16 July 2018

CLOUD SERVICES

Administration Guide

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.

Latest Version of this Document

Download the latest version of this document http://supportcontent.checkpoint.com/documentation_download?ID=31540.

To learn more, visit the Check Point Support Center http://supportcenter.checkpoint.com.

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Cloud Services Administration Guide.

Revision History

Date	Description
16 July 2018	Added limitation about running multiple instances of ADSync ("Activating the Active Directory Synchronizer" on page 39).
	Corrected syntax ("Configuring AD Synchronizer to Work with LDAP Over SSL" on page 44).
23 April 2018	Added Use Case for Client Settings Profile ("Use Case - Setting a Client Settings Profile" on page 21).
	Added LDAPS ("Configuring SSO to Work with LDAP Over SSL" on page 49), SSO and ADSync support ("Configuring AD Synchronizer to Work with LDAP Over SSL" on page 44).
	Added feature of uploading exclusion list from a CSV file ("Importing Excluded Networks from a CSV File" on page 57).
	Updated application rules for a category that is labeled uncategorized ("Advanced URL Filtering Policy Mode" on page 17).
	Added feature of exporting users to a CSV file ("Exporting Users to a CSV File" on page 28).
24 July 2017	Updated Exclude Network

Date	Description
05 June 2017	Added Client Settings Profiles ("Client Setting Profiles" on page 55)
	Updated Location Awareness ("Step 6: Location Awareness" on page 64)
	Updated Users (on page 26)
	Added Device Status (on page 29)
	Updated **Not supported for Cloud Services** in Setting up the Central Management Security Policy ("Central Management Security Policy" on page 19)
09 February 2017	Added Customizing UserCheck Messages ("Customizing UserCheck Messages in SmartDashboard" on page 62)
	Updated Location Awareness ("Step 6: Location Awareness" on page 64)
06 November 2016	Updated Cloud Services utility upgrade instructions
	Updated Mail Protection (on page 120)
	Improved formatting and document layout
11 January 2016	Added Policy Installation Progress (on page 24)
	Updated Licensing (on page 63)
	Updated Inline MTA
	Updated Running Single Sign On as a Service (on page 51)
25 November 2015	Updated Account Management
	Added Deleting an Account
	Updated Exclude Network
	Updated Inline MTA
	Removed support for Offices
19 October 2015	First release of this document

Contents

Terms

Anti-Bot

1. An application that prevents computers from being controlled by hackers.

2. Check Point Software Blade that inspects network traffic for malicious bot software.

Anti-Virus

A solution to protect a computer or network against self-propagating programs or processes that can cause damage.

Application Control

The ability to create rules that control user or computer access to specified applications.

Audit Log

A record of an action that is done by an Administrator. See also *Log* (on page 9).

Block

1. To stop traffic before it reaches its destination.

2. To stop a command from execution.

3. To deny access by rule (though allowed by permission).

Bot

Malicious software that neutralizes Anti-Virus defenses, connects to a Command and Control center for instructions from cyber criminals, and carries out the instructions.

DLP

Data Loss Prevention. Detects and prevents the unauthorized transmission of confidential information.

Drop

To not allow packets through the gateway, blocking the connection.

Firewall

The software and hardware that protects a computer network by analyzing the incoming and outgoing network traffic (packets).

HTTPS Inspection

Examines traffic that is encrypted using the Secure Sockets Layer (SSL) protocol. SSL ensures data privacy and integrity by encrypting traffic between internet browser clients and web servers.

Log

A record of an action that is done by a Software Blade.

Log Server

Physical server that hosts Check Point product log files.

Remote Access Community

A group of computers, appliances, and devices that access, with authentication and encryption, the internal protected network from physically remote sites.

Security Gateway

A Check Point computer that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Management Server

A Check Point computer that runs Check Point software to manage the objects and policies in Check Point environment.

ThreatCloud

A database of security intelligence that is dynamically updated using a worldwide network of threat sensors.

URL Filtering

The ability to create rules that control user and computer access to specified sites based on their URL.

UserCheck

Gives users a warning when there is a potential risk of data loss or security violation. This helps users to prevent security

incidents and to learn about the
organizational security policy.

Welcome

Welcome to Check Point Cloud Services.

Check Point Cloud Services refers to multiple Check Point Security Gateways maintained at various locations around the world.
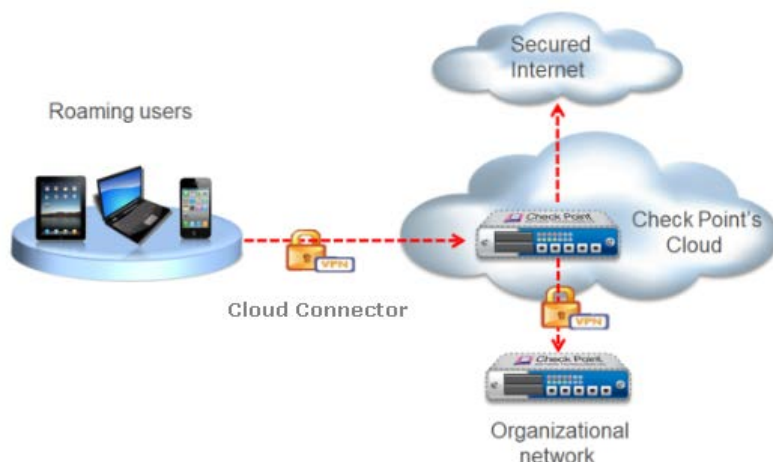
For Small Companies and Individual Users

These Security Gateways offer security services without the overhead of maintaining a physical gateway. For example, a small company of ten employees might want to protect the laptops, smart-phones and tablets issued to them. This can be done easily using Check Point Cloud Services.

Users install the Cloud Connect client on their roaming devices to connect to Cloud Services for security protection.

For Corporate Enterprises

Check Point Cloud Services helps enterprises protect roaming users (laptops and mobile devices) when they are outside the secured office environment. By tunneling all roaming user traffic to a Cloud Service for security inspection, security is extended beyond the immediate enterprise.

Cloud Services includes these services:

- URL Filtering
- Anti-Virus
- Anti-Bot
- Threat Emulation
- IPS
- HTTPS Inspection

For more about this release and technical requirements, see sk102501 http://supportcontent.checkpoint.com/solutions?id=sk102501.

Workflow for Using the Cloud Portal

Step 1: Create a Cloud account ("Step 1: Creating a New Account" on page 14)

Step 2: Configure an account policy ("Step 2: Policy" on page 16)

Step 3: Configure Cloud users ("Step 3: Users" on page 26)
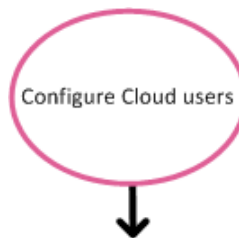
Step 4: Configure Cloud utilities ("Step 4: Utilities" on page 31)
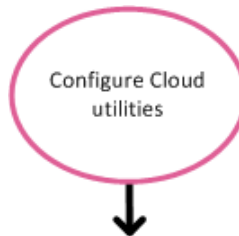
Step 5: Configure client settings profiles ("Step 5: Settings" on page 55)
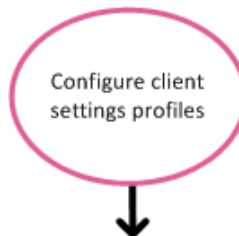
Step 6: Configure networks and servers ("Step 6: Location Awareness" on page 64)
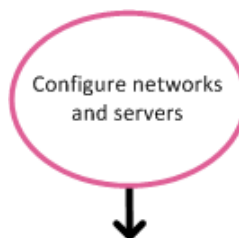
Step 7: Download the client and distribute to users ("Step 7: Installing Clients" on page 66)

Download and distribute to users

Step 1: Creating a New Account

When you access the Cloud Portal for the first time, create a new account:

1. Enter a valid email address.
2. Enter a password you will use to log into the Cloud Portal.
3. Confirm the password.
4. Click **Sign Up**.
5. A confirmation email is sent to the address specified in step 1. Click **Activate Account** in the email.

   The Cloud Portal opens in your browser and you can log in.

Logging in

After you have an account, log in to the portal with your account credentials. You can also reset a forgotten password.

To reset a forgotten password:

1. Click **Forgot Your Password?**
2. When prompted, enter your email address.

   A password reset link is sent to your email address.
3. Click the link and reset your password before the time limit expires.
4. Log in to the portal using your new password.

Using the Cloud Portal

After log in, the Cloud Portal opens to the **Overview** tab. Use these tabs to manage the Cloud Portal:

- **Overview**
  - To see the Cloud Services activity in your environment.
- **Policy**
  - To set the policy for:
    - URL Filtering
    - Threat Prevention
    - HTTPS Inspection
    - Client settings
- **Logs & Reports**
  - To see audit logs
  - To schedule reports
- **Users**
  - To add and change settings for users that can access the Cloud Services
- **Settings**
  - To change settings that relate to clients and devices

- To configure Central Management to work with SmartDashboard
- To access Cloud Services Utilities
- **Download**
  - To download Cloud Services apps and utilities

Note - The Cloud Portal automatically signs a user out, after a period of no activity.

Cloud Portal Compatibility

Best practice is to use the Cloud Portal with the Google Chrome browser.

The Cloud Portal is not supported with Mozilla Firefox browser.

Overview

The **Overview** tab shows events of all types so you can easily monitor the activities that are most important to you. You can drill-down into the data shown to see specific logs.

To define the time period shown on the page, click the calendar icon and select a time filter.

Use the free text search to filter results ("Query Syntax Reference" on page 72).

Step 2: Policy

The policy defines the rules that Cloud Services uses to protect users and devices. In this release, these functionalities are available: URL Filtering, Threat Prevention, and HTTPS Inspection.

You can define policies for user groups. See **Groups** in the **Users** tab.

URL Filtering

Choose a policy mode for URL Filtering:

- **Off**

  No policy is enforced.

- **Basic**

  The rules and configuration are pre-defined by Check Point. We recommend that beginner users use this mode.

- **Advanced**

  More granular than the Basic policy. For users who want to configure policy rules.

- **Central Management**

  Customers manage their Security Policies through the Check Point Cloud Portal and use a web-based user interface to create and change security rules ("Creating a Client Settings Profile and Rules" on page 23).

  You can configure Central Management settings from the **Settings** tab.

You can easily switch between policy modes, but only one mode is enforced at a time. You cannot mix elements of the different policy modes.

To change the policy mode for Cloud Portal:

1. Go to the **Policy** tab.
2. Select a policy mode.
3. Click **Install Policy**.

The selected policy is enforced on users and devices.

Basic URL Filtering Policy

The Basic URL Filtering Security Policy monitors and terminates all suspicious malware activity on the network.

It includes these risk groups:

- **Security Risk**

  Blocks applications and URLs from these categories:
  - Anonymizer
  - Botnets
  - Hacking
  - Phishing

- Spyware/Malicious sites and Spam

- **Inappropriate**

  Blocks applications and URLs from these categories:
  - Gambling
  - Hate / Racism
  - Illegal / Questionable
  - Illegal Drugs
  - Violence
  - Weapons and Sex

- **File Sharing**

  Blocks application and URLs from these categories:
  - P2P File Sharing
  - File storage and sharing
  - Bittorrent protocol
  - Gnutella protocol
  - eDonkey protocol
  - Share music
  - Torrent trackers and Facebook file shares

Other categories can be allowed or blocked:

- **Other Blocked categories**

  Lets you select other applications and protocols to block, or create custom URLs for specified sites.

- **Other Allowed Categories**

  Lets you select other applications and protocols to allow, or create custom URLs for specified sites.

Logging for a URL Filtering Policy

Basic policy

The options are:

- **Log All Traffic** - All internet activity is logged

- **Log Only Blocked Traffic -** Only attempts to access restricted sites are logged

- **Log None -** No activity is logged

See **Advanced policy** and **Central Management policy** to configure logs for each rule.

Advanced URL Filtering Policy Mode

The **Advanced Policy Mode** lets you configure rules for Application & URL Filtering to block or allow applications and sites.

The Rule Base has these components and functions available:

No.	Source	Application	Action	Track	Comments
	Users	Categories	**Block**		Optional
	User Groups	Applications	**Accept**		
		User-defined URLs	**Ask**		
		Uncategorized			

- You can use the **Application** category to define rules specific for your organization.
    - Click **New** > **Custom URL** to create an entry for an application or URL that is not on the list
    - Create Custom URLs with Regular Expressions. Custom URLs only work if configured with the correct syntax.
    - Custom URLs can have multiple URLs defined as a regular expression only, and *cannot* contain nested groups.

Note - If an entry in the **Application** column reads *Uncategorized*, the Rule Base ignores it.

- You can use the **Action** category to define traffic rules
    - **Block -** Traffic is blocked, and a notification shows in the browser
    - **Accept -** Traffic is allowed
    - **Ask -** The user must agree to use the site or application in accordance with company policy. Users will see an Ask page one time every 24 hours.

- You can use the **Track** category to define log rules. The log can be used for monitoring and forensic purposes. See logs in the **Logs** tab of the Cloud Portal.

Important - Policy changes are saved automatically, but they are only enforced after you click **Install Policy**.

Regular Expression Syntax

This table shows the Check Point implementation of standard regular expression metacharacters.

Metacharacter	Name	Description
\	Backslash	escape metacharacters non-printable characters character types
[ ]	Square Brackets	character class definition
( )	Parenthesis	sub-pattern, to use metacharacters on the enclosed string
{min[,max]}	Curly Brackets	min/max quantifier {n} - exactly n occurrences {n,m} - from n to m occurrences {n,} - at least n occurrences
.	Dot	match any character

Metacharacter	Name	Description
?	Question Mark	zero or one occurrences (equals {0,1})
*	Asterisk	zero or more occurrences of preceding character
+	Plus Sign	one or more occurrences (equals {1,})
|	Vertical Bar	alternative
^	Circumflex	anchor pattern to beginning of buffer (usually a word)
$	Dollar	anchor pattern to end of buffer (usually a word)
-	hyphen	range in character class

Central Management Security Policy

Set up the Cloud Services Security Policy in SmartDashboard on the Cloud Policy gateway in the same way as on a regular Security Gateway. However, because the Cloud Services security services are different than those of a regular gateway, there are some limitations. If the Rule Base for a supported blade contains rules that Central Management does not support, Cloud Services skips the rule and a warning shows in the **Install Policy** window.

To configure a Security Policy for Central Management, see Configuring Cloud Services Security Policies in SmartDashboard ("Configuring Cloud Services Security Policies in SmartDashboard" on page 60) variables. .

Threat Prevention

Threat Prevention detects and prevents malware and bots from reaching your organization. It includes these blades:

- **Anti-Virus** - Prevents and stops threats such as malware, viruses, and Trojans from infecting your network devices. It uses multiple malware detection engines and ThreatCloud technology to protect the network in real time.

- **Anti-Bot** - Detects and identifies bot-infected devices (stealth software that runs automated or remote controlled tasks over the Internet, usually malicious). It blocks the bot's Command and Control (C&C) communication to prevent damage.

- **Threat Emulation** - Prevents infections from undiscovered exploits, zero-day, and targeted attacks by inspecting files and running them in a "virtual sandbox" to discover malicious behavior.

Select a blade to enable or disable Threat Prevention.

HTTPS Inspection

HTTPS Inspection examines traffic that is encrypted using the Secure Sockets Layer (SSL) protocol. For example, if you want to track the use of encrypted file sharing applications on company laptops or mobile devices, you must enable HTTPS inspection.

From the Cloud Portal, the **HTTPS Inspection** page lets you:

- Turn HTTPS Inspection **On** or **Off**. When on, Cloud Services inspects encrypted SSL traffic for malicious payloads.

- Select a mode: **Advanced** or **Central Management**

HTTPS Inspection Advanced Mode

Select **Exclude selected https categories** to configure exceptions for SSL traffic that must not be inspected.

Select **HTTPS traffic logging** to generate logs for HTTPS inspection traffic

Configuring Exceptions

- Exceptions can be categories of websites or URLs, or common applications such as Skype or Facebook chat.

- You can use Regular Expressions with the correct syntax ("Regular Expression Syntax" on page 18) to create exceptions.

To create an HTTPS exception:

1. Click **New**.

   The **Add HTTPS Exception** window opens.

2. Click a column to edit its contents.

   - **Source** - Add or remove users, devices, or user groups. The rule applies when these objects initiate the traffic.

   - **Applications** - Filter by **Categories**, **Custom**, or **All** and select categories or Apps for the rule.

   - **Track** - Choose **Log** to create a log for the rule.

3. Click **OK**.

4. Click **Install Policy**.

   Note -The exception rule is not enforced until you click **Install Policy** and the policy installed.

HTTPS Inspection Central Management Mode

When Central Management is selected the page shows exceptions configured in SmartDashboard for the Cloud Policy gateway object. See Central Management HTTPS Inspection Policy (on page 61) for details.

Download Certificate

A **Download Certificate** button shows on the HTTPS Inspection page.

When browsing the Internet (with HTTPS inspection turned on), the browser can show a warning message that the connection is not trusted. That means that the browser does not recognize the Cloud Services gateway certificate as trusted.

Preventing Browser Warnings

We recommend that users who access the Internet from behind an office gateway, install the Cloud Services browser certificate to prevent browser warnings. When Internet traffic is routed through Cloud Services and the certificate is not installed, users will get browser warnings.

To get the Cloud Services certificate:

1. In the Cloud Portal > **Policy** tab, click **HTTPS Inspection**.
2. Click **Download Certificate**.
3. Instruct users to download the certificate to their browser.
   - In Google Chrome:
     - Go to Settings > **Advanced** > **Manage Certificates**.
     - In the **Trusted Root Certification Authorities** tab.
     - Click **Import** and follow the instructions.
   - In Internet Explorer:
     - Go to **Tools** > **Internet Options**.
     - Open the **Content** tab, click **Certificates**.
     - In the **Trusted Root Certification Authorities** tab, click **Import**.
   - In Mozilla Firefox:
     - Go to **Options** > **Privacy & Security** > **Certificates** >**View Certificates**.
       The Certificate Manager opens.
     - Click the **Authorities** tab.
     - Click **Import**.
     - When asked for the certificate's purpose, select **Identifying websites**.

Client Settings

Use Case - Setting a Client Settings Profile

Use case

Susan, an administrator for ABC Hitech, wants to configure special rules for Capsule Connect Client for the IT department and the Management team. The office policy rules are configured such that there is no Internet access for company employees. These groups, however, have to access high-risk applications or resources while in the office, from time to time. That requires unblocked Internet access.

1. She has to configure the way that Capsule Client reconnects and disconnects when inside the office network.
   - Configure Location Awareness
2. She wants the IT department and Management team to be able to disconnect the Capsule Cloud client for a period of up to 4 hours so they can complete their work.
   - Configure Disconnection Durations

Workflow for Setting a Client Settings Profile

Step 1: Add users to the Client.

Step 2: Create the user groups.

> **Note** - If you use AD Sync and you have groups set up in your directory, the groups synchronize automatically, and you do not have to create the groups manually. Make sure you select the correct **AD Base Node** to enable the groups.

Step 3: Add members to the User Group

Step 3: Create a client settings profile

Step 4: Configure the rules for the profile

Step 5: Add User Groups to the profile

Step 6: Create a new client settings rule for the User Group

Creating User Groups and Adding Users

To add users to your system:

1. From the **Users** tab, click **New**.
   The **New Local User** window shows.
2. Enter the **User Email** and enter the credentials.
3. Configure the settings for your network.
4. Check the box to **Send registration email to user**.
5. Click **Apply**.

This is how the list of Users shows:

Name	Device Status	Last Connected	Comments
johnb_ceo@abchitech.com	Status of the device he is using	Date/Time she last connected	CEO, John Burns, at ABC Hitech
susana_admin@abchitech.com	Status of the device she is using	Date/Time she last connected	Susan Anders, Chief System Administrator at ABC Hitech

To create the User Group for the IT and Management Team:

1. From the **Users** tab, click **Groups**.
2. Click **New**.
   The **New Group** window shows.
3. Enter the credentials for the group.
   a) **Group name**
   b) **Comments** (a description to identify the group)
   c) **Group members**

To add members to the Group:

1. Check the box for each of the users you want to add to the group.

2. Click **Apply**.

To view the Users in your system, click the **Users** tab.

