a Security Management Server

- Full log, if you specified the parameter "`-session=<Name of Management Session without Spaces>`":

  ```
  watch -d cat $CDTDIR/CDT_status_<Name of Management Session without Spaces>.txt
  ```

  Example:

  ```
  watch -d cat $CDTDIR/CDT_status_MySession.txt
  ```

- Full log, if you did not specify the parameter "`-session`":

  ```
  watch -d cat $CDTDIR/CDT_status.txt
  ```

- Brief log, if you specified the parameter "`-session=<Name of Management Session without Spaces>`":

  ```
  watch -d cat $CDTDIR/CDT_status_<Name of Management Session without Spaces>_brief.txt
  ```

  Example:

  ```
  watch -d cat $CDTDIR/CDT_status_MySession_brief.txt
  ```

- Brief log, if you did not specify the parameter "`-session`":

  ```
  watch -d cat $CDTDIR/CDT_status_brief.txt
  ```

Log files on a Multi-Domain Security Management Server

- Full log, if you specified the parameter "`-session=<Name of Management Session without Spaces>`":

  ```
  watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_<Name of Management Session without Spaces>.txt
  ```

  Example:

  ```
  watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession.txt
  ```

- Full log, if you did not specify the parameter "`-session`":

```
watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>.txt
```

  Example: `watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain.txt`

- Brief log, if you specified the parameter "`-session=<Name of Management Session without Spaces>`":

```
watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_<Name of Management Session without Spaces>_brief.txt
```

  Example:

  `watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession_brief.txt`

- Brief log, if you did not specify the parameter "`-session`":

```
watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_brief.txt
```

  Example:

  `watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession_brief.txt`

Retrying a failed installation

Important - You must run this command in a new SSH shell.

```
$CDTDIR/CentralDeploymentTool -retry [-server=<IP Address or Name of Domain Management Server>] [-session=<Name of Management Session without Spaces>]
```

Resuming an installation

```
$CDTDIR/CentralDeploymentTool -resume -deploymentplan=<Path to Deployment Plan File>.xml [-server=<IP Address or Name of Domain Management Server>] [-session=<Name of Management Session without Spaces>]
```

CLI Syntax Quick Reference for the RMA Mode

Generating an Installation Candidates List File for RMA backup

```
$CDTDIR/CentralDeploymentTool -rma -generate [-additional_
files=<Path to File with List of Additional Files, including
File Extension>] -candidates=<Path to and Desired Name of
Installation Candidates List File>.csv [-server=<IP Address or
Name of Domain Management Server>] [-session=<Name of Management
Session without Spaces>]
```

Viewing the RMA backup information of a specified remote Security Gateway

```
$CDTDIR/CentralDeploymentTool -rma -info -gateway=<Name of
Security Gateway or Cluster Member Object>
```

Collecting RMA backup from specified remote Security Gateways based on the Installation Candidates List File

```
$CDTDIR/CentralDeploymentTool -rma -backup [-additional_
files=<Path to File with List of Additional Files, including
File Extension>] -candidates=<Path to Installation Candidates
List File>.csv [-server=<IP Address or Name of Domain Management
Server>] [-session=<Name of Management Session without Spaces>]
```

Collecting RMA backup information from all remote Security Gateways (Installation Candidates List File is not needed)

```
$CDTDIR/CentralDeploymentTool -rma -backupall [-additional_
files=<Path to File with List of Additional Files, including
File Extension>] [-server=<IP Address or Name of Domain
Management Server>] [-session=<Name of Management Session
without Spaces>]
```

Restoring the RMA backup information on a remote Security Gateway

```
$CDTDIR/CentralDeploymentTool -rma -restore -gateway=<Name of
Security Gateway or Cluster Member Object> -license=<Path to
License File, including File Extension> [-server=<IP Address or
Name of Domain Management Server>] [-session=<Name of Management
Session without Spaces>]
```

Specifying a CPUSE Clean Install package when you restore the RMA backup information

```
$CDTDIR/CentralDeploymentTool -rma -restore -gateway=<Name of
Security Gateway or Cluster Member Object> -license=<Path to
License File, including File Extension> -package=<Path to CPUSE
Offline Package, including File Extension> [-server=<IP Address
or Name of Domain Management Server>] [-session=<Name of
Management Session without Spaces>]
```

Monitoring the RMA backup or RMA restore progress

Note - The CDT writes the progress details at 5 seconds intervals to these log files in the `$CDTDIR` directory.

