QUANTUM

14 March 2025

DATA LOSS PREVENTION

R81.20

Administration Guide

Check Point Copyright Notice

Important Information

Latest Software

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

Certifications

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

Check Point R81.20

For more about this release, see the R81.20 home page.

Latest Version of this Document in English

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

Feedback

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

Revision History

Date	Description
13 March 2025	Removed: ■ Chapter about "UserCheck Client" was moved to the *R81.20 Quantum Security Gateway Guide*.
27 June 2024	Updated: ■ *"Installation and Configuration" on page 25*
05 April 2024	Updated: ■ *"Advanced Data Types" on page 178*
14 May 2023	Updated: ■ The chapter *"Configuring UserCheck" on page 76* ■ The chapter *"Configuring User Access to an Integrated DLP Gateway" on page 245*
19 January 2023	Updated: ■ The chapter *"UserCheck" on page 74*
20 November 2022	First release of this document

Table of Contents

Introduction to Data Loss Prevention

The Need for Data Loss Prevention

Data is more accessible and transferable today than ever before, and the vast majority of data is sensitive at different levels. Some is confidential simply because it is part of an internal organization and was not meant to be available to the public. Some data is sensitive because of corporate requirements, national laws, and international regulations. Often the value of data depends on its constant confidentiality - consider intellectual property and competition.

Leakage of your data could be embarrassing or worse, cost you industrial edge or loss of accounts. If you let your organization to act in non-compliance with privacy acts and other laws, it could be worse than embarrassing - the integrity of your organization may be at stake.

You want to protect the privacy of your organization, but with all the tools making information sharing easier, it is easier to make an irrecoverable mistake. To make the matter more complex, along with the severity of data leakage, we now have tools which inherently make it easier to happen: cloud servers, Google docs, and simple unintentional abuse of company procedures - such as an employee who takes work home. In fact, most cases of data leakage occur because of unintentional leaks.

The best solution to prevent unintentional data leaks is to implement an automated corporate policy that catches protected data before it leaves your organization. Such a solution is known as Data Loss Prevention (DLP).

Data Loss Prevention identifies, monitors, and protects data movement through deep content inspection and analysis of transaction parameters (such as source, destination, data object, and protocol), with a centralized management framework. In short, DLP detects and prevents the unauthorized transmission of confidential information.

Note - Data Loss Prevention is also known as Data Leak Prevention, Information Leak Detection and Prevention, Information Leak Prevention, Content Monitoring and Filtering, and Extrusion Prevention.

Data Loss Prevention and Privacy

DLP captures original data that caused a rule match, including the body of the transmission and attached files.

Best Practice - Disclose to your users how your DLP environment works. Tell users that transmissions that violate the data security guidelines of your organization are stored, and security personnel can read them.

Information disclosure recommendations:

1. Disclose the privacy policy BEFORE you configure DLP.
2. Translate the most important DLP rules into guidelines and tell your users what is not allowed and brings to captured transmissions.
3. Explain that DLP scans only transmissions that originate from computers inside the organization (including any source that uses organization resources, such as Remote Access or VPN connections).
4. Explain how to handle Ask User violations.

   DLP incident notifications can be sent by email (for SMTP traffic) or shown in a system tray pop up from the UserCheck Client (for SMTP, HTTP, FTP, and so on).

   If the incident of the notification is in Ask User mode, the user can click the **Send** or **Discard** link in the pop up of UserCheck Client: to handle the incident in real-time.

Important - Make your users are aware of the purpose of the UserCheck Client: handle the DLP options directly from the pop up.

If the user exits the client, the alternative web page that provides the Ask User options may not function.

1. Explain that captured transmissions are logged and saved, and that some may be reported to managers (Data Owners).
2. Explain that captured emails, attachments, web posts, and so on are available for review by security personnel.
3. Explain that review of original transmissions is for organization data security alone - you do not collect personal information. Therefore, your users have no option to prevent the scan on their transmission, or disable it, or both.
4. Make sure that you maintain your guidelines: do not keep or use original transmissions for any use other than review of DLP incidents and rules.

The Check Point Solution for DLP

The Check Point Data Loss Prevention Software Blade provides the ability for you to quickly configure realistic out-of-the-box detection capabilities based on expert heuristics.

However, optimal DLP must take time. To specify data prevented from transmission, you must take into account many variables, different in the context of the particular transmission, for example:

- What type of data is it?
- Who owns it?
- Who is sending it?
- Who is the intended receiver?

- When is it being sent?
- What is the cost if tasks are disrupted because the policy is stricter than needed?

Data Loss Prevention Features

Check Point solves the complexity of Data Loss Prevention with unique features.

- **UserCheck™** - Provides rapid response for incident handling with automated user notification and the unique Ask User mode. Each person in your organization learns best practices as needed, preventing future unintentional leaks - the vast majority of DLP incidents - and quickly handling immediate incidents. The user handles these incidents either through the DLP Self Incident Handling Portal , or through the UserCheck Client.

  Without UserCheck, a security administrator, or even a security team, would have to check every email and data movement in real time and approve or reject each. For this reason, other products offer only detection of suspicious incidents. With UserCheck, the decision-making is distributed to the users. They are presented with the reason for the data capture and must provide a reason for letting it pass (if the notification did not change their minds about sending it on). User decisions (send or discard) and reasons for sending are logged. With the original message and user decisions and reasons, you can develop an effective prevention policy based on actual use.

- **MultiSpect™** - Provides unmatched accuracy in identifying and preventing incidents through multi-parameter correlation with Compound Data Types and customizable Data Types with CPcode.

- **Out of the Box Security** - A rich set of pre-specified Data Types recognizes sensitive forms, templates, and data to be protected. The Data Types are enforced in an effective out-of-the-box policy.

- **Data Owner Auditing** - The Data Owner is the person responsible for controlling the information and files of his or her own area in the corporation. Data Owners get timely and relevant information through automated notifications and reports that show exactly how their data is being moved. Check Point DLP gives Data Owners the information they need to handle usage issues directly related to their areas of responsibility. Without Data Owner control, the security administrator would often be placed in an awkward position between managers and employees.

- **CPcode** - DLP supports fully customized data identification through the use of CPcode. You specify how data is to be matched by DLP, with the greatest flexibility possible. See the *R77 versions CPcode DLP Reference Guide*. .

Data Loss Prevention Benefits

Check Point DLP saves time and significantly improves ROI. Its innovative technologies provide automation that negates the need for long and costly analysis and a team for incident handling. You can now move from a detection-only policy to an accurate and effective prevention policy without bringing in outside consultants or hiring a security team.

All of this functionality is easy to manage through the SmartConsole, in an interface similar to other Software Blades. You are not expected to be a DLP expert from the day of configuration. Check Point Data Loss Prevention guides you on how to customize and improve your DLP policy - with the Improve Accuracy flag, for example. The DLP Software Blade comes with a large number of built-in Data Types that can be quickly applied as a default policy. You can fine-tune the out-of-the-box policy to easily convert the confidentiality and integrity guidelines of your organization into automated rules. And later, you can create your own Data Types. This cycle of updating the policy, moving from a detection policy to a preventative policy, is close with the Check Point Logs & Monitor tool.

Content Awareness Software Blade

Content Awareness and Data Loss Prevention both use Data Type. However, they have different features and capabilities. They work independently, and the Security Gateway enforces them separately.

For more information on the Content Awareness Software Blade see the *R81.20 Quantum Security Gateway Guide*.

How DLP Works

General Description

Item	Description
1	Internal network
2	Data Loss Prevention Software Blade enabled on a Security Gateway
3	Security Management Server
4	HTTP proxy
5	Mail server
6	Active Directory or LDAP server
7	Logs & Monitor view

DLP Workflow:

1. The Data Loss Prevention Software Blade is enabled on a Security Gateway (2) (or ClusterXL Security Cluster). This makes it a DLP Gateway (or a DLP security cluster). In other way, you can install a dedicated DLP Gateway behind a protecting Security Gateway.

2. You use the SmartConsole and the Security Management Server to install the DLP Policy on the DLP Gateway.
3. The DLP Gateway (2) uses the built-in Data Types and rules to provide out-of-the-box Data Loss Prevention. It may use the Active Directory or LDAP server (6) to identify the internal organization.

   It catches all traffic that contains data and goes through supported protocols. When users send data that goes to an HTTP proxy (4) or a mail server (5), for example, the DLP Gateway catches the data before it goes outside the organization.

   It scans the traffic, with email attachments, to find data that must not go outside the organization. To recognize this data, it uses protocol, source, destination, and complex Data Type representations.

   It can also scan internal traffic between Microsoft Exchange clients within the organization. The installation of the Exchange Security Agent on the Microsoft Exchange server is necessary for this. The agent forwards internal emails to the DLP Gateway which then scans them. If the organization only uses Exchange servers for managing emails (internal and external), you can use this setup to also scan emails that are sent outside of the organization.

   If the data does not match any of the rules of the DLP policy, the traffic is allowed to pass.
4. Use Logs & Monitor view (7) to effectively log, track, analyze events, and report of incidents that the DLP Gateway captures.

Integrated DLP Security Gateway Configuration

In an *Integrated DLP Security Gateway* configuration, the Data Loss Prevention Software Blade is enabled on a Security Gateway (or a cluster). This makes it the DLP Gateway (or DLP Security Cluster). The Firewall Software Blade, and optionally, other Network Security Software Blades, are also enabled on the Security Gateway.

If the DLP Gateway is on the perimeter, the SMTP server forwards only transmissions with destinations outside of the organization to DLP. Internal and external transmissions can be inspected by DLP if they are forwarded to DLP by the Exchange Security Agent on the Exchange Server. For external transmissions through the Exchange Security Agent the Exchange Server must have an accessible IP address to the DLP Gateway.

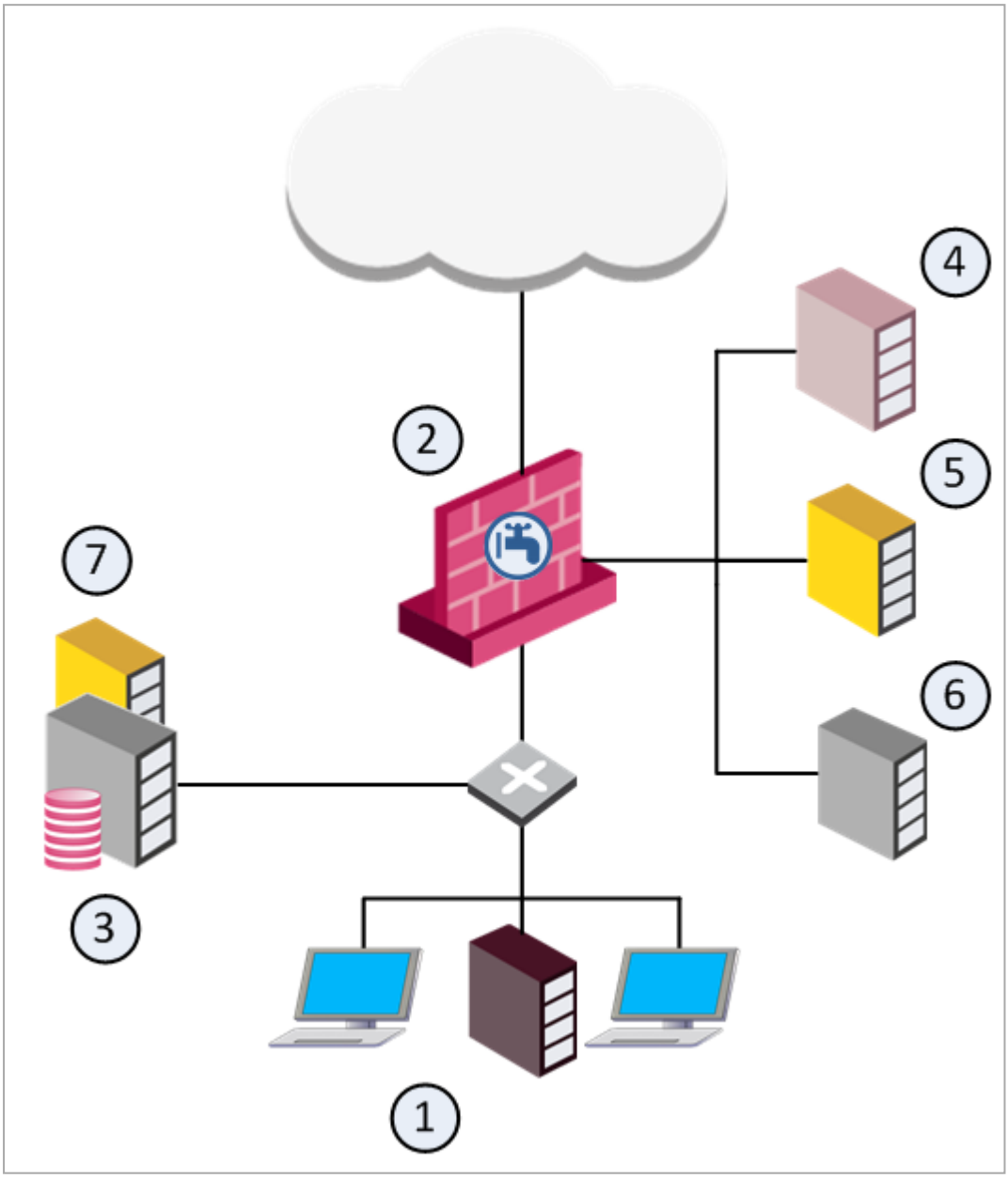
Dedicated DLP Gateway Configuration

General Description

In a *Dedicated DLP Gateway* configuration, a separate Security Gateway (2) (or cluster) is installed in addition to the protecting Security Gateway (3) (or cluster). The Data Loss Prevention Software Blade is enabled on that separate Security Gateway.

Install the dedicated DLP Gateway behind the protecting Security Gateway to ensure its protection. We recommend that you enable only the Data Loss Prevention Software Blade to maximize the use of available hardware resources.

Best Practice - When you set up a dedicated DLP Gateway, configure it in Bridge Mode. The bridge is transparent to network routing.



Item	Description
1	Internal network
2	Data Loss Prevention Software Blade enabled on a Security Gateway
3	Security Gateway

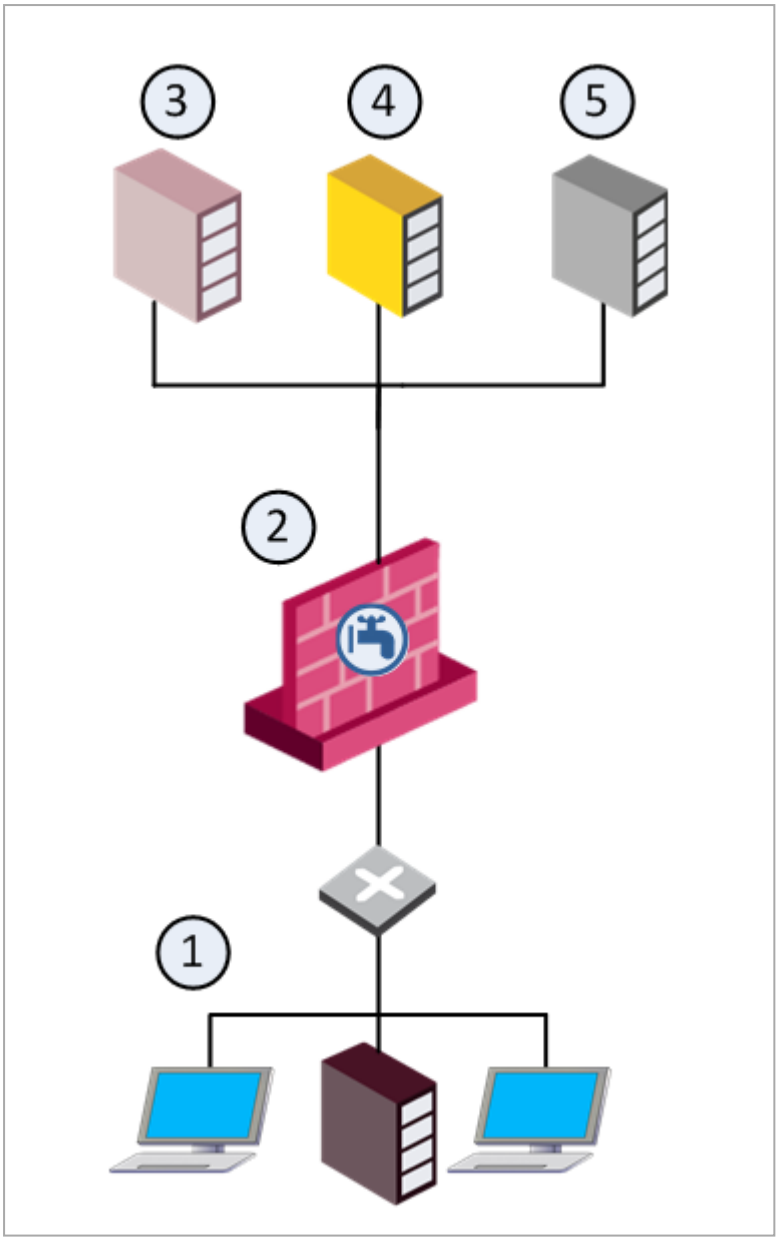
Item	Description
4	Security Management Server
5	HTTP proxy
6	Mail server
7	Active Directory or LDAP server
8	Logs & Monitor view

Alternative Gateway Configurations

General Description

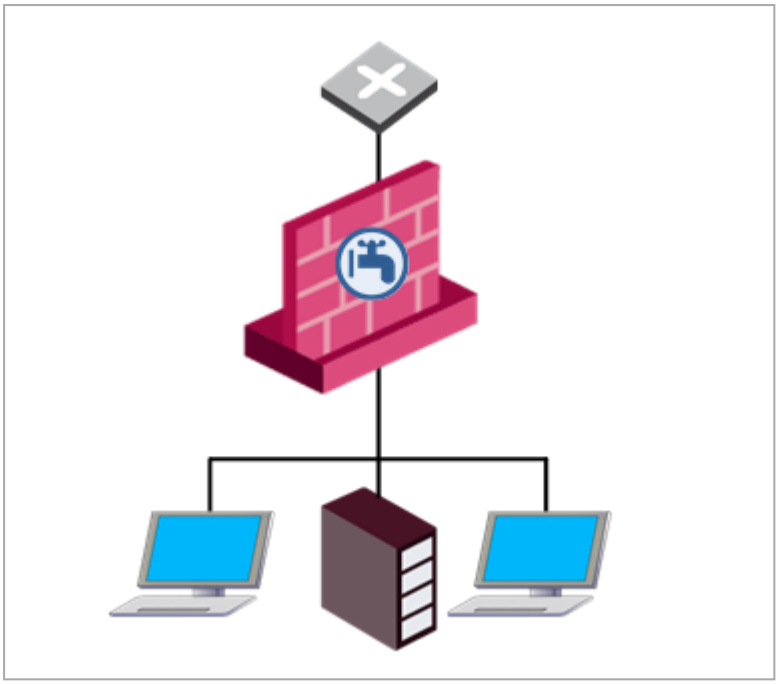
As an alternative to putting the DLP Gateway on the network perimeter, you can put the DLP Gateway between the user networks and the servers, to allow DLP to inspect traffic before it goes to the servers. This configuration is the necessary configuration if you want to use a DLP rule that inspects data transmissions between departments.

For example, you can create a DLP rule that checks emails between internal groups: **Source** is a specific network, **Destination** is **Outside Source** (anything outside of this **Source**). This rule applies only for this configuration.



Item	Description
1	Internal network
2	Data Loss Prevention Software Blade enabled on a Security Gateway
3	HTTP proxy
4	Mail server
5	Active Directory or LDAP server

You can put the DLP Gateway between the users and the switch, to directly protect a subnet.



What Happens on Rule Match

The DLP Gateway captures traffic and scans it against the Data Loss Prevention policy.

If the data in the traffic matches a rule in the policy

1. Incident is logged.
    - The data is stored in a safe repository on a log server or Security Management Server that stores DLP logs.
    - The DLP Gateway logs an incident with the Logs & Monitor view.
2. Action of rule is performed.

- If the matched rule is set to **Detect**, the user gets no notification. A DLP log incident is created, and the actual data is stored.

  Action of rule is performed.

  - **Detect** - The user gets no notification. A DLP log incident is created, and the actual data is stored.
  - **Inform User** - DLP notifies the user that the captured traffic violates DLP rules. The traffic is passed.
  - **Ask User** - DLP notifies the user that the message stays, and sends a link to the DLP Portal, where the user decides whether the transmission goes through or not. User decisions, and reasons to send, are kept for your analysis.
  - **Prevent** - The traffic is blocked. You can notify the user and the Data Owner.

- If the matched rule is set to **Inform User**, DLP notifies the user that the captured traffic violates DLP rules. The traffic is passed.
- If the matched rule is set to **Ask User**, DLP notifies the user that the message is being held and contains a link to the DLP Portal, where the user decides whether the transmission should go through or be dropped. User decisions, and reasons for sending, are logged for your analysis.
- If the matched rule is set to **Prevent**, the traffic is blocked. The user and the Data Owner may be notified.

3. Optionally, Data Owners, and other users configured for notifications get a notification about the incident.

Role of a DLP Administrator

DLP provides many auditing tools:

- Receive automatic notifications to data owners when transmission of protected data was attempted.
- Receive user notifications and self-handling portal.
- Track and log event details, charts, graphs, filtered lists, and reports from the Logs & Monitor view.

Before you begin your audit, configure your DLP policy.

Workflow to create and refine the DLP policy:

1. Define Data Types.
2. Configure out-of-the-box Data Loss Prevention with a basic policy.

   This policy provides strong detection capabilities from Day-1.
3. Customize pre-defined Data Types to improve policy accuracy.

   Some provided Data Types are placeholders for dictionaries of proprietary information. These Data Types are flagged for your attention. Integrate your organization's data with your DLP policy to make it more accurate for your needs.
4. Select Data Types.

   Become familiar with the wide range of provided Data Types. Enable and disable the rules in the DLP policy that suit your needs.
5. Create your own Data Types with the easy to use wizard.

   Enforce confidentiality guidelines of your organization. Ensure that information belonging to Data Owners stays within their control. Enforce data protection by using your Data Types in DLP rules.
6. Monitor incidents and communicate to data owners.

   The DLP Gateway catches attempted transmissions of protected data and logs incidents. You can see these incidents in the Logs & Monitor Logs view. You and the Data Owners specify the incidents require notification to the Data Owners. As you monitor the incidents, create guidelines to make a fine tuning to the DLP policy.
7. Refine the policy.