To view the Users in each Group, from the **Groups** tab, double-click the group and the list of Group members shows.

Creating a Client Settings Profile and Rules

Now, lets create a **Client Settings Profile**, and later we will add the Groups, IT and Management Team, to this profile.

In this example, lets call our **Profile** 'PowerUsers'. First lets define the rule **Location Awareness**, and then lets define the rule **Disconnection Durations**. After that, lets add this new profile to the client settings policy by adding a new rule to match the user group and the profile.

To create a Client Settings Profile:

1. From the **Settings** tab, click **New**.

   In the **Comments** field, enter a description for this group.

   In our example, create the **Profile Name** - PowerUsers, and add a description to the **Comments** field, such as Rules for IT and Management Team.

   Now lets configure the rules for this profile.

2. From the menu at the left:

   a) Select **Location Awareness**.

      Check the box **Connect to Cloud when inside the office**.

   b) Select **Internal Servers**.

      Add a new **Internal server address**

      OR

      Select the server with an IP address and Port Number that can access the Internet from the office. This allows the users in the PowerUsers group to have Internet access while in the office.

   c) Select **Disconnection Durations**.

      Check the box **Allow users to suspend application**

      Uncheck any boxes that do not apply to your rules. In this example, uncheck all the boxes except **4 hours**.

      This allows the users to connect to the Internet while in the office, for a period of up to 4 hours.

Now, lets add User Groups to this profile.

To create a new client settings rule for your User Group:

1. From the **Policy** tab, click **Client Settings**.

   The User Groups show.

2. Click **New**.

   The **New Client Settings Rule** window shows.

   In the **Groups** column, the default group, **All Users**, shows.

3. Click **All Users** from the **Groups** column.

The **Select Groups** window shows.

4. Check the **Name** of the groups to add to the Client Settings Profile.

5. Click **Select**.

6. Click **Select a Profile** from the **Profile** column.

7. Add the name of the profile. In our example, it is PowerUsers.

8. Click **Select**.

9. Click **Add**.

This is how the Client Settings Policy in our example appears:

No	Groups	Profile	Comments
1	IT Management Team	PowerUsers	These users have four hours a day of open Internet use (no restrictions).
2	All users	All company employees	These users have restricted Internet access at all times.

Note - The order of rules is very important. When you add rules to the policy, add any specially configured rules to the top of the Rule Base. The Rule Base enforces the rules in the order in which it sees it. Therefore, any general rules for All Users have to show below.

Policy Installation Progress

After you install policy, if you click on the installation progress bar at the bottom, a window opens that shows:

- The policy installation status on each Cloud Services data center used recently.

- The policy installation status on each Cloud Services unused data center.

When the policy installation finishes, the status shows:

- **Policy installed** - The policy is successfully installed on all data centers.

- **Partial policy installation** - The policy is successfully installed on some gateways. Click on the links to see the progress on different data centers.

Central Management

In Check Point Cloud Services, customers manage their Security Policies through the Check Point Cloud Portal and use a web-based user interface to create and change security rules.

With Central Management, customers use the Check Point SmartDashboard to manage the Security Policy. This lets existing Check Point customers manage their on-site and Cloud Services Security Gateways from one interface. The security administrator has a full view of the organization Security Policy enforced over the internal network and the roaming users.

When you configure and activate Central Management, the SmartDashboard policy shows in the **Policy** tab > **URL Filtering** page under **Central Management**. This policy is enforced. Note that the policy shown is read-only. Changes to the policy can only be made in SmartDashboard.

If Central Management is not configured, click the **configure** link. See Setting up Cloud Services Central Management ("Cloud Services Central Management" on page 58) for configuration instructions.

Step 3: Users

Users

Users can connect their laptops and mobile devices to the Check Point cloud.

These functionalities are available from the **Users** menu:

- Add a **New** user
- **Edit** a user profile
- **Delete** a user
- **Import Users**
- **Actions**
  - **Send Registration Code** ("Sending a Registration Code" on page 28)
  - **Create Suspend Code** ("Creating a Suspend Code" on page 29)
  - **Create Uninstall Code** ("Creating an Uninstall Code" on page 29)
- **Refresh**

You can perform the actions below from the users profile:

Action	What to do
See the connection status of all devices that have Cloud Connect installed.	Look in the **Device Status** column ("Device Status" on page 29). • Hover over the icon to see the device name. • Hover over the status to see when it was updated.
See the status of users' registration codes.	Look in the **Device Status** column ("Device Status" on page 29). See which kind of codes a user has and if they are valid.
Import users from a CSV file.	Click **Import Users.** Use the **Example CSV file** to build a user list CSV file and upload it to the portal to import all users on the list. **Note** - CSV file import is limited to100 users at a time.
Send registration codes, create suspend codes, and create uninstall codes.	Click **Actions** and select an option.
Export users to a CSV file.	Click **Actions** > **Export Users**. **Note** - Exporting Users is limited to 3,000 users.

Double-click a column heading to sort by that column.

Creating New Users

If the new user is an administrator, give them Administrator or Help Desk permissions.

Administrator

- Can see all tabs and do all operations in the Cloud Portal

Help Desk

- Can manage users and devices and create new users
- Cannot see the **Policy** and **Account Settings** tabs
- Cannot change passwords

To create a new user:

1. Click **New**.

2. The **New Local User** window opens.

   a) Enter the user's email address.

   b) Optional: Enter related comments.

   c) Select **Is Admin** if the user is a Cloud Portal administrator

      OR

      Select **Is Help Desk Admin** if the user is a technical support administrator.

   d) Set a password for the administrator account and enter it again to confirm.

   e) Make sure that **Send registration email to user** is selected. Clear it if you do not want the user to get an email with Registration codes.

3. Click **Apply**.

   The user is immediately sent an email with links to the Cloud Connect client and installation instructions.

Note - You can also import users with the Active Directory Synchronizer or from a CSV (Comma Separated values) file ("Importing Users from a CSV File" on page 27).

Importing Users from a CSV File

To import users from a CSV file:

1. Click **Import Users**.

   The **Import Users from CSV File** window opens. From this window, you can download the sample **Example CSV file**.

   Before you import the CSV file, make sure it matches the formatting of the example file. You can use the example file as a template, but:

   - Do not change the first line.
   - The file must not contain more than a 100 users. If you want to add 500 users, then you have to create 5 CSV files, each with 100 users.

2. Browse to the CSV file and select it.

3. Click **Import**.

Notes:

- All the users listed in the file will immediately receive an email with download links to Cloud Connect. Therefore, if you do not want all of the users to get an email, you have to sort through the users.

- Make sure that there is no firewall rule that will prevent emails with the same source address from reaching the corporate network. For example, an anti-spam rule.

Exporting Users to a CSV File

Use Case

An administrator can create a report with details about the users in the network. You can use the **Export Users** option to create a CSV file with that information.

From the **Users** page, click **Actions** > **Export Users**.

The file **UserDevices.csv** is downloaded. You can configure the fields in the report.

Editing User Properties

Only users with administrator permissions can change a user's password. The administrator's password is required to make the change.

To edit a user's permissions or details:

1. Select the user from the table in the **Users** tab.
2. Click **Edit**, to edit the values.
3. Enter your password, if necessary.
4. Click **Apply**.

Deleting Users

To delete a user:

1. In the **Users** tab, select a user and click **Delete**.
2. Deleted users have to uninstall Cloud Connect client from their devices. If they do not delete the client, it will continue to try to connect to Cloud Services.

Sending a Registration Code

Registration codes:

- Register the Cloud Connect clients to Check Point Cloud Services
- Are unique for each user
- Cannot be sent to groups

You can see the status of a user's registration codes in the **Users** tab > **Device Status** column.

When users get a registration email, it contains a **Registration Key** for use with Windows or Mac Cloud Connect.

To send a registration code:

1. Select a user.

2. Click **Actions** > **Send Registration Code**.

    The user receives an email with the registration key and links to Cloud Connect clients.

    Notes:

    - The user must enter the registration code before requesting a code for a second device. For example, a user can have two or more laptops. If the first code was not entered and a second code is requested, the first code becomes invalid.

    - The registration code can be used one time for each operating system. For example, a user can use the same registration code on a Windows laptop, and Mac laptop. Users cannot use the same registration code on two Windows laptops.

    - If the user uninstalls Cloud Connect and then installs it again, the user must get a new registration code.

    - If a user receives a registration key and does not connect within 5 minutes, a second email, that contains a QR code and link, is sent to the user.

Creating a Suspend Code

If you have to suspend traffic from the roaming device to the cloud, create and send the user a suspend code. For example, when troubleshooting a connection problem.

To create a suspend code

1. Select a user.
2. Click **Actions** > **Create Suspend Code**.

    Notes:

    The suspend code:

    - Is valid only for the time period specified, and enforced the moment the user enters the code into the client.

    - Must be entered into Cloud Connect within one hour from the time the code is generated.

Creating an Uninstall Code

If **Prevent users from uninstalling the Cloud Connect client** is selected in **Account Settings** > **Windows Settings**, users must enter an **uninstall code** to uninstall the client. If that option is not selected, users can uninstall the windows client without a code.

The code must be entered into the Cloud Connect within approximately one hour from the time it is generated.

To create an uninstall code:

1. In the Cloud Portal, **Users** tab, select a user.
2. Click **Actions** > **Create Uninstall Code**.
3. Send the code to the user.

Device Status

The device status is the last status reported by the user to Cloud Services.

These are common statuses that might show in the **Devices Status** column of the **Users** page:

Status	Description
Connected	When the user was last connected.
Session End	When the user shut down the computer.
Inside Office Network	When the user is inside the office and Cloud Services is disconnected.
Disconnected	When the user intentionally disconnected the Cloud Services client.
No valid registration codes available	When the user did not receive the client and did not yet register.

These are rare statuses that might show in the **Devices Status** column of the **Users** page:

Status	Description
Service Stop	When the user manually stopped the client Windows service (if allowed to), or is in the process of stopping it.
No Network	When the user does not have network connectivity.
Suspended	When the user entered a suspension code and temporarily does not report to Cloud Services.
Inside Captive Portal	When the user is in a hotspot and did not yet authenticate, and therefore is not connected to the Internet.
Starting Upgrade	An upgrade process was initiated on the client machine.
Upgrade Download Failed	A newer version download started but did not finish successfully.

Groups

Groups can include users defined in the **Users** tab.

To create a new user group:

1. From the **Users** tab, click **Groups**.
2. Click **New**.
   The **New Group** window opens.
3. Enter a **Group name**.
4. Enter a **Comment** (optional).
5. Select users to include in the group or click **New** to create new users.
6. Click **Apply**.

Step 4: Utilities

Cloud Services Utilities work with Cloud Services to make Cloud Services more streamlined with your organizational environment.

Important - Before you configure a utility, make sure you have the technical requirements. See sk102501 http://supportcontent.checkpoint.com/solutions?id=sk102501.

Working with Cloud Services Utilities

From the **Settings** tab > **Utilities** section, create an entity for each instance of a utility. Each entity has an **Entity GUID** that shows in the table and is used in the utility configuration.

The three utilities are:

- **AD Sychronizer** ("Using the Active Directory Synchronizer" on page 39)

- **Log Transport** ("Using the Log Transport Agent" on page 32)

- **Single Sign On** ("Using the SSO Authenticator" on page 45)

Use the instructions in the section for each utility to create a new entity. The procedures below are the same for each Cloud Services utility.

Action	Description
New	Create a new entity.
Edit	Edit the fields as necessary.
Delete	Delete an entity. You must first stop the utility before you can delete it.
Renew Registration	Renew the registration using the entity GUID.

Running Behind an HTTP Proxy

If there is an HTTP proxy server between the computer that a Cloud Services utility runs on and the Cloud Services servers, edit the utility's script.

Edit only the parameters shown. Do not add lines or more information.

To edit a utility script to work through an HTTP proxy server:

- **On Linux**: Edit the *<utility>*.sh script, where (*<utility>* = ADSync, LTA, or SSO). Change the PROXY_HOST=, and PROXY_PORT= variables to match your environment.

    For example:

    PROXY_HOST="my-proxy.com" (can be a hostname or IP address)

    PROXY_PORT=8080

- **On Windows**: Edit the <utility>.bat script, where (*<utility>* = ADSync, LTA, or SSO). Change the PROXY_HOST=, and PROXY_PORT= variables to match your environment.

For example:

SET "PROXY_HOST=my-proxy.com"

SET "PROXY_PORT=8080"

Running the Correct Java Version

All utilities require Java version 1.7 release 79
http://www.oracle.com/technetwork/java/javase/downloads/jre7-downloads-1880261.html.

Make sure you have the required Java version on your computer or server.

- If your computer is on Gaia, DO NOT replace the default Java version. Do these steps to make sure you do not interfere with other Check Point products:

  a) Download the zip file instead of the installation file.

  b) Extract it with the tar command, for example:

     `tar xvzf jre-7-linux-i586.tgz`

  c) For Linux, change the `JAVA_PATH` variable to point to the correct java executable. For example edit the SSO.sh script to show

     `JAVA_PATH="/home/admin/jre1.7.0/bin/java"`

- For non-Gaia computers, download the Java release that matches your operating system.

Using the Log Transport Agent

The Log Transport Agent (LTA) utility transfers logs from your Cloud Services account to a designated Log Server inside your internal corporate network. By default, logs are stored in the Cloud Services for 30 days before being marked for deletion. These logs are:

- Logs that were generated as a result of traffic going through the Cloud Services gateways by the Check Point blades, such as Application Control and URL Filtering.

- Audit logs that record administrative actions on the Cloud Services, such as user login, policy installation, and utility instance statuses.

The designated Log Server can be:

- A Check Point Log Server

- A Check Point Security Management Server that also functions as a Log Server

Important - Make sure that you have the requirements for *Log Transport Agent* shown in sk102501 http://supportcontent.checkpoint.com/solutions?id=sk102501.

We recommend that you use the SmartLog GUI client to see and manage the logs. You can also see logs in SmartView Tracker.

To configure log transport, install the Log Transport Agent on a Linux or Windows computer. The Agent uses the Cloud Services API to communicate with Cloud Services and forwards logs to the configured Check Point Log Server in your environment. The agent uses the OPSEC infrastructure to create trust with the Log Server.

Note - Only root users can do the procedures to configure and run Log Transport.

Workflow for the Log Transport Agent

Step 1: Download the Log Transport Agent from the Cloud Portal to the computer where the agent will run ("Downloading the Log Transport Agent" on page 33).

Step 2: Configure the Log Transport Agent as an OPSEC application in SmartDashboard ("Configuring Log Transport in SmartDashboard" on page 33).

Step 3: Get an OPSEC certificate for the computer ("Getting an OPSEC Certificate" on page 34).

Step 4: Configure the Log Transport Agent entity in the Cloud Portal ("Configuring the Log Transport Agent Entity" on page 35).

Step 5: Run the log transport script ("Running the Log Transport Agent Script" on page 37).

Downloading the Log Transport Agent

Download the Log Transport Agent from the Cloud Portal, **Download** tab, to a computer where the agent will run. The Log Transport Agent is supported on Windows and Linux.

To get and install the Log Transport Agent:

1. In the Cloud Portal > **Download** tab, **Log Transport Agen**t area, click **Download**.
2. Extract the tgz file on the computer where the Agent will run.

In Windows - To a folder, such as `C:\Users\<your user name>\fwcloud_LTA\`

   (Use a program such as 7-Zip or WinRAR)

   * In Linux - To a folder, such as `/home/<your user name>/fwcloud_LTA/`

   (Run: `tar xvzf LTA.tgz`)

Note – If you are using LogServer R80 and higher, you have to install a Hotfix to support LTA. See sk121594 http://supportcontent.checkpoint.com/solutions?id=sk121594.

Configuring Log Transport in SmartDashboard

In SmartDashboard, configure the Log Transport Agent as an OPSEC application. This enables the log server to create secure trust with the Log Transport client.

To configure the Log Transport Agent in SmartDashboard:

1. In SmartDashboard object tree, click the **Servers and OPSEC Applications** icon.
2. Right-click the OPSEC Applications folder and select **New** > **OPSEC Application**.
3. In the **OPSEC Application Properties** window, enter a name for the Log Transport Agent.
4. Select the local Log Server to be the **Host** object.
5. Under **Client Entities** select **ELA**.
6. Click **Communication**.
7. In the **Communication** window:

   a) Enter and confirm a password.

   b) Click **Initialize**.

   c) Wait until the **Close** button becomes available.

   d) Click **Close**.

8. Click **OK**.

9. Double click on the newly created OPSEC Application to see its details. Make sure that it has a **DN** name (next to the **Communication** button).

10. Select **Policy** > **Install Database**.

11. Select the Log Server to send logs to and the Security Management Server.

12. Click **OK**.

13. Wait for the database installation to complete and click **Close**.

Getting an OPSEC Certificate

When you run the **Log Transport Agent** for the first time, trust is established with the Log Server automatically through the Agent's OPSEC certificate. Alternatively, you can follow the procedure described here to manually get the certificate file, and make sure the name of the certificate file matches the OPSEC application name defined in the Cloud Portal.

To get an OPSEC certificate for the Log Transport Agent:

On Windows:

Run from the downloaded package:
```
opsec_pull_cert -h <management_server_IP> -n <OPSEC_application> -p <OTP>
-o <cert_file> -od <output_sic_file>
```

On Linux:

1. Log in as the root user.

2. Make sure you have `opsec_pull_cert` and `SO/libstdc++.so.5` from the downloaded package.

3. Run:
```
./opsec_pull_cert -h <management_server_IP> -n <OPSEC_application> -p
<OTP> -o <cert_file> -od <output_sic_file>
```

opsec_pull_cert Parameters

Parameter	Description
`management_server_IP`	The IP address of the management server that the OPSEC application was configured on
`OPSEC_application`	The name of the OPSEC application that you created in SmartDashboard.
`OTP`	The one-time password you entered in SmartDashboard when you configured the OPSEC application
`cert_file`	The name of the certificate file to be created (the default is `opsec.p12`)

Parameter	Description
`output_sic_file`	The name of a file that will be created, containing the SIC name for the client.
	The SIC name is the same as the DN of the OPSEC application you created in SmartDashboard. You can find it in this file if you do not have access to SmartDashboard. You need your SIC name to run the Log Transport Agent.

Note - SIC certificates cannot be reused. After you create a SIC certificate, you cannot create another one for the same OPSEC application.

If you need another SIC certificate, repeat the Communication step for the OPSEC Application in SmartDashboard and click **Initialize** again (step 7 in Configuring Log Transport in SmartDashboard (on page 33)) and then do the rest of the steps. If the Communication window shows "Trust Established", click **Reset** and then do the steps starting with step 7.

Troubleshooting

On Linux: If an error message, `Opsec error. rc=-1 err=-96 Connection error,` shows, make sure that the Security Management Server in your environment is accessible through port 18210.
To test it, enter: `telnet <management_server_IP> 18210`. If a terminal opens, then the connection is available.

On Windows: If a Windows Security Alert opens with this text, **opsec_pull_cert has been blocked by Windows Firewall,** click **Allow access**. Also, make sure that no external firewall blocks port 18210 from your client.

Configuring the Log Transport Agent Entity

In the **Settings** tab> **Utilities** section, open the **Log Transport** page. On this page you can create or edit a Log Transport Agent entity and define its settings. After you enter the details for all of the entity settings, an entry is added to the table on the page.

To configure an LTA entity:

1. In the Cloud Portal, in the **Settings** tab, click **Log Transport**.
2. Click **New**.
   The **Create New LTA Entity** window opens
3. Configure the **Log Transport Agent Settings (on page 36).**
4. If there is an HTTP proxy server between the Log Transport Agent computer and the Cloud Services servers, see Running Behind An HTTP Proxy (on page 31).
5. Click **Apply**.
6. You get a Registration code. Keep this code for when you run the LTA script.
   The Registration Code is valid for 24 hours. After 24 hours you must renew the registration.
7. In the **Registration Code** window, click **Download LTA** to download the **Log Transport Agent** package file. You can also get the same file from the **Download** tab of the Cloud Portal.