Log files on a Security Management Server

- Full log, if you specified the parameter "`-session=<Name of Management Session without Spaces>`":

  ```
  watch -d cat $CDTDIR/CDT_status_<Name of Management Session without Spaces>.txt
  ```

  Example:

  ```
  watch -d cat $CDTDIR/CDT_status_MySession.txt
  ```

- Full log, if you did not specify the parameter "`-session`":

  ```
  watch -d cat $CDTDIR/CDT_status.txt
  ```

- Brief log, if you specified the parameter "`-session=<Name of Management Session without Spaces>`":

  ```
  watch -d cat $CDTDIR/CDT_status_<Name of Management Session without Spaces>_brief.txt
  ```

  Example:

  ```
  watch -d cat $CDTDIR/CDT_status_MySession_brief.txt
  ```

- Brief log, if you did not specify the parameter "`-session`":

  ```
  watch -d cat $CDTDIR/CDT_status_brief.txt
  ```

Log files on a Multi-Domain Security Management Server

- Full log, if you specified the parameter "`-session=<Name of Management Session without Spaces>`":

  ```
  watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_<Name of Management Session without Spaces>.txt
  ```

  Example:

  ```
  watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession.txt
  ```

- Full log, if you did not specify the parameter "`-session`":

  ```
  watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>.txt
  ```

  Example: `watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain.txt`

- Brief log, if you specified the parameter "`-session=<Name of Management Session without Spaces>`":

  ```
  watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_<Name of Management Session without Spaces>_brief.txt
  ```

  Example:

  ```
  watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession_brief.txt
  ```

- Brief log, if you did not specify the parameter "`-session`":

  ```
  watch -d cat $CDTDIR/CDT_status_<Name of Domain Management Server>_<Name of Domain>_brief.txt
  ```

  Example:

  ```
  watch -d cat $CDTDIR/CDT_status_MyDomainServer_MyDomain_MySession_brief.txt
  ```

CDT in Gaia Clish

Background

Starting from version 1.9.0, you can run the CDT commands from Gaia Clish with the help of the Gaia Dynamic CLI (see sk144112).

Dynamic CLI enhances Gaia Clish with commands from the Expert mode.

Each CLI command is granted with the full set of Role Based Access capabilities, from read-write granularity to a varied number of roles and permission levels (depending on your needs).

The Dynamic CLI commands have the same syntax, concept, and documentation as the Gaia Clish commands.

Dynamic CLI was created for these purposes:

- To secure access to the "Expert" capabilities without compromising the "Expert" passwords or sharing all the "Expert" capabilities.
- To separate between monitor roles or read-only users and administrators.

  For example, users with monitor roles can see Security Gateway logs without an access to the "Expert" space.

Installation Instructions

Management Server Version	Installation Instructions
R81.10 and higher	The minimum required CDT version is integrated.
R81	Install the CDT package v1.9.0 or higher from sk111158.
R80.40	Follow these steps: 1. Install the R80.40 Jumbo Hotfix Accumulator Take 77 or higher. 2. Install the CDT package v1.9.0 or higher from sk111158. 3. Run this script in the Expert mode: `/opt/CPcdt/Clish_Cdt_Installer.py`

Management Server Version	Installation Instructions
(End of Life since Sep 2022) R80.30	Follow these steps: 1. Install the R80.30 Jumbo Hotfix Accumulator Take 215 or higher. 2. Install the latest Gaia Dynamic CLI from sk144112. 3. Install the CDT package v1.9.0 or higher from sk111158. 4. Run this script in the Expert mode: `/opt/CPcdt/Clish_Cdt_Installer.py`
(End of Life since Sep 2022) R80.20.M2 R80.20 R80.20.M1 R80.10	Follow these steps: 1. Install the latest Gaia Dynamic CLI from sk144112. 2. Install the CDT package v1.9.0 or higher from sk111158. 3. Run this script in the Expert mode: `/opt/CPcdt/Clish_Cdt_Installer.py`