   When an email or FTP upload is held because it matches a rule in the Data Loss Prevention policy, it disrupts users. Sometimes this is the best preventative action, but in other situations it is unnecessary. Monitor user actions to see whether users agree that the data should not have been sent or that users have reasons for the transmissions.
8. Maintain policy over time.

   Generate Data Owner reports and audit user actions. Look at the logs that the Logs & Monitor Logs view provides and make sure the DLP policy works smoothly and prevents transmission of protected data.

DLP Permissions for Administrator Accounts

You can assign a DLP administrator full DLP permissions or a subset of permissions.

With full permissions, a DLP administrator can:

- See all fields of the logs in the Logs & Monitor Logs view.
- See the captured data (the actual email, FTP files and HTTP posts).
- Send or discard quarantined user emails.

An alternative to assigning a full set of permissions is to configure a subset. This gives you the flexibility to assign only some of the permissions. For example, permissions to only see the fields of the logs but not to see the captured data or send or discard quarantined emails.

Configuring Full DLP Permissions

To configure full permissions:

1. In SmartConsole, select **Manage & Settings > Permissions & Administrators**.
2. Double-click the administrator account or click **New** create a new administrator user account.

   The **Administrator Properties** window opens, and shows the **General** page.
3. In Permission Profile, click the drop-down menu and then click **New**.

   The **Permissions Profile Properties** window opens.
4. In **Enter Object Name**, enter the name for the DLP admin profile.
5. Make sure **Read/Write All** is selected.
6. From the navigation tree, click **Monitoring and Logging**.
7. Select these options:
   - **DLP logs including confidential fields**
   - **View/Release/Discard DLP messages**
8. Click **OK**.
9. Close the **administrator** window.
10. Publish the SmartConsole session.

Configuring a Subset of Permissions

To configure a subset of permissions for the DLP administrator:

1. In SmartConsole, select **Manage & Settings > Permissions & Administrators**.
2. Double-click the administrator account or click **New** create a new administrator user account.

   The **Administrator Properties** window opens, and shows the **General** page.

3. In Permission Profile, click the drop-down menu and then click **New**.

   The **Permissions Profile Properties** window opens.

4. In **Enter Object Name**, enter the name for the DLP admin profile.
5. Select **Customized** and click **Edit**.
6. From the navigation tree, click **Access Control**.
7. In the Additional Policies section, configure **Read** or **Write** permissions for **Data Loss Prevention**.
8. From the navigation tree, click **Monitoring and Logging**.
9. Select one or more of these options:

   - **DLP Logs including confidential fields** - Permissions to view all fields of DLP logs in the Logs & Monitor Logs view. When this check box is cleared, an administrator sees the text "***** Confidential *****" and not the actual content of fields defined as confidential.
   - **View/Release/Discard DLP messages** - Permissions to view emails and related incidents from within the Logs & Monitor Logs view. With this permission, administrators can also release (send) or discard quarantined emails from within the Logs & Monitor Logs view.

     Note - If you select all of these options with Write permissions, the administrator has full DLP permissions.

10. Click **OK**.
11. Close the **administrator** window.
12. Publish the SmartConsole session.

Installation and Configuration

The environment must include a DNS server.

Important - Before you enable the DLP Software Blade, you must review the requirements and supported platforms for DLP in the *R81.20 Release Notes*.

Installing the DLP Gateway

For instructions on how to install the DLP Gateway, see the *R81.20 Installation and Upgrade Guide*.

DLP Software Blade Trial License

The DLP Software Blade has a 30 day trial license.

To activate the trial license:

1. In **SmartConsole**, in the Security Gateway object, select the **DLP** Software Blade.
2. In **SmartConsole**, install policy on the DLP Gateway.

During the trial period, when you install a policy on the DLP Gateway, a warning message shows how many days stay until the trial license expires.

After the trial period, you must install a full DLP Software Blade license. If you do not, the DLP Software Blade operation stops, and you cannot install a policy on the DLP Gateway. You must remove the selection mark from the DLP Software Blade, and then you can install a policy on the Security Gateway.

Configuring a DLP Gateway or Security Cluster

For DLP integrated configuration, enable the DLP Software Blade as one of the Software Blades on a Security Gateway. In a *dedicated* DLP Gateway, the Data Loss Prevention Software Blade is enabled on an individual Security Gateway (or Security Cluster).

In ClusterXL Load Sharing cluster, the DLP Software Blade works only when the policy contains DLP rules that use the Detect, Inform, or Prevent actions (see *"DLP Rule Actions" on page 110*). ClusterXL Load Sharing do not support the **Ask** DLP action.

In a Cluster with enabled DLP Software Blade, state synchronization occurs at two minutes' interval. Therefore, if there is a cluster failover, the new Active cluster member can possibly not know about DLP incidents that happened in the two minutes since the cluster failover.

Configuring Integrated Environments

In an integrated environment you can:

- Enable the DLP blade on an current Security Gateway or Security Cluster.
- Configure a new Security Gateway or cluster and enable the DLP blade on it.

To enable DLP on an current Security Gateway or cluster:

1. Open SmartConsole, open the Security Gateway or Security Cluster object.

   The Security Gateway window opens and shows the **General Properties** page.

2. For a Security Cluster: in the **ClusterXL** page, select **High Availability** or **Load Sharing** mode .

   For ClusterXL Load Sharing, the **Ask** action in the DLP rules is not supported.

3. In the **Software Blades** section, click the **Data Loss Prevention** Software Blade.

   Note - On a Security Cluster, this enables the DLP blade on every cluster member.

   The **Data Loss Prevention Wizard** opens.

4. Complete the **Data Loss Prevention Wizard** (see *"Data Loss Prevention Wizard" on page 29*).

5. Install policy.

Configuring Dedicated Configurations

To configure a dedicated DLP Gateway behind a current Security Gateway or Security Cluster:

1. Install an individual Security Gateway (or cluster) behind the current Security Gateway.
2. In SmartConsole, create a new object for the individual Security Gateway or cluster.

   Note - If you created a cluster, in the ClusterXL Load Sharing modes, there is no support for **Ask** action in the DLP rules.
3. In the Security Gateway or cluster object, go to the **General Properties** page.
4. In the **Network Security** tab, clean the **Firewall** Software Blade and select the **Data Loss Prevention** Software Blade.

   The **Data Loss Prevention Wizard** opens.
5. Complete the **Data Loss Prevention Wizard** (see *"Data Loss Prevention Wizard" on page 29*).
6. Install policy on the individual Security Gateway or cluster object.

Best Practice - When you set up a dedicated DLP Gateway, configure it in Bridge Mode. The bridge is transparent to network routing.

Data Loss Prevention Wizard

DLP Blade Wizard Options

- **Email Domain in My Organization** - Provide the domain of the organization, to allow the DLP Gateway to distinguish between internal and external email addresses.
- **Connect to Active Directory** - Enable the DLP Gateway to access the Active Directory server and automatically populate the users and user groups that make up the definition of **My Organization** and to validate users. You can do this now or later. For instructions of how to do this, see *"Configuring Active Directory and LDAP for DLP" on page 33*.
- **Activate DLP Gaia Portal for Self Incident Handling** - Select to activate the port.

  The default URL is: *https://<IP Address of DLP Gateway>/dlp*.
- **Mail Relay** - Select a mail server from the list of existing network objects, or click **New** and define a new mail server (SMTP). If the mail server needs the DLP Gateway to authenticate itself, click the **Authentication** drop-down and provide the credentials of the mail server.

  If the Mail Server is a Microsoft Exchange server, set the Exchange server to be an SMTP Relay for this newly created DLP Gateway.
- **My Organization Name** - Enter different names and phrases used to identify your organization. These names are used by the DLP feature to accurately detect incidents of data loss.
- **Protocols** - Select protocols to which the DLP policy applies.

Completing the Wizard

After you complete the wizard for a DLP Gateway of any platform, enable the Software Blade and install policy.

1. Make sure that the **Data Loss Prevention** Software Blade is enabled.
2. Review the topology of the DLP Gateway.

   DLP by default scans traffic from internal networks to external networks, so you must properly define the DLP Gateway interfaces as **internal** or **external**. You can do this when you define **My Organization** in the **Data Loss Prevention** tab of SmartConsole.
3. Install policy on the DLP Gateway only:
   a. In SmartConsole, install the policy.
   b. In the **Install Policy** window, select the DLP Gateways.

Note - On a dedicated DLP Gateway, only the *DLP Policy* is installed. This is not a security policy. Make sure you have another Security Gateway in the environment to enforce the *Security* Policy.

Configuring a DLP Gateway in Bridge Mode

Best Practice and Limitations

Best Practice - When you set up a dedicated DLP Gateway, Check Point recommends that you configure the DLP Gateway as a bridge, so that the DLP Gateway is transparent to network routing.

You can configure DLP in bridge mode, with the requirements described in this section for routing, IP address, and VLAN trunks.

Note the current limitations:

- In an environment with more than one bridge interface, the DLP Gateway must not see the same traffic twice on the different interfaces. The traffic must not run from one bridged segment to another.
- Inter-bridge routing is not supported. This includes inter-VLAN routing.
- If the bridge interface is connected to a VLAN trunk, all VLANs are scanned by DLP. You cannot keep out specific VLANs.
- Routing from the bridge interface to a Layer3 interface, and from Layer3 interface to the bridge, is not supported. Traffic on the bridge interface must run through the bridge or be designated to the DLP Gateway.
- From R76, the DLP Gateway in bridge mode can be in a cluster, in High Availability mode. But the **Ask User** action and the UserCheck Agent are not supported.
- If the DLP Gateway in bridge mode is *behind* a cluster, the cluster must be in High Availability mode.
- Bond High Availability (HA) or Bond Load Sharing (LS) (including Link Aggregation) are not supported in combination with bridge interfaces.

Necessary Routing in Bridge Mode

There must be routes between the DLP Gateway and the necessary servers:

- Security Management Server
- DNS server
- Mail server, if an SMTP Relay server is configured to work with the Security Gateway
- Active Directory or LDAP server, if configured to work with the Security Gateway

There must be a default route. If this is not a valid route, it must reach a server that answers ARP requests.

If UserCheck is enabled, configure routing between the DLP Gateway and the network.

Configuring Bridge IP Address

The bridge interface can be configured without an IP address, if another interface is configured on the Security Gateway intended to connect to the UserCheck Client and the DLP Portal.

If you do add an IP address to the bridge interface after the Security Gateways are started, run the `cpstop` and `cpstart` commands to apply the change.

Necessary VLAN Trunk Interfaces

- A single bridge interface must be configured to bind the DLP Gateway for a VLAN trunk.
- If an IP address is configured on the bridge, the IP address must not belong to any of the networks going through the bridge. Users must have routes that run traffic through the bridge interface of the DLP Gateway. The Security Gateway handles this traffic and answers to the same VLAN of the original traffic.
- In a VLAN trunk interface, another interface must be configured as the management interface for the necessary bridge routing.

Configuring Active Directory and LDAP for DLP

You can configure the DLP Gateway to access a Microsoft Active Directory or LDAP server to:

- Authenticate to the DLP Portal with Active Directory credentials
- Authenticate to UserCheck with Active Directory credentials
- Define Active Directory or LDAP groups to be used in the DLP policy
- Define the **My Organization** object

If you run the wizard from a computer in the Active Directory domain, the Data Loss Prevention Wizard asks for your Active Directory credentials to create the LDAP account unit automatically. You can run the wizard again from a computer in the Active Directory domain to create the LDAP account unit.

Procedure

1. From a computer that is a member of the Active Directory domain, create the DLP Gateway object.
2. Enter your Active Directory credentials in the Active Directory page.

   It is not necessary to enter credentials with administrator privileges.

   Best Practice - Create an Active Directory account that is dedicated for use by Check Point products to connect to Active Directory.
3. When you complete the wizard, the LDAP account unit is created automatically.

   If you have multiple Active Directory servers:

   a. Review the created account unit.

   b. Remove unnecessary servers.

   c. Assign applicable priorities to all the servers.

The DLP Wizard asks for Active Directory credentials only if no LDAP account unit exists. If you already have an LDAP account unit, the wizard does not ask for your credentials. To create the LDAP account unit from the DLP Wizard, delete the existing LDAP account unit and run the wizard again.

Note - If you configure the LDAP Account Unit manually, with the username and password authentication method, you must set the **Default Authentication Scheme** to **Check Point Password**.

If you need more LDAP account units, you can create the LDAP account unit manually. See the *R81.20 Security Management Administration Guide*.

Rerunning the Data Loss Prevention Wizard

If you run the DLP Wizard from a computer that is not part of the Active Directory domain, you can run it again from a computer in the Active Directory domain to create the LDAP account unit.

To run the Data Loss Prevention Wizard again:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. Clear the **Data Loss Prevention** Software Blade.
3. Select the **Data Loss Prevention** Software Blade.

   The Data Loss Prevention Wizard starts.

Configuring a DLP Gateway for a Web Proxy

You can use a Web Proxy server or servers for HTTP and HTTPS traffic. If you want the DLP Gateway to scan this traffic, you must configure the DLP Gateway.

Note - You can enable HTTPS Inspection on the Security Gateway to scan HTTPS connections.

To configure DLP for a Web Proxy, use these procedures if the proxy or proxies are between the DLP Gateway and the Internet, or in a DMZ.

Best Practice - If a proxy is in a DMZ, use the DLP Gateway to scan the HTTP traffic between the user network and the proxy in the DMZ.

Configuring an R75 or higher DLP Gateway for Web Proxies

If you have one Web proxy server between the DLP Gateway and the Internet, use either **Procedure 1** or **Procedure 2**.

If you have more than one proxy between the DLP Gateway and the Internet, use **Procedure 2**.

If you configure both **Procedure 1** and **Procedure 2**, the DLP Gateway drops HTTP and HTTPS traffic sent to any web proxy that is not specified in **Procedure 1**.

Procedure 1

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Data Loss Prevention** > **Protocols**.
3. Make sure that **HTTP** is selected for this Security Gateway or for the **default protocols**.
4. From the navigation tree, click **Network Management** > **Proxy**.
5. Configure the proxy server settings:
   - To use the proxy server that is configured in **Global Properties**, click **Use default proxy settings**.

- To use a proxy server for this Security Gateway:
  a. Click **Use custom proxy settings for this network object**.
  b. Click **Use proxy server**.
  c. Enter the IP address and **Port** of the Web proxy server.

6. Click **OK**.
7. Install Policy.

   DLP only scans traffic to the specified web proxy.

Procedure 2

1. In SmartConsole, click **Gateways & Servers** and double-click the **Security Gateway**.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Data Loss Prevention** > **Protocols**.
3. Make sure that **HTTP** is selected for this Security Gateway or for the **default protocols**.
4. From the navigation tree, click **Network Management** > **Proxy**.
5. Click **Use custom proxy settings for this network object**.
6. Click **Use proxy server**.
7. Enter the IP address and **Port** of the Web proxy server.
8. Click **OK**.
9. Install Policy.

Configuring a Pre-R75 DLP Gateway for a Web Proxy

For a pre-R75 DLP Gateway, if you have one Web proxy between the DLP Gateway and the Internet, use **Procedure 1**:

Procedure 1

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Data Loss Prevention** > **Protocols**.

3. Make sure that **HTTP** is selected for this Security Gateway or for the **default protocols**.
4. From the navigation tree, click **Network Management** > **Proxy**.
5. Configure the proxy server settings:
   - To use the proxy server that is configured in **Global Properties**, click **Use default proxy settings**.
   - To use a proxy server for this Security Gateway:
     a. Click **Use custom proxy settings for this network object**.
     b. Click **Use proxy server**.
     c. Enter the IP address and **Port** of the Web proxy server.
6. Click **OK**.
7. In SmartConsole, install the policy.

   DLP only scans traffic to the specified web proxy.

If you have more than one Web proxy, put the DLP Gateway between the proxies and the Internet.

Configuring DLP for an Internal Web Proxy

If the DLP Gateway is between the Web (HTTP) proxy server or servers and the Internet, use these procedures.

Configuring the DLP Gateway for an Internal Web Proxy

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartConsole opens and shows the **DLP** tab.
2. From the navigation tree, click **Additional Settings** > **Protocols**.
3. Click **HTTP**. Either for the Security Gateway, or on the **default protocols**.
4. Click **OK**.
5. From the navigation tree, click **My Organization**.
6. In the **Networks** section, if **Select specific networks and hosts** is selected, do these steps:

a. Click **Edit**.

b. In the **Networks and Hosts** window, make sure that the internal Web Proxy is listed. Or click **Add**, and select the objects for the internal Web Proxy.

c. Click **OK**.

7. Click **Save** and then close SmartDashboard.
8. In **SmartConsole**, install policy.

Configuring Proxy Settings after Management Upgrade

For a Security Management server that is upgraded from R70 and lower, traffic that passes through a DLP Gateway to a web proxy server contains the Security Gateway's IP as the source address instead of the original client IP address. For new installations and for installations that were upgraded from R71, the original client IP address is used.

If the traffic that contains the Security Gateway's IP as source address reaches another Security Gateway which either logs traffic or enforces access based on identity, the source IP address does not represent the user's IP address.

Using the client's IP address as source address for the traffic leaving the DLP Gateway

1. On the SmartConsole computer, run:

   ```
   C:\Program
   Files\CheckPoint\SmartConsole\R80.30\PROGRAM\Database Tool
   (GuiDBEdit Tool).exe
   ```

2. Log in with your SmartConsole credentials.
3. In the left pane, select **Table** > **Network Objects** > **network_objects**.
4. In the right pane, select the DLP Gateway.
5. In the bottom pane, in the Field Name column, select **firewall_settings**.
6. Change the `http_unfold_proxy_conns` attribute to `true`.

Mail Server Required Configuration

Action Settings for DLP Rules

DLP rules have these action settings:

Action	Description
Detect	The data transmission event is logged in the **Logs & Monitor** view. Administrators with permission can view the data that was sent. The traffic is passed.
Inform User	The transmission is passed, but the incident is logged and the user is notified.
Ask User	The transmission is held until the user verifies that it should be sent. A notification, usually with a remediation link to the Self Incident Handling portal, is sent to the user. The user decides whether the transmission should be completed or not. The decision is logged and can be viewed under the **User Response** category in a log entry. Administrators with full permissions or the **View, Release, or Discard DLP messages** permission can send or discard the message.
Prevent	The data transmission is blocked.
Watermark	Tracks outgoing Microsoft Office documents (Word, Excel, or PowerPoint files from Office 2007 and higher) by adding visible watermarks or invisible encrypted text.

When you set Data Owners to be notified, a mail server becomes a required component of the DLP system.

The DLP Gateway sends mail notifications to users and Data Owners, therefore it is necessary for the Security Gateway to access the mail server as a client.

Important:

- **The mail server must be set to act as a mail relay**. This lets users or administrators with permissions to release (Send) emails that DLP captured and quarantined on **Ask User** rules.
- You must configure the mail server to trust anonymous SMTP connections from the DLP Gateway. Alternatively, if your environment requires it, configure your mail relay server to trust authenticated SMTP connections from the DLP Gateway.

Configuring Mail Relay

Configuring Settings for the Mail Relay

You can use the Data Loss Prevention Wizard to configure the settings for the mail relay.

Use these procedures to configure the settings without the Wizard

Open the DLP tab in SmartDashboard:

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.
2. From the navigation tree, click **Additional Settings** > **Mail Server**.

Configure the mail relay for anonymous SMTP connections:

1. Click **Send emails using this mail server**.
2. Select the mail server.

   If the mail server object does not exist, create it.
3. Click **OK**.

Configure the mail server object for authenticated SMTP connections:

1. Click **Send emails using this mail server**.
2. Select a mail server from the list.
3. If the mail server does not exist, create it.
4. Click **Mail Servers**.
5. Select the server from the list.
6. Click **Edit**.

   The **Mail Server** window opens.
7. Click **Server Requires Authentication**.
8. Enter the authentication credentials: **User Name** and **Password**.

Complete the Mail Relay configuration:

1. Click **Save** and then close SmartDashboard.
2. In SmartConsole, install policy.

3. On the mail server itself:

   Configure the mail relay to accept anonymous connections from the DLP Gateway. For details, consult the vendor documentation. For example, on Microsoft Exchange Servers, configure the permissions of the default receive connector (or other relevant connector that handles SMTP traffic) for anonymous users.

Configuring a Dedicated DLP Gateway and Relay on DMZ

Procedure

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. Click **Send emails using this mail server**.
3. Select the mail server.

   If the mail server object does not exist, create it.

4. Click **OK**.

Configure the mail server object for authenticated SMTP connections:

1. Click **Send emails using this mail server**.
2. Select a mail server from the list.
3. If the mail server does not exist, create it.
4. Click **Mail Servers**.
5. Select the server from the list.
6. Click **Edit**.

   The **Mail Server** window opens.

7. Click **Server Requires Authentication**.
8. Enter the authentication credentials: **User Name** and **Password**.

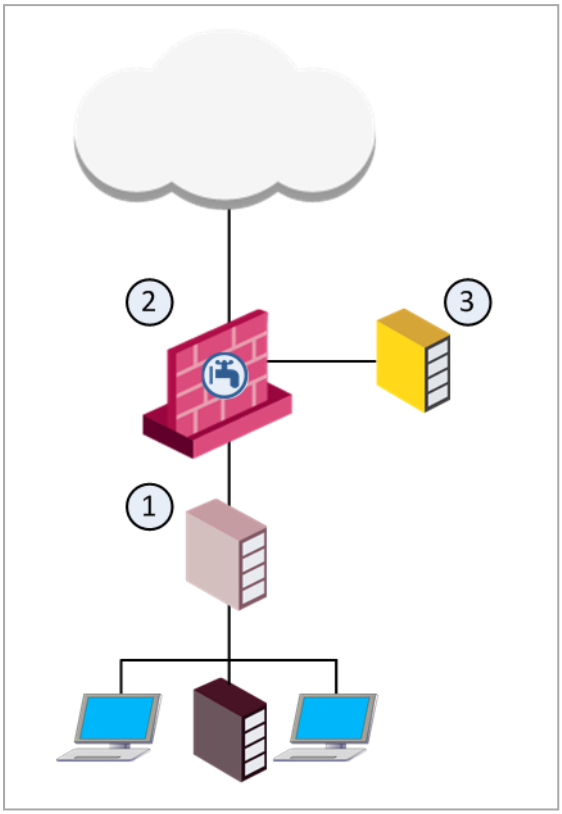
Complete the Mail Relay configuration:

1. Click **Save** and then close SmartDashboard.
2. In SmartConsole, install policy.
3. On the mail server itself:

Configure the mail relay to accept anonymous connections from the DLP Gateway. For details, consult the vendor documentation. For example, on Microsoft Exchange Servers, configure the permissions of the default receive connector (or other relevant connector that handles SMTP traffic) for anonymous users.