Log Transport Agent Settings

Parameter	Description	Example Value
Name	A meaningful name for the Log Transport Agent. Must not be blank.	`LTA_logServer1`
Client's Log Server		
IP Address	The IP address of the Log Server, to which the logs are transferred.	`192.0.2.1`

SIC Name	The SIC name of the client's Log Server. Get it in one of these ways:
	
	• For R77.x or earlier Management Server:
	
	  a) In SmartDashboard, edit the Log Server object.
	
	  b) Click `Test SIC Status`.
	
	  c) Copy the text from the `DN` field.
	
	• For R80 and higher Management Server:
	
	  a) On the Security Management Server, run (see skI3301 http://supportcontent.checkpoint.com/solutions?id=skI3301): `dbedit`
	
	  b) In the *dbedit*, run: `print network_objects <name of client log server object>`
	
	  c) Copy the `sic_name` value from the output.
	
	  d) In the *dbedit*, run: `-q`
	
	• On the Log Server, run: `ckp_regedit -p SOFTWARE/CheckPoint/SIC | sed -n -e 's/^.*MySICname=\[s\]//p' | awk -F' ' '{print $1}'`
		`CN=logServerName,O=mgmtName..abc123`

OPSEC Application		
Management IP Address	The IP address of the Management Server (the Certificate Authority for the Log Server)	`192.0.2.2`
Application Name	The name of the OPSEC application as you defined it in SmartDashboard	`LTA_logServer1`
One-Time Password	The password as you defined it in SmartDashboard when configuring the OPSEC application (**Communication** button)	`password`

Parameter	Description	Example Value
Logging		
Number of log files to keep	The number of log files to keep. When the log file reaches 10 MB, logs are written to a new file. Default: 3 Range: 1-100	99
Enable debug logging	Select this to write Log Transport Agent debug logs to the LTA log file, `client_messages.log`. Note: Errors are always logged. Default: Not selected	Selected - Write logs that detail the LTA operations
Keep transported logs	Whether to keep the transported log records on the LTA computer (in the directory `<instance GUID>/archive/`). Default: Not selected	Selected - Keep a log file for each transported log record (in the directory `<instance GUID>/archive/)`
Miscellany		
Log Fetching Interval (Optional)	The number of minutes the Agent waits between each iteration of log fetching and sending Default: 5 Range : 1-60	10
SmartEvent Version	The version of SmartEvent or NGSE used for logs. Default: Older Version	**Older Version** or **R80 or NGSE**

Running the Log Transport Agent Script

Run all utilities as an administrator.

To run the Log Transport Agent Script on Windows and Linux

1. On the Log Transport Agent computer, extract the files in the Log Transport Agent package to a folder.
2. If there is an HTTP proxy server between the Log Transport Agent computer and the servers in the Cloud Services, see Running Behind An HTTP Proxy (on page).
3. Run the script:
   - **Linux:** `./LTA.sh run`
   - **Windows**: `LTA.bat run`

By default the script uses `settings.ini`. To use a different settings file, add it as the first parameter in the command. For example: `./LTA.sh run settings2.ini`

4. The first time you run the script, you are prompted for the **Instance GUID**. Enter the entity Registration Code.

   The Registration Code is valid for 24 hours. After 24 hours you must renew registration.

Run the script again after each reboot.

Notes for Ubuntu:

- If you see this:

  `error while loading shared libraries: libstdc++.so.5: cannot open shared object file: No such file or directory`

  Run:
  `sudo apt-get install libstdc++.so.5`

- If you see this:

  `cannot run program "./<executable name>": error=2, No such file or directory`

  Run:
  `sudo dpkg --add-architecture i386`
  `sudo apt-get update`
  `sudo apt-get install libc6:i386 libncurses5:i386 libstdc++6:i386`

Running Log Transport as a Service

You must run the Log Transport Agent Script at least one time before you run it as a service. This gives the service the required password.

To install Log Transport to run as a service on Linux:

- Run: `./LTA.sh service install [<settings file>]`

  The service will now run automatically when the machine boots.

You can start and stop the agent with the native Linux interface:

`service lta {start | stop | restart | status}`

To install Log Transport to run as a service on Windows:

.NET Framework is required to run a Cloud Services utility as a service on Windows. See sk102501 http://supportcontent.checkpoint.com/solutions?id=sk102501 for the required version.

1. Make sure you have `lta_service.exe`.
2. Open the command prompt as an administrator.
3. Run: `lta_service.exe {install | start | stop | uninstall} [<settings file>]`

   The command `install` also starts the service, and the command `uninstall` stops it before the uninstallation.

You can start and stop the LTA with the native Windows interface.

Upgrading the Log Transport Agent Utility

We recommend that you upgrade all instances of Cloud Services utilities to the latest version.

To upgrade the LTA utility to a new version:

1. Stop the running instances of LTA that you want to upgrade. You can stop the LTA script that is running or the LTA service.

2. Back up the instance sub-directories with all of their content to a backup location. For example, copy *<current LTA dir>* to *<old LTA dir>*.

3. Download the new version from the Cloud Portal, and extract it to a new folder.

   a) Extract the .TGZ content.

   b) Extract the .TAR file.

4. Copy all of the extracted tar files to the current ADSync directory to replace all of the existing files except for: the `settings.ini` file and relevant SIC certificate files, for example, `LTA_OPSEC1.p12`.

5. Make sure that the `settings.ini` and SIC certificate files, for example, `LTA_OPSEC1.p12` are the original ones, or copy them from the backup directory to the new LTA folder.

6. Run LTA.

Using the Active Directory Synchronizer

The Active Directory Synchronizer synchronizes users in an Active Directory environment with the Cloud Services database. You can define which nodes of the Active Directory are scanned and synchronized. The nodes to scan are defined in Active Directory Synchronizer entities.

Use the Active Directory Synchronizer on a computer that has connectivity to the Active Directory Server and Cloud Services.

Important - Make sure that you have the requirements for *Active Directory Synchronizer* shown in sk102501 http://supportcontent.checkpoint.com/solutions?id=sk102501.

By default, any user you add with the Active Directory Synchronizer does NOT get a registration email from Cloud Services. You can change this when you configure the Active Directory Synchronizer Entity, in the **Advanced Settings** > **Send Registration Email**.

Workflow for the Active Directory Synchronizer

Step 1: Download and activate the Active Directory Synchronizer ("Activating the Active Directory Synchronizer" on page 39).

Step 2: Configure the Active Directory Synchronizer Entity ("Configuring the Active Directory Synchronizer Entity" on page 40).

Step 3: Run ADSync as a service ("Running ADSync as a Service" on page 43).

Activating the Active Directory Synchronizer

Run all utilities as an administrator.

To use the Active Directory Synchronizer:

1. Download the **Active Directory Synchronizer** from the **Download** tab of the Cloud Portal to the computer that will run it.
   The ADSync.tgz opens in the location that you selected.

2. Extract all of the files in the archive:

   - **In Windows** - To a folder, such as `C:\Users\<your user name>\fwcloud_ADSync\`

     (Use a program such as 7-Zip or WinRAR)

   - **In Linux** - To a folder, such as `/home/<your user name>/fwcloud_ADSync/`

     (Run: `tar xvzf ADSync.tgz`)

3. Do the procedure in *Configuring the Active Directory Synchronizer Entity.* ("Configuring the Active Directory Synchronizer Entity *" on page* 40)Note the entity GUID that you get.

4. From the folder that contains the extracted files, run the script file for your operating system.

   - For Windows - run: `ADsync.bat run`
   - For Linux - run: `ADSync.sh run`

5. When you are prompted for the **Instance GUID**, enter the entity GUID.

6. If you did not enter an AD user name and password when configuring the entity in the Cloud Portal, enter them when prompted.

7. The script activates the Synchronizer. The Synchronizer runs continuously until the process is stopped, or until it encounters an error that it cannot recover from.

   If an error occurs, look in the **Audit Logs** page of the Cloud Portal and <*Instance GUID*>`/client_messages.log` file in the logs folder for details. Each Active Directory Synchronizer instance has a sub-folder with its GUID as the folder name.

   The Active Directory objects show in the **Users** tab of the Cloud Portal.

Notes:

- To stop the Active Directory Synchronizer go to the window or terminal running the script and enter Ctrl+c.

- To scan multiple nodes, create multiple AD Synchronizer entities in the Cloud Portal settings and use a different settings file for each entity.

  To use a specified settings file, run the appropriate script for your OS, and include the settings file as a parameter. For example, `./ADSync.sh run settings2.ini`. Do NOT copy the groups.txt and users.txt files from one folder to another. Each Active Directory Synchronizer instance has a sub-folder, with its GUID as the folder name, which contains these files.

- Do not move or delete the `groups.txt` and `users.txt` files. The Active Directory Synchronizer uses these files each time it scans the Active Directory for changes.

Important - If you want to run multiple instances of ADSync, you can only run one as a service. You have to run the other instances from the command line.

Configuring the Active Directory Synchronizer Entity

You can create or edit a Synchronizer Entity and define its settings on this page. After you enter the details for all of the Synchronizer Entity settings, there is a new entry in the table on the page. You can also **Edit** any entry.

The AD Synchronizer Entities table shows these fields:

- **Description**

  The description entered during configuration of the entity.

- **Scanned AD Object**

  The Active Directory root node that is scanned.

- **Entity GUID**

  The ID of the synchronizer entity for a specified scan node.

- **Status**

  - **Uninitialized** - The script for the synchronizer entity has not been run.
  - **Running** - The script is running and functional.
  - **Stopped** - The script was stopped.
  - **Error** - The script stopped because an error was encountered. Look at the Audit Logs page and the log file.
  - **Warning** -The script is still running but there is an issue to handle. Look at the Audit Logs page and the log file.
  - **No update** - The script was running, but has not updated the Cloud Services for at least 10 minutes. See the Last Update time. This can happen if the script cannot reach the Web Server or if the Synchronizer fails unexpectedly.

- **Last Update**

  Shows the last status update time.

- **Version**

  Shows the version of the Synchronizer utility.

To add a new Active Directory Synchronizer Entity:

1. In the **Settings** tab > **Utilities** section.
2. Click **AD Synchronizer** > **New**.

   The **Create New AD Synchronizer (ADSync) Entity** window shows.
3. Fill in the values for the New **ADSync Settings**.

You can create multiple entities if it is necessary to scan multiple nodes in the Active Directory.

- Fill in the form and click **Apply** and the Instance Registration window opens and shows you the entity GUID. Enter this GUID when you run the startup script. This ID is valid for 24 hours. After 24 hours you must renew registration (see below).

- Click **Close** and an entry is added to the table with the GUID for the configured node.

Adding Advanced Settings to an ADSync Entity

From the **Create New AD Synchronizer (ADSync) Entity** window, enter the **Name** and **Domain Name**. Use the **Advanced Settings** fields for addtional values.

Setting	Description	Example Value
Logging		
Number of Log Files to Keep	Maximum number of log files to allow (up to 10) Each file has a maximum size of 10MB Default = 3 Range = 1-100	99

Setting	Description	Example Value
Enable debug logging	Scanner writes logs to the `client_messages.log` file **Note** - Errors are always logged Default = Not selected (disabled)	Not selected - Do not write debug logs (only error logs) Selected - Write all logs

Miscellany

Setting	Description	Example Value
Domain Address	The IP address or DNS name of the Active Directory. This field is necessary when the domain address is different from the domain name.	`www.my-domain-example.com`
Edit the AD Base Node	Lets you edit the **AD Base Node** field below. If this is not selected, the Base Node field is generated automatically from the Domain Name. AD Sync starts the scan from the OU set in this field as the Base Node. The value of this field can contain only OU or CN objects. It cannot point to a group. Default = Not selected Note: Instances that were created before this option existed have this option selected.	Selected - Can edit the LDAP **Base Node** field
DN	Which LDAP node the scan starts from. This is taken from the Domain Name. If you enabled **editing the LDAP Base Node**, then you can edit it.	`CN=users,DC=my-domain-example,DC=com`
Scan AD (in minutes)	Time (in minutes) between scans for updates Default = 5 Range = 1-60	10
Upload at most	Number of users/groups uploaded at one time Default = 1000 Range = 10-1,000	500
Upload Disabled Users	Scanner uploads disabled user accounts Default = Not selected - Do not upload disabled accounts	Selected - Upload disabled accounts
Upload Empty Groups	Scanner uploads empty user groups Default = Not selected - Do not upload empty groups	Selected - Upload empty groups

Setting	Description	Example Value
Send Registration Email	Scanner sends each user uploaded with AD Sync an email with his registration code. Default: Not selected	Not selected - Do not send an email Selected - Send an email

Running ADSync as a Service

You must run the AD Synchronizer script at least one time before you run it as a service. This gives the service the required password.

To install AD Synchronizer to run as a service on Linux:

- Run: `./ADSync.sh service install [<`*settings file*`>]`

  The service will now run automatically when the machine boots.

You can start and stop the agent with the native Linux interface:

`service adsync {start | stop | restart | status}`

To install AD Synchronizer to run as a service on Windows:

.NET Framework is required to run a Cloud Services utility as a service on Windows. See sk102501 http://supportcontent.checkpoint.com/solutions?id=sk102501 for the required version.

1. Make sure you have `adsync_service.exe`.
2. Open the command prompt as an administrator.
3. Run: `adsync_service.exe {install | start | stop | uninstall} [<`*settings file*`>]`

   The command `install` also starts the service, and the command `uninstall` stops it before the uninstallation.

You can start and stop ADSync with the native Windows interface.

Upgrading the AD Synchronizer Utility

We recommend that you upgrade all instances of Cloud Services utilities to the latest version.

To upgrade the ADSync utility to a new version:

1. Stop the running instances of ADSync that you want to upgrade. You can stop the ADSync script that is running or the ADSync service.
2. Back up the instance, including its sub-directories with all of their contents, to a backup location. For example, copy <*current ADSync dir*> to <*old ADSync dir*>.
3. Download the new version from the Cloud Portal, and extract it to a new folder:

   a) Extract the .TGZ content.

   b) Extract the .TAR file.

   c) Copy all of the extracted tar files to the current ADSync directory to replace all of the existing files, except for the `settings.ini` file.

4. Make sure that the `settings.ini` file is the original one, or copy it from the backup directory to the new ADSync folder.

5. Run ADSync.

Configuring AD Synchronizer to Work with LDAP Over SSL

Verify that LDAP over SSL is installed. If it is not installed, the feature will not work.

To configure Active Directory Synchronizer to work with LDAP over SSL:

1. Confirm that LDAP over SSL is enabled on the Active Directory.

   a) Start the Active Directory Administration Tool, `Ldp.exe`

   b) On the Connection menu, click **Connect**.

   c) Type the name of the domain controller to which you want to connect.

   d) Type 636 as the port number.

   e) Click **OK**.

   f) If the connection is successful, root-DSE information prints in the right pane.

   If the verification fails, contact your administrator to enable LDAP over SSL on the Active Directory.

2. Export the certificate in the **Personal** > **Certificates** folder.

   a) Right-click the certificate under the **Personal** > **Certificates**. Select **All Tasks** > **export** > **Next**.

   b) Select **No, do not export the private key**> **Next**.

   c) Select **DER encoded binary X.509 (.CER)** > **Next**.

   d) Enter the filename > **Finish**.

3. Copy the exported certificate to a machine running the Active Directory Synchronizer.

   If the certificate was not issued by a trusted certificate authority, import the certificate into the Java certificate authority store so Java will trust the certificate.

4. Open the command prompt.

5. Run:

```
"%ProgramFiles%\Java\jre7\bin\keytool.exe" -importcert -alias <ca certificate alias> -keystore <java keystore> -storepass changeit  -file <certificate>.cer
```

For example:

```
"%ProgramFiles%\Java\jre7\bin\keytool.exe" -importcert -alias adcert
-keystore "%ProgramFiles%\Java\jre7\lib\security\cacerts" -storepass
changeit -file "C:\adcert.cer",
```

Before you run the Active Directory Synchronizer:

1. Edit the file `settings.ini` from the folder that contains the Active Directory Synchronizer.

2. On a new line add the field `LDAP_SSL_SERVER_NAME:`<*AD Server*> where AD Server is the name of the Active Directory that has LDAP SSL enabled.
   For example: `LDAP_SSL_SERVER_NAME:test.ad.com`

3. Save the file.
4. Continue to run ADSync.

Best Practices for Planning AD Synchronization

The ADSync is designed to synchronize an entire OU.

To plan for a gradual controlled synchronization of your AD structure or to synchronize only specified parts of the OU, use this workflow:

1. Create a new OU.
2. Create a new Security Group inside the newly created OU.
3. Add groups and users from other existing OUs as Members of the new Security Group.
4. Use this new OU as the base node for the ADSync entity configuration.

This lets you dynamically control the users and groups you want to synchronize to the Cloud Portal within Active Directory.

Using the SSO Authenticator

Use the SSO Authenticator to make it possible for users to access organization resources without authenticating. The Single Sign-on (SSO) Authenticator works in Active Directory environments and automatically registers Cloud Connect for Windows users when they install the Cloud Connect client.

Important - Make sure that you have the requirements for *SSO Authenticator* shown in sk102501 http://supportcontent.checkpoint.com/solutions?id=sk102501.

The SSO Authenticator computer requires Java version 1.7 from Oracle, to run. If you use a Gaia server for the SSO Authenticator, note that Gaia comes with the IBM Java program. You must download Oracle's Java to run the Authenticator on Gaia. See Running the Correct Java Version (on page 32).

Workflow for the SSO Authenticator

Step 1: Create a computer or VM for the SSO Authenticator ("Create SSO Authenticator Computer" on page 46).

Step 2: Configure the DNS server for the SSO Authenticator computer ("Configure the DNS Server" on page 46).

Step 3: Configure the SSO Authenticator computer to work with Active Directory ("Configuring SSO Integration with Active Directory" on page 46).

Step 4: Configure the SSO entity in the Cloud Portal ("Configuring the SSO Authenticator Entity" on page 47).

Step 5: Run the SSO Authenticator script on the SSO Authenticator computer ("Running the SSO Authenticator Script" on page 50).

Best Practice- We recommend that you enable Ping from each of the end devices that might use SSO. This allows for troubleshooting that may be required. When necessary, ping the SSO server to check connectivity.

Create SSO Authenticator Computer

Create a physical computer or VM for the SSO Authenticator with the hostname:
`fwcloudSSO_Server.<domain name>`

For example, `fwcloudSSO_Server.my-domain.com`

- The operating system can be Windows or Linux.

- If the operating system is Windows, the SSO Authenticator Computer must be part of the Active Directory (AD) office domain.

- Make sure the computer has connectivity to the Active Directory (AD) server.

- Make sure that DNS is configured correctly on the computer.

- Install the java jre on the computer. See Running the Correct Java Version (on page 32).

Configure the DNS Server

Make sure that the DNS configuration on the SSO Authenticator computer is correct. Ping the Active Directory server to make sure it has connectivity with the AD server.

Do these procedures on the DNS server that the SSO computer connects to:

- Define a reverse DNS lookup zone

- Create a host for the SSO Authenticator computer

To define a reverse DNS lookup zone:

1. Enter the DNS server utility.
2. Right click **Reverse Lookup Zones** and select **New Zone** > **Next** > **Primary Zone** > **Next**.
3. Select **To all DNS servers in this forest** > **Next**.
4. Select **IPv4 Reverse Lookup Zone** > **Next**.
5. In the **Network ID** field, enter the network IP address that the SSO Authenticator computer is on. For example if the new machine has the IP address 192.0.2.31, enter the network 192.0.2.
6. Click **Next** > **Next** > **Finish**.

To create a host for the SSO Authenticator computer:

1. Right-click on the <my-domain.com> under the Forward Lookup Zones and select **Other New Records** > **Host (A or AAAA)**.
2. In the **New Host** window:
   - Enter the name **fwcloudSSO_Server**.
   - Enter the IP address of the SSO Authenticator computer.
3. Make sure that **Update associates pointer (PTR) record** is selected.