Description of Directories

During the installation, the CDT creates these directories:

Directory	Description
`/opt/CPcdt/CandidateListsRepository/`	Repository to keep the Installation Candidates List Files that Gaia Clish users create. Gaia Clish users have a "read" and "write" access to this directory. For security reasons, all Installation Candidates List Files are located in this directory.
`/opt/CPcdt/DeploymentPlanRepository/`	Repository to keep the Deployment Plan Files that Gaia Clish users configure. Gaia Clish users have a "read" and "write" access to this directory. For security reasons, all Deployment Plan Files are located in this directory.

Important Note for Multi-Domain Security Management Server:
A SuperUser must **manually** create the Deployment Plan Files directory for **each** applicable Domain Management Server.
The required permissions for this directory are "read" (`r`), "write" (`w`), and "execute" (`x`).
Run this command in the Expert mode on the Multi-Domain Security Management Server:

```
mkdir -m777 /opt/CPcdt/DeploymentPlanRepository/<Name of Domain Management Server as configured in SmartConsole>
```

CDT Syntax in Gaia Clish

Syntax for all commands:

```
show cdt[ESC][ESC]
set cdt[ESC][ESC]
start cdt[ESC][ESC]
```

Syntax for the '`show`' commands:

```
show cdt
      candidates
            candidates-list "<Path to Installation Candidates List
File>.csv"
                  server <IP Address or Name of Domain Management
Server> [session <Name of Management Session without Spaces>]
                  [session <Name of Management Session without
Spaces>]
      execute-output
            server <IP Address or Name of Domain Management
Server> [session <Name of Management Session without Spaces>]
            [session <Name of Management Session without Spaces>]
      generate-output
            server <IP Address or Name of Domain Management
Server> [session <Name of Management Session without Spaces>]
            [session <Name of Management Session without Spaces>]
      status
            server <IP Address or Name of Domain Management
Server> [session <Name of Management Session without Spaces>]
            [session <Name of Management Session without Spaces>]
```

Note:
The parameter "`session <Name of Management Session without Spaces>`" is optional (available from CDT v1.9.8).
Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Parameters for the 'show' commands

Parameter	Description
`show cdt candidates`	Shows all Installation Candidates List Files.
`show cdt candidates candidates-list "<Path to Installation Candidates List File>.csv" [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Shows the specified Installation Candidates List File on the Security Management Server (in the specified Management Session).

Parameter	Description
`show cdt candidates candidates-list "<Path to Installation Candidates List File>.csv" server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Shows the specified Installation Candidates List File for the specified Domain Management Server (in the specified Management Session).
`show cdt execute-output`	Shows the output of the last '`start cdt execute`' command.
`show cdt execute-output [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Shows the output of the last '`start cdt execute`' (in the specified Management Session).
`show cdt execute-output server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Shows the output of the last '`start cdt execute`' command on the specified Domain Management Server (in the specified Management Session).
`show cdt generate-output`	Shows the output of the last '`start cdt generate-candidates`' command.

Parameter	Description
`show cdt generate-output [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Shows the output of the last '`start cdt generate-candidates`' command (in the specified Management Session).
`show cdt generate-output server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Shows the output of the last '`start cdt generate-candidates`' command on the specified Domain Management Server (in the specified Management Session).
`show cdt status`	Shows the installation progress. CDT updates this information in the background in the applicable file each 5 seconds.
`show cdt status [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Shows the installation progress (in the specified Management Session). CDT updates this information in the background in the applicable file each 5 seconds.

Parameter	Description
`show cdt status server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Shows the installation progress on the specified Domain Management Server (in the specified Management Session). CDT updates this information in the background in the applicable file each 5 seconds.