4. In SmartConsole, install policy.

Recommended Configuration - DLP Gateway with Mail Relay



Item	Description
1	Internal mail server
2	DLP Gateway
3	Mail relay in the DMZ

Make sure that the DLP Gateway does NOT scan emails as they pass from the mail relay to the target mail server in the Internet.

Configuring the internal mail relay behind a DMZ interface of the DLP Gateway

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The **Security Gateway Properties** window opens and shows the **General Properties** page.

2. Make sure that mails from the internal mail server (for example, Microsoft Exchange) (1) arrive at the Security Gateway using an internal Gateway interface.

a. From the navigation tree, click **Network Management**.

b. Double-click the Security Gateway interface that leads to the internal mail server.

c. From the **General** page, click **Modify**.

d. In the **Leads To** section, click **Override** > **This Network (Internal)** > **Network defined by the interface IP and Net Mask**.

e. Click **OK** and close the interface window.

3. Configure the internal mail relay (2) behind a DMZ interface of the DLP Gateway:

   In the **Topology** page of the DLP Gateway object, define the Security Gateway interface that leads to the Mail relay as **Internal** and also as **Interface leads to DMZ**.

4. In the **Networks** section of the **My Organization** page:

   a. Select **Anything behind the internal interfaces of my DLP Gateways**

   b. Do NOT select **Anything behind interfaces which are marked as leading to the DMZ**

Configuring the internal mail relay that is not behind a DMZ interface of the DLP Gateway

Note - If the DLP Gateway interface leading to the internal mail relay is internal, and you cannot configure the internal mail relay behind a DMZ interface of the DLP Gateway.

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **My Organization** page.

3. In the **Networks** section, click **Select specific networks and hosts**.

4. Click **Edit**.

5. Select the networks that include the internal mail server, but do NOT include the relay server.

6. Click **OK**.

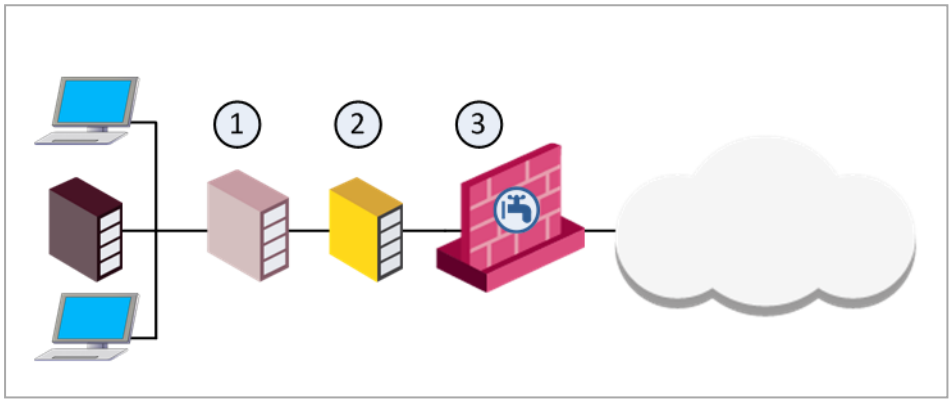
7. Click **Save** and then close SmartDashboard.

8. In SmartConsole, install policy.

Workarounds for a Non-Recommended Mail Relay Configuration

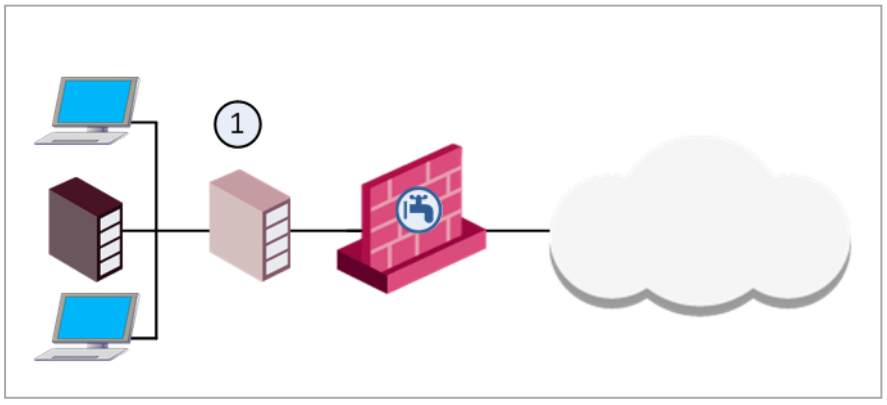
A non-recommended configuration is to have the DLP Gateway scan emails as they are sent from an internal mail relay that is in My Organization to the target mail server in the Internet. In this configuration, the DLP Gateway communicates with the target mail servers on behalf of the mail relay. If the target mail server does not respond, some mail relays (such McAfee IronMail, postfix 2.0 or earlier and qmail) do not try the next DNS MX record, and so does not try to resend the email to another SMTP mail server in the same domain.

- The internal mail server (1) and the internal relay (2) are in My Organization



Item	Description
1	Internal mail server
2	Internal mail relay
3	DLP Gateway

- The internal mail server (1) is in My Organization, and there is no other internal mail relay



Why Some Mail Relays Do Not Resend Emails

If the mail relay does not succeed to send an email because the target mail server does not respond, the mail relay resends the email to another SMTP server in the same domain. The relay sends the mail to the next DNS MX record.

Most mail relays try the next MX record if it is impossible to get an access to the target, or if the target server returns a 4xx SMTP error. However, other mail relays (such as Mcafee IronMail, postfix 2.0 or earlier and qmail) do not connect to the next MX if the target server returns a 4xx error. They do not send the email.

In these environments, the DLP Gateway communicates with mail servers in the internet on behalf of the mail relay. If the target mail server does not respond, the DLP Gateway sends a 4xx response to the mail relay in behalf of the mail server. Therefore, if your mail relay does not try the next MX when the target server returns a 4xx error, no email goes out.

Workarounds for the Non-Recommended Configurations

- Configure your internal mail relay to re-send when it receives a 4xx error from the target mail server.
- If you cannot configure your mail relay in this way, configure the DLP Gateway between two internal mail servers. For example, put the DLP Gateway in the DMZ with the relay server (see *"Configuring a Dedicated DLP Gateway and Relay on DMZ" on page 41*).
- If you cannot apply these workarounds, see sk58960.

Untrusted Mail Relays and Microsoft Outlook

If Outlook does not trust the mail relay server, it fails to correctly render the **Send** and **Discard** buttons in the violation notification email. The buttons render correctly only after the mail relay is trusted and a new email sent.

To avoid this issue, instruct users to add the mail relay address to Outlook's safe senders list.

TLS-Encrypted SMTP Connections

TLS-encrypted SMTP connections are not scanned by the DLP Software Blade. If an Exchange Server uses TLS to encrypt emails, you can use the Exchange Security Agent to inspect them (see *"Configuring the Exchange Security Agent" on page 51*).

Configuring Incident Log Handling

You can configure disk management for DLP incidents.

1. In SmartConsole, click **Gateways & Servers** and double-click the log server or Security Management Server that manages the DLP logs.

   The server window opens and shows the **General Properties** page.

2. From the navigation tree, click **Logs** > **Storage**.

3. In **When disk space is below MBytes, start deleting old log files**, enter the minimum amount of free disk space on the server.

   This setting applies to DLP incidents and logs, and to all other logs. The default setting is 5000 MBytes. When the free disk space becomes less than this limit, old DLP incidents and logs, and other logs are deleted to free up disk space.

4. Click **OK**.

5. Publish the SmartConsole session.

6. Open the *Database Tool (GuiDBEdit Tool)* and log in with your SmartConsole credentials.

7. In the left pane, select **Table** > **Network Objects** > **network_objects**.

8. In the right pane, select the Log server or Security Management Server that manages DLP logs.

9. In the bottom pane, in the **Field Name** column, find **log_policy**.

10. **Configure these fields**

Field Name	Description	Default value
`dlp_blob_delete_above_value_percentage`	The maximum % of disk space that incidents are allowed to occupy.	20%

Field Name	Description	Default value
`dlp_blob_delete_on_above`	Whether or not to delete incidents if the incidents take up more disk space than `dlp_blob_delete_above_value_percentage`. ■ `true` - Delete incidents. However, logs that are associated with the incidents are not deleted. ■ `false` -Do not delete incidents. Incidents are only deleted if free disk space becomes less than the **Required Free Disk Space** that is configured in SmartConsole, in the **Logs and Masters** page of the Log server or Security Management Server that manages DLP logs.	`false`
`dlp_blob_delete_on_run_script`	Whether or not to run a script before deleting incidents. For example, to copy the logs to a different computer before they are deleted. ■ `true` - Run the script that is defined in SmartConsole, in the Log server or Security Management Server that manages DLP logs, in the **Logs and Masters** > **Advanced** page. ■ `false` - Do not run a script.	`false`

Configuring the Exchange Security Agent

Internal emails between Microsoft Exchange clients use a proprietary protocol for Exchange communication. This protocol is not supported by the DLP Gateway. To scan internal emails between **Microsoft Exchange** clients, you must install an Exchange Security Agent on the **Exchange Server**. The agent sends emails to the DLP Gateway for inspection using the SMTP protocol encrypted with TLS. You must have a connectivity between the Exchange server and the DLP Gateway.

An Exchange Security Agent must be installed on each Exchange Server that passes traffic to the DLP Gateway. Each agent is centrally managed through SmartConsole and can only send emails to one DLP Gateway.

If your organization uses Exchange servers for all of its emails, you can also use this setup for scanning all emails.

To use the Exchange Security Agent it is necessary to configure settings in SmartConsole and on the Exchange server.

For more about using the Exchange Security Agent to examine internal emails, see some scenarios (see *"Out of the Box" on page 90*).

Configuring SmartConsole for the Exchange Security Agent

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Gateways**.

3. Click **Actions** > **New Exchange Agent**.

   The **Check Point Exchange Agent** wizard opens.

4. Click **Next**. There are four pages in the wizard:

   - **General**

     a. Use the **General** page to enter information for the Exchange Security Agent.

Object	Description
Name	Enter a name for the Exchange Security Agent.
Inspected Exchange Server	Select the host object that represents the **Exchange server** on which the Exchange Security Agent is installed. If necessary, click **New** to create one.
Exchange contact person (optional)	You can select the user object that represents the **Exchange server administrator**.
Enforcing DLP Gateway	Select the DLP Gateway object that get emails for the inspection from the Exchange Security Agent. If you use a name to represent the DLP Gateway in the Exchange Security Agent on the Exchange server, make sure to use the same name as this object.

     b. Click **Next**.

- **Trusted Communication**

  a. Use the **Trusted Communication** page - Enter the one-time password used to initialize SIC (Secure Internal Communication) between the Exchange Security Agent and the enforcing DLP Gateway. This step creates a security certificate that is then used by the Exchange Security Agent.

  b. Use the **One-time password** option - Enter the one-time password and confirm it. Make sure that the same one-time password is entered in the Trusted Communication window of the Exchange Security Agent snap-in on the **Exchange server**.

  c. Click **Next**.

- **Inspection Scope**

  a. Use the **Inspection Scope** window to define which emails to send for inspection. You can select all users or only specified users or user groups. It is recommended to start with specified users or user groups before inspecting all emails.

  Note - You can define users or groups that do not get emails for inspection in an **Exceptions** list. You can also set a percentage of emails to inspect for the rest of the organization. This lets you gradually increase the inspection coverage of your organization's emails.
  To define these options, edit the Exchange Security Agent in SmartConsole and open the Inspection Scope page.

  - **Inspect emails sent only by these users or user groups** - Define the Active directory, internal or LDAP users, to inspect their emails.
  - **Inspect all emails** - The Exchange Security Agent sends all emails to the enforcing DLP Gateway for inspection.

  b. Click **Next**.

- **Configuration Summary**

To install the Exchange Security Agent:

a. On the Exchange Server, download the DLP Exchange agent MSI from the R81.20 Home Page:

i. From the Table of Contents, select **Tools**.

ii. Click **Show / Hide the download matrix**.

iii. In the **Agents** section, download the DLP Exchange agent MSI.

b. Do the steps of the installation wizard.

5. Complete the wizard. Click **Save** and then close SmartDashboard.
6. In **SmartConsole**, install policy.

Exchange Server Configuration

After the Exchange Security Agent has been installed on the Exchange server, you can:

- **Initialize trusted communication between the Check Point Exchange Security Agent and the Security Gateway**

  There are two possible communication states:

  - **Uninitialized** is where trusted communication has not been established.
  - **Trust established** is where the Exchange Security Agent got the security certificate and can get data securely from the Security Gateway.

  To initialize trusted communication:

  1. On the Exchange server, open the Exchange Security Agent: **Start > Check Point > Check Point Exchange Agent > Configure Check Point Exchange Agent**.
  2. In the Navigation pane, click **Check Point Exchange Agent**.
  3. Click **Communication**.

     The Trusted Communication window opens.
  4. Enter information in these fields:
     - **Gateway name or IP** - The same name or IP that is given to the DLP Security Gateway in SmartConsole.
     - **Exchange agent object name** - The same name that is set for the Exchange agent object in SmartConsole.
     - **One time password** - Used only for establishing the initial trust. When trust is established, trust is based on security certificates. This password must be the same as the one time password defined for the Exchange Security Agent in SmartConsole.
  5. Click **Initialize** to start the trusted communication procedure.

- **Start or stop the Exchange Security Agent that runs as an extension of the Microsoft Exchange Transport service**

  The Exchange Security Agent runs as an extension of the Microsoft Exchange Transport service. When you start or stop the agent. Each time you start or stop the agent, you restart the Microsoft Exchange Transport service.

  After you click **Start**, messages are sent to the Security Gateway for DLP inspection. The messages sent are based on the users or groups defined for inspection.

To start the Exchange Security Agent:

In the **Check Point Exchange Agent** window, click **Start**.

- **Exchange Security Agent statistics**

  The Statistics page in the Exchange Security Agent shows performance statistics and the number of emails it handles and sends to the Security Gateway.

  The graph you see in the window is the Windows Performance Monitor graph. It shows some of the Windows counters plus the `CPExchangeAgent` counters. Alternatively, you can use the Windows Performance Monitor and add the `CPExchangeAgent` counters.

  Statistics shown:

  - **Latency per any message** - The average latency in seconds of all email messages that go through the Exchange Security Agent.
  - **Latency per scanned message** - The average latency in seconds of all email messages that go through the Exchange Security Agent and are then sent to the Security Gateway for inspection.
  - **Message queue length** - Then number of emails that are currently being handled by the Exchange Security Agent.
  - **Total messages** - Total number of emails handled by the Exchange Security Agent.
  - **Scanned messages** - Total number of emails inspected by the DLP policy (includes dropped and allowed messages).
  - **Dropped messages** - Emails dropped after being inspected by the DLP policy.

- **Monitor message status with the Message Tracking log - Message Tracking**

  In the **Message Tracking** window you can see logs for each message that goes through the Exchange Security Agent. You can do a **search** on all of the fields in the log and **refresh** the log.

  You can see these values in the Event Id column

Value	Description
Receive	The message has been received by the Exchange Security Agent. The Reason column for this entry is always blank.
Release	The message has been inspected by DLP and has been sent to its destination.

Value	Description
Drop	The message has been dropped by DLP and has not been sent to its destination.
Bypass	The Exchange Security Agent has not sent the message to DLP for inspection. The message is sent to its destination.

The possible reasons for each of the event IDs

Event ID	Reason
Receive	Empty - indicates that the message is being handled by the Exchange Security Agent
Release	Tap mode - when all of the rules in the Rule Base are detect or inform, the Exchange Security Agent automatically sends the message to its destination. The agent does not receive a response from the Security Gateway
	Scanned by Security Gateway
	Timeout
Drop	Dropped by Security Gateway - after Security Gateway inspection the message matched an ask or prevent rule
Bypass	DLP scanning is disabled - when DLP inspection is not enabled on the Security Gateway
	Fail open active - if one of the bypass settings in the Advanced window is matched
	Message is too big
	Incoming message scanning is disabled
	Internal message scanning is disabled
	Incoming message scanning from other domains is disabled
	Sender is included in the Inspection Scope exceptions
	Sender is not included in Inspection Scope settings

- **Advanced: configure when to bypass inspection of messages**

In the Advanced window you can configure log parameters and when not to send emails to the Security Gateway for DLP inspection.

The available options:

- **Enable debug logs** - Enables logs that contain debugging information about each email received (this is mainly for Check Point support).
- **Bypass inspection of a single email after timeout of X seconds** - Defines the timeout of sending an email to the Security Gateway for inspection. The default value is 60. The valid range of values is 1 to 120.
- **Bypass email inspection for X seconds if:** - Defines the time interval to not inspect emails. The default value is 120. The valid range of values is 30 to 3600.

  Email inspection is bypassed in these situations:

  - **Additional latency exceeds X seconds** - When the added average latency of traffic passing through the Exchange Security Agent is more than the defined time interval. The default value is 10. The valid range of values is 1 to 60.
  - **Emails queue length exceeds X emails** - When the number of emails in the Exchange queue is more than the defined number of emails. The default value is 50. The valid range of values is 1 to 300.
  - **Exchange server CPU usage exceeds X %** - When the Exchange server CPU uses more than the defined percentage. The default value is 90. The valid range of values is 20 to 100.
  - **Gateway doesn't respond to the last X emails** - When the Security Gateway does not respond to the last defined number of attempts. The default value is 25. The valid range of values is 1 to 100.

Configuring SMTP Mirror Port Mode

In Mirror Port Mode, the DLP Gateway scans SMTP and HTTP traffic for possible violations. The DLP Gateway connects to the SPAN port of a switch and monitors traffic without enforcing a policy. Mirror Port Mode lets you run a full data leak assessment of all outgoing SMTP/HTTP traffic with minimal configuration risk.

How it works

When the DLP Security Gateway is connected to a SPAN port of the switch, the Security Gateway gets a copy of all packets passing through the switch. The DLP tap mechanism builds TCP streams of SMTP and HTTP traffic. These streams are scanned by the DLP engine for possible violations of the policy.

Enabling Mirror Port Mode scanning of SMTP and HTTP Traffic

Before enabling Mirror Port Mode scanning, you must prepare the Security Gateway.

- If the Security Gateway is SecurePlatform, DLP scans traffic only on interfaces that are defined as SPAN ports.
- If the Security Gateway is Gaia, Gaia must be in *Monitor Mode*.

  Monitor Mode lets the Security Gateway listen to traffic from a Mirror port or Span port on a switch. To configure Monitor Mode on the Gaia operating system, see: sk70900.

Note - For R77.10 and higher, Mirror Port Mode scanning is enabled by default when one of the interfaces is configured as monitor mode or tap. For R77 and below, you must manually enable mirror port mode.

To enable Mirror Port Mode (for R77 and below):

use the `dlp_smtp_mirror_port` command.

Description

Enables SMTP Mirror Port Mode

Syntax

```
dlp_smtp_mirror_port {status | enable |disable}
```

Parameters

Parameter	Description
`status`	Shows the status, whether mirror port mode is enabled or disabled.

Parameter	Description
`enable`	Enables Mirror Port Mode
`disable`	Disables Mirror Port Mode

Example

```
dlp_smtp_mirror_port enable
```

Output

```
# dlp_smtp_mirror_port enable
Enabling SMTP mirror port requires running local policy
installation. continue? (yes)

yes

Installing Security Policy Standard on all.all@dlpgw

Fetching Security Policy from local succeeded

# dlp_smtp_mirror_port status
SMTP mirror port is enabled
```

Comments

SMTP mirror mode stays enabled after a Security Gateway reboot.

Configuring HTTPS Inspection

HTTPS Internet traffic uses the SSL (Secure Sockets Layer) protocol and is encrypted to give data privacy and integrity. However, HTTPS traffic has a possible security risk and can hide illegal user activity and malicious traffic. Security Gateways cannot inspect HTTPS traffic because it is encrypted. You can enable the HTTPS Inspection feature to let the Security Gateways create new SSL connections with the external site or server. The Security Gateways are then able to decrypt and inspect HTTPS traffic that uses the new SSL connections.

There are two types of HTTPS Inspection:

- **Outbound HTTPS Inspection** - To protect against malicious traffic that is sent from an internal client to an external site or server.
- **Inbound HTTPS Inspection** - To protect internal servers from malicious requests that arrive from the Internet or an external network.

A Security Gateway uses certificates and becomes an intermediary between the client computer and the secure web site. All data is kept private in HTTPS Inspection logs. Only administrators with HTTPS Inspection permissions can see all the fields in such a log.

Inspecting HTTPS Packets

Outbound HTTPS Connections

Outbound connections are HTTPS connections that arrive from an internal client and connect to an external server.

Outbound connection flow

1. An HTTPS request (from an internal client to an external server) arrives at the Security Gateway.
2. The Security Gateway intercepts the HTTPS request.
3. The Security Gateway determines whether the HTTPS request matches an existing HTTPS Inspection rule:
   - If the HTTPS request does **not** match a rule, the Security Gateway does not intercept the HTTPS connection. In this case, HTTPS Inspection is bypassed.
   - If the HTTPS request matches a rule, the Security Gateway intercepts the HTTPS connection and continues to the next step.
4. The Security Gateway validates the certificate of the external server.

   By default, the Security Gateway uses the Online Certificate Status Protocol (OCSP) standard to check for certificate revocation.

If the certificate does not support OCSP, the Security Gateway uses the Certificate Revocation List (CRL) to check for certificate revocation.

5. The Security Gateway creates a new certificate for the connection to the external server.
6. The Security Gateway decrypts HTTPS traffic.
7. The Security Gateway calls the enabled Software Blades to inspect the decrypted HTTPS connection.
8. If the Security Policy allows this traffic, the Security Gateway encrypts the HTTPS connection.
9. The Security Gateway sends the HTTPS request to the external server.

Inbound HTTPS Connections

Inbound connections are HTTPS connections that arrive from an external client and connect to a server in the DMZ or the internal network.

Inbound connection flow

1. An HTTPS request (from an external client to an internal server) arrives at the Security Gateway.

   Note - By design, the Security Gateway/Cluster is intentionally configured not to perform HTTPS Inspection on traffic directed towards it. To change this behavior, follow sk114574.