Configuring SSO Integration with Active Directory

Configure the SSO Authenticator computer to work with Active Directory.

To configure integration with Active Directory on the SSO Authenticator computer:

1. In the Active Directory Users and Computers utility, add the user `fwcloudSSO_Server`

   Important - `fwcloudSSO_Server` MUST be the user name or the service will not work correctly.

a) Enter `fwcloudSSO_Server` as the **First name** and **User logon name.**

b) Click **Next**.

c) Enter a **Password** for the user.

d) Set the password to **Never expire**.

2. If your Active Directory is on Windows Server 2003, install Windows Support Tools on the Server.

3. Create the SPN (Service Principal Name).

   SPN is the identifier that Active Directory uses to grant users tickets to access services using the Kerberos authentication. These tickets are used between the client and the service provider to do the authentication.

   - Open the command line interface (`cmd`), and enter

     ```
     setspn -A fwcloud_SSO_Service/fwcloudSSO_Server.<domain name>
     fwcloudSSO_Server
     ```

   For example: `setspn -A` `fwcloud_SSO_Service/fwcloudSSO_Server.my-domain.com fwcloudSSO_Server`

4. Create the keytab file.

   The keytab file is an encrypted file that stores the ticket for Kerberos authentication.

   - In the command prompt window enter:

     ```
     ktpass -princ fwcloud_SSO_Service/fwcloudSSO_Server.<domain
     name>@DOMAIN-NAME -pass <password from step 1c> -mapuser
     <NETBIOSDOMAINNAME>\fwcloudSSO_Server -kvno 0 -pType KRB5_NT_PRINCIPAL
     -out <output path>\fwcloudSSO.keytab
     ```

   `-pass` is the password created for the `fwcloudSSO_Server` user in step 1c.

   For example: `ktpass -princ` `fwcloud_SSO_Service/fwcloudSSO_Server.my-domain.com@MY-DOMAIN.COM -pass 123456 -mapuser DOMAIN\fwcloudSSO_Server -kvno 0 -pType KRB5_NT_PRINCIPAL -out c:\temp\fwcloudSSO.keytab`

   Important: Use the same capitalization pattern as shown in the example.

5. Copy the `fwcloudSSO.keytab` file you created to the SSO Authenticator directory on your computer.

Configuring the SSO Authenticator Entity

You can create or edit an SSO Authenticator entity and define its settings on this page. After you enter the details for all of the synchronizer entity settings, there is a new entry in the table on the page. You can also **Edit** any entry.

The SSO Authenticator Entity table has these fields:

- **Description**

  The description entered during configuration of the entity.

- **Scanned AD Object**

  The Active Directory root node that is scanned.

- **Entity GUID**

  The ID of the synchronizer entity for a specified scan node.

- **Status**

- **Uninitialized** - The script for the synchronizer entity has not been run.
- **Running** - The script is running and functional.
- **Stopped** - The script was stopped.
- **Error** - The script stopped because an error was encountered. Look at the Audit Logs page and the log file.
- **Warning** -The script is still running but there is an issue to handle. Look at the Audit Logs page and the log file.
- **No update** - The script was running, but has not updated the Cloud Services for at least 10 minutes. See the Last Update time. This can happen if the script cannot reach the Web Server or if the Synchronizer fails unexpectedly.

- **Last Update**

  Shows the last status update time.

- **Version**

  Shows the version of the Synchronizer utility.

To add a new SSO entity:

1. Make sure the keytab file, created in Configure Integration with Active Directory ("Configuring SSO Integration with Active Directory" on page 46) is in the SSO Authenticator directory on your computer.

2. If there is a firewall between the computer and the AD server, make sure the Kerberos ports are open (UDP/TCP ports 88).

3. In the Cloud Portal, in the **Settings** tab, click **Single Sign On**.

4. Click **New**.

   The **Create New SSO Entity** window opens

5. Configure the **SSO settings**

6. If there is an HTTP proxy server between the SSO authenticator computer and the Cloud Services servers, see Running Behind An HTTP Proxy (on page 31).

7. Click **Apply**.

   The Instance Registration window opens and shows you the entity GUID. Enter this GUID when you run the startup script. This ID is valid for 24 hours. After 24 hours you must renew registration (see below).

8. In the **Registration Code** window, click **Download SSO** to download the SSO Authenticator files. You can also get the same files from the **Download** tab of the Cloud Portal.

9. Click **Close**.

   An entry is added to the table with the GUID for the configured node.

Adding Advanced Settings to an SSO Entity

From the **Create New Single Sign On (SSO) Entity** window, enter the **Name, Domain Name** and **AD Server Name**. Use the **Advanced Settings** fields for additional values.

Setting	Description	Example Value
Logging:		
Number of log files to keep	The number of log files to keep. When the log file reaches 10 MB, logs are written to a new file. Default: 3 Range: 1-100	99
Enable debug logging	Select this to write SSO Authenticator debugs logs to the Note: `client_messages.log` file. Errors are always logged. Default = Not selected - Do not write logs	Selected - Write logs
Miscellany:		
Domain Address	IP address or DNS name of the Active Directory Server. This field is necessary when the domain address is different from the domain name.	`www.my-domain-example.com`
Edit the AD Base Node	Lets you edit the **AD Base Node** field below. If this is not selected, the Base Node field is generated automatically from the Domain Name. The value of this field can contain only OU or CN objects. It cannot point to a group. Default = Not selected Note: Instances that were created before this option existed have this option selected.	Selected - Can edit the LDAP **Base Node** field
DN	Which LDAP node the scan starts from. This is taken from the Domain Name. If you enabled **editing the LDAP base node**, then you can edit it.	`CN=users,DC=my-domain-example,DC=com`

Configuring SSO to Work with LDAP Over SSL

Important - Confirm that LDAP over SSL is enabled on the Active Directory or the feature will not work.

To configure SSO to work with LDAP over SSL:

1. Confirm that LDAP over SSL is enabled on the Active Directory
2. Start the Active Directory Administration Tool, `Ldp.exe`

a) On the Connection menu, click **Connect**.

b) Type the name of the domain controller to which you want to connect.

c) Type 636 as the port number.

d) Click **OK**.

If the connection is successful, Root-DSE information prints in the right pane.

If the verification fails, contact your administrator to enable LDAP over SSL on the Active Directory .

3. Export the certificate in the **Personal** > **Certificates** folder.

a) Right-click the certificate under the **Personal** > **Certificates** and select **All Tasks** > **export**... > **Next**.

b) Select **No, do not export the private key** > **Next**.

c) Select **DER encoded binary X.509 (.CER)** > **Next**.

d) Enter the filename > **Finish**.

4. Copy the exported certificate to a machine running Single Sign On.

5. If the certificate was not issued by a trusted certificate authority, then import the certificate into the Java certificate authority store so that Java will trust the certificate.

6. Open the command prompt.

7. Run:

```
"%ProgramFiles%\Java\jre7\bin\keytool.exe" -importcert -alias <ca
certificate alias> -keystore <java keystore> -storepass changeit  -file
<certificate>.cer
```

For example:

```
"%ProgramFiles%\Java\jre7\bin\keytool.exe" -importcert -alias adcert
-keystore "%ProgramFiles%\Java\jre7\lib\security\cacerts" -storepass
changeit -file "C:\adcert.cer",
```

Before running Single Sign On:

1. Edit the file `settings.ini` located in the folder that contains the Single Sign On.

2. On a new line add `USE_SSL=1`

3. Save the file.

4. Continue to run ADSync.

Running the SSO Authenticator Script

After configuring the SSO service in the Cloud Portal, and downloading the SSO Authenticator files, run the SSO Authenticator Script on the SSO Authenticator computer.

Run all utilities as an administrator.

To run the SSO Authenticator Script:

1. On the SSO Authenticator computer, extract the files from `SSO.tgz`:

   • In Windows - To a folder, such as `C:\Users\<your user name>\fwcloud_SSO\`

(Use a program such as 7-Zip or WinRAR)

- In Linux - To a folder, such as `/home/<your user name>/fwcloud_SSO/`

  (Run: `tar xvzf SSO.tgz`)

2. If there is an HTTP proxy server between the SSO authenticator computer and the servers in the Cloud Services, see Running Behind An HTTP Proxy (on page 31).

3. From the folder that contains the extracted files, run the script file for your operating system:
   - For Windows, run: `SSO.bat run`
   - For Linux, run: `./SSO.sh run`

4. The first time you run the script, you are prompted for the **Instance GUID**. Enter the entity Registration Code.

   The Registration Code is valid for 24 hours. After 24 hours you must renew registration (see below).

5. If you did not enter an AD user name and password when configuring the SSO entity, and this is the first time you are running the script, you are prompted to enter them. Enter the AD user name and password.

6. The script activates the SSO Authenticator. The SSO Authenticator runs continuously until the process is stopped or until it encounters an error that it cannot recover from. If an error occurs, open the `<entity GUID>/client_message.log` file for details.

Note: To stop the SSO Authenticator, go to the window or terminal running the script and enter Ctrl+c.

Running Single Sign On as a Service

You must run the SSO Script at least one time before you run it as a service. This gives the service the required password.

To install Single Sign On to run as a service on Linux:

- Run: `./SSO.sh service install [<settings file>]`

  The service runs automatically when the machine boots.

You can start and stop the agent with the native Linux interface:

`service sso {start | stop | restart | status}`

To install Single Sign On to run as a service on Windows:

.NET Framework is required to run a Cloud Services utility as a service on Windows. See sk102501 http://supportcontent.checkpoint.com/solutions?id=sk102501 for the required version.

1. Make sure you have `sso_service.exe`.

2. In Windows 2012 and Windows 8: Open the command prompt as an administrator.

   In Windows 7: Open the command prompt from the system account.

3. Run: `sso_service.exe {install | start | stop | uninstall} [<settings file>]`

   The command `install` also starts the service, and the command `uninstall` stops it before the uninstallation.

4. Open the native Windows Services interface to edit the service, **Check Point SSO Service.** Make sure it is run by the Administrator account (and not by the System account).

   a) Run: `services.msc`

> The Windows **Services** utility opens.

b) Right-click **Check Point SSO Service** and select **Properties**.

c) In the **Log On** tab, select **This account**.

d) Enter the Administrator username and password

e) Click **OK.**

f) Start the service.

Configuring SSO Service on Gaia or Linux

The SSO Authenticator installation is completed automatically when you run it for the first time. Alternatively, do the procedure below manually.

To complete the SSO configuration on Linux:

1. Find the `/etc/krb5.conf` file.
2. Edit the domain information in the `/etc/krb5.conf` file to match your domain environment. For example:

```
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = MY-DOMAIN.COM
 dns_lookup_realm = true
 dns_lookup_kdc = true
 ticket_lifetime = 24h
 renew_lifetime = 7d
 forwardable = true
 default_tkt_enctypes = rc4-hmac des-cbc-crc des-cbc-md5
 default_tgs_enctypes = rc4-hmac des-cbc-crc des-cbc-md5

[realms]
 MY-DOMAIN.COM = {
  kdc = adserver.my-domain.com
  admin_server = adserver.my-domain.com
  default_domain = my-domain.com
 }

[domain_realm]
  .my-domain.com = MY-DOMAIN.COM
 my-domain.com = MY-DOMAIN.COM
```

3. In the command line interface, enter `su` to change to the root user account. Alternatively, add `sudo` at the beginning of each command in this procedure to use root permissions.
4. Install the necessary Kerberos packages for your operating system:
   - For Red Hat, Cent-OS, or Fedora - `yum install krb5-workstation`
   - For Debian or Ubuntu - `apt-get install krb5-user`
   - For Gaia -
      (i) Download the `krb5-workstation` package manually (CentOS 5 flavor)
      (ii) Install the `krb5-workstation` package with the command: `rpm -ivh <rpm file>`

(iii) Find the Kerberos utilities: `ktutil`, `klist`, and `kinit`, from the installed package and copy them to the directory `/usr/bin`.

(iv) Give the Kerberos utilities execution permission: `chmod +x kinit ktutil klst`

(v) If you get an error message about preliminary packages that are necessary to install the `krb5-workstation` package, download and install them also.

5. In a terminal window, enter: `ktutil`.

    The **ktutil** command line interface opens.

6. In the **ktutil** command line interface, enter:

    ```
    rkt <path to keytabfile>/fwcloudSSO.keytab
    ```

    This reads the keytab file and adds the data from the keytab to the data on the computer.

7. Write the keytab file that will be used for authentication. In the **ktutil** command line interface, enter:

    ```
    wkt /etc/krb5.keytab
    ```

    The new keytab file is created in the `/etc/` folder.

8. Press **q** to exit **ktutil**.

9. Start the Kerberos credentials for the service:

    ```
    kinit -k -t /etc/krb5.keytab
    fwcloud_SSO_Service/fwcloudSSO_Server.<domain name>
    ```

10. Enter: `klist`

    Make sure that the SPN created earlier is listed.

11. Copy the authenticator TGZ file to the machine, and extract it to a folder such as:

    `/home/<your user name>/fwcloud_SSO/`

    (Run: `tar xvzf SSO.tgz`)

12. Make sure port 50000 is allowed through the Linux firewall (IP tables if used).

13. If your default Java version is not Oracle 1.7, see Running the Correct Java Version (on page 32).

14. Run the script: `./SSO.sh run`

Configuring SSO Service on Windows

The SSO Authenticator installation is completed automatically when you run it for the first time. Alternatively, do the procedure below manually.

Log in to Windows with the user `fwcloudSSO_Server` that you created in Configure Integration with Active Directory ("Configuring SSO Integration with Active Directory" on page 46).

To complete the SSO configuration on Windows:

1. Make sure the computer is connected to the Active Directory.

2. Copy the keytab file to a secure folder on the Windows computer that only you can access.

3. Edit the `gss.conf` file so the keytab shows the path to the keytab file. For example

    ```
    com.sun.security.jgss.krb5.accept {
        com.sun.security.auth.module.Krb5LoginModule required
        storeKey=true
        keyTab="c:/<path to file>/fwcloudSSO.keytab"
        doNotPrompt=true
        useKeyTab=true
    ```

```
    realm="MY-DOMAIN.COM"

principal="fwcloud_SSO_Service/fwcloudSSO_Server.my-domain.com@MY-DOM
AIN.COM"
;
};
```

4. If there is a firewall between the client and this computer, make sure that port 50000 is allowed.

5. If your default Java version is not Oracle 1.7, see Running the Correct Java Version (on page 32).

6. Run the batch file: `SSO.bat run`

Upgrading the Single Sign On Utility

We recommend that you upgrade all instances of Cloud Services utilities to the latest version.

To upgrade the SSO utility to a new version:

1. Stop the running instances of SSO that you want to upgrade. You can stop the SSO script that is running or the SSO service.

2. Back up the instance, including its sub-directories with all of their contents, to a backup location. For example, copy *<current SSO dir>* `to` *<old SSO dir>* .

3. Download the new version from the Cloud Portal, and extract it to a new folder.

   a) Extract the .TGZ content.

   b) Extract the .TAR file.

   c) Copy all of the extracted tar files to the current SSO directory to replace all of the existing files, except for the `settings.ini` and `fwcloudSSO.keytab` files.

4. Make sure that the `settings.ini` and `fwcloudSSO.keytab` files are the original ones, or copy them from the backup directory to the new SSO folder.

5. Run SSO.

Step 5: Settings

The **Settings** tab contains settings for your Cloud Services environment and the Cloud Connect clients in it.

It also contains the configuration for utilities that work with Cloud Services. See Cloud Services Utilities ("Step 4: Utilities" on page 31) for details.

Client Setting Profiles

Define the profiles that have settings for Windows clients. Go to **Settings** > **Client Settings Profiles**.

These options are available:

- **Add**
- **Edit**
- **Delete**
- **Duplicate**

To **Add** or **Edit** a profile double-click a profile and the **Cloud Connect Settings** menu shows.

Editing or Adding a Client Profile

After you add a profile, or if you want to edit a profile, configure the profile in the **General Settings** page of the profile. Double-click a profile to access the **General Settings** window and **Add** a profile or **Edit Settings Profile**.

From the **Cloud Connect Settings** menu, these options are available:

- **General**
- **Location Awareness**
- **Windows Settings**
- **Email Notifications**
- **Disconnection Durations**

General Settings

The **General** menu shows these three fields:

- **Enable Cloud Connect**
  Select if the client is **ON** or **OFF** for all users assigned to the profile.
- **Profile Name**
- **Comments**

Windows Settings

These settings let administrators configure how the Windows Cloud Connect client behaves for end users. The settings are enforced the next time a user connects to the Cloud Portal. The Cloud Connect client automatically connects every 24 hours.

Anti Tampering

- **Prevent users from stopping the Cloud Connect service** - When selected, users cannot stop the Cloud Connect service from the Service Manager. Users can still end the process from the Task Manager if you do not enable Anti Tampering.

- **Prevent users from uninstalling the Cloud Connect client** - When selected, users must enter an uninstall code from their administrator before they can uninstall the Cloud Connect client. Create the uninstall code on the **Users and Devices** page.

- **Turn on "Anti Tampering" for the Cloud Connect client** - When selected, users cannot edit the files in the Cloud Connect installation directory and cannot end the process from the Task Manager.

Identification Method

- **Different credentials for each user per device** - When the client connects, different credentials are used for each Windows user.

- **One set of credentials used by all users on a device** - When the client connects, the same credentials are used for all Windows users.

  Note - The client uses the credentials from the first user that connects.

Email Notifications

These settings apply to user registration.

Disable email notification after successful client registration

Usually users get an email after they successfully register to Cloud Services. If you select this option, users will not get an email.

Disable email notification after failed client registration

If a user receives a registration key and does not connect within 5 minutes, a second email, that contains a QR code and link, is sent to the user. If you select this option, users will not get a second email.

Disconnection Durations

Allow users to suspend application

This gives users the option to temporarily stop routing traffic through the cloud. Select one or more periods of time that users can select when they temporarily suspend the application.

Registration Code validation period

Select the time period for which registration codes are valid.

Excluding a Network

If a client sends traffic to one of the networks defined here, the traffic is not sent to the cloud. For example, in a home network consisting of laptop, media center, and printer, traffic sent from the laptop to the printer must not go through Cloud Services.

Make sure to exclude internal DNS servers. If not, clients might not be able to resolve DNS names.

If you exclude a Domain Name, all of the IP addresses that the domain name is resolved to at the time of client connection are excluded and not sent to Cloud Services. This is resolved at the domain name level and not by IP addresses used in the site's content.

Note - Domain Name exclusion is only supported for Windows clients.

These IP address ranges are already defined on the Account Settings tab as internal:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Changes take effect after clients reconnect to the cloud. If you do not reconnect them manually, each client is reconnected by the server within 24 hours from the time the changes are made.

Exclusions apply to all supported devices.

To exclude a network:

1. Click **New**.

   The **New Network Object** window opens.
2. Enter a **Name** for the object. Spaces in the name are permitted.
3. Select the **Type**:
   - **IP** / **Domain Name**
   - **Network**.
4. Enter the **IP Address** (IPv4).
5. Enter the **Subnet mask**.
6. Click **Apply**.

Importing Excluded Networks from a CSV File

If you want to upload a CSV file of the networks that are excluded, you can do that from the **Settings** tab > **Exclude Network**.

1. Click **Import Networks**.

   The **Import Networks from CSV File** window shows.
2. Select **Browse** to import the list of networks.
3. Click **Import**.

To build your list of excluded networks, use the **Example CSV file**. You can access the sample file in the Import Networks from CSV File window.

Below is an example of some entries in a file:

IP/Domain	Subnet	Name
Alegros.com		ExcludeDomain
185.49.108.52	255.255.255.255	ExcludeSpecificIP
101.103.142.151	255.255.255.0	ExcludeNetwork

Notes:

- The list of excluded networks replaces any other previously excluded networks.

- If the CSV file contains duplicate entries, such as the same IP, Range, or FQDN, the file fails to upload.