Syntax for the '`set`' commands:

```
set cdt candidates
      candidates-list "<Path to Installation Candidates List File>.csv"
            disable-candidate <Name of Security Gateway or Cluster Member Object>
                  server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]
                  [session <Name of Management Session without Spaces>]
            enable-candidate <Name of Security Gateway or Cluster Member Object>
                  server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]
                  [session <Name of Management Session without Spaces>]
```

Note:
The parameter "`session <Name of Management Session without Spaces>`" is optional (available from CDT v1.9.8).
Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Parameters for the 'set' commands

Parameter	Description
`set cdt candidates candidates-list "<Path to Installation Candidates List File>.csv"`	Edits the specified Installation Candidates List File.
`set cdt candidates candidates-list "<Path to Installation Candidates List File>.csv" disable-candidate <Name of Security Gateway or Cluster Member Object> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Disables the specified Security Gateway or Cluster Member object in the Installation Candidates List File (in the specified Management Session). You must enter the name of the Security Gateway or Cluster Member object must be as configured in SmartConsole.
`set cdt candidates candidates-list "<Path to Installation Candidates List File>.csv" disable-candidate <Name of Security Gateway or Cluster Member Object> server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Disables the specified Security Gateway or Cluster Member object in the Installation Candidates List File on the specified Domain Management Server (in the specified Management Session). You must enter the name of the Security Gateway or Cluster Member object must be as configured in SmartConsole.

Parameter	Description
`set cdt candidates candidates-list "<Path to Installation Candidates List File>.csv" enable-candidate <Name of Security Gateway or Cluster Member Object> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Enables the specified Security Gateway or Cluster Member object in the Installation Candidates List File (in the specified Management Session). You must enter the name of the Security Gateway or Cluster Member object must be as configured in SmartConsole.
`set cdt candidates candidates-list "<Path to Installation Candidates List File>.csv" enable-candidate <Name of Security Gateway or Cluster Member Object> server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Enables the specified Security Gateway or Cluster Member object in the Installation Candidates List File on the specified Domain Management Server (in the specified Management Session). You must enter the name of the Security Gateway or Cluster Member object must be as configured in SmartConsole.

Syntax for the '`start`' commands:

```
start cdt
      execute
            deployment-plan "<Path to Deployment Plan File>"
                  candidates-list "<Path to Installation
Candidates List File>.csv"
                        server <IP Address or Name of Domain
Management Server> [session <Name of Management Session without
Spaces>]
                        [session <Name of Management Session
without Spaces>]
                  filter <Path to Filter File>
                        server <IP Address or Name of Domain
Management Server> [session <Name of Management Session without
Spaces>]
                        [session <Name of Management Session
without Spaces>]
      generate-candidates
            deployment-plan "<Path to Deployment Plan File>"
                  candidates-list "<Path to Installation
Candidates List File>.csv"
                        server <IP Address or Name of Domain
Management Server>
                  filter <Path to Filter File>
                        candidates-list "<Path to Installation
Candidates List File>.csv"
                              server <IP Address or Name of Domain
Management Server> [session <Name of Management Session without
Spaces>]
                              [session <Name of Management Session
without Spaces>]
```

Notes:

- The CDT automatically looks for the specified Installation Candidates List File in the `/opt/CPcdt/CandidateListsRepository/` directory.
  Example file name: `"Candidates.csv"`
- The CDT automatically looks for the specified Deployment Plan File in the `/opt/CPcdt/DeploymentPlanRepository/` directory.
  Example file name: `"DeploymentPlan.xml"`
- SNIPPET: This explanation is for Gaia ClishThe parameter "`session <Name of Management Session without Spaces>`" is optional (available from CDT v1.9.8).Use it to run several different CDT sessions at the same time (enter a desired session name - a text string without spaces).