2. The Security Gateway intercepts the HTTPS request.
3. The Security Gateway determines whether the HTTPS request matches an existing HTTPS Inspection rule:
   - If the HTTPS request does **not** match a rule, the Security Gateway does not intercept the HTTPS connection.
   - If the HTTPS request matches a rule,the Security Gateway intercepts the HTTPS connection and continues to the next step.
4. The Security Gateway uses the certificate for the internal server to create an HTTPS connection with the external client.
5. The Security Gateway creates a new HTTPS connection with the internal server.
6. The Security Gateway decrypts the HTTPS connection.
7. The Security Gateway calls the enabled Software Blades to inspect the decrypted HTTPS traffic.
8. If the Security Policy allows this traffic, the Security Gateway encrypts the HTTPS connection.
9. The Security Gateway sends the HTTPS request to the internal server.

Configuring Gateways to Inspect Outbound and Inbound HTTPS

This section gives an example of how to configure a Gateway to inspect outbound and inbound HTTPS traffic

Workflow overview

1. Enable HTTPS Inspection on the Security Gateway.
2. Configure the Security Gateway to use the certificate for inspection.

- Outbound Inspection - Generate a new certificate for the Security Gateway.
- Inbound Inspection - Import the certificate for the internal server.

3. Configure the HTTPS Inspection Rule Base.
4. Install the Access Control Policy.

Enable HTTPS Inspection on the Security Gateway

You must enable HTTPS Inspection on each Security Gateway.

To enable HTTPS Inspection on a Security Gateway:

1. From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2. Click **HTTPS Inspection** > **Step 3**.
3. Select **Enable HTTPS Inspection**.

The first time you enable HTTPS Inspection on one of the Security Gateways, you must create an outbound CA certificate for HTTPS Inspection or import a CA certificate already configured on your organization. This outbound certificate is used by all Security Gateways managed on the Security Management Server.

Create an CA Certificate for the Outbound Inspection on the Security Gateway

The outbound CA certificate is saved with a P12 file extension and uses a password to encrypt the private key of the file. The Security Gateways use this password to sign certificates for the sites accessed. You must keep the password because it is also used by other Security Management Servers that import the CA certificate to decrypt the file.

After you create an outbound CA certificate, you must export it so it can be distributed to clients. If you do not configure the generated outbound CA certificate on clients, users receive SSL error messages in their browsers when connecting to HTTPS sites. You can configure a troubleshooting option that logs such connections.

After you create the outbound CA certificate, a certificate object named Outbound Certificate is created. Use this object in rules that inspect outbound HTTPS traffic in the HTTPS Inspection Rule Base.

Procedure

1. In SmartConsole Gateways & Servers view, right-click the Security Gateway object and select **Edit**.

   The **Gateway Properties** window opens.
2. In the navigation tree, select **HTTPS Inspection**.
3. In **Step 1** of the **HTTPS Inspection** page, click **Create**.

The **Create** window opens.

4. Enter the necessary information:
   - **Issued by (DN)** - Enter the domain name of your organization.
   - **Private key password** - Enter the password that is used to encrypt the private key of the CA certificate.
   - **Retype private key password** - Retype the password.
   - **Valid from** - Select the date range for which the CA certificate is valid.
5. Click **OK**.
6. Export and configure the CA certificate (see *"Export and Configure the Generated CA" on the next page*).

Import the CA Certificate for the Internal Server

You can import a CA certificate that is already configured in your organization or import a CA certificate created on one Security Management Server to use on another Security Management Server.

Best Practice - Use *private* CA Certificates.

For each Security Management Server that has Security Gateways enabled with HTTPS Inspection, you must:

- Import the CA certificate.
- Enter the password the Security Management Server uses to decrypt the CA certificate file and sign the certificates for users. Use this password only when you import the certificate to a new Security Management Server.

To import a CA certificate:

1. If the CA certificate was created on another Security Management Server, export the certificate from the Security Management Server on which it was created (see *"Exporting a Certificate from the Security Management Server" on the next page*).
2. In the SmartConsole **Gateways & Servers** view, right-click the Security Gateway object and select **Edit**.

   The **Gateway Properties** window opens.
3. In the navigation tree, select **HTTPS Inspection**.
4. In **Step 1** of the **HTTPS Inspection** page, click **Import**.

   The **Import Outbound Certificate** window opens.
5. Browse to the certificate file.

6. Enter the **private key password**.
7. Click **OK**.
8. If the CA certificate was created on another Security Management Server, configure it on clients (see *"Export and Configure the Generated CA" below*).

Exporting a Certificate from the Security Management Server

If you use more than one Security Management Server in your organization, you must *first* export the CA certificate with the `export_https_cert` CLI command from the Security Management Server on which it was created before you can import it to other Security Management Servers.

Command syntax:

```
export_https_cert [-local] | [-s server] [-f certificate file
name under FWDIR/tmp][-help]
```

To export the CA certificate:

On the Security Management Server, run this command:

```
$FWDIR/bin/export_https_cert -local -f [certificate file name
under FWDIR/tmp]
```

Example

```
$FWDIR/bin/export_https_cert -local -f mycompany.p12
```

Export and Configure the Generated CA

To prevent users from getting warnings about the generated CA certificates that HTTPS Inspection uses, install the generated CA certificate used by HTTPS Inspection as a trusted CA. You can distribute the CA with different distribution mechanisms such as Windows GPO. This adds the generated CA to the trusted root certificates repository on client computers.

When users run standard updates, the generated CA get in the CA list, and they do not receive browser certificate warnings.

To distribute a certificate with a GPO:

1. From the **HTTPS Inspection** window of the Security Gateway, click **Export certificate**.
2. Save the CA certificate file.
3. Use the Group Policy Management Console to add the certificate to the Trusted Root Certification Authorities certificate store.

4. Push the Policy to the client computers in the organization.

   Note - Make sure that the CA certificate is pushed to the client computer organizational unit.

5. Test the distribution by browsing to an HTTPS site from one of the clients and verifying that the CA certificate shows the name you entered for the CA certificate that you created in the **Issued by** field.

Configuring Certificates by Using Group Policy

You can use this procedure to configure a certificate to multiple client machines with Active Directory Domain Services and a Group Policy Object (GPO). A GPO can contain multiple configuration options, and is applied to all computers in the scope of the GPO.

Membership in the local Administrators group, or equivalent, is necessary to complete this procedure.

To configure a certificate using Group Policy:

1. On the Microsoft Windows Server, open the **Group Policy Management Console**.
2. Find an existing GPO or create a new GPO to contain the certificate settings. Make sure the GPO is associated with the domain, site, or organization unit whose users you want affected by the policy.
3. Right-click the GPO and select **Edit**.

   The **Group Policy Management Editor** opens and shows the contents of the policy object.
4. Open **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Publishers**.
5. Click **Action** > **Import**.
6. Do the instructions in the **Certificate Import Wizard** to find and import the certificate you exported from SmartConsole.
7. In the navigation pane, click **Trusted Root Certification Authorities** and repeat steps 5-6 to install a copy of the certificate to that store.

Configure Inbound HTTPS Inspection

Configure the Security Gateway for inbound HTTPS Inspection.

To enable inbound HTTPS traffic inspection:

1. From the SmartConsole **Gateways & Servers** view, edit the Security Gateway object.
2. Click **HTTPS Inspection** > **Step 3**.

3. Select **Enable HTTPS Inspection**.
4. Import server certificates for servers behind the organization Security Gateways (see *"HTTPS Inspection Policy" on the next page*).
5. Define an HTTPS Inspection policy:
   - Create rules.
   - Add a server certificate to the **Certificate** column of each rule.

Assign a Server Certificate for Inbound HTTPS Inspection

Add the server certificates to the Security Gateway. This creates a server certificate object

When a client from outside the organization initiates an HTTPS connection to an internal server, the Security Gateway intercepts the traffic. The Security Gateway inspects the inbound traffic and creates a new HTTPS connection from the Security Gateway to the internal server. To allow HTTPS Inspection, the Security Gateway must use the original server certificate and private key. The Security Gateway uses this certificate and the private key for SSL connections to the internal servers.

After you import a server certificate (with a P12 file extension) to the Security Gateway, add the object to the HTTPS Inspection Policy.

Do this procedure for all servers that receive connection requests from clients outside of the organization.

To add a server certificate for inbound HTTPS Inspection:

1. In SmartConsole, go to **Security Policies** > **Shared Policies** > **HTTPS Inspection**.
2. Click **Open HTTPS Inspection Policy In SmartDashboard**.

   SmartConsole opens.
3. Click **Server Certificates**.
4. Click **Add**.

   The **Import Inbound Certificate** window opens.
5. Enter a **Certificate name** and a **Description** (optional).
6. Browse to the certificate file.
7. Enter the **Private key password**. Enter the same password that was used to protect the private key of the certificate on the server.
8. Click **OK**.

The **Successful Import** window opens the first time you import a server certificate. It shows you where to add the object in the HTTPS Inspection Rule Base. Click **Don't show this again** if you do not want to see the window each time you import a server certificate and **Close**.

HTTPS Inspection Policy

The HTTPS Inspection rules define how the Security Gateways inspect HTTPS traffic. The HTTPS Inspection rules can use the URL Filtering categories to identify traffic for different websites and applications. For example, to protect the privacy of your users, you can use a rule to ignore HTTPS traffic to banks and financial institutions.

The HTTPS Inspection rules are applied to all the Software Blades that have HTTPS Inspection enabled. These are the Software Blades that support HTTPS Inspection:

- Access Control
  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention
  - IPS
  - Anti-Virus
  - Anti-Bot
  - Threat Emulation
- Data Loss Prevention

To open the HTTP Inspection Policy

1. In SmartConsole, go to **Security Policies** > **Shared Policies** > **HTTPS Inspection**.
2. Click **Open HTTPS Inspection Policy In SmartDashboard**.

HTTPS Inspection rules in SmartConsole

The fields that manage the rules for the HTTPS Inspection Security Policy.

Field	Description
No.	Rule number in the HTTPS Inspection Rule Base.
Name	Name that the system administrator gives this rule.

Field	Description
Source	Network object that defines where the traffic starts.
Destination	Network object that defines the destination of the traffic.
Services	The network services that are inspected or bypassed. By default, the services `HTTPS` on port 443 and `HTTP_and_HTTPS proxy` on port 8080 are inspected. You can add or delete services from the list.
Site Category	Categories for applications or web sites that are inspected or bypassed.
Action	Action that is done when HTTPS traffic matches the rule. The traffic is inspected or ignored (**Bypass**).
Track	Tracking and logging action that is done when traffic matches the rule.
Install On	Network objects that get the HTTPS Inspection rule. You can only select Security Gateways that have HTTPS Inspection enabled.
Certificate	The certificate that is used for this rule. ■ Inbound HTTPS Inspection - Select the certificate that the internal server uses. ■ Outbound HTTPS Inspection - Select the Outbound Certificate object that you are using for the computers in the network. When there is a match to a rule, the Security Gateway uses the selected server certificate to communicate with the source client. You can create server certificates from **HTTPS Inspection > Server Certificates > Add**.
Comment	An optional field that lets you summarize the rule.

Configuring HTTPS Inspection Rules

Create different HTTPS Inspection rules for outbound and inbound traffic.

The outbound rules use the certificate that was generated for the Security Gateway.

The inbound rules use a different certificate for each internal server.

You can also create bypass rules for traffic that is sensitive and is not inspected. Make sure that the bypass rules are at the top of the HTTPS Inspection Rule Base.

After creating the rules, install the Access Control Policy.

Sample HTTPS Inspection Rule Base

This table shows a sample HTTPS Inspection Rule Base for a typical policy. (The **Track** and **Install On** columns are not shown. **Track** is set to **None** and **Install On** is set to **Any**.)

No	Name	Source	Destination	Services	Site Category	Action	Blade	Certificate
1	Inbound traffic	Any	WebCalendar Server	HTTPS	Any	Inspect	Any	WebCalendar Server CA
2	Financial sites	Any	Internet	HTTPS HTTP_HTTPS_proxy	Financial Services	Bypass	Any	Outbound CA
3	Outbound traffic	Any	Internet	HTTPS HTTP_HTTPS_proxy	Any	Inspect	Any	Outbound CA

1. **Inbound traffic** - Inspects HTTPS traffic to the network object WebCalendarServer. This rule uses the WebCalendarServer certificate.
2. **Financial sites** - This is a bypass rule that does not inspect HTTPS traffic to websites that are defined in the Financial Services category. This rule uses the Outbound CA certificate.
3. **Outbound traffic** - Inspects HTTPS traffic to the Internet. This rule uses the Outbound CA certificate.

Bypassing HTTPS Inspection for Software Update Services

Check Point dynamically updates a list of approved domain names of services from which content is always allowed. This option makes sure that Check Point updates or other 3rd party software updates are not blocked. For example, updates from Microsoft, Java, and Adobe.

To bypass HTTPS Inspection for software updates:

1. In SmartConsole, go **Manage & Settings** > **Blades** > **HTTPS Inspection** > **Configure In SmartDashboard**.
2. In SmartDashboard, click the **HTTPS Inspection** tab.
3. Click **Policy**.
4. In the Policy pane, select **Bypass HTTPS Inspection of traffic to well known software update services (list is dynamically updated)**. This option is selected by default.
5. Click **list** to see the list of approved domain names.

Manage Certificates by Gateway

The **Gateways** pane lists the Security Gateways with HTTPS Inspection enabled. Select a Security Gateway and click **Edit** to edit the Security Gateway properties.

In the CA Certificate section, you can **renew** the certificate validity date range if necessary and **export** it for distribution to the organization client machines.

If the Security Management Server which manages the selected Security Gateway does not have a generated CA certificate installed on it, you can add it with **Import certificate from file**.

- You can import a CA certificate already configured in your organization.
- You can import a CA certificate from another Security Management Server. Before you can import it, you must first export it from the Security Management Server on which it was created (see *"Exporting a Certificate from the Security Management Server" on page 66*).

Add Trusted CAs for Outbound HTTPS Inspection

When a client initiates an HTTPS connection to a web site server, the Security Gateway intercepts the connection. The Security Gateway inspects the traffic and creates a new HTTPS connection from the Security Gateway to the designated server.

When the Security Gateway establishes a secure connection (an SSL tunnel) to the designated web site, it must validate the site server certificate.

HTTPS Inspection comes with a preconfigured list of trusted CAs. This list is updated by Check Point when necessary and is automatically downloaded to the Security Gateway. The system is configured by default to notify you when a Trusted CA update file is ready for installation. The notification in SmartConsole shows as a pop-up notification or in the **Trusted CAs** window in the **Automatic Updates** section. After you install the update, make sure to install the policy. You can select to disable the automatic update option and manually update the Trusted CA list.

If the Security Gateway receives a non-trusted server certificate from a site, by default the user gets a self-signed certificate and not the generated certificate. A page notifies the user that there is a problem with the website security certificate, but lets the user continue to the website.

You can change the default setting to block untrusted server certificates.

Saving a CA Certificate

You can save a selected certificate in the trusted CAs list to the local file system.

To export a CA certificate:

1. In SmartConsole, open **HTTPS Inspection** > **Trusted CAs**.
2. Click **Actions** > **Export to file**.
3. Browse to a location, enter a file name and click **Save**.

   A CER file is created.

HTTPS Validation

In the **HTTPS Validation** page of SmartConsole you can set options for

- Fail mode
- HTTPS site categorization mode
- Server validation
- Certificate blacklisting
- Troubleshooting

To learn more about these options, see the Help. Click **?** in the **HTTPS Validation** page.

Show HTTPS Inspection Logs

The predefined log query for HTTPS Inspection shows all HTTPS traffic that matched the HTTPS Inspection policy, and was configured to be logged.

To see HTTPS Inspection Logs:

1. In the SmartConsole **Logs & Monitor** > **Logs** tab, click **Favorites**.
2. Select the **HTTPS Inspection** query.

The **Logs** tab includes an **HTTP Inspection Action** field. The field value can be *inspect* or *bypass*. If HTTPS Inspection was not done on the traffic, this field does not show in the log.

UserCheck

This section describes how to configure and use UserCheck.
When you enable the UserCheck feature, the Security Gateway sends messages to users about possible non-compliant behavior or dangerous Internet browsing, based on the rules an administrator configured in the Security Policy. This helps users prevent security incidents and learn about the organizational security policy. You can develop an effective policy based on logged user responses. Create UserCheck objects and use them in the Rule Base, to communicate with the users.

These Software Blades support the UserCheck feature:

- Data Loss Prevention
- Access Control:
  - Application Control
  - URL Filtering
  - Content Awareness
- Threat Prevention:
  - Anti-Bot
  - Anti-Virus
  - Threat Emulation
  - Threat Extraction
  - Zero Phishing

Getting Started with UserCheck for the Data Loss Prevention Software Blade:

1. In SmartConsole, in the **Security Gateway** / Cluster object:
   a. Enable the applicable Software Blades.
   b. Configure the applicable UserCheck settings.

      See *"Configuring UserCheck" on page 76*.
   c. Optional: Download the UserCheck Client and install it on endpoint computers.

      See the *R81.20 Quantum Security Gateway Guide* > Chapter "UserCheck Client".
2. Optional: In SmartConsole, in the **Global Properties**, configure the applicable UserCheck settings.
3. In SmartDashboard, configure the applicable UserCheck Interaction Objects.

See *"UserCheck Interaction Objects" on page 80*.

4. In SmartDashboard, configure the applicable Data Loss Prevention Policy.

   See:

   a. *"Data Loss Prevention Policies" on page 101*.

   b. *"Data Loss Prevention by Scenario" on page 143*.

5. In SmartConsole, install the Access Control Policy on the **Security Gateway** object.

6. Additional Configuration:

   - *"Localizing and Customizing the UserCheck Portal" on page 89*

Configuring UserCheck

Enable or disable UserCheck directly on the Security Gateway. When UserCheck is enabled, the user's Internet browser shows the UserCheck messages in a new window. If users connect to the Security Gateway remotely, set the internal interface of the Security Gateway (on the **Topology** page) to be the same as the **Main URL** for the UserCheck Portal.

To configure UserCheck on a Security Gateway

Step	Instructions
1	From the left navigation panel, click **Gateways & Servers**.
2	Double-click the Security Gateway / Cluster object.
3	In the left panel, click **UserCheck**.
4	Select **Enable UserCheck for active blades**.
5	In the **UserCheck Web Portal** section, the **Main URL** field shows the primary URL for the web portal that shows the UserCheck notifications. You can use the suggested **Main URL** or manually enter a different **Main URL**.
6	Optional: Click **Aliases** to add URL aliases that redirect different hostnames to the **Main URL**. For example: `usercheck.mycompany.com` The aliases must be resolved to the portal IP address on the corporate DNS server.
7	In the **Certificate** section, click **Import** to import a certificate that the portal uses to authenticate to the Security Management Server. By default, the portal uses a certificate from the Check Point Internal Certificate Authority (ICA). This might generate warnings if the user browser does not recognize Check Point as a trusted Certificate Authority. To prevent these warnings, import your own certificate from a recognized external authority. **Note** - After you download your certificate, you can click **Replace** to replace it with a different certificate, and click **View** to see the certificate information.

Step	Instructions
8	In the **Accessibility** section, click **Edit** to configure interfaces on the Security Gateway through which the portal can be accessed. These options are based on the topology configured in the Security Gateway object. You must configure the topology settings on the **Network Manegment** page. Select the applicable option when the Security Gateway must send users to the UserCheck Portal based on how they connect: ■ **Through all interfaces** ■ **Through internal interfaces** (default) • **Including undefined internal interfaces** • **Including DMZ internal interfaces** • **Including VPN encrypted interfaces** (default) Applies to interfaces used for establishing route-based VPN tunnels (VTIs) ■ **According to the Firewall Policy** Select this option if there is an Access Control rule that determinces who can access the UserCheck Portal. If the **Main URL** is set to an external interface, you must set the **Accessibility** to one of these: ■ **Through all interfaces** You must select this option if this is a VSX Gateway / VSX Cluster. ■ **According to the Firewall Policy**
9	**UserCheck Client** - The UserCheck Client is installed on user devices to communicate with the Security Gateway and show UserCheck Interaction notifications to users. ■ **Activate UserCheck Client support** This enables UserCheck through the UserCheck Client. ■ **Download Client** This downloads the installation file for the UserCheck Client. **Note** - The link is not active until the UserCheck Portal is up. See the *R81.20 Quantum Security Gateway Guide* > Chapter "UserCheck Client".

<table>
<tr><th>Step</th><th>Instructions</th></tr>
<tr><td>10</td><td>In the Mail Server section, configure a mail server for UserCheck.
This server sends notifications to users that the Security Gateway cannot notify using other means, if the server knows the email address of the user.
For example, if a user sends an email which matched on a rule, the Security Gateway cannot redirect the user to the UserCheck Portal because the traffic is not HTTP.
If the user does not have a UserCheck Client, UserCheck sends an email notification to the user.

■ Use the default settings
Click the link to see which mail server is configured.
■ Use specific settings for this gateway
Select this option to override the default mail server settings.
■ Send emails using this mail server
Select a mail server from the list, or click New and define a new mail server.</td></tr>
<tr><td>11</td><td>Click OK to close the Security Gateway / Cluster object.</td></tr>
<tr><td>12</td><td>If there is encrypted traffic through an internal interface, add a new rule to the Firewall Layer of the Access Control Policy.
Example rule:
<table>
<tr><th>Source</th><th>Destination</th><th>VPN</th><th>Services & Applications</th><th>Action</th></tr>
<tr><td>Any</td><td>Security Gateway on which UserCheck Client is enabled</td><td>Any</td><td>UserCheck</td><td>Accept</td></tr>
</table></td></tr>
</table>

Step	Instructions
13	Install the Access Control Policy to enable UserCheck for these Access Control Software Blades. ■ Application Control ■ URL Filtering ■ Content Awareness ■ Data Loss Prevention Install the Threat Prevention Policy to enable UserCheck for these Threat Prevention Software Blades: ■ Anti-Bot ■ Anti-Virus ■ Threat Emulation ■ Threat Extraction ■ Zero Phishing

UserCheck CLI

See the *R81.20 CLI Reference Guide* - Chapter "Security Gateway Commands" - Section "usrchk".

UserCheck Interaction Objects

This section describes how to configure UserCheck Interaction Objects.

UserCheck Interaction Objects add flexibility and give the Security Gateway a mechanism to communicate with users.

You use the UserCheck Interaction Objects in the "**Action**" column of the Data Loss Prevention Policy to:

- Help users with decisions that can be dangerous to the organization security.
- Share the organization changing internet policy for web applications and sites with users, in real-time.

Note - You must create and edit UserCheck Interaction objects for Data Loss Prevention only in SmartDashboard.

Default UserCheck Interaction Objects for Data Loss Prevention

Default Objects

1. In SmartConsole, open SmartDashboard and go to the **Data Loss Prevention** tab in one of these ways:

   In "Manage & Settings" view

   a. From the left navigation panel, click **Manage & Settings**.

   b. In the top left pane, click **Blades**.

   c. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.