Cloud Services Central Management

In Central Management mode, users use the Check Point SmartDashboard to manage the Security Policy. Use **Central Management Settings** to enable Central Management and configure these elements in SmartDashboard.

Workflow for Central Management

Step 1: Enable Central Management in Cloud Portal ("Enabling Central Management" on page 58).

Step 2: Create a Cloud Policy gateway Object in SmartDashboard ("Creating a Cloud Policy gateway in SmartDashboard" on page 58).

Step 3: Configure the Cloud Services Security Policies in SmartDashboard ("Configuring Cloud Services Security Policies in SmartDashboard" on page 60).

Step 4: Configure Central Management HTTPS Inspection policy ("Central Management HTTPS Inspection Policy" on page 61).

Enabling Central Management

To enable Central Management, you have to turn the switch in the Cloud Portal to **On**.

1. In the Cloud Portal, **Settings** tab, select **Central Management Settings**.
2. Move the switch to **ON**.

    The status shows that set up is required. Complete the setup instructions that are shown.

Do the configuration that follows in SmartDashboard.

Creating a Cloud Policy gateway in SmartDashboard

To enable the Cloud Policy gateway to communicate with the Security Management Server, you have to create a Cloud Policy gateway object in SmartDashboard. When you install the Security Policy from SmartDashboard on to the Cloud Policy gateway, it is enforced on the Cloud Services Security Gateways.

The Cloud Policy gateway uses SIC authentication to establish trust and communicate with the Security Management Server. The Central Management Settings page contains a link that you

click to generate the password information to enter in SmartDashboard. After you click the link, you have five minutes to enter the information in SmartDashboard. If necessary, you can click the link again to get another password.

If you turn the Central Management switch to OFF after trust is established, you must regenerate a password for SIC and do the SmartDashboard communication steps again for the gateway object (see steps 3 - 4 below).

Note - The steps in the procedure below are also shown in the Central Management Settings page when it is turned **ON**. Make sure the Cloud Portal is open so you can get the IPv4 address and generate a SIC password from this page.

To create a Cloud Policy gateway object:

1. In SmartDashboard, create a new Security Gateway object:

    a) In the Network Objects Tree at the bottom of the screen, right-click **Check Point** > **Check Point** > **Security Gateway/Management**.

    b) Select **Classic Mode**.

2. On the **General Properties** page:

    *   **Name** - Enter the name **Check_point_cloud_security** for the Central Management Security Gateway object.

    *   **IPv4 Address** - Enter the Cloud Services gateway IP address that is shown on the Central Management Settings page.

    *   Click **Communication.**

        The **Trusted Communications** window opens.

3. In Cloud Portal, in **Settings** > **Central Management**, click the **Click here to generate password for SIC** link in step 2.

    A password is shown the page.

4. In SmartDashboard, in the **Trusted Communications** window:

    a) Enter the password from the Central Management Settings page in the **One-time password** and **Confirm one-time password** fields.

    b) Click **Initialize**.

        The status changes from *Waiting for SIC* to *Trust Established* when trust is successfully established.

    c) Click **OK**.

5. Continue configuration on the **General Properties** page:

    *   **Hardware** - Select **Open server**

    *   **Version** - Select **R75.40**

        Check Point supports this version for backward compatibility reasons, to support integration with older Management server releases.

    *   **OS** - Select **Gaia**

6. Select these **Network Security** blades:

    *   F**irewall**

    *   **Identity Awareness** - The Identity Awareness wizard opens.

        ▪ On the **Methods for Acquiring Identity** page, select only **Browser-Based authentication**.

- On the **Integration with Active Directory** page, select **I do not wish to configure an Active Directory at this time**.
        - Click **Next**.
        - Click **Finish**.
    - **Application Control**
    - **URL Filtering**

7. On the Topology page:

    a) Click **Add** to add an interface for the cloud gateway.

    b) Select **eth0** for the interface name.

    c) Set the IP address that is shown on the Central Management Settings page.

    d) Set the netmask to 255.255.255.0.

    e) Select **External**.

    f) Clear **Perform Anti-Spoofing based on interface topology**.

    g) Click **OK**.

8. Click **Save**.

    Make sure a policy is set up for Central Management. See Setting up the Central Management Security Policy ("Central Management Security Policy" on page 19).

9. **Install Policy** on all gateways or on cloud specific gateways.

10. Close SmartDashboard.

    You can see the installed policy in Cloud Portal in **Policy** > **URL Filtering** > **Central Management**. It is read-only and can only be updated in SmartDashboard.

Configuring Cloud Services Security Policies in SmartDashboard

Set up the Cloud Services Security Policy in SmartDashboard on the Cloud Policy gateway in the same way as on a regular Security Gateway. However, because the Cloud Services security services are different than those of a regular gateway, there are some limitations. If the Rule Base for a supported blade contains rules that Central Management does not support, Cloud Services skips the rule and a warnings shows in the **Install Policy** window.

This section contains guidelines for which blades and features can be used in the Check Point Cloud Services security policy rules:

You can configure Cloud Services Security Policies for these blades:

- HTTPS inspection

- Application Control and URL Filtering

Application & URL Filtering has three modes for setting a policy, **Basic**, **Advanced**, and **Central Management**. When you use the **Advanced** policy setting, the policy has these requirements:

- **Source** - Can contain:
    - Access roles that represent user groups.
    - LDAP Groups that are synced with the Active Directory Synchronizer.
    - User Groups that you create in the Cloud Portal and manually add their users.

    Networks, IP addresses or computers are not supported for Cloud Policy gateway rules.

- **Destination** - Must be **Internet**.

- **Application/Sites** - Can include categories, applications, and user-defined URLs. Custom sites can contain multiple URLs. Custom URL groups cannot include nested groups.

- **Action** - Select **Allow**, **Ask** or **Block**. Custom UserCheck pages are supported for the **Ask** and **Block** actions. You can change the tex. You can also change the logo. See Customizing UserCheck Messages ("Customizing UserCheck Messages in SmartDashboard" on page 62).

- **Track** - Select **None** or **Log**.

- **Install On** - Select the Cloud Policy gateway.

  Note - Rules that are not supported by the Cloud Services Policy are automatically ignored on policy installation.

Settings not Supported for Cloud

These functions are not supported for Cloud Services:

- **Time** column.

- The **Negate Cell** operation.

- **Disabled** rules - Due to a temporary limitation, if a rule includes parts that are not supported in the Central Management Security Policy, an error occurs during policy installation. This also occurs if the rule is marked as **Disabled**. To avoid the problem you can do one of these:

  - Remove the Cloud Policy gateway from the **Install On** column of the problematic rule.

  - Delete this rule.

Central Management HTTPS Inspection Policy

Enable HTTPS inspection on the Cloud Policy gateway object to enforce SSL Inspection for traffic to and from roaming users.

To enable HTTPS inspection on the Cloud Policy gateway object:

1. In SmartDashboard, open the Cloud Policy gateway object.
2. In the **Gateway Properties**, select **HTTPS Inspection** from the tree.
3. Follow **Step 1** and **Step 2**.
4. Click **Step 3** to **Enable HTTPS Inspection**.

An inspect rule is created automatically when you set the SSL Inspection feature to **On** in the Cloud Portal. This rule enforces inspection on all HTTPS traffic. Only rules that exclude traffic from HTTPS inspection can go above the default inspect rule.

To exclude sites or users groups from HTTPS inspection, add rules for the traffic to exclude. These rules must be above the default inspect rule in the HTTPS Inspection Rule Base.

Use Case - Excluding Sources from HTTPS Inspection

Promax, a pharmaceutical company, wants their employees to have private access to bank and health care websites. That means that their administrator has to exclude banks and health care sites from HTTPS Inspection.

This table shows an example of exclude rules above the default inspect rule.

Name	Source	Destination	Service	Applications/Sites	Action
Exclude Banks Rule	Any	Internet	HTTPS HTTP and HTTPS proxy	Banking	Bypass
Exclude ABC Insurance Company	Any	Internet	HTTPS HTTP and HTTPS proxy	ABC Insurance Company	Bypass
HTTPS Inspect Rule (default)	Any	Internet	HTTPS HTTP and HTTPS proxy	Any	Inspect

Notes:

- Keep the **Destination** of all rules as **Internet**.

- Do not change the services in the **Services** column

Customizing UserCheck Messages in SmartDashboard

A UserCheck message shows when there is a potential risk of data loss or security violation. When the **Action** of an Application & URL Filtering rule is set to **Block** or **Ask** in SmartDashboard, you can configure a UserCheck message that is shown to users.

- **Ask**

- **Block**

You can customize the content of the UserCheck message and change the logo.

To change a UserCheck message:

1. In the **Application & URL Filtering** > **Policy** Rule Base, right-click in the **Action** column, and configure one of these interaction modes:

   - **Ask**

     Indicates to users that the activity is not allowed based on company policy and asks them to confirm that they want to continue. Users can enter a justification for the activity.

   - **Block**

     Indicates to users that the activity is not allowed based on company policy. There is no option to continue.

2. Select **New UserCheck** or one of the existing UserCheck Interaction objects.

   If you select **New UserCheck**, the **UserCheck Interaction** window opens on the **Message** page.

3. Edit the message.
4. Click **OK.**

Data Center Selection

Cloud Services has servers in many countries that enforce Cloud Services policy on Cloud Connect clients. The Data Center Selection page lets you choose which countries clients in your organization can work with.

This satisfies requirements for some organizations that have restrictions about which countries they can work with.

Select a country to allow connections to it. Clear the checkbox to not allow it. You can only select a country, not individual servers in the country.

Licensing

Cloud Services requires a Cloud Services license from the Check Point User Center http://usercenter.checkpoint.com.

After you get a license, attach your Cloud Services account to your User Center account to activate the license on Cloud Services. If you attach your Cloud Services account to your User Center account and then remove the association, you revert to a Cloud Services trial version. This has a 25 user quota.

To attach a Cloud Services account to a User Center account:

1. Get a Cloud Services license from the Check Point User Center http://usercenter.checkpoint.com.

2. In the Cloud Portal, in the **Settings** tab, click **Licensing**.

3. Click **Associate Account**.

4. In the window that opens, enter the credentials for your User Center account. Click **Continue**.

5. Select a license to use and click **Set Account**.

   A message shows: **User Center account successfully set**.

6. Click **Close**. The license is activated.

Note – If there is a mismatch in the license period (for example: it shows 1 year rather than 3 years) or if the license cannot be activated through the Cloud Portal, contact Check Point support and open a ticket for the licensing team.

To remove a Cloud Services account from a User Center account:

1. In the Cloud Portal, in the **Settings** tab, click **Licensing**.

2. Click **Remove Association**.

Delete Account

You can delete an account if you are not going to use it again, however, that account cannot be reactivated. After it is deleted, you cannot retrieve any of the content and information

Step 6: Location Awareness

Choose if the client connects to Cloud Services when inside the office, and define the settings for **Location Awareness**. The settings detect if roaming clients are in the organizational network or outside of it.

You must define at least one method for location awareness, either **Internal Networks** or **Internal Servers**, even if you want a client to connect to Cloud Services when inside the office. This is used to determine when the client is in the office. A DNS server is configured to use an Internal DNS server when in the office, and a Cloud Services server when out of the office.

If **Internal Networks** and **Internal Servers** are defined, the client checks both options to determine the location. If a client can reach the internal networks or the internal servers, it is considered inside the office.

Select the Cloud Connect behavior when inside the organizational network:

- **Connect to Cloud Services when inside the office**

- **Do not connect to Cloud Services when inside the office**

When the option **Also use information from Endpoint Security** is selected, Endpoint Security information is also used to verify the client's location.

Define methods used to detect the location:

- **Internal Networks** ("Configuring Internal Networks" on page 64) - Define the IP address range of one or more internal networks. If clients have an IP address in a defined range, they do not connect to Cloud Services. This is the default behavior. If you keep this option, make sure to edit the IP range to that of your office network.

- **Internal Servers** ("Configuring Internal Servers" on page 65) - Define the IP address (or domain name) and port of one or more servers in your network, for example, an Active Directory server. If clients can access at least one of the defined servers, they do not connect to Cloud Services.

You must add internal DNS server IP addresses to the excluded networks in the **Settings** > **Exclude Network** page. This makes sure that internal DNS resolving can occur when inside the office.

When **Connect to Cloud Services when inside the office** is selected, the DNS servers used first are those set on the client machine for the user. The Cloud Services external DNS servers are used if the internal DNS servers are not available.

Configuring Internal Networks

Internal Networks

Use this option to define the IP address range of one or more internal networks. If clients have an IP address in a defined range, they do not connect to Cloud Services. This is the default behavior. If you keep this option, make sure to edit the IP range to that of your office network.

To configure internal networks for location awareness:

1. Double-click a profile and the **Edit Settings Profile** page opens.

2. From the menu > **Location Awareness**, click **Internal Networks**.

3. Click **Add a new internal network object**.

4. In the window that opens, select an Internal Network to be your office network or click **Create New Network**.

5. If you select **Create New Network**, enter the details:

    a) For **Type**, select **Single IP** or **Network** for a range of IPs.

    b) Enter the **IP address** and **Subnet mask** (for a range only).

    c) **Object Name** (optional), enter a name that you give the internal server.

    d) Click **Apply**.

    The IP address or range is added to the table.

6. Select the checkboxes next to the entries in the Internal Network table that are considered internal, for location awareness. If you do not want a defined network to be considered internal, clear the checkbox.

7. Click **Select**.

8. In the **Internal Networks** page, click **Apply** or **OK**.

You can use a defined Internal Network object in multiple **Client Setting Profiles**.

Configuring Internal Servers

Internal Servers

Use this option to define the IP address (or domain name) and port of one or more servers in your network, for example, an Active Directory server. If clients can access at least one of the defined servers, they do not connect to Cloud Services.

You must add internal DNS server IP addresses to the excluded networks in the **Settings** > **Exclude Network** page. This makes sure that internal DNS resolving can occur when inside the office.

To configure internal servers for location awareness:

1. Double-click a profile and the **Edit Settings Profile** page opens.

2. From the menu > **Location Awareness**, click **Internal Servers**.

3. Click **Add a new internal server address**.

4. In the window that opens, click **Create New Server**.

5. In the **New Server Address** window, enter the details:

    a) In **IP / Domain Name**, enter the IP address of the server or its domain name.

    b) Enter the **Port** of the server.

    c) **Object Name** (optional) Enter a name that you give the internal server.

    d) Click **Apply**.

    The server is added to the table.

6. Select the checkboxes next to the entries in Internal Servers table that are considered internal for location awareness. If you do not want a defined server to be considered internal, clear the checkbox.

7. Click **Select**.

8. In the **Internal Servers** page, click **Apply** or **OK**.

Step 7: Installing Clients

This section describes client installation.

Client Requirements

Cloud Connect for Windows is supported with these Microsoft Windows Enterprise and Professional releases:

- Windows Vista SP1 or higher

- Windows 7

- Windows 8 and 8.1

- Windows 10 (not compatible with the Device Guard feature)

Cloud Connect for Mac is supported with these Mac OS X releases:

- 10.9

- 10.10

- 10.11

Installing the Windows Cloud Connect

This section describes how to install the Cloud Connect on Windows clients.

Single sign-on (SSO) is available for Active Directory environments and automatically registers Cloud Connect for Windows users when they install the client. For more about the SSO Authenticator, see Configuring the SSO Authenticator ("Using the SSO Authenticator" on page 45).

For the administrator:

1. Log in to the Cloud Portal.
2. Create a new user. Use an email address that the user can access from the Windows device.

    The user receives an email with links to download the Cloud Connect clients and a registration key.

To install the Windows Cloud Connect client:

1. On the device where you will install the Cloud Connect, open an email application that can access the email sent by the administrator.
2. Open the email that has the subject **Your cloud connector registration code**.
3. Click **Download** to download the **Windows version**.
4. Double-click `CheckPointCloudConnector.msi` The installation wizard opens.
5. Click **Next**.
6. Read and accept the terms of the license agreement. Click **Next**.
7. Change the installation folder, or accept the default. Click **Next**.
8. Click **Install**. Wait for the Cloud Connect to install. Click **Next**.
9. Click **Finish**. The registration window opens:
10. Enter the registration code you received by email. Click **OK**.

The client icon shows in Notification Area.

The client connects to the Cloud Services.

Opening the Cloud Connect client:

1. Right click the Cloud Connect icon in the Notification Area.
2. The Right-click menu shows these options:

Option	Description
Disconnect	Disconnects from the Cloud, or prompts you to enter the registration code if you have not yet entered it.
Help	• Lets you collect logs • Opens the help file
Show Client	Opens the Cloud Connect client main window
Show Progress	Shows progress if the client is attempting to connect to the Cloud Services.

For more on client options, open the Cloud Connect help file.

Deploying Cloud Connect for Windows in an Organization

Cloud Connect for Windows can be deployed to your organization's users with deployment tools such as GPO or Symantec.

To deploy Cloud Connect for Windows with a deployment tool:

1. Download the Cloud Connect for Windows application from the **Download** page in the Cloud Portal.
2. Run this on the command line of a Windows computers to install the application silently on user's computers:

    ```
    %SYSTEMROOT%\System32\msiexec.exe /i "<MSI_FILE_PATH>" /qn
    /promptrestart INSTALLDIR="C:\Program Files (x86)\CheckPoint\Cloud
    Connector"
    ```

    Where <MSI_FILE_PATH> is the name of the downloaded file, for example, `CheckPointCloud Connect.msi`.

Installing the Mac Cloud Connect

Users must have administrator privileges to install Cloud Connect on Mac

For the administrator:

1. Log in to the Cloud Portal.
2. Create a new user. Use an email address that the user can access from the Mac device.

    The user receives an email with links to download the Cloud Connect clients and a registration key.

To install the Mac Cloud Connect client:

1. On the device where you will install the Cloud Connect, open an email application that can access the email sent by the administrator.

2. Open the email that has the subject **Your Cloud Connect registration code**.

3. Click **Download** to download the **Mac version**.

4. Double-click `Cloud_Connector.dmg`.

   A Finder window shows the contents of the DMG file

5. Double-click `Cloud_Connector.pkg`.

   The installation wizard opens,

6. On the **Introduction** page, click **Continue**.

7. On the **Installation Type** page, click **Install**.

8. Enter an administrator username and password.

9. Click **Install Software**.

10. Wait while the Cloud Connect installs.

    An installation summary message shows

11. Click **Close**.

    A Check Point Cloud Connect window opens.

12. Enter the registration code from the email you received.

13. Click **OK**.

    The client icon show in the menu bar.

    The client automatically connects to the Cloud Services.

Opening the Cloud Connect client:

1. Right click the Cloud Connect icon in the menu bar.

2. The Right-click menu shows these options:

Option	Description
Disconnect	Disconnects from the Cloud, or prompts you to enter the registration code if you have not yet entered it.
Help	• Lets you collect logs • Opens the help file
Show Client	Opens the Cloud Connect client main window
Show Progress	Shows progress if the client is attempting to connect to the Cloud Services.

For more on client options, open the Cloud Connect help file.

Administrator credentials are required to uninstall Cloud Connect.

To uninstall the Mac Cloud Connect:

1. Run this command from the terminal:

   `/Library/Application\ Support/Checkpoint/Cloud\ Connector/uninstall`

   or go to this folder:

   `/Library/Application Support/Checkpoint/Cloud Connector/uninstall` and double-click the uninstall file.

2. When a message shows: **Do you wish to continue?** enter **yes**.

3. Enter administrator credentials to enable the uninstallation.

Preventing Browser Warnings on Mac

To prevent browser warnings, we recommend that Mac users install the Cloud Services certificate. Network administrators can push this certificate to all of their Mac Cloud Services users. When internet traffic is routed through Cloud Services and the certificate is not installed, users get browser SSL or certificate warnings.