Parameters for the 'start' commands

Parameter	Description
`start cdt execute`	Runs a Deployment Plan File on Security Gateways and Cluster Members. You must specify the Installation Candidates List File.
`start cdt execute deployment-plan "<Path to Deployment Plan File, including File Extension>" candidates-list "<Path to Installation Candidates List File>.csv" [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Runs the specified Deployment Plan File on Security Gateways and Cluster Members listed in the specified Installation Candidates List File (in the specified Management Session).
`start cdt execute deployment-plan "<Path to Deployment Plan File, including File Extension>" candidates-list "<Path to Installation Candidates List File>.csv" server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Runs the specified Deployment Plan File on Security Gateways and Cluster Members listed in the specified Installation Candidates List File on the specified Domain Management Server (in the specified Management Session).

Parameter	Description
`start cdt execute deployment-plan "<Path to Deployment Plan File, including File Extension>" filter <Path to Filter File, including File Extension> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Runs the specified Deployment Plan File on Security Gateways and Cluster Members listed in the specified Filter File (in the specified Management Session). Description of a Filter File: ■ A plain-text file with a list of the object names of applicable Security Gateways and Clusters (**not** Cluster Members). ■ The object names in the file must be as they are configured in SmartConsole or SmartDashboard. ■ You must write each object name on a separate line in this file. ■ You can save this file anywhere on the hard disk. The CDT only reads this file (and does not modify it).

Parameter	Description
`start cdt execute deployment-plan "<Path to Deployment Plan File, including File Extension>" filter <Path to Filter File, including File Extension> server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Runs the specified Deployment Plan File on Security Gateways and Cluster Members listed in the specified Installation Candidates List File on the specified Domain Management Server (in the specified Management Session). The command runs the specified Deployment Plan File for specific Security Gateways and Cluster Members listed in the Filter File. Description of a Filter File: ■ A plain-text file with a list of the object names of applicable Security Gateways and Clusters (**not** Cluster Members). ■ The object names in the file must be as they are configured in SmartConsole or SmartDashboard. ■ You must write each object name on a separate line in this file. ■ You can save this file anywhere on the hard disk. The CDT only reads this file (and does not modify it).

Parameter	Description
`start cdt generate-candidates deployment-plan "<Path to Deployment Plan File, including File Extension>"`	Creates the Installation Candidates List File. The command runs the specified Deployment Plan File.
`start cdt generate-candidates deployment-plan "<Path to Deployment Plan File, including File Extension>" candidates-list "<Path to Installation Candidates List File>.csv" [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Creates the Installation Candidates List File and saves the output to the specified file. The command runs the specified Deployment Plan File (in the specified Management Session).
`start cdt generate-candidates deployment-plan "<Path to Deployment Plan File, including File Extension>" candidates-list "<Path to Installation Candidates List File>.csv" server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Creates the Installation Candidates List File and saves the output to the specified file. The command runs the specified Deployment Plan File on the specified Domain Management Server (in the specified Management Session).

Parameter	Description
`start cdt generate-candidates deployment-plan "<Path to Deployment Plan File, including File Extension>" filter <Path to Filter File, including File Extension>`	Creates the Installation Candidates List File for objects of specific Security Gateways and Clusters listed in the specified Filter File. The command runs the specified Deployment Plan File. Description of a Filter File: ■ A plain-text file with a list of the object names of applicable Security Gateways and Clusters (**not** Cluster Members). ■ The object names in the file must be as they are configured in SmartConsole or SmartDashboard. ■ You must write each object name on a separate line in this file. ■ You can save this file anywhere on the hard disk. The CDT only reads this file (and does not modify it).

Parameter	Description
`start cdt generate-candidates deployment-plan "<Path to Deployment Plan File, including File Extension>" filter <Path to Filter File, including File Extension> candidates-list "<Path to Installation Candidates List File>.csv" [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Security Management Server. Creates the Installation Candidates List File for objects of specific Security Gateways and Clusters listed in the specified Filter File. The command runs the specified Deployment Plan File for specific Security Gateways and Cluster Members listed in the Filter File (in the specified Management Session). The command saves the output to the specified file. Description of a Filter File: ■ A plain-text file with a list of the object names of applicable Security Gateways and Clusters (**not** Cluster Members). ■ The object names in the file must be as they are configured in SmartConsole or SmartDashboard. ■ You must write each object name on a separate line in this file. ■ You can save this file anywhere on the hard disk. The CDT only reads this file (and does not modify it).