   In the "Security Policies" view

   a. From the left navigation panel, click **Security Policies**.

   b. In the **Shared Policies** section, click **DLP**.

   c. In the middle of the screen, click **Open DLP Policy in SmartDashboard**.

2. From the navigation tree, click **UserCheck**.
3. These are the default UserCheck Interaction Objects:

UserCheck Interaction Object	Action Type	Description
Ask User	**Ask**	Appears when the action for the rule is **Ask**. It informs users what the company policy is for that site and they must click **OK** to continue to the site.
Blocked Message	**Block**	Appears when a request is blocked.
Cancel Page	**Cancel**	Appears after a user gets an **Inform** or **Ask** message and clicks **Cancel**.
Inform User	**Inform**	Appears when the action for the rule is **Inform**. It informs users what the company policy is for that site.
Success Page	**Approve**	Appears when the information was sent according to the user's request.
Successfully Discarded	**Discard**	Appears when the information was successfully discarded according to the user's request.

Notes:

- The UserCheck Interaction Objects you create in the future also appear on this page.
- The **Ask** and **Inform** pages include the **Cancel** button that users can click to cancel the request.
- You can preview each UserCheck Interaction page in these views:

View	Description
Regular view	Shows how the message appears in a web browser on a PC or laptop
Mobile Device	Shows how the message appears in a web browser on a mobile device
Email	Shows how the message appears in an email
Agent	Shows how the UserCheck Client shows this message

- The top toolbar provides these actions:

Action	Meaning
New	Creates a new UserCheck object
Edit	Modifies an existing UserCheck object
Delete	Deletes an UserCheck object
Clone	Clones the selected UserCheck object.

Creating New UserCheck Interaction Objects for Data Loss Prevention

Procedure

1. In SmartConsole, open SmartDashboard and go to the **Data Loss Prevention** tab in one of these ways:

   In "Manage & Settings" view

   a. From the left navigation panel, click **Manage & Settings**.

   b. In the top left pane, click **Blades**.

   c. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.

In the "Security Policies" view

a. From the left navigation panel, click **Security Policies**.

b. In the **Shared Policies** section, click **DLP**.

c. In the middle of the screen, click **Open DLP Policy in SmartDashboard**.

2. Open the required Security Policy:

   a. From the top left corner, click the **Menu** button > **File** > **Open**.

   b. Select the applicable policy.

   c. Click **Open**.

3. Create a new UserCheck Interaction Object in one of these ways:

   On the "UserCheck" page

   a. From the navigation tree, click **UserCheck**.

   b. From the top toolbar, click **New** > click the applicable UserCheck Interaction:

      i. **New Ask UserCheck**

      Shows a message to users that asks them if they want to continue with the request or not. To continue with the request, the user is expected to supply a reason.

      ii. **New Inform UserCheck**

      Shows an informative message users. Users can continue to the application or cancel the request.

      iii. **New Prevent UserCheck**

      Shows a message to users and block the application request.

   On the "Policy" page

   a. From the navigation tree, click **Policy**.

   b. Locate the applicable rule.

c. In the **Action** column, right-click > **hover** over the applicable UserCheck Interaction > click **New**:

- **Ask User**

  Shows a message to users that asks them if they want to continue with the request or not. To continue with the request, the user is expected to supply a reason.

- **Inform User**

  Shows an informative message users. Users can continue to the application or cancel the request.

- **Prevent**

  Shows a message to users and block the application request.

4. See the section *"Configuring UserCheck Interaction Objects for Data Loss Prevention" below*.

Configuring UserCheck Interaction Objects for Data Loss Prevention

Procedure

1. Create a new UserCheck Interaction Object, or open an existing UserCheck Interaction Object.

   See:

   - *"Default UserCheck Interaction Objects for Data Loss Prevention" on page 80*
   - *"Creating New UserCheck Interaction Objects for Data Loss Prevention" on page 82*

2. From the left tree, click the **Message** page:

   a. Enter a name for this object.

   b. **Optional:** Enter a comment for this object.

   c. To select a language for the message (English is the default), above the message section, click the **Languages** button > select the required languages > click **OK**.

   Note - The corresponding tab appears for each language you select.

d. To insert a variable field into the message, from the top toolbar, click **Insert Field** and click the applicable variable.

Notes:
- When the **Ask User**, **Inform User**, or **Prevent** action occurs, the UserCheck Portal and UserCheck Client replaces these variables with applicable values in the message.
- To resolve the **Username** variable, you must enable the **Identity Awareness** Software Blade and configure the required settings. See the *R81.20 Identity Awareness Administration Guide*.

e. To add your logo, in the message body, click the Check Point logo image > click **Add** > browse to the required image file and select it > click **Open**.

Notes:
- The height of the image must be 176 pixels or less.
- The width of the image must be 52 pixels or less.

f. To insert special fields for user input, from the top toolbar, click **Insert User Input** and click the applicable option.

Important:
- To change the view to raw HTML code, right-click anywhere inside the message and click **Switch to Text Mode**.
  To go back, right-click anywhere inside the message and click **Switch to HTML Mode**.
- To preview the current message, in the bottom right corner, click **Preview in browser**.

3. From the left tree, click the **Languages** page:

   If on the **Message** page you selected several languages, then on this page you can select a default language for the UserCheck message.

   This control message language if the language setting in the user's web browser cannot be determined.

4. From the left tree, click the **Fallback Action** page:

   Select an alternative action (**Allow** or **Block**) for cases when it is not possible to show the UserCheck notification in the web browser or application that caused the notification.

Fallback Action	Action	Behavior
Allow	**Inform User**	Allow the user to access the website or application. The UserCheck Client (if installed) shows the notification.
Block	**Ask User**	The Security Gateway tries to show the notification in the application that caused the notification. If it cannot, and the UserCheck Client is installed, the UserCheck Client shows the notification. Blocks the website or application, even if the user does not see the notification.

5. From the left tree, click the **Conditions** page:

   Select actions that must occur before users can access the application.

Condition	Behavior
User accepted and selected the confirm checkbox	This applies if on the **Message** page from the **Insert User Input** menu you inserted the element **Confirm Checkbox**. In the message, users must select the checkbox before they can access the application.
User filled some textual input	This applies if on the **Message** page from the **Insert User Input** menu you inserted the element **Textual Input**. Users must enter text in the text field before they can access the application. For example, you might require that users to enter an explanation for use of the application.

6. Click **OK**.
7. Preview your UserCheck Interaction in the right pane in each available view.
8. From the top SmartDashboard toolbar (**Menu** button > **File** menu), click **Update**.
9. Close SmartDashboard.
10. In **SmartConsole**, install the Access Control Policy.

Send Email Notifications in Plain Text

Not all emails clients can handle emails in rich text or HTML format.

To accommodate such clients, you can configure the Security Gateway to send email notification in plain text without images, in addition to the HTML format.

The user's email client decides which format to show.

1. Connect to the command line to the Security Gateway / each Cluster Member / Scalable Platform Security Group.
2. Log in to the Expert mode.
3. Back up the configuration file:
   - On a Security Gateway / each Cluster Member:

     ```
     cp -v $FWDIR/conf/usrchkd.conf{,_BKP}
     ```

   - On a Scalable Platform Security Group:

     ```
     g_all cp -v $FWDIR/conf/usrchkd.conf{,_BKP}
     ```

4. Edit the configuration file:

   ```
   vi $FWDIR/conf/usrchkd.conf
   ```

5. Change the value of the applicable parameter:

   from

   ```
   :send_emails_with_no_images (false)
   ```

   to

   ```
   :send_emails_with_no_images (true)
   ```

6. Save the changes in the file and exit the editor..
7. On a Scalable Platform Security Group, copy the modified file to all Security Group Members:

   ```
   asg_cp2blades $FWDIR/conf/usrchkd.conf
   ```

8. Kill the `userchkd` process to load the new configuration:

- On a Security Gateway / each Cluster Member:

```
killall userchkd
```

- On a Scalable Platform Security Group:

```
g_all killall userchkd
```

The Security Gateway / Cluster Member / Security Group automatically restarts this process.

Localizing and Customizing the UserCheck Portal

For more information, see sk83700.

Out of the Box

Default Environment

The first stage of DLP environment uses the Data Loss Prevention policy provided Out of the Box.

- Automatic inspection of data is based on built-in Check Point expert heuristics and compliance to various regulations.
- Users in your organization transmit data as a part of their daily tasks. DLP catches incidents that match rules of the policy. In this stage you set the Rules to **Detect**, it allows you to monitor usage and understand the specific needs of your organization, and you do not disrupt your users.
- You audit the data as you use experience-driven severity ratings, and the Logs & Monitor tracks to find the key data leaks.

Data Loss Prevention in SmartDashboard

To show these pages in SmartDashboard:

In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

SmartDashboard opens and shows the **DLP** tab.

DLP Tab items

Page	Function
Policy	Manage the rule base for Data Loss Prevention policy.
Whitelist Policy	Manage files that the DLP Rule Base never matches.
Data Types	Define representations of data assets to protect.
Repositories	Manage the fingerprint and whitelist repositories. The fingerprint repository contains documents that are not allowed to leave the organization. The whitelist repository contains documents that can leave the organization.
My Organization	Define the internal environment: networks, users, email addresses, and VPN communities.

Page	Function
Gateways	Enable the Data Loss Prevention Software Blade on Check Point Security Gateways. You can define DLP Gateways and Exchange Agents. An Exchange Agent lets you scan internal emails between Microsoft Exchange clients once you install the Exchange Security Agent on the Exchange Server. The table shows status, uptime, inspected items, version, CPU usage and comments for the Security Gateways and Exchange Agents. You can see a graphical representation of this information in SmartView Monitor.
UserCheck	Manage UserCheck objects that are used in a Rule Base to: ■ Help users with decisions that can be dangerous to the security of the organization. ■ Share the organization's changing internet policy for web applications and sites with users, in real-time.

Additional Settings

Page	Function
Protocols	Enable the protocols to be checked on individual DLP Gateways.
Mail Relay	Configure the mail server for DLP to send notification emails.
Email Addresses or Domains	Manage email address lists and domains for use in DLP rules and Data Types.
Watermarks	Configure the tracking option that adds visible watermarks or invisible encrypted text to Microsoft Office documents (Word, Excel, or PowerPoint files from Office 2007 and higher) that are sent as email attachments (outgoing and internal emails).

Page	Function
Advanced	■ Incident Tracking - Define whether to log all emails (to calculate ratio of incidents) or just DLP incidents. ■ Email Notifications - Define if users are notified after a DLP violation on the selected protocols. ■ Learn User Actions - Define whether DLP learns Ask User answers for all messages of a thread, or asks each time a message violates a DLP rule. ■ Extreme Conditions - Lets you define if to bypass DLP SMTP, FTP and HTTP inspection and prefer connectivity under these extreme conditions: • CPU load levels are more than the high CPU load watermark • Other extreme conditions including: ◦ Internal errors ◦ Protocol message sizes are more than the default value ◦ File attachments are more than the default value ◦ Archive depth level is more than the default value If necessary, you can change the default values (see *"Advanced Configuration" on page 244*). ■ Watermarks - Define whether watermarks are applied on DLP rules and how to handle a document that already has a watermark.
HTTPS Inspection (located in a separate tab)	Configure inspection of HTTPS / SSL traffic from enterprise networks to external destinations.

Defining My Organization

The My Organization page shows what DLP recognizes as data movement in the internal network (where data leakage is not an issue) and what is external (where data transmission must be monitored).

By default, **My Organization** includes all hosts and networks that are behind the internal interfaces of the DLP Gateway. **My Organization** also includes specific users, user groups, and all users in the LDAP groups defined in the Security Management Server.

Note - The SmartConsole must be in the Active Directory domain to take advantage of the LDAP User List features.

1. Click **My Organization**.
2. In the **Email Addresses** area, enter a domain or specific email address.
3. Click **Add**.

Adding Email Addresses and Domains to My Organization

You specify the DLP internal domains and specific email addresses that are included in My Organization. You can add domains to include your remote offices and branch offices as part of the definition of what is My Organization.

Important - If your organization uses cloud servers, you should not add them. The technology governing cloud servers makes them inherently insecure, taking the control of your data away from your administration and giving it to a third party. It is recommended to detect all sensitive data sent to and from cloud servers, rather than to trust a service provider to make sure that other clients do not have access to your data.

Add email addresses to include those that are safe for general data sharing. You should not add the private email addresses of any employees or managers. Taking home confidential data is a bad practice that you should discourage and eventually prevent.

Notes:

- When you add domains, do not use the @ sign. A valid domain example is: `example.com`
- If you add a domain, it catches all sub domains as well. For example, if the domain is `example.com`, email addresses such as `jsmith@uk.example.com` are also considered part of **My Organization**.
- SMTP traffic is considered internal if the domain of the email is specified in My Organization **and** if the IP address of the sender is an interface/network specified in My Organization.

Important - Do not remove the default domain definition. You must have a domain in the My Organization definition, or an LDAP server specified. If you do not have the domain defined (either by Email Address Domain or LDAP Account Unit) for My Organization, DLP does not scan emails.

To add domains and email addresses to My Organization:

1. In SmartConsole, open the **Data Loss Prevention** tab.
2. Click **My Organization**.
3. In the **Email Addresses** area, enter a domain or specific email address.
4. Click **Add**.

Managing Users

Most organizations use an external LDAP server (for example, Active Directory) to manage users and user groups.

Defining Internal Users

You can define an internal user account to use as a source or destination in the Rule Base when:

- Your organization does not use an LDAP server.
- You want to define a user that is not defined in the LDAP server.

You can add accounts for individual users from the **Data Loss Prevention** tab in SmartConsole.

To define user accounts as internal users:

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. From the left tree, click **Blades**.
4. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
5. Expand **User** section > **Users**.
6. Right-click **User** > **New User**.

   The **User Properties** window opens.
7. Define the user account.

   The most important field is the email address. This lets DLP recognize the user for email scans.

   The user is added to the other Software Blades managed by SmartConsole.

Defining Internal User Groups

DLP may require different user groups than those in the LDAP server. For example, you may want a group for new employees, whose rules are set to **Ask User** rather than **Prevent**, to give them time to become familiar with the organization guidelines. You may also want a group for temporary employees or terminating employees, to give them stricter rules.

To define user groups:

1. Expand **User** section > **User Groups**.
2. Right-click **User Group** > **New Group**.

The **New User Group** window opens.

3. Name the group.
4. Select the users, user groups, or external user profiles that you want in this group and click **Add**.
5. Click **OK**.

Excluding Users from My Organization

If the default option for the **Users** area is selected (**Users, user groups and LDAP groups defined in the Security Management Server**), you can define exclusions to this definition of **My Organization**.

For example, you can exclude the CEO. This lets the CEO send any data without having it scanned.

To exclude users from My Organization:

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. From the left tree, click **Blades**.
4. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
5. Open **Data Loss Prevention** > **My Organization**.
6. In the **Users** area, click **All users** > **Exclusions**.

   The **Networks and Hosts** window opens.
7. Select the listed items that you want to exclude from **My Organization**.
8. Click **Add**.
9. Click **OK**.

Managing Networks

By default, **My Organization** includes networks, network groups, and hosts that are defined as being behind the internal interface of the DLP Gateway.

In large sites it is often more efficient to define exclusions to the internal interfaces than to define the internal environment piece by piece.

Specifying Internal Networks

If you give names to specific networks or hosts to specify My Organization, then DLP considers any internal networks or hosts that you did not give a name as internal.

Note - The networks and hosts must already be defined in the Objects Tree of SmartConsole.

To define specific networks and hosts:

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. From the left tree, click **Blades**.
4. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
5. In SmartConsole, open the **Data Loss Prevention** tab.
6. Click **My Organization**.
7. In the **Networks** section, select the option **Select specific networks and host**.
8. Click **Edit**.
9. In the **Networks and Hosts** window, select items from the list of defined networks and hosts and then click **Add**.
10. Add as many items as needed to define **My Organization**.
11. Click **OK**.

Excluding Networks from My Organization

If the default option in **My Organization** is selected (**Anything behind the internal interfaces of my Security Gateways**), you can define exclusions to internal **Networks**.

Data Loss Prevention recognizes as **Outside My Org** all networks, network groups, or hosts that you specify as an exclusion. To scan data sent from these networks, you must change the default **Source** of rules from **My Org** to the network object.

To exclude networks from My Organization:

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. From the left tree, click **Blades**.
4. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
5. Click **My Organization**.
6. In the **Networks** section, select **Anything behind the internal interfaces of my DLP Gateways** and click **Exclusions**.

   The **Networks and Hosts** window opens.
7. Select the listed items that you want to exclude from **My Organization**.
8. Click **Add**.
9. Click **OK**.

Managing VPNs

Remote Access communities in **VPN** of **My Organization** are supported only in Office Mode. You can define Internal VPNs, include them in My Organization and exclude them.

Configuring Office Mode for support of Remote Access communities

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **VPN Clients** > **Office Mode**.
3. Select **Perform Anti spoofing on Office Mode addresses**.
4. In **Additional IP Addresses for Anti-Spoofing**, select the applicable network object.
5. Click **OK**.
6. Publish the SmartConsole session.

Including VPN traffic in My Organization

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.
2. From the navigation tree, click **My Organization**.
3. In the VPN section, make sure the **All VPN traffic** is selected.
4. Click **Save** and then close SmartDashboard.
5. In **SmartConsole**, click **Install Policy**.

Discovering VPNs known to DLP

1. In SmartConsole, click **Gateways & Servers**, and find the VPN Security Gateway that protects the DLP Gateway.

   For an integrated DLP configuration, this is the DLP Gateway itself. The protecting VPN Security Gateway includes the IP address of the DLP Gateway in its encryption domain.
2. Double-click the VPN Security Gateway.

   The Security Gateway window opens and shows the **General Properties** page.
3. From the navigation tree, click **IPSec VPN**.

   The DLP Gateway is aware of the VPN communities that are shown in this page.

Excluding VPNs from My Organization

1. In SmartConsole, select **Security Policies** > **Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the left tree, click **My Organization**.

3. In the **VPN** section, click **Exclusions**.

   The **VPN Communities** window opens.

4. Select the VPNs that you want to exclude from **My Organization** and click **Add**.

   Ignore the VPNs that are not relevant to the protecting VPN Security Gateway; they are excluded by default.

5. Click **Save** and then close SmartDashboard.

6. In SmartConsole, click **Install Policy**.

Data Loss Prevention Policies

The DLP policy defines which data is to be protected from transmission, including: email body, email recipients, email attachments (even if zipped), FTP upload, web post, web mail, and so on. The policy determines the action that DLP takes if a transmission is captured.

Manage the rules of the policy in the **Data Loss Prevention** > **Policy** page.

Supported Archive Types

The DLP blade supports the extraction and scanning of these compressed archive types:

- zip
- zip-exe
- rar
- 7z
- gzip
- tar
- jar

Overview of DLP Rules

A Data Loss Prevention rule consists of:

- **Flag** - your indicator for rules to handle. **No Flag, Follow Up, Improve Accuracy** - mark rules for scanning in Policy and for access from the Overview page.
- **A Data Type to protect** - some Data Types are complex, others are as simple as one word. You can make your rule base as long as needed.
- **A transmission source** - by default, your entire internal organization (the policy checks all data transmissions coming from any user in your organization containing the defined Data Type), or a selected user, group, segment, or network.

  Best Practice - Create user groups for data access. For example: users with access to highly sensitive data, newly hired employees, employees on notice of termination, managers with responsibilities over specific types of data.
- **A destination** - By default, anything that is outside of the internal organization. You may select to make the destination any network object defined in the SmartConsole to protect data movement between groups of users inside your organization. You can make the destination a specific domain, such as Gmail or Hotmail for private emails.
- **A protocol** - By default **Any**, but you can select to have the rule apply only to HTTP posts, or only to FTP uploads. To view the protocol column, right-click the heading line of the policy and select *Protocol*.
- **Exceptions** - If exceptions to this rule have been added to allow specific traffic. A value valid for the main rule is valid in an exception. Be careful! Exceptions are matched first. If a data transmission matches an exception in the policy, it stops the procedure.
- **An action to take** - DLP responses if a data transmission matches the other parameters of the rule: detect and log, inform sender or data owner, delay until user decides, or prevent the transmission.
- **A tracking option** - When data transmissions match Data Loss Prevention rules, they are logged as incidents in the Logs & Monitor view by default. You can add email notifications here and other tracking methods.
- **A severity level** - Set the severity of the rules in your policy, to help in filtering and reporting while auditing Data Loss Prevention incidents through the Logs & Monitor view. High and Critical rules should be the first that you audit and, if you decide to keep this severity level, they should be moved from **Detect** to **Ask** as soon as your users understand what is expected of them.
- **Install On** - Security Gateways with Data Loss Prevention enabled. Default value is all DLP Security Gateways.
- **A time range** - A period of time during which the DLP rule is enforced.

- **Category** - Label for types of rules. Built-in rules have default categories. To change the category of a new rule, right-click and select from the list.
- **Comment** - Optional notes for rules.

The rule base of the DLP Gateway should look familiar if you have experience with the Check Point Firewall rule base, but there are differences.

- DLP rules are based on Data Types and are created through an easy-to-use wizard. Protocols (services) used to transmit data and the people who transmit data are secondary, defining issues.
- DLP rules usually scan communications from the internal organization going out. Firewall rules usually scan communications from outside coming into the internal network.
- The method that DLP rules match data is different.

DLP and Identity Awareness

When Identity Awareness is enabled, you can create access role objects and use them in the DLP policy. When Identity Awareness is enabled, in DLP:

- Emails notifications can be sent when DLP violations occur when you use the FTP or HTTP protocols. (Before R76, DLP email notifications were only sent when the violation occurred on the SMTP protocol.)
- Access role objects can be used in the **Source** or **Destination** column of a DLP rule.
- The **Action** column of a DLP rule can redirect unknown users to the Identity Captive Portal for authentication.
- The Logs & Monitor logs identify users that violate the DLP policy.

Email Notifications for FTP and HTTP DLP violations

Together with email notifications on SMTP DLP violations, you can configure notifications to be sent when the violation occurs using the FTP or HTTP protocols.

To send the email notifications:

1. Enable Identity Awareness.
2. In **Data Loss Prevention Additional Settings Advanced > Email Notifications**, select:
   - **Web**
   - **FTP**

When you select **Web** or **FTP** in the **Email Notifications** area, the **Web** and **FTP** options are also selected in the **Learn User Actions** area. This lets DLP learn how the user decides to manage a DLP incident and apply the same decision for subsequent messages (see *"Learning Mode" on page 142*).