To download the Cloud Services certificate:

1. In the Cloud Portal > **Policy** tab, click **HTTPS Inspection**.

2. Click **Download Certificate**.

3. Distribute the certificate to users.

To add the certificate manually to a Mac computer:

1. Click the certificate file to add it to the Mac keychain. Add it to **Login** or for the whole **System**.

2. Open the keychain app and make sure that **When using this certificate** is set to **Always Trust**.

Logs & Reports

In This Section:

The **Logs and Reports** tab contains:

- **Log Viewer**

- **Audit Logs**

- **Report Scheduling**

Log Viewer

You can use the **Log Viewer** menu to view logs by date range.

Audit Logs

The **Audit logs** page shows logs generated for activities on the Cloud Portal and Cloud Services utilities. When you select a row in the table , the details show in the window at the right.

You can see:

- **Log info**

- **Traffic**

- **General Event Information**

- **More** details

Report Scheduling

On the **Report Scheduling** page, you can configure periodic reports on network activity and threats detected and prevented on your network.

Adding a Report

From the **Type** menu, you can choose:

- **User Activity** - High risk applications, security incidents, and remote access activity

- **Network Security** - Attacks that were not prevented, hosts infected with bots, and allowed high risk applications

- **Application and URL Filtering** - High risk applications and users, and high bandwidth applications and users

- **Threat Prevention** - Top protections, top infected hosts, most common malware, and malicious activity

- **IPS** - Attacks that were prevented, and attack origins

From the **Frequency** menu you can choose:

- **Daily**

- **Weekly**

- **Every 30 Days**

- **Generation Time**

- **Active**
  - Check the checkbox to start generating reports as scheduled
  - Clear the checkbox to save the report settings, but not generate the reports

- **Recipients**
  Email addresses separated by commas.

Deleting a Report

To delete a scheduled report:

1. Select a report from the table on the **Report Scheduling** page, and click **Delete**.
2. Click **Yes** to confirm.

Editing a Report

To edit report settings:

1. Select a report from the table on **Report Scheduling** page, and click **Edit**.
2. In the **Edit Schedule Report** page, edit settings as necessary.
3. Click **Apply**.

Generating a Report On-Demand

To generate a report on-demand:

1. Select a report from the table on the **Report Scheduling** page, and click **Generate Now**.
2. Select the period for which you want to generate the report:
   - **Last 24 hours**
   - **Last 7 days**
   - **Last 30 days**

   The notification window shows the **Info** window with the message that the **Generation request was sent successfully**.
3. Click **OK**.

Querying the Logs

To enter a search query, go to the **Audit Logs** page. To configure the **Query Syntax**, right-click a cell in a row to see the filter options.

Example:

Filter: "Report Dispatcher"

Filter Out: "Report Dispatcher"

- The syntax for searching for that field keyword (for example, time, blade, action, or user) or NOT that keyword is added to the search field.

- You can add other field keywords to the query. The keywords are linked by these Boolean operators:
  - <keyword> AND <keyword>
  - <keyword> AND NOT <keyword>
  - <keyword> OR <keyword>
  - <keyword> OR NOT<keyword>

This is the primary way to add a filter.

Logs can also be manually searched by entering a query in the search field. For example:

- Blade: "URL Filtering"

- Action: Block and user:"john.doe@checkpoint.com"

- dns_udp

- Source:192.168.1.1 or (not Destination:8.8.8.8).

Query Syntax Reference

This section explains syntax query in detail.

Query Language Overview

The portal includes a powerful query language that lets you show only selected records from the log files. Based on your criteria, you can create complex queries by using Boolean operators, wildcards, fields, and ranges. This section is a detailed reference to the query language.

The basic query syntax is `[<Field>:] <Filter Criterion>`.

You can put together many criteria in one query by using Boolean operators:

`[<Field>:] <Filter Criterion> AND|OR|NOT [<Field>:] <Filter Criterion> ...`

Query keywords and filter criteria are not case sensitive.

If your query does not include filter criterion, the query searches all fields in all log records.

Criteria Values

Criteria values are written as one or more text strings. You can enter one text string, such as a word, IP address or URL, without delimiters. Phrases or text strings that contain more than one word must be surrounded by apostrophes or quotation marks.

One character string examples

- John

- inbound

- 192.0.2.1

- mahler.ts.example.com

- dns_udp

Phrase examples

- 'John Doe'

- 'log out'

- 'VPN-1 Embedded Connector'

  Note - You cannot put numbers or IP addresses in quotation marks. For example, 'John 1234' is invalid.

IP Addresses

IPv4 and IPv6 addresses used in queries are one word. You can enter IPv4 address using dotted decimal or CIDR notation. IPv6 addresses are typically entered using CIDR notation.

Examples:

- 20.20.20.1

- 10.0.0.0/24

IP Address Ranges

You can use IP address ranges in free text queries or with the Source and Destination fields. Enter the range criteria using this notation:

<starting IP address>–<ending IP address>

The query shows all IP addresses in the range, and includes the starting and ending addresses.

Example: 192.0.2.0-192.0.2.255

Null Ranges

You can use ranges for numeric values in free text and numeric field queries, such as the port fields.

Syntax

<Number>–<Number>

Examples

- 65000-66000

- port:80-660

Null Values

You can use null (empty) values with field keywords in queries with one of these syntax options:

- *<field>* ""

- *<field>* []

You can also use the Boolean NOT operator to return fields that are not null:

- NOT <*field*> ""

- NOT <*field*> []

Null value queries only work with fields contained in the field keywords table.

Wildcards

You can use the standard wildcard characters (* and ?) in queries, to match variable characters or strings in log records. The wildcard character cannot be the first character in a query criterion. You can use more than one wildcard character in query criteria.

Wildcard syntax

- The **?** (question mark) matches one character

- The ***** (asterisk) matches a character string

Examples:

- Jo* shows John, Jon, Joseph, Joshua, John Paul III and so on.

- Jo? shows Joe and Jon, but not Joseph.

If your criteria value contains more than one word, you can use the wildcard in each word. For example, 'Jo* N*' shows Joe North, John Natt, Joshua Named, and so on.

Using Wildcards with IP Addresses

The wildcard character is useful when used with IPv4 addresses. It is a best practice to put the wildcard character after an IP address delimiter.

Examples:

- 192.0.2.* shows all records for 192.0.2.0 to 192.0.2.255 inclusive

- 192.0.* shows all records for 192.0.0.0 to 192.0.255.255 inclusive

Field Keywords

You can use predefined field names, followed by a colon, as keywords in filter criteria. The Cloud Portal only shows log records that match the criteria in the specified field. If you do not use field names, records that contain the criteria in all fields are shown.

This table shows the predefined field keywords. Some fields also support keyword aliases that you can type as alternatives to the primary keyword.

Keyword	Keyword Aliases	Description
action		Action taken by a security rule
blade	product	Software Blade
destination	dst, dest, to	Traffic destination IP address, DNS name, or Check Point network object name
ipproto	protocol	IP Protocol number
origin		Name of originating Security Gateway

Keyword	Keyword Aliases	Description
port	dport, d_port, dst_port, destination_port	Destination TCP/UDP port
rule		Security rule that generated the log entry
service		Service that generated the log entry
source	src, from	Traffic source IP address, DNS name, or Check Point network object name
source_port	sport, s_port, src_port	Source TCP/UDP port
user		User name

The syntax for a field name query is: *<field name>*`:`*<values>*

- **<field name>** - One of the predefined field names

- **<values>** - One or more filter criteria

When using the **Rule** field as a criterion, you must specify rule number or rule UID together as one string. This is the syntax for this special case:

`rule:`*<rule number or rule UID>*`/`*<policy name>*

Examples:

- `source:192.0.2.1`

- `rule:2/my_policy`

- `action:(drop or reject or block)`

  You can use the OR Boolean operator in parentheses to include multiple criteria values.

Notes:

- When using fields with multiple criteria values, you must explicitly write the Boolean operator. Cloud Portal does not automatically presume the **AND** operator if it is not specified.

- You must use parentheses when using multiple criteria with fields.

Boolean Operators

You can use the Boolean operators **AND**, **OR**, and **NOT** to create filters with many different criteria. You can put multiple Boolean expressions in parentheses.

If you enter more than one criteria without a Boolean operator, the **AND** operator is implied. When using multiple criteria without parentheses, the **OR** operator is applied before the **AND** operator.

Examples:

- `blade:"application control" AND action:block` - Shows log records from the Application & URL Filtering Software Blade where traffic was blocked.

- `192.0.2.133 10.19.136.101` - Includes log entries that match the two IP addresses. The **AND** operator is presumed.

- `192.0.2.133 OR 10.19.136.101` - Includes log entries the match one of the IP addresses.

- `(blade:Firewall or blade:IPS or blade:VPN) AND NOT action:drop` - Includes all log entries from the Firewall, IPS or VPN blades that are not dropped. The criteria in the parentheses are applied before the `AND NOT` criterion.

- `Source:(192.0.2.1 OR 192.0.2.2) AND destination:17.168.8.2` - Includes log entries from the two source IP addresses if the destination IP address is `17.168.8.2`. This example also shows how you can use Boolean operators with field criteria.

Note - Boolean operators are not case sensitive.

Date and Time Ranges

You can define a query that shows logs generated during the preceding period of time using the **last** or **past** keywords. The applicable periods of time are:

- minute
- hour
- day
- week
- month
- year

The syntax for this criterion is:

`last|past [<`*number*`>] <`*period of time*`>`

You can specify the period of time in the singular or the plural. If you do not enter a number, the value is presumed to be the most recent period.

Examples

- `last 12 hours` - Shows logs generated during the last 12 hours.
- `past 10 week` - Shows logs generated during the last 10 weeks. Using the singular is permitted.
- `last year` - Shows logs generated during the last year.

Preceding Time Period Queries

You can define a query that shows logs generated during the preceding period of time using the **last** or **past** keyword.

Preceding period of time queries show log records based on the time that you run the query. For example, if your criterion is `'last 2 weeks'` at 3:15 PM, the Cloud Portal shows all logs starting from 3:15 on the 14th day before today. A log generated at 1:15 PM on the 14th day does not show, but one generated at 6:50 PM does show.

The valid periods of time are:

- minute
- hour
- day
- week
- month
- year

The syntax is:

`last|past [<`*number*`>] <`*period of time*`>`

Examples

- `last 12 hours` - Shows logs generated during the last 12 hours before the most recent time.

- `past 10 week` - Shows logs generated during the last 10 weeks before the most recent date and time. This example shows that you can use the singular or plural interchangeably.

- `last year` - Shows logs generated during the last 365 days starting from the most recent date and time. This example shows that the number one is assumed if no number value is entered.

Notes:

- You can specify the period of time in the singular or the plural.

- If you do not enter a <number> value, the number one is assumed.

From-To-Queries

You can define queries that show log records between a starting date and time and an ending date and time. Cloud Portal shows records between and including the specified dates.

Syntax

`dd/mmm/yyyy hh:mm:ss[-dd/mmm/yyyy hh:mm:ss]`

- dd - Day of the month. The leading 0 is optional.

- mmm - Three character mnemonic for the month. This value is case insensitive.

- yyyy - Year (four digits are required).

- hh - Hour in 24 hour time notation. The leading 0 is optional.

- mm - Minutes. The leading 0 is optional.

- ss - Seconds. The leading 0 is optional.

Syntax Notes

- You can use the `yesterday` and `today` keywords as alternatives to the date parameter. You can use these with or without time values.

- The 'to' value is optional. If not specified, Cloud Portal shows all values on the specified 'from' value.

- The time value is optional. If no time is specified, Cloud Portal shows all records from 00:00 to 23:59 on the specified date.

- If you specify a time value, you must specify the hours and minutes. You can ignore the second values.

- The day and year values are optional. If you do not specify these values the most recent day and/or year is assumed.

- You can ignore the date value. Today is assumed.

- You must always specify the month value.

- You cannot use wildcards with dates and times.

Examples

- `1/mar/2012-5/mar/2012` - Shows all logs on and between these dates.

- `5/mar/2012` - Shows all logs for 5 March only.

- `yesterday-today` - Shows all logs from 00:00 yesterday to 23:59 today.

- `5/mar/2012 07:00-08:59` - Shows all logs from 7:00 on 5 March to 8:59 today. This example illustrates the fact that you can ignore the date value. Today is assumed.

Collecting Logs on Cloud Connect Clients

Collecting Logs on Windows

To collect logs in Windows Cloud Connect:

1. Right-click the Cloud Connect icon.
2. Select **Help** > **Collect Logs**.

   Logs are sent to a folder in a compressed file. A window opens to show the file:

   `%APPDATA%\Check Point Cloud Connector\trlogs_<`*DATE_TIME*`>.cab`

Collecting Logs on Mac

To collect logs in Mac Cloud Connect:

1. Click the Cloud Connect icon in the menu bar.
2. Select **Help** > **Collect Logs**.

   Logs are sent to a folder in a compressed file. A Finder window opens to show the file.

Threat Report Settings

On the **Report Settings** page, you can select when to notify administrators and users on detected threats:

- **Notify Admin on threats** - **Daily**, **Weekly**, or **Immediately**

- **Notify User on threats** - **Immediately**

API

In This Section:

The API of Check Point Cloud Services lets you manage your organization's use of the Cloud Services. Each command is a web service request.

Users account must have admin permissions before they can use Cloud Services web service API. Go to the **Users & Groups** tab and click the **Is Admin** option.

Request Format

You can send the requests in XML or json. You can get the response in the same format or the other format.

⚠️ **Important** - In Cloud Services version 1.2 and higher, you must use the POST method for command requests. GET is not supported.

This is the basic syntax of a Check Point Cloud Services web service request.

json:

```
curl -d
'json={"command":"<command>","LoginData":{"email":"<email>","password":"<password>","api
Key":"<key>"},"params":{"<param>":"<value>",.."<param_n>":"<value>"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

xml:

```
curl -d
'xml=<fwcloud><command>cmd</command><params><param1>param_value</param1></para
ms><LoginData><email>email</email><password>password</password><apiKey>key</apiKey><
/LoginData></fwcloud>' 'https://cloud.checkpoint.com/cp-cloud-api.php?format=xml'
```

Parameter	Description
format	Optional. The output format of the command. Valid values: `json` (default) or `xml`

Parameter	Description
command	Command name. (See the next sections.)
LoginData	Your login credentials. The email is required with LoginData. You can use the password or the API Key, or both.
	The first time you register with the cloud, send the command with your email and password only. (You do not have the API Key yet). The return value of the command will have the key. It is valid for one hour. After the first time, use the API Key and the password. If the key expires, you are registered automatically and get a new key in the response.
key	API Key. Valid for one hour. Example: `"apiKey":"JL1H-K58M-KR1R-L2HE-ACHC-639T-3HB8-NBGZ"`
param and value	Add parameters and values according to each command syntax.

Example request and response in json format:

```
curl -d 'json={"command":"REGISTER","LoginData":{"email":"
lsmith@mycomp.com","password":"123456"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'

{
    "api_key": "ANUZ-ZZPF-UABK-9Q7V-KIL8-N3LT-1NKP-SL51",
    "error_code": 200,
    "error_description": "ok"
}
```

Example request and response in xml format:

```
curl- -d 'xml=<fwcloud><command>REGISTER</command><LoginData><email>
lsmith@mycomp.com </email><password>123456</password></LoginData></fwcloud>'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=xml'

<?xml version="1.0"?>
<response>
    <api_key>58Q6-5AEY-342F-FQ65-LB6S-TRTP-U645-BGFM</api_key>
    <error_code>200</error_code>
    <error_description>success api key sent</error_description>
</response>
```

Response Format

When you send a request with the API, you get a response with sections of data.

Error Code and Error Description

Check Point Cloud Services API uses a set of error/status codes from the HTTP 1.1 codes
http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html.

Code	Status / Error Type
200	ok

Code	Status / Error Type
400	Error in request syntax
401	Client request is unauthorized
503	Server is unavailable for maintenance or during heavy load

Example in Response - xml:

```
<errorCode>200</errorCode>
<errorDescription>ok</errorDescription>
```

Example in Response - json:

```
"errorCode": 503,
"errorDescription": "Problem occurred while trying to connect to DB server"
```

API Key

If the request includes the password and does not include a valid API Key, a new key is generated.

Example in Response - xml:

```
<apiKey>65C5-LZH2-YG1U-5S66-MLGG-XCRH-UD8J-S15F</apiKey>
```

Example in Response - json:

```
"apiKey": "65C5-LZH2-YG1U-5S66-MLGG-XCRH-UD8J-S15F",
```

Data

The data in the response is according to the command. Some responses are simple. The response data is in one tag or one line. Some are complex, when the response data is a list. Complex data is structured in rows, showing the same data in each row with different values, according to the command. A row starts with rowID_*index* - where i*ndex* is the row number, starting from **1**. The total number of rows is given at the end.

Example of complex data syntax - json:

```
 "data": {
  "results": {
   "rowID_1": {
    "<datum>": "<value>",
    "<datum>": "<value>",
   },
  },
   "total": 1
 }
```

Example of complex data syntax - xml:

```
<data>
  <results>
   <rowID_1>
    <datum><value><datum>
    <datum><value><datum>
   </rowID_1>
  </results>
  <total>1</total>
</data>
```

Example of Cloud Services API in Script

This is an example of the `register` and `getUsersList` commands, in json format, in a PHP script.