Parameter	Description
`start cdt generate-candidates deployment-plan "<Path to Deployment Plan File, including File Extension>" filter <Path to Filter File, including File Extension> candidates-list "<Path to Installation Candidates List File>.csv" server <IP Address or Name of Domain Management Server> [session <Name of Management Session without Spaces>]`	**Note** - This command applies only to the Multi-Domain Security Management Server. Creates the Installation Candidates List File for objects of specific Security Gateways and Clusters listed in the specified Filter File. The command runs the specified Deployment Plan File on the specified Domain Management Server (in the specified Management Session). The command saves the output to the specified file. Description of a Filter File: ■ A plain-text file with a list of the object names of applicable Security Gateways and Clusters (**not** Cluster Members). ■ The object names in the file must be as they are configured in SmartConsole or SmartDashboard. ■ You must write each object name on a separate line in this file. ■ You can save this file anywhere on the hard disk. The CDT only reads this file (and does not modify it).

Gaia Clish Permissions for CDT Commands

To run specific CDT commands in Gaia Clish, a Gaia administrator must configure the feature **cdt** in the applicable user role.

CDT Commands in Gaia Clish	Gaia Clish Requirement
`show cdt`	There are no requirements.
`set cdt`	To run these commands, a Gaia administrator must configure the feature **cdt** (**Central Deployment Tool**) with the **Read / Write** permission in the applicable user role.
`start cdt`	To run these commands, a Gaia administrator must configure the feature **cdt** (**Central Deployment Tool**) with the **Read / Write** permission in the applicable user role.

For more information about Gaia roles, see the *Gaia Administration Guide* for your version of the Management Server (Chapter "*User Management*").

Examples

Example 1 - The 'show cdt candidates candidates-list' command

```
MgmtServer> show cdt candidates candidates-list test.csv
Central Deployment Tool Candidates List:
=========================================

**************************
Generation time: 23-09-2020 15:48:21
This installation candidates list was generated for use with the following deployment plan
(Name, MD5 sum):
/var/log/CPcdt/logs_2020-09-23-15-47-43/DepPlan.xml, 67f3b9a71a5c3b8d51c51c9c1d63f3bb
**************************

         Object Name ,         Cluster Name ,      IP Address ,  Version/JHF Take ,
     State , Upgrade Order

=============================================================================================
============================


                gw1 ,             cluster1 ,     172.29.0.80 ,        R80.20/205 ,
    active ,             1
                gw2 ,             cluster1 ,     172.29.0.79 ,        R80.20/205 ,
   standby ,             1
```

Example 2 - The 'show cdt status' command

```
MgmtServer> show cdt status
================================================= Current execution status
=================================================

Deployment plan file: /var/log/CPcdt/logs_2020-09-23-15-53-43/DepPlan.xml

Initialize all candidates for execute

Last updated at: 15:54:19
```

Example 3 - The 'show cdt generate-output' command

```
MgmtServer> show cdt generate-output
Wed Sep 23 15:47:43 2020 *E* [Main]: The SendTo setting in the CentralDeploymentTool.xml file
is not empty, but an email server is not configured in Gaia. Notification email will not be
sent.
Wed Sep 23 15:47:45 2020 *A* [Main]: Central Deployment Tool (version 1.9.0 build #990180576)
Wed Sep 23 15:47:45 2020 *A* [Main]: ============================================================

Wed Sep 23 15:47:45 2020 *A* [Main]: Current execution logs are in: /var/log/CPcdt/logs_2020-
09-23-15-47-43/
Wed Sep 23 15:47:45 2020 *N* [Main]: Please wait while generating the installation candidates
list...
Wed Sep 23 15:47:45 2020 *N* [Main]: This process may take a few minutes.
Wed Sep 23 15:48:21 2020 *N* [Main]: The generated candidates list is:
/opt/CPcdt/CandidateListsRepository/test.csv

Wed Sep 23 15:48:21 2020 *N* [Main]:
Central Deployment Tool Candidates List:
========================================

**************************
Generation time: 23-09-2020 15:48:21
This installation candidates list was generated for use with the following deployment plan
(Name, MD5 sum):
/var/log/CPcdt/logs_2020-09-23-15-47-43/DepPlan.xml, 67f3b9a71a5c3b8d51c51c9c1d63f3bb
**************************

         Object Name ,         Cluster Name ,      IP Address ,  Version/JHF Take ,
     State , Upgrade Order

================================================================================================
============================


                gw1 ,             cluster1 ,     172.29.0.80 ,        R80.20/205 ,
    active ,             1
                gw2 ,             cluster1 ,     172.29.0.79 ,        R80.20/205 ,
   standby ,             1

Wed Sep 23 15:48:21 2020 *N* [Main]: Total execution time: 0 hours 0 minutes 37 seconds
```