Access Roles in the Source or Destination of a Rule

Access role objects can be used in the **Source** or **Destination** column of a DLP rule. The presence of access roles makes DLP *user aware*. The access role object identifies users, computers, and network locations as one object. You can select specified users, user groups, or user branches as the object.

Redirection to an Authentication Captive Portal

Captive Portal redirection only applies to the HTTP and HTTPS protocols. Redirection occurs when the sender is unknown (the IP address does not map to no user in the AD) and the **Action** of the DLP rule is **Identity Captive Portal** and one of these conditions is also met:

1. No access role objects are in the **Source** or **Destination** column of the policy rule, but the **Source** and **Destination** do agree with the **Source** and **Destination** of the HTTP connection that the DLP Gateway examines.
2. The **Source** column of the DLP rule contains an access role.

With the redirection to the Captive Gaia Portal, the DLP can:

- Identify unknown users and record their FTP and HTTP activity.

  Then you can align the identified users with access roles in the policy.
- Send notification emails for FTP and HTTP violations.

  Note - Captive Portal redirection occurs:
  - To whatever data transferred in the message.
  - Before the data payload of the connection is scanned for violation of a policy rule.

To Redirect HTTP traffic to the Captive Gaia Portal:

1. Right-click the **Action** and select **Identity Captive Portal**.
2. Select **Redirect HTTP connections to an authentication Captive Portal**.
3. Click **OK**.

   The **Action** column shows **Identity Captive Portal**.

Identifying Users Behind a Proxy

If your organization uses an HTTP proxy server behind the Security Gateway, the identities of users behind the proxy shows after you configure:

- The company proxy server to use an X-Forwarded-For HTTP Header.
- The DLP Gateway to use the X-Forward-For HTTP Header.

You can also configure the DLP Gateway to strip the X-Forward-For header in outgoing traffic. Without the header, internal IP addresses are not be shown in requests to the internet.

To use X-Forwarded-For HTTP header:

1. Configure your proxy server to use X-Forwarded-For HTTP Header.
2. In SmartConsole, on the **Identity Awareness** page of the DLP Gateway object, select **Detect users located behind HTTP proxy using X-Forward-For header**.

3. To configure the DLP Gateway to stop the X Forwarded-For header that shows internal IP addresses in requests to the Internet, select **Hide X Forward-For header in outgoing traffic**.
4. Install the policy.

Example DLP rules with Identity Awareness

These three rules show how Identity Awareness works with DLP:

Rule 1

Data	Source	Destination	Protocol	Action
PCI - Credit Card Numbers	Finance_ Dept (Access Role)	Outside My Org	Any	Prevent

In this rule:

- Access role objects are used in the Source column. This rule forbid a known user in the Finance department to send credit numbers outside of the organization. It does not forbid known users that are not listed in the access role to send credit card numbers outside of the organization.
- An unknown user (a computer with an IP address that is not mapped to no user in the Active Directory) who tries to send credit card numbers outside of the organization - This rule does not stop them.
- A user that is known but not part of the access role - This rule does not forbid them to send credit card numbers.
- Unknown sender is not redirected to the Captive Gaia Portal - No identification for unknown sender.

Rule 2

Data	Source	Destination	Protocol	Action
PCI - Credit Card Numbers	My Organization	Outside My Org	Any	Prevent Identity Captive Gaia Portal

In this rule:

- Known users inside the organization no longer can send out credit card data, and receive email notification of the policy violation.

- Unknown users inside the organization that send out all types of data are directed to the Captive Gaia Portal for identification. When they are identified, DLP scans the data for a possible violation.

  Note - When you enable Identity Captive Gaia Portal on this rule, it means that HTTP or HTTPS connections that pass from inside to outside of the organization must identify with a user.

Rule 3

Data	Source	Destination	Protocol	Action
PCI - Credit Card Numbers	Finance_ Dept (Access Role)	Outside My Org	Any	Prevent Identity Captive Gaia Portal

In this rule:

- A known user in the Finance department cannot anymore send credit numbers outside of the organization.
- An access role in the Source (plus Captive Gaia Portal in the Action column) means that for HTTP connections there is a redirect if the source user is unknown and the destination agrees with the destination that the policy specifies.
- A user that is known but not part of the access role is not:
  - Prevented from distribution of credit card numbers.
  - Redirected to the Captive Gaia Portal.

DLP Rule Matching

DLP Rule Matching Order

The DLP rule order does not matter. In this rule base, each transmission is checked against each rule.

Because the rule order does not matter, you can change the display of the DLP policy for your convenience.

- To show rules in a different order, click a column header. The rules are sorted by the selected column.
- To show rules in groups, select an option from the **Grouping** menu in **Data Loss Prevention** > **Policy**.
- To show or hide columns, right-click the policy column header and select an item.
- To change the arrangement of columns, drag a column to a new position.

DLP Rule Matching with Exceptions

If data matches a rule, and the rule has exceptions, the exceptions to a rule are checked. If the data matches any exception, DLP allows the transmission.

For example, consider a rule that captures emails containing more than fifteen employee names in the body of a message. If a user in the HR department sends a list of twenty employees to an outside address (such as their contractor), the email is allowed without incident logging or any Data Loss Prevention action taken - because the same rule has an exception that allows users in the HR group to send lists of employee names outside your organization.

If the data matches multiple rules, one with an exception and one without exceptions, the rule without exceptions is used.

DLP Rule Matching with Multiple Matches

If the data matches multiple rules, the most restrictive rule is applied.

For example, if a user sends an email with an attached unencrypted PDF, the email can match two rules. One rule is **Detect**: detect emails to an external destination that contain PDF files. A second rule is **Ask User**: delay emails with PDF files that are unencrypted, until the user specifies that it is good to send. This rule in addition informs the Marketing and Technical Communications manager that the PDF was released from the company to an external destination. For more information, see *"Setting and Managing Rules to Ask User" on page 136*.

In this case:

1. The email is quarantined.
2. The user gets a notification and has to make a decision relating to what to do.
3. The data owner gets a notification.
4. The rule violations (one for **Detect** and one for **Ask User**) are logged.

DLP Rule Actions

For each DLP rule that you create for a Data Type, you also define what action is to be taken if the rule matches a transmission.

Action	Description
Detect	The transmission is passed. The event is logged, and you can review and analyze it in the Logs & Monitor view. The data and the email itself, or the properties of the transmission if not email, are saved in storage for future reference. You can notify Data Owners of the event. This is true for all the next actions as well.
Inform User	The transmission is passed, but the incident is logged and the user is notified.
Ask User	The transmission is held until the user verifies that it should be sent. A notification, usually with a remediation link to the Self Incident Handling portal, is sent to the user. The user decides whether the transmission should be completed or not. The decision itself is logged in the Logs & Monitor Logs view under the User Response category. Administrators with full permissions or with the View/Release/Discard DLP messages permission can also decide whether the transmission should be completed or not from the Logs & Monitor view. This can be useful in the event that a user is not available to make sure if it should be sent.
Prevent	The data transmission is blocked. **Best Practice** - Check Point does not recommend using the **Prevent** action as a first choice. The action may prove disruptive. To improve the accuracy of rule matches, set rules to **Prevent** only when you have tested them with the less strict actions over a reasonable amount of time.
Watermark	Tracks outgoing Microsoft Office documents (Word, Excel, or PowerPoint files from Office 2007 and higher) by adding visible watermarks or invisible encrypted text. ■ By default, all rules are created without a watermark action. ■ Watermarks can be created and edited without having to apply them. ■ Once a watermark object is created, it can be reused in multiple rules.

Note - If data matches multiple rules, the rule of the most restrictive action is applied. The order from most restrictive to least is: **Prevent, Ask User, Inform User, Detect**.

Managing Rules in Detect

The **Detect** action is set to rules by default because it is the least disruptive of the action options. When Data Loss Prevention discovers a transmission containing protected data, an incident is logged in the Logs & Monitor Logs view and other logging actions (if any) are taken.

You might want to leave all your rules in Detect at first. Then you can review the logs and decide which rules are needed according to your organization's actions. This could save you and your users a lot of time and make your explanations of what they need to know and what to do much more specific to their needs.

Setting DLP Rule Tracking

A primary consideration for creating Data Loss Prevention rules is how to audit incidents.

In the rule base of the Data Loss Prevention policy, the **Track** column offers these options:

Option	Meaning
Email	Sends an email to a configured recipient
Log	Records the incident in the **Logs & Monitor** view (All the other tracking options also log an incident).
Alert	Opens a pop-up window in the SmartView Monitor.
SNMP Trap	Sends an SNMP alert to the SNMP GUI. This uses the **fwd** process, to run the `internal_snmp_trap` script that sends an ID, the trap type, source port, community, and host name.
User Defined (alert)	Sends one of three possible customized alerts. The alerts are defined by the scripts specified in the main **Menu** > **Global Properties** > **Log and Alert** > **Alert Commands**. The alert process on the Log server runs the scripts.
Store Incident	Determines how the data should be stored and deleted (if at all). The options are: ■ Yes ■ Only as text ■ Don't store (depending on other conditions) ■ Delete

Store Incident

Store Incident tracking options determine how data that matches a DLP rule is stored (or not stored).

Available Options

Store Option	Meaning
Yes	■ Email data is stored as an `.eml` file ■ FTP data is stored in the `.zip` format. ■ HTTP • Text entered onto a web page is saved as HTML and viewed in the default browser when the data is opened through a link in the **Log Details** window. • An uploaded file is stored in the `.zip` format. **Note** - For FTP and HTTP, only those elements of the message that violate DLP rules are stored.
Only as Text	■ Textual data extracted from the email (header and body) and the attachment is stored as HTML, but only those sections that triggered the violation. ■ FTP data is stored as HTML. ■ HTTP text entered onto a web page is saved as HTML and viewed in the default browser when the data is opened through a link in the **Log Details** window. **Note** - For FTP and HTTP, only those elements of the message that violate DLP rules are shown in the HTML page which stores the information.
Don't Store	When the rule is matched, the incident is logged and the data deleted so that it cannot be viewed in the **Logs & Monitor** view. **Note** - The deletion of the data can be prevented by other store options. If a scanned message matches a number of store incident options, the option with highest priority has precedence: ■ **Delete** - Priority 1 ■ **Yes** - Priority 2 ■ **Only as Text** - Priority 3 ■ **Don't Store** - Priority 4
Delete	Logs the incident and immediately deletes the data. Select this example for sensitive data such as credit card numbers. **Note** - If the email that contains the sensitive data also has an attachment that must be watermarked, the email is not deleted. The email is saved but you cannot view it with the **Logs & Monitor** view.

Resolving Store Incident Conflicts

If a scanned message matches a number of different DLP rules, and each rule has a different store option, the option with highest priority has precedence. For example, if an email matches these rules:

Rule	Store Incident Option	Priority
Rule_1	**Only as text**	3
Rule_2	**Yes**	2
Rule_3	**Don't store**	4

The store incident option related to Rule_2 has the highest priority. The DLP Gateway stores the data even though the email matched a rule (Rule_3) configured to delete the data.

Changing the Priority

The **Only as Text** store option can be configured to have a higher priority than **Yes** To change the priority:

1. On the Security Gateway, open: `$DLPDIR/config/dlp.conf`

   Each message protocol has its own section. For example:

)

   :ftp (

   :enabled (1)

   :maximum_words_to_log (14)

   :maximum_chars_to_words_in_log (490)

   :cleanup_session_files (1)

   :save_incident_quota_percentage (85)

   :allow_append_cmd (0)

   :view_incident_dispute_option (yes)

)

2. Search for: `view_incident_dispute_option`

   The default value is `Yes`.

3. For all protocols (SMTP, FTP, HTTP), change `Yes` to `Text`.
4. Save and close `dlp.conf`.

Setting a Time Restriction

The **Time** column in the DLP Rule table holds a time object or group of time objects. The time object is the same time object as used in the Firewall Rule Base.

- A time object defines:
  - A time period during which the DLP rule is enforced (in hours) or
  - A time period defined by activation and expiration dates.
- Time objects apply for each rule.

Notes:
- A DLP rule that incorporates a time object is not enforced when the time object expires.
- Time objects are not supported for UTM-1 Edge appliances and QoS. If you install a DLP policy that contains a time object in a rule, you fail.
- An object that does not have an activation or expiration date is always active.

Creating a time object

1. Open the **Data Loss Prevention** tab > **Policy** page.
2. Right-click in the **Time** column of a rule.
3. From the pop-up menu, select **Time**.

   A window opens showing a list of existing time objects. You can select an existing time or create a new one.

   Note - Existing time object can be reused.

4. Click **New** > **Time**.
5. The **Time Properties** window opens.
6. On the **General** page, enter a name for the object
7. On the **Time** page:
   a. In the **Time Period** section, configure when the *time object* activates and expires.
   b. In the **Restrict to specific hour ranges** section, specify up to 3 ranges when the time object enforces the DLP rule. During these periods, the related DLP rule is enforced. The time specified here refers to the local time on the Security Gateway.

c. **Specify days**.

The days when the time object enforces the DLP rule. The time object can be enforcing the DLP rule each day, specified days of the week, a specified month or all months.

8. Click **OK**.

Creating a time group object

If you have more than one time object, you can merge them into a group. When a condition in one of the time objects in the group is met, the DLP rule is enforced.

1. Click the **Data Loss Prevention** tab > **Policy** page.
2. Right-click in the **Time** column of a rule.
3. From the pop-up menu, select **Group**.

   The **Time Group** window opens.
4. Enter a name for the group.
5. **Add** or **Remove** time objects from the group.
6. Click **OK**.

DLP Selective Configuration

You can configure the Data Loss Prevention rules on specific Enforcing Gateways using various data transmission protocols.

Gateways

For any rule in the policy, you can select to configure it on specific Enforcing Gateways.

To configure a rule on specific Enforcing DLP Gateways:

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. From the left tree, click **Blades**.
4. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
5. In the rule you want, click in the plus in the **Install On** column.

   Defined DLP Gateways appear in a menu.
6. Select the Gateways on which you want to configure this rule.
7. Install policy on the DLP Gateway.

Protocols

Check Point Data Loss Prevention supports various data transmission protocols.

It is recommended that you enable protocols as needed in your configuration. Start with only SMTP. Observe the logs on detected emails and user responses for handling them. Later, add FTP to the policy. For emails and large uploads, users do not expect instant responses. They can handle incidents in the Gaia Portal or UserCheck Client for emails and uploads without disturbing their work, especially if your users know what to expect and how to handle the incidents.

HTTP, which includes posts to web sites, comments on media sites, blogging, and web mail, is another matter. Users do expect that when they press Enter, their words are sent and received instantly. If an employee uses HTTP for mission-critical work, having to decide whether a sentence is OK to send or not every instance is going to be extremely disruptive. Therefore, it is recommended that you enable HTTP only after you have run analysis on usage and incidents.

You can also enable inspection for Exchange Security Agent emails (see *"Configuring the Exchange Security Agent" on page 51*) and the HTTPS protocol.

To select protocol configuration for all Security Gateways:

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. From the left tree, click **Blades**.
4. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
5. Expand **Additional Settings** and click **Protocols**.
6. Clear the checkbox of any of the protocols that you do not want to inspect.

Important - If you clear all of the protocol checkboxes, Data Loss Prevention has no effect.

To select protocol configuration per Security Gateway:

1. From the left navigation panel, click **Gateways & Servers**.
2. Double-click the Security Gateway object.
3. In **General Properties** > **Software Blades** > **Network Security**, make sure **Data Loss Prevention** is selected.
4. From the left tree. click **Data Loss Prevention**.
5. In the **Protocols** area, select one of these:
   - **Apply the DLP policy on the default protocols** - as selected in the Data Loss Prevention tab, according to the procedure before.
   - **Apply the DLP policy to these protocols only** - select the protocols that you want this Security Gateway to check for the Data Loss Prevention policy.
6. Click **OK**.
7. Install the Access Control Policy.

Auditing and Analysis of Incidents

In the process of Data Loss Prevention, analysis of incidents is essential.

Before you begin, make sure that the severity of rules in the policy is accurate.

While auditing rules in the **Logs & Monitor** view, use the Follow Up flag. If you find an incident or a set of incidents that you want to fine-tune, or for which you doubt whether the action is best, you can set the Data Type or the rule to Follow Up.

Using the Logs & Monitor Logs View

The DLP Gateway issues logs for various events.

To open the Logs & Monitor Logs view:

Go to the **Logs & Monitor** > **Logs** > **Queries** > **DLP**.

The Data Loss Prevention logs are categorized for filtering.

To see more information:

1. Click **DLP Log**.

   The **DLP Log Details** window opens. It shows more information about the incident in an easy-to-read format, with links back to the Data Loss Prevention tab in SmartConsole or to specific information on the Data Type.

2. From the log of a specific incident open the actual data that caused the incident.

   Best Practice - Do not review most of the incidents manually. The original transmission (for example, the email or its attachment) stays, in case there is a question from the sender or the data owners.

Important - You must let users know that someone can capture, store, and show personal emails and web posts. If you do not do it, you organization can have issues with local privacy laws.

Note - To view DLP incidents in the Logs & Monitor view or SmartEvent SmartConsole application on a Windows 7 computer, Microsoft Office 2010 is necessary. DLP incidents may not show if the incidents (which are in EML file format) are associated with any other application.

Event Analysis Views Available in SmartConsole

As of R80, the Event Analysis views of the SmartEvent GUI have been incorporated into the SmartConsole Logs & Monitor view. They provide advanced analysis tools with filtering, charts, and statistics of all events that pass through enabled Security Gateways.

DLP Actions

Actions for DLP incidents include:

DLP Action	Description
Ask User	DLP incident captured and put in Quarantine, user asked to decide what to do.
Do not Send	User decided to drop transmission that was captured by DLP. An administrator with full permissions or with the View, Release or Discard DLP messages permission can also drop these transmissions. Email notification is sent to the user.
Send	User decided to continue transmission after DLP capture. An administrator with full permissions or with the View/Release/Discard DLP messages permission can also decide to continue transmission. Email notification is sent to the user.
Quarantine Expired	DLP captured data transmission cannot be sent because the user did not make a decision in time. Expired incidents may still be viewed, until they are deleted (routine cleanup process).
Prevent	DLP transmission was blocked.
Allow	DLP transmission was allowed; usually by exception to rule.
Inform User	DLP transmission was detected and allowed, and user notified.
Deleted Due To Quota	DLP incidents are deleted from Security Gateway for disk space.

DLP General Columns

DLP incidents can show some or all of these columns and are available to all administrators.

DLP Columns	Description
Incident UID	Unique ID of the incident.
DLP Action Reason	Reason for the action. Possible values: Rule Base, Internal Error, Prior User Decision
Related Incident	Internal incident ID related to the current log.
DLP Transport	Protocol of the traffic of the incident: HTTP, FTP, Email.

Using the Incident UID as a key between multiple logs:

Each DLP incident has a unique ID included in the log and sent to the user as part of an email notification. User responses (Send, Do not Send) are assigned the same Incident UID that was assigned to the initial DLP incident log.

If a user/administrator sends an email with a DLP violation and then decides to discard it, two logs are generated. The first log is a DLP incident log with **Ask User** action and is assigned an Incident UID. On the user action, the second log is generated with the same UID, with the **Do not Send** action.

Each matched Data Type generates its own log. The Security Gateway makes sure that all the Data Type logs of one incident show the same unique Incident UID and rule action (Prevent, Ask, Inform, or Detect). This happens also if Data Types were matched on different rules. The same action shown for an incident is the most restrictive.

For example, in a case that a transmission matches two Data Types. Each Data Type is used in a different rule. The action of one rule is Prevent. The action in the second rule is **Detect**. The two generated logs show **Prevent** as the action. The action implemented shows **Prevent**. The log of the Detect rule shows **Rule Base (Action set by different rule)** in the **DLP Action Reason** column.

DLP Restricted Columns

These columns are restricted to administrators with permissions.

Restricted Filters	Description
UserCheck	
User Response	Comment entered by the user in the text box shown in the UserCheck notification.
UserCheck Message to User	The message shown to the user.
Interaction Name	The interaction name as shown in SmartConsole.
Fingerprint	
Matched File	The file name and path in the scanned fingerprint repository that matches the inspected message.
Matched File Percentage	How much is this file similar to Matched File. In "exact match" this always is 100%.

Restricted Filters	Description
Matched File Text Segments	In a partial match, the number of file parts/segments that are matched between the Matched File and the inspected file (parts/segment may overlap).
DLP Type	
DLP Rule Name	Name of the DLP rule on which the incident was matched.
Message to User	Message sent, as configured by administrator, for the rule on which the incident was matched.
DLP Words List	If the Data Type on which the incident was matched included a word list (keywords, dictionary, and so on), the list of matched words.
DLP Relevant Data Types	If matched Data Type is a group Data Type. This field specifies which Data Types from that group were matched.
User Information	
DLP Recipients	For SMTP traffic, list of recipients of captured email.
Mail Subject	For SMTP traffic, the subject of captured email.
Scanned Data Fragment	Captured data itself: email and attachment of SMTP, file of FTP, or HTTP traffic.
More	
UserCheck	A Boolean field that shows if the log is produced by UserCheck or by another DLP.
Data Type Name	Name of the matched Data Type.
Data Type UID	Internal ID of the Data Type on which the incident was matched.
DLP Categories	Category of Data Type on which the incident was matched.

Restricted Filters	Description
DLP Template Score	A measurement, expressed as a percentage, that shows how closely a document matches the template file. 0% - The document and template are very different. 100% - The document and template are a close match.

Data Owner and User Notifications

This section describes how to define Data Owners, prepare their corporate guidelines, communicate with the Users and with the Data Owners, set and manage the Rules to Ask User, and handle incidents from the DLP Portal and from the UserCheck Client.

Defining Data Owners

Data Owners are the people who are responsible for data, such as managers and team leaders. They have specific responsibilities beyond those of regular users. Each Data Owner should discuss with you the types of data to protect and the types that have to be sent outside.

To define Data Owners:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.
2. From the navigation tree, click **Data Types**.
3. Double-click a Data Type in the list.

   The properties window of the Data Type opens.
4. Click **Data Owners**.
5. Click **Add**.

   The **Add Data Owners** window opens.
6. Select the user or group who is responsible for this data.
7. Add as many data owners as necessary.
8. Click **OK**.
9. Click **Save** and then close **SmartDashboard**.
10. In SmartConsole, install policy.

Preparing Corporate Guidelines

Allow users to become familiar with the local guidelines for data transmission and protection. For example, corporate guidelines should ensure that your organization is compliant with legal standards (such as privacy laws) and protects intellectual property.