```php
function register()
{
  $request=array();

  // set the login param
  $request["LoginData"]= array("email" => "lsmith@mycomp.com","password" =>
"123456");

  // set the command name
  $request["command"]="register";

  //build the url
  $url="https://cloud.checkpoint.com/cp-cloud-api.php?json=
".json_encode($request);

  //use curl to connect to the web service
  $ch = curl_init();
  curl_setopt($ch, CURLOPT_URL,$url);

  //set this to true so we can get the response
  curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);

  // execute the query
  $result=curl_exec ($ch);

  $jsonArr=json_decode($result);
  curl_close ($ch);
}


function getUserList($apiKey)
{
  $arr=array();

  // set the login param
  $request["LoginData"]= array("email" => "lsmith@mycomp.com","password" =>
"123456");

  // set the command name
  $request["command"]="getUserList";

  //build the url
  $url="https://cloud.mc.com/cp-cloud-api.php?json=".json_encode($request);

  $ch = curl_init();
  curl_setopt($ch, CURLOPT_URL,$url);

  //set this to true so we can recive the response
  curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);

  // execute the query
  $result=curl_exec ($ch);


  $jsonArr=json_decode($result);
  curl_close ($ch);

}
```

Typical Response in json:

response to register:

```
{
  "apiKey": "QF6R-QHZN-7N7X-G7BT-U7DW-UA18-14NI-B6F8",
  "errorCode": 200,
  "errorDescription": "ok"
}
```

response to getUserList:

```
{
  "errorCode":200,
  "errorDescription":"ok",
  "data":
  {
    "results":
    {
      "rowID_1":{"userID":"37","userName":"a","userEmail":"a@ex.com","userComme
nts":null},
      "rowID_2":{"userID":"191","userName":"b","userEmail":"b@ex.com",
"userComments":null},
      "rowID_3":{"userID":"193","userName":"c","userEmail":"c@ex.com",
"userComments":null},
      …
      "rowID_11":{"userID":"201","userName":"x@ex.com","userEmail":
"x@ex.com","userComments":null}
    },
    "total":11
  }
}
```

Typical Response in xml:

response to register:

```
<apiKey>QF6R-QHZN-7N7X-G7BT-U7DW-UA18-14NI-B6F8</apiKey>
<errorCode>200</errorCode>
<errorDescription>ok</errorDescription>
```

response to getUserList:

```
<?xml version="1.0"?>
<response>
  <errorCode>200</errorCode>
  <errorDescription>ok</errorDescription>
  <data>
    <results>
      <rowID_1>
        <userID>37</userID>
        <userName>a</userName>
        <userEmail>a@ex.com</userEmail>
        <userComments></userComments>
      </rowID_1>
      <rowID_2>
        <userID>191</userID>
        <userName>b</userName>
        <userEmail>b@ex.com</userEmail>
        <userComments></userComments>
      </rowID_2>
      <rowID_3>
        <userID>193</userID>
        <userName>c</userName>
        <userEmail>c@ex.com</userEmail>
```

```
         <userComments></userComments>
      </rowID_3>
...
      <rowID_11>
         <userID>201</userID>
         <userName>x</userName>
         <userEmail>x@ex.com</userEmail>
         <userComments></userComments>
      </rowID_11>
    </results>
    <total>11</total>
  </data>
</response>
```

register

Use this command to register with Check Point Cloud Services the first time.

Request Parameters

Parameter	Description
email	Required to register. Email of the web service user.
password	Required to register. Password of the web service user.

Response Data

Parameter	Description
apiKey	The key to run the web services.

Request Example

```
curl -d
'json={"command":"register","LoginData":{"email":"lsmith@mycomp.com","password
":"123456"}}' 'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "apiKey": "QF6R-QHZN-7N7X-G7BT-U7DW-UA18-14NI-B6F8",
  "errorCode": 200,
  "errorDescription": "ok"
}
```

Managing Users and User Groups

In This Section:

createUser

Make user names, one for each user. A user can log in to the Cloud Services from multiple devices.

Request Parameters

Parameter	Description
userName	Name. Required, but can be an email or other text.
userEmail	Email address. Required.
userComments	Optional text.
sendRegistrationEmail	If true, the user gets an email with the registration code or password to connect to the Cloud Services. If not given (default is false), no email is sent automatically. Give the OTP to the user as you choose.

Response Data

Parameter	Description
OTP	One-Time Password. Send this to the user for their first login, to use in the time of validity.
userID	ID of the user. Use this for more API actions.

Request Example

```
curl -d
'json={"command":"createUser","params":{"userName":"LindaSmith","userEmail":"l
smith@mycomp.com","sendRegistrationEmail":"true"},"LoginData":{"email":"admin@
mycomp.com","password":"654321","apiKey":"JL1H-K58M-KR1R-L2HE-ACHC-639T-3HB8-N
BGZ"}}' 'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
createUser ={
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "otp": "EZP1-J9I8-XJ41-A3KI",
    "userID": "000001"
  }
}
```

createGroup

You can create user groups. The default group is **All Users**. By default, each Cloud Services account has one **All Users** group. You cannot delete this group, directly add users to this group, or remove users from this group. You can use this group in the Check Point Rule Base as a regular group.

Request Parameters

Parameter	Description
groupName	Name of the new group. Required.
groupComments	Optional text.

Response Data

Parameter	Description
groupID	ID of the group.

Request Example

```
curl -d
'json={"command":"createGroup","params":{"groupName":"temps","groupDescription
":"temporary
employees"},"LoginData":{"email":"admin@mycomp.com","password":"654321","apiKe
y":"JL1H-K58M-KR1R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "groupID": "300001"
  }
}
```

createUserOtp

Use this command to make a One-Time Password for an existing user. Usually, you use this command if the last OTP expired or the user wants to register a new device.

Request Parameters

Parameter	Description
userEmail	Email of user.

Response Data

Parameter	Description
OTP	One-Time Password. Send this to the user.

Request Example

```
curl -d
'json={"command":"createUserOtp","params":{"userEmail":"rjones@mycomp.com"},"L
oginData":{"email":"lsmith@mycomp.com","password":"654321","apiKey":"JL1H-K58M
-KR1R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "otp": "EZP1-J9I8-XJ41-A3KI"
  }
}
```

getUserOtp

Use this command to get the OTP again for a user who needs the string again, while it is still valid.

Request Parameters

Parameter	Description
userEmail	Email of user ("getUserInfo" on page 88).

Response Data

Parameter	Description
OTP	One-Time Password. Send this to the user.

Request Example

```
curl -d
'json={"command":"getUserOtp","params":{"userEmail":"rjones@mycomp.com"},"Logi
nData":{"email":"lsmith@mycomp.com","password":"654321","apiKey":"JL1H-K58M-KR
1R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "OTP": "EZP1-J9I8-XJ41-A3KI"
}
```

getUserID

Use this command to get the userID value, to reference the user in other API functions.

Request Parameters

Parameter	Description
userEmail	Email of the user for whom you want the ID.

Response Data

Parameter	Description
userID	Check Point Cloud Services ID of the user

Request Example

```
curl -d
'json={"command":"getUserID","params":{"userEmail":"rjones@mycomp.com"},"Login
Data":{"email":"lsmith@mycomp.com","password":"654321","apiKey":"JL1H-K58M-KR1
R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "UserID": "37000016"
}
```

getUserInfo

Use this command to get the user name and email when you have the userID.

Request Parameters

Parameter	Description
userID	ID of the user ("getUserID" on page 88).

Response Data

Parameter	Description
userID	ID of the user
userName	Name of the user

userEmail	Email address
userDescription	Your comments about the user, or `"null"`

Request Example

```
curl -d
'json={"command":"getUserInfo","params":{"userID":"37000016"},"LoginData":{"em
ail":"lsmith@mycomp.com","password":"654321","apiKey":"JL1H-K58M-KR1R-L2HE-ACH
C-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "userID": "37000016",
  "userName": "rjones@mycomp.com",
  "userEmail": "rjones@mycomp.com",
  "userDescription": null
}
```

addUserToGroup

After you create users and groups, you can add users to the groups.

Request Parameters

Parameter	Description
groupID	ID of the group ("getGroupIDByName" on page 89).
userID	ID of the user to add to the group ("getUserID" on page 88).

Response Data

None.

Request Example

```
curl -d
'json={"command":"addUserToGroup","params":{"groupID":37000007,"userID":191000
030},"LoginData":{"email":"lsmith@mycomp.com","assword":"654321","apiKey":"JL1
H-K58M-KR1R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "data": null
}
```

getGroupIDByName

Use this command to get the groupID value, to reference the group in other API functions.

Request Parameters

Parameter	Description
groupName	Name of the group for which you want the ID.

Response data

Parameter	Description
groupID	Check Point Cloud Services ID of the group.

Request Example

```
curl -d
'json={"command":"getGroupIDByName","params":{"groupName":"All%20Users"},"Logi
nData":{"email":"lsmith@mycomp.com","password":"654321","apiKey":"JL1H-K58M-KR
1R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
    u'errorCode': 200,
    u'errorDescription': u'ok',
    u'data': {
            u'groupID': u'164004088'
    }
}
```

getGroupInfo

Use this command to get the unique names, display name, and comments of a group.

Request Parameters

Parameter	Description
groupID	ID of the group ("getGroupIDByName" on page 89).

Response Data

Parameter	Description
groupID	ID of the group, for each group in your Cloud Services environment.
groupDisplayName	Name of the group in the WebUI.
comments	Your comments about the group, or `"null"`.
groupName	Unique name of the group, in the database.

Request Example

```
curl -d
'json={"command":"getGroupInfo","params":{"groupID":197000017},"LoginData":{"e
mail":"lsmith@mycomp.com","password":"654321","apiKey":"JL1H-K58M-KR1R-L2HE-AC
HC-639T-3HB8-NBGZ"}}'
```

```
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "groupID": "37000007",
  "groupDisplayName": "All Users",
  "comments": "All users in this account",
  "groupName": "GRP-9b834857-8b8b-af4a-49d4-98c22924bf51"
}
```

getUserList

Use this command to get the IDs, names, and emails of all users.

Request Parameters

None

Response Data

Parameter	Description
userID	ID of the user ("getUserID" on page 88), for each user in your Cloud Services environment.
userName	Name of the user.
userEmail	Email address of the user.
userComments	Your comments about the user, or `"null"`.

Request Example

```
curl -d
'json={"command":"getUserList","LoginData":{"email":"lsmith@mycomp.com","passw
ord":"654321","apiKey":"JL1H-K58M-KR1R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "results": {
      "rowID_1": {
"userID": "37000016",
"userName": "lsmith@mycomp.com",
"userEmail": "lsmith@mycomp.com",
"userComments": null
      },
      "rowID_2": {
"userID": "191000043",
"userName": "rjones@mycomp.com",
"userEmail": "rjones@mycomp.com",
"userComments": null
      },
```

```
...
  }

      "total": 90
    }

}
```

getUserGroupsList

Use this command to get the data of the groups to which a given user belongs.

Request Parameters

Parameter	Description
userID	ID of the user to add to the group ("getUserID" on page 88).

Response Data

Parameter	Description
groupID	ID of the group, for each group of the user.
groupDisplayName	Name of the group to see in the WebUI of the Cloud Services.
comments	Your comments about the group, or `"null"`.
groupName	Unique name of the group.

Request Example

```
curl -d
'json={"command":"getUserGroupsList","param":{"userID":000001}"LoginData":{"em
ail":"lsmith@mycomp.com","password":"654321","apiKey":"JL1H-K58M-KR1R-L2HE-ACH
C-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "results": {
    "rowID_1": {
      "groupID": "37000007",
      "groupDisplayName": "All Users",
      "comments": "All users in this account",
      "groupName": "GRP-9b834857-8b8b-af4a-49d4-98c22924bf51"
    },
    "rowID_2": {
      "groupID": "37000010",
      "groupDisplayName": "Temps",
      "comments": "Temporary employees",
      "groupName": "GRP-9b834816-8b7a-af3a-d494-98c229240000"
    }
  },
```

```
      "total": 2
   }
}
```

getGroupsList

Use this command to get the IDs, names, and data of all groups.

Request Parameters

None

Response Data

Parameter	Description
groupID	ID of the group, for each group in your Cloud Services environment.
groupDisplayName	Name of the group in the WebUI.
comments	Your comments about the group, or `"null"`.
groupName	Unique name of the group, in the database.

Request Example

```
curl -d
'json={"command":"getGroupsList","LoginData":{"email":"lsmith@mycomp.com","pas
sword":"654321","apiKey":"JL1H-K58M-KR1R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  u'errorCode': 200,
  u'errorDescription': u'ok',
  u'data': {
          u'total': 3,
          u'results': {
          u'rowID_1': {
                      u'groupDisplayName': u'grp_admin_syNfMqhrwTbtbsvb',
                      u'groupID': u'164004089',
                      u'comments': u'Group for admin users',
                      u'value_3': u'GRP-dc705d71-3e6e-3169-b827-d75c98e6525d'
                                   }
```

removeUserFromGroup

Use this command to remove a user from a group. The user account still exists. You cannot remove a user from the **All Users** group. You cannot remove your own user account.

Request Parameters

Parameter	Description
userID	ID of the user to remove from the group ("getUserID" on page 88).

groupID	ID of the group ("getGroupIDByName" on page 89).

Response Data

None.

Request Example

```
curl -d
'json={"command":"removeUserFromGroup","params":{"userID":"00654","groupID":"1
0056"},"LoginData":{"email":"lsmith@mycomp.com","password":"654321","apiKey":"
JL1H-K58M-KR1R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
removeUserFromGroup ={
  "errorCode": 200,
  "errorDescription": "ok",
  "data": null
}
```

deleteUser

If you delete a user name, all its data are permanently deleted. The user will not be able to connect to the cloud.

Request Parameters

Parameter	Description
userID	ID of the user to delete ("getUserID" on page 88).

Response Data

None

Request Example

```
curl -d
'json={"command":"deleteUser","params":{"userID":191000030},"LoginData":{"emai
l":"lsmith@mycomp.com","password":"123456"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
deleteUser ={
  "errorCode": 200,
  "errorDescription": "ok",
  "data": null
}
```

Managing URL Filtering

In This Section:

addBasicPolicyAllowedCategory

Use this command to set categories to Allow.

Request Parameters

Parameter	Description
categoryID	ID of the category ("getBasicPolicyCategories" on page 100).

Response Data

None

Request Example

```
curl -d
'json={"command":"addBasicPolicyAllowedCategory","LoginData":{"email":"lsmith@
mycomp.com","password":"123456"},"params":{"categoryID":52000137}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
addBasicPolicyAllowedCategory ={
```

```
    "apiKey": "CSR1-AVD5-1B2H-VCXL-V68B-34NM-J2BP-26NT",
    "errorCode": 200,
    "errorDescription": "ok",
    "data": null
}
```

addBasicPolicyBlockedCategory

Use this command to set categories to Block.

Request Parameters

Parameter	Description
categoryID	ID of the category ("getBasicPolicyCategories" on page 100).

Response Data

None

Request Example

```
curl -d
'json={"command":"addBasicPolicyBlockedCategory","LoginData":{"email":"lsmith@
mycomp.com","password":"123456"},"params":{"categoryID":52000137}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{"apiKey":<apiKey>,"errorCode":200,"errorDescription":"ok","data":null}
```

addBasicPolicyAllowedCustom

Use this command to set custom URLs to Allow.

Request Parameters

Parameter	Description
customSiteID	ID of the custom site ("policyGetCustomSiteList" on page 106).

Response Data

None

Request Example

```
curl -d
'json={"command":"addBasicPolicyAllowedCustom","LoginData":{"email":"lsmith@my
comp.com","password":"123456"},"params":{"customSiteID":191000037}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
addBasicPolicyAllowedCustom ={
    "apiKey": "SRRV-UQ1B-174E-JYAH-EHGC-I14T-4AAW-7FX3",
    "errorCode": 200,
    "errorDescription": "ok",
    "data": null
```

```
}
```

addBasicPolicyBlockedCustom

Use this command to set custom URLs to Block.

Request Parameters

Parameter	Description
customSiteID	ID of the custom site ("policyGetCustomSiteList" on page 106).

Response Data

None

Request Example

```
curl -d
'json={"command":"addBasicPolicyBlockedCustom","LoginData":{"email":"lsmith@my
comp.com","password":"123456"},"params":{"customSiteID":191000037}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
addBasicPolicyBlockedCustom ={
   "apiKey": "SRRV-UQ1B-174E-JYAH-EHGC-I14T-4AAW-7FX3",
   "errorCode": 200,
   "errorDescription": "ok",
   "data": null
}
```

getBasicPolicyAllowedItems

Use this command to get data on applications that the Firewall allows.

Request Parameters

None

Response Data

Parameter	Description
categories	ID and name of policy category that allows traffic, application, or URL.
applications	If the allowed item was a known application: the ID, name, and description of the blocked application.
customApplications	If the allowed item was a custom application: the ID, name, and description of the blocked applications.

Request Example

```
curl -d
'json={"command":"getBasicPolicyAllowedItems","LoginData":{"email":"lsmith@myc
omp.com","password":"123456"},"params":[]}'
```

```
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
getBasicPolicyAllowedItems ={
  "apiKey": "VIYG-NQLC-BX8K-ZQ9N-J9EN-WLUK-4G2X-M4LR",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "categories": [
      [
"52000137",
"Web Desktop"
      ]
    ],
    "applications": [
      [
      "52000137",
      "Web Desktop",
      "[CATEGORY]Also referred to as a WebTop. This is a desktop environment that
is ran within a web browser. These environments integrate web applications,
services, application servers, and applications on the local client into a desktop
environment using a simulated desktop resembling Windows, Mac, or Unix systems.
In a web desktop most of the computing happens remotely."
      ]
    ],
    "customApplications": [
      [
      "191000037",
      "www.test.com",
      "0"
      ]
    ]
  }
}
```

getBasicPolicyBlockedItems

Use this command to get data on applications that the Firewall blocks.

Request Parameters

None

Response Data

Parameter	Description
categories	ID and name of policy category that blocked traffic, application, or URL.
applications	If the blocked item was a known application: the ID, name, and description of the blocked application.
customApplications	If the blocked item was a custom application: the ID, name, and description of the blocked applications.

Request Example

```
curl -d
```

```
'json={"command":"getBasicPolicyBlockedItems","LoginData":{"email":"lsmith@myc
omp.com","password":"123456"},"params":[]}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
getBasicPolicyBlockedItems ={
  "apiKey": "9UTF-8AFD-1VL3-7NDT-YIWI-F73N-ZWHP-9ZA7",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "categories": [
      [
      "52000137",
      "Web Desktop"
      ]
    ],
    "applications": [
      [
      "52000137",
      "Web Desktop",
      "[CATEGORY]Also referred to as a WebTop. This is a desktop environment that
is ran within a web browser. These environments integrate web applications,
services, application servers, and applications on the local client into a desktop
environment using a simulated desktop resembling Windows, Mac, or Unix systems.
In a web desktop most of the computing happens remotely."
      ]
    ],
    "customApplications": [
      [
      "191000037",
      "www.test.com",
      "0"
      ]
    ]
  }
}
```

removeBasicPolicyAllowedCategories

Use this command to delete allowed categories of Applications from the Firewall.

Request Parameters

Parameter	Description
categoryID	ID of the category to remove ("getBasicPolicyBlockedItems" on page 98).

Response Data

None

Request Example

```
curl -d
'json={"command":"removeBasicPolicyAllowedCategories","LoginData":{"email":"ls
mith@mycomp.com","password":"123456"},"params":{"categoryID":52000137}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
removeBasicPolicyAllowedCategories ={
  "apiKey": "RNK4-5FZI-2PI2-YTZI-5SS6-T5CE-SLT1-IHPW",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": null
}
```

removeBasicPolicyBlockedCategories

Use this command to delete blocked categories of Applications from URL Filtering.

Request Parameters

Parameter	Description
categoryID	ID of the category to remove ("getBasicPolicyBlockedItems" on page 98).

Response Data

None

Request Example

```
curl -d
'json={"command":"removeBasicPolicyBlockedCategories","LoginData":{"email":"ls
mith@mycomp.com","password":"123456"},"params":{"categoryID":52000137}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
removeBasicPolicyBlockedCategories ={
  "apiKey": "RNK4-5FZI-2PI2-YTZI-5SS6-T5CE-SLT1-IHPW",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": null
}
```

getBasicPolicyCategories

Use this command to get data on the categories of URL Filtering.

Request Parameters

None

Response Data

Parameter	Description
category name	Name of the category
boolean	If `true`, the category is enabled.

Request Example

```
curl -d
'json={"command":"getBasicPolicyCategories","LoginData":{"email":"lsmith@mycom
p.com","password":"123456"},"params":[]}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
getBasicPolicyCategories ={
   "apiKey": "ZSW2-P6ER-34C9-SC62-9CXK-JPSR-U4W3-YITK",
   "errorCode": 200,
   "errorDescription": "ok",
   "data": {
      "SecurityRisks": false,
      "FileSharing": false,
      "Inappropriate": false
   }
}
```

removeBasicPolicyAllowedCustom

Use this command to delete custom categories that are allowed.

Request Parameters

Parameter	Description
customSiteID	ID of custom site ("policyGetCustomSiteList" on page 106)

Response Data

None

Request Example

```
curl -d
'json={"command":"removeBasicPolicyAllowedCustom","LoginData":{"email":"lsmith
@mycomp.com","password":"123456"},"params":{"customSiteID":52000137}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
removeBasicPolicyAllowedCustom={
   "apiKey": "RNK4-5FZI-2PI2-YTZI-5SS6-T5CE-SLT1-IHPW",
   "errorCode": 200,
   "errorDescription": "ok",
   "data": null
}
```

removeBasicPolicyBlockedCustom

Use this command to delete custom categories that are blocked.

Request Parameters

Parameter	Description
customSiteID	ID of custom site ("policyGetCustomSiteList" on page 106)

Response Data

None

Request Example

```
curl -d
'json={"command":"removeBasicPolicyBlockedCustom","LoginData":{"email":"lsmith
@mycomp.com","password":"123456"},"params":{"customSiteID":52000137}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
removeBasicPolicyBlockedCustom={
   "apiKey": "RNK4-5FZI-2PI2-YTZI-5SS6-T5CE-SLT1-IHPW",
   "errorCode": 200,
   "errorDescription": "ok",
   "data": null
}
```

advancedPolicyAddEditRule

Use this command to add or change a rule in the URL Filtering policy.

Request Parameters

Parameter	Description
ruleID	ID of the rule in the policy ("advancedPolicyGetRuleBase" on page 104). To make a new rule, this value is `null`.
groups	ID of group ("getGroupIDByName" on page 89) or groups on which to enforce this rule. To empty the list, make the value empty square brackets [] .
userIDs	ID of users ("getUserID" on page 88) on which to enforce this rule. To empty the user list, make the value empty square brackets [].
applications	ID of applications ("policyGetApplicationList" on page 107) to make an Application Control rule.
categories	ID of categories ("policyGetCategoryList" on page 108) to make an Application Control rule.
action	Action of the rule. Valid values: ACCEPT, BLOCK, ASK.
customSites	ID of custom sites ("policyGetCustomSiteList" on page 106) to make a URL Filtering rule based on your own URLs (optional).
log	If `true`, events of this rule will be logged.
comment	Optional description of the rule.

Notes -

- If you do not include entries for `groups`, `userIDs`, `applications`, `categories`, or `customSites` no changes are made to that part of the rule. If values were already included in that part of the rule, they do not change.

- To make sure that no values are included in part of a rule, include the parameter with the empty square brackets [].

- To make a rule apply to all users, the value for all of these parameters must be empty square brackets: `groups` and `userIDs`.

Response Data

None

Request Example