Example 4 - The 'set cdt candidates' command

```
MgmtServer> set cdt candidates candidates-list test.csv disable-candidate gw1
Candidate file was changed successfully.
```

Example 5 - The 'start cdt generate-candidates' command

```
MgmtServer> start cdt generate-candidates deployment-plan DepPlan.xml candidates-list
test.csv
Operation started. To see the command result view the output.(ID: 1)
```

Example 6 - The 'start cdt execute' command

```
MgmtServer> start cdt execute deployment-plan DepPlan.xml candidates-list test.csv
Operation started. To see the command result run: show cdt status...(ID: 2)
```

Glossary

A

Advanced Mode
CDT operation mode, in which it runs a Deployment Plan File - a list of configured actions on the specified Security Gateways and Cluster Members.

Anti-Bot
Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam
Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus
Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control
Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

Audit Log
Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

B

Basic Mode
CDT operation mode, in which it installs a package and runs Pre-Installation and Post-Installation scripts on the specified Security Gateways and Cluster Members.

Bridge Mode
Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Cluster
Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member
Security Gateway that is part of a cluster.

Compliance
Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness
Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

CoreXL
Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance
On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND
Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE
Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway
Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Loss Prevention
Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type
Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Deployment Plan File
Special configuration file for the CDT Advanced Mode, in which you configure a sequence of actions for remote Security Gateways and Cluster Members. This is an XML file, which you create in a desired location with a desired name.

Distributed Deployment
Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object
Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management
Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode
The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia
Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish
The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal
Web interface for the Check Point Gaia operating system.

H

Hotfix
Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection
Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA
Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness
Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging
Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

Installation Candidates List File
A CSV (comma-separated values) file the CDT generates. This list contains the supported Security Gateways and Cluster Members in the Security Management Server or Domain Management Server database. In this file, you select the Security Gateways and Cluster Members, on which to install the CPUSE packages.

Internal Network
Computers and resources protected by the Firewall and accessed by authenticated users.

IPS
Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN
Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator
Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos
An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

L

Log Server
Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status
Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface
(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server
Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules
Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Mobile Access
Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server
Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server
Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object
Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management
Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

O

Open Server
Physical computer manufactured and distributed by a company, other than Check Point.

P

Primary Configuration File
Main configuration file for the CDT (CentralDeploymentTool.xml).

Provisioning
Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Q

QoS
Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Resume
Operation, or mode, in which CDT contiinues the installation of a CPUSE package from the point of failure, after the installation failed on some of the Security Gateways or Cluster Members.

Retry
Operation, or mode, in which CDT tries to install a CPUSE package again after the installation failed on some of the Security Gateways or Cluster Members.

RMA
Return Merchandise Authorization. A part of the process of returning a product to receive a refund, replacement, or repair during the product's warranty period.

RMA Mode
CDT operation mode, in which it automates the RMA backup and RMA restore process to reconfigure the replacement Security Gateway.

Rule
Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base
All rules configured in a given Security Policy. Synonym: Rulebase.

S

SecureXL
Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway
Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server
Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy
Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

SIC
Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SmartConsole
Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard
Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning
Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate
Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

Software Blade
Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone
Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

T

Threat Emulation
Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction
Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

U

Updatable Object
Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering
Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory
Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

VSX
Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway
Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing
Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.