In particular, you must protect your organization from legal issues in companies and locations where employees are protected from having their emails opened by others. In most cases, if you tell your users that all emails that violate a DLP rule get captured and possibly reviewed, the requirements of the law is fulfilled.

You can include a link to the corporate guidelines in DLP notifications to users and to Data Owners.

When you have the corporate guidelines page ready, modify the DLP Gateway to link directly to the corporate guidelines.

To modify a DLP Gateway to link to your corporate guidelines:

1. On the Security Gateway, open: **$DLPDIR/config/dlp.conf**
2. Find the `corporate_info_link` parameter and change the value to be the URL of your corporate guidelines (format = http://www.example.com).
3. Save the file and close it.
4. Install Policy on the DLP Gateway.

Connecting with Data Owners

Before installing the first policy, send an email to Data Owners:

- Explain the Data Owner responsibility for protecting data.
- Provide an example of automated notification and discuss corporate guidelines for responding to incidents.
- Ask the Data Owners to provide the Data Types that they want protected and any exceptions.
- Decide ahead of time what exceptions you do not want to allow. For example, you can create a corporate DLP guideline that no one sends protected data to home email addresses. Organization-wide guidelines prevent conflicts if a Data Owner makes a request that is not good business practice; you can direct the Data Owner to the guidelines, and not redirect the request personally.

If you notify the Data Owner every time an incident occurs, it can overwhelm the person and reduce the effectiveness of the system. On the other hand, you must notify the Data Owner enough. Keep the balance. The notification system must help Data Owners maintain control over their data and help resolve issues of possible leakage.

Rule Action	Recommendation for Data Owner Notification
Detect	In general, you should not notify Data Owners for **Detect** rules.
Inform User	Sometimes Data Owners want to know what data is sent out, but are not ready to delay or prevent the transmission. Notification of these incidents depends on the needs of the Data Owners.
Ask User	The user handles these incidents in the Self Incident-Handling portal. Whether the Data Owner needs to be notified depends on the severity of the rule and the preferences of the individual Data Owners.
Prevent	Any rule that is severe enough to justify the immediate block of a transmission, is often enough to justify the Data Owner being notified.

Connecting with the Users

Best Practice - Before you install the first policy, let all the users in the organization know how the DLP policy works. Send an email with this information:

- Declare the date for the policy to start to work.
- Let them know that the policy works on emails, uploads, and web posts. Make sure to let users know that such transmissions can be captured and read by others if they violate DLP rules.
- Let them know that each user is expected to respond to notifications, to handle incidents and to learn from the incident about the corporate policy. Perhaps include a screen shot of the Self Incident Handling Portal and give instructions on the options that users have. Let them know that administrators with permissions can send or discard quarantined transmissions. They get email notifications when this occurs.
- Give a link to the corporate policy.
- Let them know that if they do not abide to specific rules, their managers get notification about it. These notifications contain the user's name and the type of data that was leaked.
- Give the expiration time (default is 7 days) to manage the incidents.

After you install the policy, you can set automatic notification (as part of each rule) of incidents to users. This enforces the corporate guidelines and explains to the users what happens and why, when this data is related.

When a user's action matches a rule, DLP handles the connection and logs in automatically.

Notification of DLP violations to users is an email or a pop-up from the tray client. It describes the un-allowed action and can include a link to the corporate guidelines and to the Self Incident-Handling portal. Other actions are based on the severity and action of the matched rule.

Rule Action	Recommended Communication
Detect	In general, you should not notify users for **Detect** rules.
Inform User	Transmissions are passed on Inform, but notifications at this stage help the user prepare for stricter rules later on.
Ask User	Communication is imperative in this type of rule. The user must decide how to handle the transmission. Notifications of **Ask User** incidents should include a link to the Portal, to allow the user to perform the appropriate handling option. The link to the corporate guidelines should also be included.

Rule Action	Recommended Communication
Prevent	An email for this type of rule does not offer handling options, but does provide necessary information. The user needs to know that the transmission "failed". In addition, the user should learn from the event, and change the behavior that caused the incident.

Notifying Data Owners

DLP can send automatic messages to Data Owners if an incident occurs involving a Data Type over which the Data Owners have responsibility.

Configuring Data Owner notification

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. Configure specific data owners of the Data Type:

   a. From the navigation tree, click **Policy**.

   b. Right-click the **Track** column of the rule and select **Email**.

   The **Email Notification** window opens.

   c. Click **When data is matched, send an email to the following recipients**.

   Data Owners option is selected by default.

   d. For additional email recipients, click **Add** and select the user.

   e. Configure the email text that is sent, select one of these options:

   - **Use the default text** - "`The Check Point Data Loss Prevention system has found traffic which matches a rule`".
   - **Customize** - Enter the email text.

   f. Click **OK**.

3. Click **Save** and then close SmartDashboard.

4. In SmartConsole, install policy.

To customize Notifications, see *"Customizing Notifications" on page 133*.

Notifying Users

While users learn the Organization Guidelines enforced by the DLP Gateway, take advantage of the self-education tools. The vast majority of data leaks are unintentional, so automatic explanations or reminders when a rule is broken significantly improve user leaks over a relatively short amount of time.

Best Practice:

- Configure rules of the Data Loss Prevention policy to **Inform User** - the user receives the automatic explanation about why this data is protected from leakage - but for now, the traffic is passed, ensuring minimal disruption.
- Configure rules to ask the user what to do with the captured data - send it on or delete it.

To configure user notification:

1. Connect with SmartConsole to the Management Server.
2. From the left navigation panel, click **Manage & Settings**.
3. From the left tree, click **Blades**.
4. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
5. Click **Policy**.
6. In the **Action** column of the rule to change, right-click and select **Inform User** or **Ask User**.

To customize Notifications, see *"Customizing Notifications" on page 133*.

Customizing Notifications

Notifications sent to users can be customized to match your organizational culture and needs. It is important to maintain an impersonal and nonjudgmental format.

When you handle an incident:

- Focus on the issue.
- Focus on helping users change future behavior.

User notification contains this:

- The data as an attachment (if an email).
- A subject/title that lets the user know this incident should be handled quickly.
- If the data was a zip file, the email lists the zipped files and explains why they should not be transmitted.
- Explanation of what is being done. For example:
  ```
  The message is being held until further action.
  ```

  Best Practice - Explain that the data may be read by others, for the protection of organization-wide data or legal compliance.
- Links to the Self Incident-Handling Gaia Portal, to continue, discard, or review the offending transmission.
- Link to the corporate information security guidelines.
- The main body of the email explains the rule. For example:

  ```
  The attached message, sent by you, is addressed to an external
  email address. Our Data Loss PreventionData Loss Prevention
  system determined that it may contain confidential information.
  ```

To include more information, add these fields:

Field	Description
Part name	Location of the data in violation: **Email's Body** or the name of the attachment
Rule name	Name of the rule that matched the transmission
Data objects	Name of the Data Types that represent matched data in the transmission

The next fields are applied to emails that match **Unintentional Recipient** or **External BCC** rules.

Field	Description
Internal Recipients Number	Number of intended destinations inside **My Organization**
External Recipient	List of external addresses (user@domain.com) in the destination

Customizing Notifications to Data Owners

To change the text of a notification to Data Owners:

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLPPolicy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.
2. From the navigation tree, click **Policy**.
3. Right-click in the **Track** column of a rule and select **Email**.

   The **Email** window opens.
4. Click Customize and enter the text for the email message.
5. Click **OK**.
6. Click **Save** and then close **SmartDashboard**.
7. In **SmartConsole**, install policy.

Customizing Notifications for Self-Handling

To change the text of a notification to users to handle an incident:

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLPPolicy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.
2. From the navigation tree, click **Policy**.
3. Right-click in the **Action** column of a rule and select **Edit Rule Notification**.

To notify the user and pass the data, change the action to **Inform User**.

1. In the window that opens, change the text with your own message to fit the rule. You can use text or variables.
2. Click **OK**.

3. Click **Save** and then close **SmartDashboard**.
4. In **SmartConsole**, install policy.

Setting and Managing Rules to Ask User

Important - The mail server must be able to act as a mail relay. This allows users to release (Send) emails that DLP captured on **Ask User** rules. The mail server must be configured to trust the DLP Gateway (see *"Mail Server Required Configuration" on page 39*).

Setting Rules to Ask User

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Policy**.
3. Right-click in the **Action** column of the rule and select **Ask User**.

   Ask User rules depend on the users getting notification and having options to either Send or Discard a message. Before you install a policy with new Ask User rules, make sure the DLP Gateway is set up for Ask User options.

4. Click **Save** and then close SmartDashboard.
5. In SmartConsole, click **Install Policy**.

To set up the Security Gateway for Ask User rules:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The **Security Gateway Properies** window opens and shows the **General Properties** page.

2. From the navigation tree, click **Data Loss Prevention**.
3. In the **DLP Portal** area, select **Activate DLP Portal for Self Incident Handling**.
4. From the navigation tree, click **Data Loss Prevention** > **Mail Server**.
5. Select the mail server that the DLP Gateway uses to send notification emails.
6. Click **OK**.
7. Install Policy.

Managing Rules in Ask User

You can audit the incident and the decisions that the user makes in the portal. With this information, you can quickly understand which rules should be made more specific, where exceptions are needed, and if a rule should be set to Prevent. Your users become the information security experts, simply by using the Portal.

To review these actions:

1. In SmartConsole, select **SmartConsole** > **SmartView Tracker**.
2. In the **Network & Endpoint** tab, select **Predefined** > **Data Loss Prevention** Software Blade.
3. Click the **All** query.
4. Click entries with **Ask User** in the **Action** column for the log record.
5. See the decision made in the **User Response** field.

DLP Self Incident-Handling Portal

The focus of Check Point Data Loss Prevention is user-led handling of incidents that match the rules you have created. If a user attempts to send data that should not be transmitted outside the organization, a notification is sent to the user. This email or alert includes a link to the Self Incident-Handling portal. From here, the user can explain why the email should be sent; or now realizing the importance of not sending the email, select to discard it.

This unique method of self-education for Data Loss Prevention reduces prevalent leakage from unintentional violations of the rules. This solution also reduces the cost of ownership. Your users, and your analysis of their usage, become the experts that lead your Data Loss Prevention configurations, rather than the much more time- and resource-consuming solutions of calling in an outside expert.

The DLP Portal is a Web portal that is hosted on the DLP Security Gateway. The SmartConsole administrator configures the DLP Portal URL in the Data Loss Prevention Wizard. By default, the URL is `https://<IP Address of Security Gateway>/dlp`. The administrator can change the URL in the **Data Loss Prevention** page of the Security Gateway that is enforcing DLP.

What Users See and Do

When a data transmission matches a rule with notification, the user receives an email, which contains a link to the Self Incident-Handling Portal.

The Captive Portal explains that decisions are logged.

- If the user selects to continue the transmission, they have the opportunity to explain why it should be sent before the action is completed.
- If the user selects to discard the transmission, DLP deletes the transmission immediately.
- If the user wants to review the transmission and then decide, the reasons why it was captured shows, and the user sees the links again - to send or discard it.
- The user can log into the Portal and view all UserCheck emails that were not yet handled. To see all the emails, the user clicks the login link in the Portal and gives authentication.

How Users Log in to the Self Incident-Handling Portal

Users can log into the portal in one of these ways:

- Click a link in the DLP notification email.
- Browse directly to the DLP Portal URL. The default URL is:

  `https://<IP Address of Security Gateway>/dlp`

- Right-click the UserCheck agent icon in the Task Bar notification area and select **Review DLP notifications**.

  Important - Internal Users and Administrators who authenticate in Multi-Portals on the Security Gateway must have different passwords.
  This applies to:
  - Identity Awareness Captive Portal
  - Data Loss Prevention Portal

Unhandled UserCheck Incidents

When data is captured by an **Ask User** rule, the data itself is stored in a safe area of the DLP Gateway. It stays there until the user decides to send or discard it.

If the user does not make a decision in less than the given interval, the incident expires and the data is automatically discarded. By default, time for handling incidents is 7 days. If a user is out of the office or cannot handle the incident for some other reason, an administrator can take care of it. The administrator must have full permissions or the View/Release/Discard DLP messages permission. Then, from the Logs & Monitor Logs view the administrator can send or discard the incident. Notification is sent to the user.

Three days before an unhandled incident expires, a new notification email is sent to the user. Then an email is sent at daily intervals, until the user/administrator takes care of it.

Expired incidents are logged in the Logs & Monitor Logs view. See **DLP Blade** > **Blocked**, where the **Action** of logged incidents is **Quarantine Expired**. For more information, see *"UserCheck Notifications" on page 141*.

Managing Incidents by Replying to Emails

Users can handle their incidents by replying to notification emails without entering the portal. This option is not allowed by default.

To allow users to manage incidents by replying to emails:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The **Security Gateway Properties** window opens and shows the **General Properties** page.

2. From the navigation tree, click **Data Loss Prevention**.
3. In the **Reply by Email** section, click **Allow users to manage their incidents by replying to the notification emails**.
4. Click **OK**.
5. In SmartConsole, install the policy.

UserCheck Notifications

If you configure and install the UserCheck Client on user machines, popup notifications show in the notification area.

These popups show the same information as email notifications.

For more information, see *"DLP Self Incident-Handling Portal" on page 138*.

If the incident is in the **Ask User** mode, the popups contain **Send**, **Discard**, and **Cancel** links.

Users can handle the incidents directly from UserCheck, without going to the DLP Portal.

If users click **Cancel**, they can handle the incident at a later time from their email or the Self Incident-Handling Portal.

Learning Mode

To configure learning mode for email threads, HTTP posts, or FTP uploads:

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Additional Settings** > **Advanced**.

3. In the **Learn User Actions** section, select the applicable options:

   - **Email** - When you select this checkbox, the user makes one decision for a complete thread, and that decision is applied to all messages of the same thread. When you clear this checkbox, the user is informed of all messages that match a DLP rule, even if a message is matched on carried-over text of an older message. The checkbox is cleared by default. When DLP scans Exchange emails, learning mode is also applied to Exchange traffic.
   - **Web** - When you select this checkbox, the user makes one decision for a post to a site, and that decision is applied to all posts that contain content from a post before, within 12 hours. When you clear this checkbox, the user is informed of all posts that match a DLP rule, even if a post is matched on carried-over text of an older post. The checkbox is selected by default. When HTTPS Inspection is enabled, learning mode is also applied to HTTPS posts.
   - **FTP** - When you select this checkbox, the user makes one decision for FTP uploads, and that is decision is applied to all uploads with 12 hours. When you clear this checkbox, the user is informed of all uploads that match a DLP rule, even if an upload is matched on carried over content of an older upload. This checkbox is cleared by default.

Note - For Web violations, turning off **Learn User Actions** disables the **Send** and **Discard** buttons in the UserCheck Portal. Users can only close the portal. Suspected data is not posted to the site.

Data Loss Prevention by Scenario

This section describes how to create and manage rules for Data Loss Prevention in your organization.

Analytical Configuration

After you audit incidents identified by heuristic-driven rules, you understand the needs of your organization. You can add more Data Types to the DLP policy to fit known scenarios. You can set more rules of the DLP policy to **Ask User**, to gather incident-handling data from users and better analyze their needs.

- Automatic inspection of data based on Check Point heuristics. You may select to combine provided Data Types to make your policy stricter, or to create Exceptions to allow specific conditions.
- Rules in this stage are set to **Ask User**, which lets your users learn what is acceptable and what is not, to improve accuracy, and to provide explanations for their self-handling decisions.
- In the Logs & Monitor Logs view, you review the self-handling actions and the explanations of users.

Creating New Rules

Create the rules that make up the DLP policy.

To create DLP rules:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Policy**.

3. Click **New Rule**.

   A new line opens in the rule base table. The order of rules in the DLP policy does not matter. Each DLP Gateway checks all installed rules.

4. In the **Data** column, click the plus to open the Data Type picker. Select the Data Type that you want to match against inspected content.

   If you add multiple Data Types to one rule, they are matched on **OR** - if at least one of the Data Types is matched, the rule is matched.

5. In the **Source** column, leave **My Organization** or click the plus to select a specific item from **Users, Emails, or Networks**.

   Note - If **My Organization** is the **Source**, you can right-click and select **Edit**. This opens the **My Organization** window, in which you can modify the definition of your internal organization. However, this definition is changed for all of DLP, not just this rule.

6. In the **Destination** column, select one of these:

   - Leave **Outside My Org** - to inspect data transmissions going to a destination that is not defined in My Organization.
   - Click the plus to select a specific item from **Users, Emails, or Networks**.
   - If Source is not **My Organization**, you can select **Outside Source**.

     Outside Source is a destination of a DLP rule. This value means any destination that is external to the Source. For example, if the source of the rule is Network_A, and Outside Source is the destination, then the rule inspects data transmissions that go from Network_A to any address outside of Network_A. If the destination is Outside My Org, the rule inspects only data transmissions that go from Network_A to any address outside of the organization. Use Outside to create inter-department rules.

7. In the **Action** column, do one of these:

- **Detect** (default) - To have a matching incident logged, but the data transmission is not disrupted.
- Right-click and select **Inform User** - To pass the transmission but send notification to user.
- Right-click and select **Ask User** - To wait until user decides to pass or discard.
- Right-click and select **Prevent** - To stop the transmission.

8. In the **Track** column, leave **Log** (to log the incident and have it in the Logs & Monitor Logs view for auditing), or right-click and select another tracking option.

   (Optional): To add a notification to the Data Owners:

   a. Select the **Email** option.

   b. Customize the notification that the Data Owners see if this rule is matched.

9. In the **Install On** column, select **DLP Blades** to apply this rule to all DLP Gateways, or click the [+] icon and select a specific DLP Gateway.
10. In the **Time** column, set a date and time of day that this is policy is enforced.

    A rule that uses a time object applies only to connections that begin during the specified date and time period. If the connection continues after that time frame, it is allowed to continue. The relevant time zone is that of the Check Point Security Gateway that enforces the rule.
11. In the **Category** column, right-click and select a defined category.
12. In the **Comment** column, right-click and select **Edit** to enter a comment for the rule.
13. Click **Save** .
14. Close SmartDashboard.
15. In SmartConsole, install the policy.

Internal DLP Policy Rules

Here are examples of how to create different types of rules that define when to examine traffic in environments you configure with the Exchange Security Agent (see *"Configuring the Exchange Security Agent" on page 51*).

Scenario 1: I want DLP to examine financial reports sent by users in the Finance department to all internal users (other than Finance department users) and external users. How can I do this?

- Create a rule:
  - Data = Financial Reports
  - Source = Finance Dept
  - Destination = Outside Source - rule matching occurs for all internal users other than Finance users and all external users
  - Action = Ask User

Data	Source	Destination	Exceptions	Action
Financial Reports	Finance_ Dept	Outside Source	None	Ask User

  This rule covers the scenario example. If an organization wants fuller coverage and have stricter definitions as to what traffic is allowed and by whom, the next scenario includes a wider source definition.

Scenario 2: How do I make sure that financial reports are not sent by users outside of the Finance department?

1. Create another rule.

   This rule applies to all traffic sent by all users in the organization (it includes Finance department users) to any destination.

   - **Data** = Financial Reports
   - **Source** = My Organization

- **Destination** = Any - rule matching occurs for any destination internal and external
- **Action** = Prevent

Data	Source	Destination	Exceptions	Action
Financial Reports	Finance_Dept	Outside Source	None	Ask User
Financial Reports	My Organization	Any	1	Prevent

2. To make sure there are no double matches in regards to reports sent by Finance department users, add an exception to the rule (see *"Creating Exceptions" on page 152*).

   Without an exception, if a Finance department user sends a financial report to anyone, it matches the second rule (source=My Organization) and the first rule. When data matches more than one rule, the most restrictive action is applied and multiple logs are created. So without an exception, a financial report sent from a Finance department user is blocked because of the Prevent action in the second rule and there are multiple logs that audit the incident.

   Exception Rule:

Data	Source	Destination	Protocol
Financial Reports	Finance_Dept	Any	Any

To summarize the results of these two rules:

- The *Ask User* action applies for financial reports that Finance department users send to all internal users other than Finance users.
- The *Ask User* action applies for financial reports that Finance department users send to all external users.
- The *Prevent* action applies for financial reports that each user not in the Finance department sends to each external or internal user.

Scenario 3: Financial reports can only be sent within the Finance department. A user that sends a financial report from outside the Finance department gets a notification and must make a decision that relates to what to do. How can I do this?

1. Create a rule.
   - **Data** = Financial Reports
   - **Source** = My Organization

- **Destination** = Any - rule matching occurs for any destination internal and external
- **Action** = Ask User

Data	Source	Destination	Exceptions	Action
Financial Reports	My Organization	Any	1	Ask User

2. Add an exception to not include reports sent from the Finance department to the Finance department.

Data	Source	Destination	Protocol
Financial Reports	Finance_Dept	Finance_Dept	Any

More Options for Rules

After you set up the basics of a rule, you can do more.

Viewing Rule Names and Protocols

The name of DLP rules is not visible by default, but you may need to see or change the name. For example, if you follow the logs of a rule, you can match the name in the logs to the name in the policy.

To see rule names in the policy:

1. Right-click the rule base headers.
2. Select **Name**.

By default, all rules of the DLP policy scan data over the protocols as defined in the Security Gateway properties. You can set a rule to scan only specified protocols.

To see the protocols of rules:

1. Right-click the rule base headers.
2. Select **Protocol**.

Setting Rule Severity

You can set the severity rating of a rule. This enables you to filter results and provide more relevant reports in the Logs & Monitor view .You can also sort and group the Rule Base by severity.

To set severity of a rule:

1. Go to the **Severity** column.
2. Do one of these:
   - Keep the default level (for example, **Medium**).
   - Right-click and select a severity.

Flagging Rules

You can flag a rule for different reminders. Flag a rule as **Improve Accuracy** if it did not catch data as expected. Flag a rule as **Follow up**, to set a reminder that you want to make changes to this rule or the Data Types that it uses.

You can jump to flagged rules from **Overview**. In **Policy** you can group rules by flags.

For example, you use the built-in Data Type **Employee Names** and create a new rule. You know that this is a placeholder Data Type, and you supply the list of names of employees in your organization. You flag this rule for **Improve Accuracy** and continue your work on the rule base. Later you can find the rule for Employee Names easily: group the rules by flags or by the **Overview** link. Then you can edit the Data Type. Start from **Policy**.

Best Practice - If you import Data Types from Check Point or your vendor, flag rules with these Data Types as **Follow up**, and check the results of these rules in the Logs & Monitor view as soon as you can. This ensures that you get any needed assistance in understanding the Data Types and how they can be optimally used.