```
curl -d
'json={"command":"advancedPolicyAddEditRule","LoginData":{"email":"lsmith@myco
mp.com","password":"123456"},"params":{"ruleID":null,groups":[10002623,1000255
6],
userIds:[10003587],"applications":[10002087,10002092],"action":"BLOCK","custom
Sites":[],"log":"true",comment:"Interesting_comment"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
advancedPolicyAddEditRule ={
   "apiKey": "P8TE-PIKQ-GSPR-FVNJ-W5W5-X27I-GBA4-TN2F",
   "errorCode": 200,
   "errorDescription": "ok",
   "data": null
}
```

advancedPolicyDeleteRule

Use this command to remove a rule from the firewall policy.

Request Parameters

Parameter	Description
ruleID	ID of the rule to delete ("advancedPolicyGetRuleBase" on page 104).

Response Data

None

Request Example

```
curl -d
'json={"command":"advancedPolicyDeleteRule","LoginData":{"email":"lsmith@mycom
p.com","password":"123456"},"params":{"ruleID":191000268}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
advancedPolicyDeleteRule ={
        "apiKey": "HHXM-ME5Y-L4HX-8LXL-13IV-DSFY-RY15-67H2",
        "errorCode": 200,
```

```
        "errorDescription": "ok",
        "data": null
}
```

advancedPolicyGetRuleBase

Use this command to get data on the rules of the policy.

Request Parameters

None

Response Data

Parameter	Description
ruleID	ID of the rule in the policy.
ruleBaseOrder	Order of the rule in the policy.
action	Action of the rule: ACCEPT, BLOCK, or ASK.
comments	Optional description of the rule.
isLog	Whether a log is created when the rule is enforced.
categories	If the rule is for Application Control, these are the application categories of the rule.
customSites	If the rule is for URL Filtering, these are the custom sites of the rule.
apps	If the rule is for Application Control: the ID, name, and description of the application.
groups	ID of user group ("getGroupIDByName" on page 89) or groups on which to enforce this rule. To enforce on all users, make the value empty square brackets [].
userIDs	IDs of users ("getUserID" on page 88) on which to enforce this rule.

Note - To make a rule apply to all users, the value for all of these parameters must be empty square brackets: `groups` and `userIDs`.

Request Example

```
curl -d
'json={"command":"advancedPolicyGetRuleBase","LoginData":{"email":"lsmith@myco
mp.com","password":"123456"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
advancedPolicyGetRuleBase ={
  "apiKey": "X9V5-FUGS-1C3H-UAPP-C9A3-YJEN-FQ56-ZF2E",
  "errorCode": 200,
```

```
  "errorDescription": "ok",
  "data": [
    {
      "ruleID": "191000491",
      "ruleBaseOrder": "1",
      "userIds": [
      ],
      "action": "BLOCK",
      "comments": "",
      "isLog": "1",
      "categories": [
      ],
      "customSites": [
      ],
      " ": [
    ],"
      "groups": [
      ]
    },
    {
      "ruleID": "191000394",
      "ruleBaseOrder": "1",
      "action": "BLOCK",
      "comments": "",
      "isLog": "1",
      "categories": [
      ],
      "userIds": [["124587932","user123"]
      ],
      "customSites": [
      ],
      "apps": [
        [
          "10002092",
          "RealPlayer",
          "[APP]High Bandwidth,Supports Streaming,UDP Protocol,Media Sharing"
        ],
        [
          "10002087",
          "iTunes",
          "[APP]Autostarts\/Stays Resident,High Bandwidth,Port agility,Supports
File Transfer,Bundles Software,Encrypts communications,Supports Streaming,UDP
Protocol,Media Sharing"
        ]
      ],
      "groups": [
      ]
    }
...
    {
      "ruleID": "191000483",
      "ruleBaseOrder": "5",
      "action": "BLOCK",
      "comments": "",
      "isLog": "1",
      "categories": [
      ],
      "customSites": [
      ],
      "apps": [
      ],
      "groups": [
      ]
      "userIds": [
```

```
      ]
    }
  ]
}
```

policyCreateCustomSite

Use this command to add a site to the URL Filtering policy.

Request Parameters

Parameter	Description
siteUrl	URL of the site to add to the policy.

Response Data

Parameter	Description
customsiteID	ID of the custom URL in the policy.

Request Example

```
curl -d
'json={"command":"policyCreateCustomSite","LoginData":{"email":"lsmith@mycomp.
com","password":"123456"},"params":{"siteUrl":"www.test.com"}}''https://cloud.
checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
policyCreateCustomSite ={
   "apiKey": "PFY4-TN5G-NN63-16F1-L184-CJ7Y-EMXY-5VG8",
   "errorCode": 200,
   "errorDescription": "ok",
   "data": "191000075"
}
```

policyGetCustomSiteList

Use this command to get the list of custom URLs, with site ID and URL.

Request Parameters

None

Response Data

Parameter	Description
customsiteID	ID of the custom URL.
siteUrl	URL.

Request Example

```
curl -d
'json={"command":"policyGetCustomSiteList","LoginData":{"email":"lsmith@mycomp
.com","password":"123456"}}'
```

```
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
policyGetCustomSiteList ={
  "apiKey": "WMX2-GSYH-EBD1-VTW6-LTEG-72QC-V1PQ-5MVV",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "results": {
      "rowID_1": {
      "customsiteID": "191000037",
      "siteUrl": "www.test.com"
      }
    },
    "total": 1
  }
}
```

policyGetApplicationList

Use this command to get the list of all applications in the URL Filtering policy, their IDs, and descriptions.

Request Parameters

None

Response Data

List of applications

Request Example

```
curl -d
'json={"command":"policyGetApplicationList","LoginData":{"email":"lsmith@mycom
p.com","password":"123456"},"params":[]}
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
    "apiKey": "EMCV-9V1A-FYMX-61KK-37RZ-3BEU-LFVP-5JTF",
    "errorCode": 200,
    "errorDescription": "ok",
    "data": {
        "results": {
            "rowID_1": {
                "appID": "10063778",
                "name": "mundu SMS",
                "description": "SMS Tools"
            },
            "rowID_2": {
                "appID": "10080421",
                "name": "Grub",
                "description": "Opens ports,Web Spider"
            },
            "rowID_3": {
                "appID": "10055034",
                "name": "PhotoBuzz!",
                "description": "Ning.com Widgtes"
            },
```

```
…
            "rowID_4861": {
                "appID": "60343860",
                "name": "Hulu-posting",
                "description": ""
            },
            "rowID_4862": {
                "appID": "60371006",
                "name": "Pastebin-posting",
                "description": ""
            }
        },
        "total": 4862
    }
}
```

policyGetCategoryList

Use this command to get the list of all categories in the URL Filtering policy and their IDs.

Request Parameters

None

Response Data

List of categories

Request Example

```
curl -d
'json={"command":"policyGetCategoryList","LoginData":{"email":"lsmith@mycomp.c
om","password":"123456"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
    "apiKey": "FSW6-AY91-8T24-ML8T-1GNN-88XQ-WLFM-VCL4",
    "errorCode": 200,
    "errorDescription": "ok",
    "data": {
        "results": {
            "rowID_1": {
                "categoryID": "50000103",
                "name": "Micro blogging"
            },
            "rowID_2": {
                "categoryID": "50000003",
                "name": "Opens ports"
            },
….
        "rowID_166": {
                "categoryID": "50000107",
                "name": "Windows Messenger protocol"
            },
            "rowID_167": {
                "categoryID": "50000108",
                "name": "Yahoo Messenger protocol"
            }
        },
        "total": 167
    }
```

```
}
```

getInstallPolicyStatus

Use this command to get the status of the policy on the gateways.

Request Parameters

None

Response Data

Parameter	Description
isActive	`"t"` – The policy is installed and active on all gateways.
	"f" - The policy is not installed or active.
	"n" - Policy install is in progress on at least one of the gateways.

Request Example

```
curl -d
'json={"command":"getInstallPolicyStatus","LoginData":{"email":"lsmith@mycomp.
com","password":"123456"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
getInstallPolicyStatus ={
  "apiKey": "8EY9-1WAF-PGI8-MT6P-DYFB-91E6-YF88-D45C",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "results": {
      "rowID_1": {
        "isActive": "t"
      }
    },
    "total": 1
  }
}
```

rulebaseChangeOrder

Use this command to change the order of a rules in the URL Filtering policy.

Request Parameters

Parameter	Description
ruleID	ID of the rule to change ("advancedPolicyGetRuleBase" on page 104).
destinationIndex	New number of the rule in the policy.

Response Data

None

Request Example

```
curl -d
'json={"command":"rulebaseChangeOrder","LoginData":{"email":"lsmith@mycomp.com
","password":"123456"},"params":{"ruleID":191000260,"destinationIndex":2}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
rulebaseChangeOrder ={
        "apiKey": "HHXM-ME5Y-L4HX-8LXL-13IV-DSFY-RY15-67H2",
        "errorCode": 200,
        "errorDescription": "ok",
        "data": null
}
```

Managing Anti-Virus Anti-Bot

In This Section:

enableAvAndAb

Use this command to enable Anti-Virus, Anti-Bot, Threat Emulation, and IPS.

Request Parameters

Parameter	Description
enableAvAndAb	If value is `true`, Anti-Virus, Anti-Bot, Threat Emulation, and IPS are enabled

Response Data

None

Request Example

```
curl -d
'json={"command":"enableAvAndAb","LoginData":{"email":"lsmith@mycomp.com","pas
sword":"123456"},"params":{"enableAvAndAb":"true"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
enableAvAndAb ={
  "apiKey": "D4H1-D9Z3-R5XA-CT1G-F94P-X5TP-HAWK-RZI2",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": null
}
```

setAvAndAbEmailConfig

Use this command to schedule reports for Anti-Virus and Anti-Bot alerts.

Request Parameters

Parameter	Description
adminImmediate	If `true`, system administrators are notified immediately of Anti-Virus and Anti-Bot events.
adminDaily	If `true`, system administrators are notified once a day of Anti-Virus and Anti-Bot events.

`adminWeekly`	If `true`, system administrators are notified once a week of Anti-Virus and Anti-Bot events.
`userImmediate`	If `true`, the user is notified immediately of Anti-Virus and Anti-Bot events.
`userDaily`	If `true`, the user is notified once a day of Anti-Virus and Anti-Bot events.
`userWeekly`	If `true`, the user is notified once a week of Anti-Virus and Anti-Bot events.

Response Data

None

Request Example

```
curl -d
'json={"command":"setAvAndAbEmailConfig.","LoginData":{"email":"lsmith@mycomp.
com","password":"123456"},"params":{"userID":191000186,"adminImmediate":"true"
,"adminDaily":"true","adminWeekly":"true","userImmediate":"true","userDaily":"
true","userWeekly":"true"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
setAvAndAbEmailConfig ={
  "apiKey": "D4H1-D9Z3-R5XA-CT1G-F94P-X5TP-HAWK-RZI2",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": null
}
```

Managing SSL Inspection

In This Section:

addSslInspectionException

Use this command to make SSL Inspection exceptions for specified items.

Request Parameters

Parameter	Description
`applications`	ID of applications ("policyGetApplicationList" on page 107) or categories ("policyGetCategoryList" on page 108), to make an exception.
`usersGroups`	ID of user group ("getGroupIDByName" on page 89) or groups on which to enforce this rule. To enforce on all users, the value is empty square brackets [].
`customSites`	ID of custom sites ("policyGetCustomSiteList" on page 106) to make a URL Filtering rule based on your own URLs.
`log`	If `true`, events of this rule will be logged.

Response Data

Parameter	Description
exceptionID	ID of the SSL Inspection exception.

Request Example

```
curl -d
'json={"command":"addSslInspectionException","LoginData":{"email":"lsmith@myco
mp.com","password":"123456"},"params":{"applications":[10002087,10002088],"use
rsGroups":[10002623,10002556],"customSites":[],"log":"true"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
addSslInspectionException ={
  "apiKey": "HLY3-PQ3L-Y3WG-KI4X-9H24-N71R-XSY9-22XY",
  "errorCode": 200,
  "errorDescription": "ok",
```

```
    "data": {
      "exceptionID": "191000085"
      }
}
```

getSSLInspectionExceptions

Use this command to get data on SSL Inspection exceptions.

Request Parameters

None

Response Data

Parameter	Description
exceptionID	ID of the exception. If an exception has multiple items, there is a row for each: one `exceptionID` can be listed more than once in the response.
comments	Optional description of the exception.
log	Indicates if logging is enabled (1=enabled, 0=disabled).
categoryID	ID of the category for which an SSL Inspection exception was created.
customSiteID	ID of the custom site, if the exception is for a custom site. If the exception is not for a custom site, the value is `0` (zero).
groupID	ID of the user group on which the exception is enforced. If the exception is not for a user group, the value is `null`.

Request Example

```
curl -d
'json={"command":"getSSLInspectionExceptions","LoginData":{"email":"lsmith@myc
omp.com","password":"123456"},"params":[]}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
getSSLInspectionExceptions ={
  "apiKey": "PKTE-7U97-ZU25-1R36-AECA-CC9Y-UU8W-IFKA",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "results": {
      "rowID_1": {
        "exceptionID": "191000057",
        "comments": "",
       "log": "1",
        "categoryID": "9",
        "customSiteID": "0",
        "groupID": null
      },
      "rowID_2": {
        "exceptionID": "191000057",
```

```
        "comments": "",
        "log": "0",
        "categoryID": "34",
        "customSiteID": "0",
        "groupID": null
    },"
...
    "rowID_36": {
        "exceptionID": "191000074",
        "comments": "",
        "log": "1",
        "categoryID": "59",
        "customSiteID": "0",
        "groupID": null
    }
  },
  "total": 36
  }
}
```

removeSSLInspectionException

Use this command to remove an SSL Inspection exception.

Request Parameters

Parameter	Description
exceptionID	ID of the SSL Inspection exception ("getSSLInspectionExceptions" on page 114)

Response Data

None

Request Example

```
curl -d
'json={"command":"removeSSLInspectionException","LoginData":{"email":"lsmith@m
ycomp.com","password":"123456"},"params":{"exceptionID":"191000085"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
removeSSLInspectionException ={
  "apiKey": "DPHM-MQX2-R85J-WT71-JC18-NVC5-SVIV-A7V8",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": null
}
```

updateSSLInspectionException

Use this command to change an SSL Inspection exception.

Request Parameters

Parameter	Description
exceptionID	ID of the SSL Inspection exception ("getSSLInspectionExceptions" on page 114).
applications	ID of applications ("policyGetCategoryList" on page 108) to add to the SSL Inspection exception.
usersGroups	ID of the user group ("getGroupIDByName" on page 89) for which the exception will be enforced. To enforce on all users, the value is empty square brackets [].
customSites	ID of custom sites ("policyGetCustomSiteList" on page 106) to make a URL Filtering rule based on your own URLs.
log	If true, events of this rule will be logged.

Response Data

None

Request Example

```
curl -d
'json={"command":"updateSSLInspectionException","LoginData":{"email":"lsmith@m
ycomp.com","password":"123456"},"params":{"exceptionID":"191000085","applicati
ons":[10002087,10002092],"usersGroups":[10002623,10002556],"customSites":[],"l
og":"true"}}' 'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
updateSSLInspectionException ={
  "apiKey": "DPHM-MQX2-R85J-WT71-JC18-NVC5-SVIV-A7V8",
  "errorCode": 200,
  "errorDescription": "ok",
  "data": null
}
```

updateSSLInspectionSettings

Use this command to enable and configure SSL Inspection.

Request Parameters

Parameter	Description
sslEnabled	If value is true, SSL Inspection is enabled.
loggingEnabled	If value is true, SSL Inspection logging is enabled.
exceptionsEnabled	If value is true, SSL Inspection exceptions are enabled.

Response Data

None

Request Example

```
curl -d
'json={"command":"updateSSLInspectionSettings","LoginData":{"email":"lsmith@my
comp.com","password":"123456"},"params":{"sslEnabled":"true","loggingEnabled":
"true","exceptionsEnabled":"true"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
updateSslInspectionSettings ={
   "apiKey": "D4H1-D9Z3-R5XA-CT1G-F94P-X5TP-HAWK-RZI2",
   "errorCode": 200,
   "errorDescription": "ok",
   "data": null
}
```

getLogs

Request Parameters

Parameter	Description
query	Get results that fit the query ("Query Syntax Reference" on page 72). Optional. If not used, or if used with an empty string, there is no filter.
offset	Number of the row to start, to show results from offset to max Optional. If not used, the response starts from the first row. (Default = 0)
numberOfRows	Maximum number of rows, from offset, to include in the response Optional. If not used, the response includes all rows from offset to the end. (Default = 100)

Response Data

See Logs & Reports (on page 70).

Request Example

```
curl -d
'json={"command":"getLogs","params":{"query":"","offset":0,"numberOfRows":1},"
LoginData":{"email":"lsmith@mycomp.com","password":"654321","apiKey":"JL1H-K58
M-KR1R-L2HE-ACHC-639T-3HB8-NBGZ"}}'
'https://cloud.checkpoint.com/cp-cloud-api.php?format=json'
```

Response Example

```
{
  "errorCode": 200,
  "errorDescription": "ok",
  "data": {
    "time": "",
    "show_more": "",
    "found_size": "",
    "last": "",
    "total_size": 1,
    "logs": [
    ]
  }

}
```

Download Page

The Cloud Connect client creates a transparent VPN connection to the cloud. On this page, download a Cloud Connect client for your device.

You can also download Cloud Services utilities.

Device	Options
Desktop	Download the Cloud Connect for **Windows** or **Mac**
Active Directory Synchronizer	Download the files for the Active Directory Synchronizer ("Using the Active Directory Synchronizer" on page 39)
Single Sign On	Download the files for the SSO Authenticator ("Using the SSO Authenticator" on page 45)
Log Transport Agent	Download the files for the Log Transport Agent ("Using the Log Transport Agent" on page 32)

See Installing Clients ("Step 7: Installing Clients" on page 66) for desktop and mobile installation instructions.

Cloud Services Gateway Status

The Cloud Portal login page shows different pictures in rotation before you log in. One of the images is an overview of the Cloud Services gateways, their locations, and status.

Select to see the **Historical service status** from the **last week** or **last month**.

- A green checkmark shows that the gateway was up continuously throughout the day.

- A red x shows that there were one or more issues with the gateway during the day.

Evaluating Cloud Services

When testing Cloud Services in a new office environment, make sure that:

- Users who work through VPN with Cloud Services can install Windows patches and updates easily

- Changes to a laptop's internet setting, for example, LAN or Wi-Fi settings, do not affect the connection to Cloud Services.

- Your help desk or IT administrators know how to work with Cloud Connect. Activities include: install and uninstall the Cloud Connect and register users.

- You know the time impact of policy changes, while a user is connected and while a user is disconnected.

- Installation and upgrades work on older laptops.

- Connections to Cloud Services work with non-Check Point VPN clients.

- The Cloud Services utilities that you want to use work in your environment. SSO is especially important for user registration.

- Internal networks are excluded, especially networks used for internal services, such as printers and DNS servers.

Mail Protection

SandBlast Cloud for Office365 has different options to scan incoming email messages for potentially malicious attachments. For more information see the *SandBlast Cloud Administration Guide* http://supportcontent.checkpoint.com/documentation_download?ID=50858.