To set a flag on a rule: in the Flag column, right-click and select a value.

Logs and events generated from rules that are flagged with are also marked with **Follow up**. After you view the logs and events, you can remove the **Follow up** flag.

To see logs and events generated by the Follow up rules:

1. Open **Logs & Monitor** > **Logs view**.
2. Right-click a column heading and select **Edit Profile**.
3. Add **Follow up** to the list of **Selected Fields**.

Enabling and Disabling Rules

You can define rules that you think you might need, and disable them until you want them to actually match traffic.

To enable and disable DLP rules:

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.
2. From the navigation tree, click **Policy**.
3. To disable a DLP rule, Right-click the rule to disable and select **Disable Rule**.
4. To enable a DLP rule:
   a. Right-click the disabled rule.

      It is marked with a red X in the rule base.
   b. Click **Disable Rule** to clear the selection.
5. Click **Save** and then close SmartDashboard.
6. In SmartConsole, install the policy.

Rule Exceptions

In some cases, you can create exceptions to a rule in the DLP policy.

For example, a public health clinic that must comply with the Health Insurance Portability and Accountability Act (HIPAA), does not allow patient records to leave the clinic's closed network. However, the clinic works with a specific social worker in a city office, who must have the records on hand for the patients' benefit. As the clinic's Security Administrator, you create an exception to the rule, it allows to send this data type to the specific email address. To improve this case, in the exception you can include a secondary data type, for example, a Dictionary of patient names who signed a waiver for the social worker to see their records. Thus, with one rule, you ensure that the social worker's office gets only the records that the social worker is allowed to see. DLP prevents anyone from distribution of the records to unauthorized email addresses. It ensures that no employee of the clinic deals with personal requests to send the records to unauthorized destination - it is simply impossible to do.

Creating Exceptions

To create an exception to a DLP rule:

1. In SmartConsole, select **Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. Right-click the **Exceptions** column of the rule and select **Edit**.

   The **Exceptions for Rule** window opens.

3. Click **New Exception**.

   The original rule parameters appear in the table.

4. Make the changes to the parameters to define the exception.

5. Click **Save** and then close SmartDashboard.

6. In SmartConsole, install the policy.

Creating Exceptions with Data Type Groups

You can define a combination of Data Types for an exception: "allow this data if it comes with the second type of data".

To specify complex Data Types for exceptions:

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Policy**.
3. In the **Data** column of the exception, click the plus button.
4. In the new window, select the Data Types to add to the DLP exception.
5. Click **OK**.

Creating Exceptions for Users

You can define an Exception to apply to data that comes from a specific user, group, or network: "allow this type of data if it comes from this person".

To specify Exceptions based on sender:

1. In the **Source** column, click the plus button or right-click and select **Add**.

   The list of senders includes all defined users, user groups, networks, Security Gateways, and nodes. If you make any selection, the default **My Organization** is removed.

2. Select the objects that define the source from which this data should be allowed.

   If **My Organization** is the **Source**, you can right-click and select **Edit**. This opens the **My Organization** window, in which you can change the definition of your internal organization. This definition is changed for all of DLP, not just this rule.

Creating Exceptions for Destinations

You can define an Exception to apply to data that is to be sent to specific user, group, or network: "allow this type of data if it is being sent to this person".

To specify Exceptions based on destination:

1. In the **Destination** column, click the plus button.

   The list of recipients includes all defined users, user groups, networks, Security Gateways, and nodes. If you make any selection, the default **Outside My Org** (anything that is not in **My Organization**) is removed.

2. Select the objects that define the destination to which this data should be allowed.

Creating Exceptions for Protocols

You can define an Exception to apply to data that is transmitted over a specific protocol: "allow this data if it is being sent over this protocol".

To specify Exceptions based on protocol:

1. In the **Protocol** column, click the plus button.

   The list of protocols includes DLP supported protocols. If you make any selection, the default **Any** is removed.

2. Select the protocols through which this data should be allowed.

Fine Tuning

This section describes more precise adjustment of the rules for Data Loss Prevention in your organization.

Customized Configuration

Check Point DLP provides the **MultiSpect** set of features. These features provide the flexibility you need to monitor and ensure accuracy of your DLP configuration. For example, if you find incidents that called for actions but should have passed without delay, you can change the Data Types and/or the rules to ensure that this does not occur again. In this way you fine-tune DLP over a relatively short amount of time to create a trustworthy implementation.

You can also include User Decisions to fine-tune Data Types and rules. How useful this information is depends on how well you communicate with users. Make sure they know that their input can influence the DLP - if they want a type of data to be sent without delay, and can explain why, you use their logged decisions to change the rules.

MultiSpect includes:

- **Compound Data Type** - This data type enables you to join multiple Data Types in AND and NOT checks. A rule using this a compound data type matches transmissions that have all the AND types, but does not include any of the NOT types.
- **Data Type Groups** - You can group together multiple Data Types of any category. The Data Types, when used in a rule, match transmissions on an OR check.
- **CPcode Data Type** - The CPcode syntax provides unmatched flexibility. You create the data type and its features, with all the power of an open programming language. Change the code as needed to improve accuracy, and to allow messages that user decisions tell you should be passed.
- **Flags** for Data Types and Rules - While managing Data Types and reading the logs and analysis of DLP usage, use the flags on Data Types and on rules to help ensure accuracy. Flagged Data Types and rules are added to the Overview page for efficient management.
- **Placeholder Data Types** - Several provided Data Types describe dictionaries and keywords that you should customize with your own lists. For example, the empty placeholder **Employee Names** should be replaced with your own list of employees. This Data Type is used in compound Data Types and provided rules. Placeholders are flagged with the **Improve Accuracy** flag out-of-the-box.

In this stage, you may decide to set some rules to **Prevent**. When DLP captures a Prevent incident, the data transmission is stopped completely; the user has no option to continue the send.

 **Best Practice** - Include notification to data owner and to user in such rules.

Setting Rules to Prevent

To set a rule to Prevent:

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Policy**.
3. In the **Action** column of the rule to change, right-click and select **Prevent**.
4. Click **Save** and then close SmartDashboard.
5. In SmartConsole, install policy.

Multi-Realm Authentication Support

One of the ways DLP authenticates users is by querying the Active Directory servers configured in SmartConsole. If a legitimate user has multiple accounts on different AD servers, each account associated with a different password, the user may fail to authenticate. DLP validates the user according to the credentials supplied by the first AD server to respond. To help prevent this error, and decrease the load created by constantly querying all AD servers, you can define which AD servers DLP queries when:

- A user enters credentials for the DLP portal or UserCheck agent
- DLP looks up an email address extracted from SMTP traffic to identify a user

To define AD servers Using Database Tool (GuiDBEdit Tool):

1. Open **Database Tool (GuiDBEdit Tool)**.
2. On the **Tables** tab, open **Other > authentication_objects**.
3. In the **Object Name** column, select `DLPSenderRealm`.
4. In the **Field Name** column, double-click the `ldap_au` container.

   The **Add/Edit Element** window opens.
5. In the **Object** list, select only those servers DLP must query for authentication purposes.

   On a network that contains ten AD servers, perhaps only two of them must be queried. Edit the list to include only the required AD servers.

   Note - These AD servers must first be defined in SmartConsole.
6. Click **OK**.
7. Save the database and close **Database Tool (GuiDBEdit Tool)**.
8. Install the updated policy on the DLP enabled Security Gateway.

Troubleshooting DLP-Related Authentication Issues

The Check Point database tool, Database Tool (GuiDBEdit Tool), has a number of properties that set default authentication values. These properties can be used in troubleshooting DLP related authentication issues. These objects are found under: **Database Tool (GuiDBEdit Tool)** > **Tables** > **Other > authentication_objects**:

Object	Description
`DLPSenderRealm`	Controls authentication for the DLP portal and the UserCheck agent. This object contains: ■ `Fetch_options > do_internal_fetch` True by default, meaning DLP does the email look up against user accounts in SmartConsole. ■ `Fetch_options > do_ldap_fetch` True by default, meaning if DLP fails to identify the user through a user account in SmartConsole, it then queries the AD servers defined in the `ldap_au` container object. ■ The `ldap_au` container holds objects that represent AD servers. Use `DLPSenderRealm` to solve authentication problems.
`dlp_ldap_auth_settings`	This object controls how DLP identifies users by querying the email address attribute in the Active Directory. Use this object to troubleshoot problems involving email look up in the Active directory. The `CustomLoginAttr` string lets you enter a custom LDAP query with a specified email address. The default query is: `|(mail=<<>>)(proxyAddresses=smtp:<<>>)` By default, it searches for the user with the specified email address. To refine the query, you can add other AD attributes to the query or change existing ones. **Warning** - Changing this default query might affect DLP rules that enforce a policy according to users or user groups defined by access roles. *Known* users may become *Unknown* and the data they send is allowed to leave the organization.
`dlp_internal_auth_settings`	This object controls how DLP identifies users by querying the email address attribute in the database of internal users defined in SmartConsole.

Specifying Data Types

The optimal method for defining new data type representations is to use the Data Type Wizard.

To add a new data type:

1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Data Types**.
3. Click **New**.

   The **Data Type Wizard** opens.

4. Enter a name for the new data type.
5. Select an option that specifies the type of traffic. a rule that contains this data type checks this type of traffic.
6. Enter the applicable properties in the next step (each step is relevant to the option selected in the step before).
7. Click **Finish**.
8. Click **Save** and then close **SmartDashboard**.
9. In SmartConsole, install policy.

Protecting Data by Keyword

You can create a list of keywords that to match them against data transmissions. Transmissions that contain this list of words in their data are matched. You specify how to match it (based on an ALL or ANY option).

To create a Data Type representation of specified keywords:

1. In the **Data TypeWizard**, select **Keywords**.
2. Click **Next**.
3. In the **Specify Keywords** window, enter a keyword to protect.
4. Click **Add**.
5. Enter as many keywords or phrases as you want in this data type.

   You must go for one of these options to match data:

   - If all the keywords in this list are matched.
   - If only one match is enough.
   - If a specific number of keywords is matched.

   For example, if you want to ensure that no one can send an email that contains the names of congressmen in a committee, make their names the keywords, and your options are - the **Threshold** to **At least 1**. The higher the threshold, the more precise the results are.

   If you want to allow emails that mention the congressmen, but decide that all of their names in one email are suspicious, then set **Threshold** to **All words must appear**.
6. Click **Next**.
7. Click **Finish**.
8. (Optional) To add more parameters to the Data Type, select the checkbox. Click **Finish**.

Protecting Data by Pattern

You can create a regular expression matched against content in data transmissions. Transmissions that contain strings that match the pattern in their data get matched.

Note - Use the Check Point supported regular expression syntax.

To create a data type representation of a pattern:

1. In the **Data Type Wizard**, select **Pattern (regular expressions)**.
2. Click **Next**.
3. Enter a pattern to match against content.
4. Click **Add**.
5. Enter as many regular expressions as you want in this data type.

   You must go for one of these options to match data type:

   - If the pattern is matched even once.
   - Allow it until a given number of times.

     For example, if you want to ensure that no one can send an email that contains a complete price-list of five products, set the pattern to "^[0-9]+(\.[0-9]{2})?$" and set the **Number of occurrences** to **5**.
6. Click **Next**.
7. Click **Finish**.
8. (Optional) To add more parameters to the Data Type, select the checkbox. Click **Finish**.

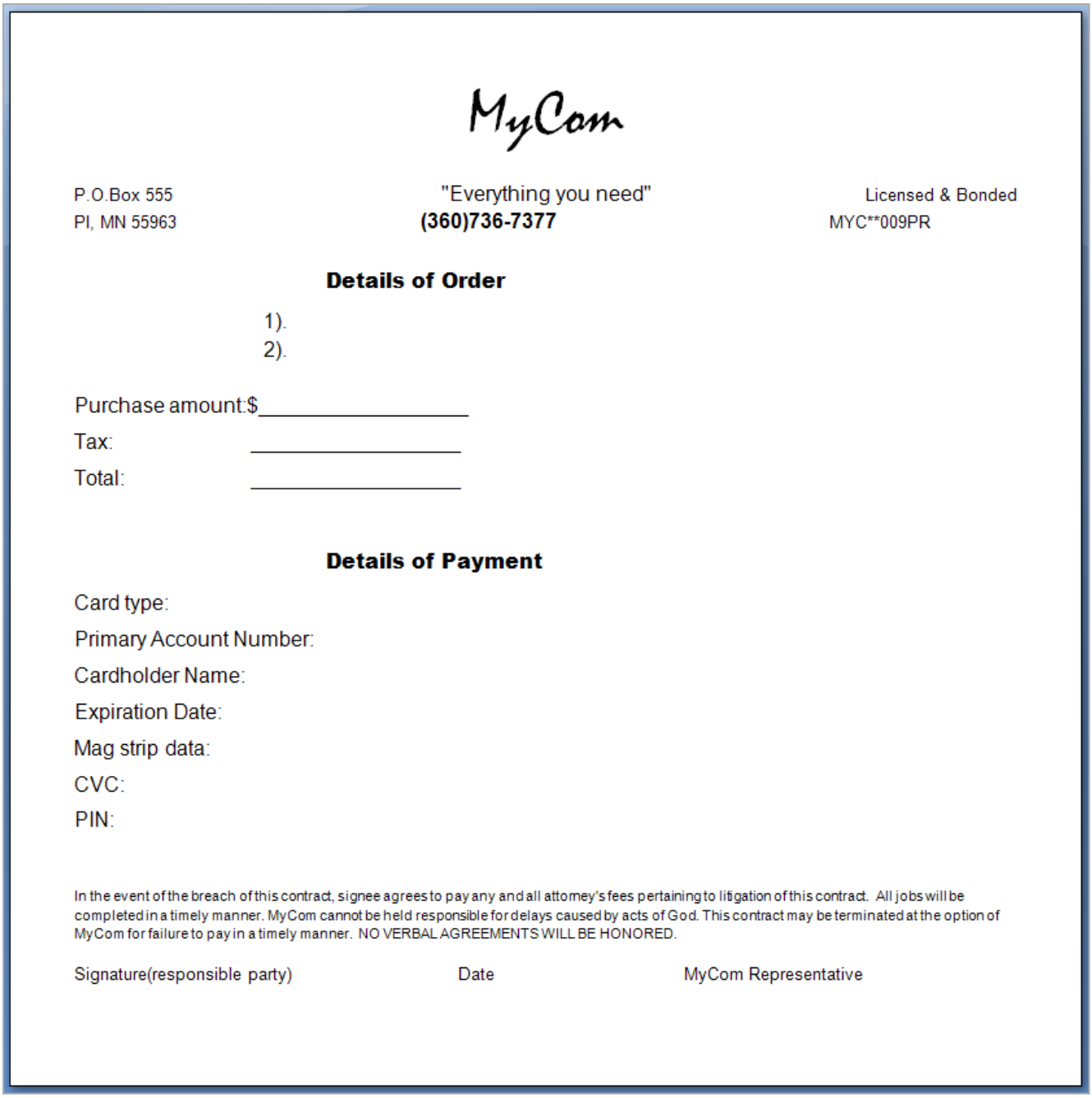
Protecting Documents by Template

Confidential and sensitive documents are often based on templates. A template specifies the headers, footers, seals, and formatting of related documents. This is what makes all court orders, for example, look the same.

You can create a Data Type that protects documents based on a specific template. You then add the Data Type to a rule and connections that contain such a document are matched by the policy.

Important - When a template including images is attached to a **DLP Template Data Type**, the image file format is important. The file format used in the template must match the file format in the user document. If the file formats are different, the rule does not trigger a DLP response. For example, if the template contains a JPG image and the user document contains the image in GIF format, there is no DLP response.

Example:



MyCom

P.O.Box 555
PI, MN 55963

"Everything you need"
(360)736-7377

Licensed & Bonded
MYC**009PR

Details of Order

1).
2).

Purchase amount:$_____
Tax: _____
Total: _____

Details of Payment

Card type:
Primary Account Number:
Cardholder Name:
Expiration Date:
Mag strip data:
CVC:
PIN:

In the event of the breach of this contract, signee agrees to pay any and all attorney's fees pertaining to litigation of this contract. All jobs will be completed in a timely manner. MyCom cannot be held responsible for delays caused by acts of God. This contract may be terminated at the option of MyCom for failure to pay in a timely manner. NO VERBAL AGREEMENTS WILL BE HONORED.

Signature(responsible party) Date MyCom Representative

To create a Data Type representation of documents based on a template:

1. In the **Data TypeWizard**, select **Documents based on corporate template**.
2. Click **Next**.
3. Browse to the template file on your system.

   This file does not have to be known as a template in the application: the template for the Data Type may be a *.doc file and does not have to be a *.dot file. Select any file that is a basic example of documents that might be sent.

4. Move the **Similarity** slider to determine how closely a document must match the given template to be considered protected.

   Best Practice - Set this slider quite low first. The higher it is, the less the rule catches. After you complete the wizard, send a test email with such a document, and check the Logs & Monitor Logs view to see if the document was caught. Slowly increase the Similarity level until the rule catches the documents you want. This is different for each template.

5. Click **Next**.
6. Click **Finish**.
7. To configure additional properties for the Data Type, select **Configure additional Data Type properties**.

Property	Description
Match empty templates	■ Select this option if you want DLP to match the Data Type on an empty template. An empty template is a template that is identical to the uploaded corporate template. ■ If the option is not selected, an empty template is detected but the Data Type is not matched. The template is not considered confidential until it contains inserted private data. **Note** - the rule is bypassed for this document, but the document may still be matched by another DLP rule in the policy.
Consider template's images	■ Incorporates a template's graphic images into the matching process. Including template images increases the similarity score calculated between the template and the examined document. The higher the score, the more accurate the match. ■ Select this option if the graphic images used in a template document suggest that the document is confidential.

If you want to catch documents that match on different levels with different actions, make an alternative to slider tests.

Procedure:

1. Create a Data Type for the template. Set the slider to 10%.
2. In the **Policy** window, create a **Detect** rule that tracks the documents that match but does not stop them.
3. Create a second Data Type. Set the slider to 50%.

4. In the **Policy** window, create an **Ask User** rule that tracks the matching documents and holds the transmission until the user decides to send them or to delete because they are too sensitive.
5. Create a third Data Type. Set the slider to 90%.
6. In the **Policy** window, create a **Prevent** rule that tracks the matching documents and blocks the transmission.

Protecting Data by Fingerprint

Many Data Types identify data by classifying it according to keywords or file attributes such as document type, name, or size. Classifications and attributes are used to describe the data. The fingerprint Data Type does not rely on a description of the data. The fingerprint Data Type identifies the data according to a unique signature known as a fingerprint. A fingerprint accurately identifies confidential files or parts of confidential files.

Fingerprint Data Type can accurately identify files that the organization considers confidential. This Data Type accurately matches files or parts of it.

Generating the unique signature:

- First you identify a repository. A repository is a network location that contains files that must not go outside of the organization. The **Data Loss Prevention** Software Blade scans these data files and generates a unique signature for each file.
- When a file passes through a DLP Gateway, the file is scanned and a signature generated.
- When the file passes through the DLP Gateway, the DLP Gateway compares the signature of this file against the signatures of files in the repository. If there is a signature match, the DLP Gateway prevents the scanned file from distribution outside of the organization.

Repository Scanning

Files in the repository are constantly changing. New files are added, existing files modified or deleted. To keep file signatures up to date, the repository must be scanned on a regular basis. By default, the repository is automatically scanned every day. If a file is added or modified after a scan, the file's signature is not updated until the next scheduled scan.

Supported file shares for repositories:

- CIFS
- NFS

Note - Scans of a repository that has already been scanned takes less time. Unchanged files in a repository are skipped.

Filtering the Repository for Efficiency

A large repository might also contain many files that are not confidential and do not need to be scanned.

The scan can be made more efficient by:

- Accurately defining the location of data in the repository.

  Select only those folders that are known to contain confidential files.

  You may need help from the related department heads to do this.

  For example not all the folders in the Finance department may contain confidential information.

  These folders do not have to be included in the scan.

- Only scanning files that match specific Data Types, for example spreadsheet files or credit card numbers.

  If you add **Credit Card Numbers** as the Data Type in the filter, all the files in the repository that contain credit card numbers are scanned and fingerprinted.

  If **Spreadsheet file** is selected as the Data Type in the filter, only spreadsheet files in the repository are scanned and fingerprinted.

Granularity

Complete files do not have to go outside of an organization for data to be lost.

Confidential data can be lost if sections from files in the repository are copied into other files, copied to email or posted to the web.

A file in the repository may be saved locally and then modified in a way that it no longer matches the unique fingerprint signature.

To identify such incidents, a partial match between files scanned by the DLP Gateway and files in the repository can be configured.

A partial match can be:

- **According to a percentage value**

  The number of text segments in the sent file is divided by the number of text segments in the repository file, and the result expressed as a percentage.

  A match occurs if this percentage is higher than the percentage configured on the **General Properties** page of the Data Type.

- **A number of identical text segments**

  A match occurs when the number of identical text segments in a scanned file and a file in the repository is higher than the number configured on the **General Properties** page of the Data Type.

Scan Times

For large repositories, a scan can run all day.

To prevent this, you might want to limit the scan to a specified range of hours.

If a scan does not complete before the time range expires, the scan recommences where it stopped when the next scheduled scan occurs.

Generating Logs

Repository scans generate logs that can be viewed in the **Logs & Monitor** view. In the **Logs & Monitor** view, the **Fingerprint** query shows all logs generated by a scan.

Cases when logs are generated

- The fingerprint Data Type is matched.

  In the log:

  - The **Matched File** field shows which file in the repository matches the scanned data.

- The **Matched File Percentage** field shows percentage of segments in the scanned data that match segments from the file in the repository. A 100% match means the scanned data and the file in the repository are identical.
- The **Matched File Text Segments** shows how many segments of the scanned data were matched to segments in the repository file.

- A Whitelist files scan has been started
- A whitelist repository scan is running
- A Whitelist files scan has ended successfully
- A repository scan has been started
- A repository scan is running
- A repository scan ends successfully

Note - Running logs are generated every two hours. For a scan that lasts less than two hours, only the start and finish logs appear.

Log Details

Fingerprint

Parameter	Description
Scan ID	A unique scan identification to distinguish between logs
Next Scheduled Scan Date	Time the scan started
Duration	How long the scan lasted
Scan Status	The status can be Running, Paused, Canceled, or Success
Number of errors	Number of errors encountered.

Creating a fingerprint Data Type

1. In the **Data Type Wizard**, select **Fingerprint**.
2. Enter a name and informative comments for the Data Type.

   This is the name that appears on the **Data Loss Prevention > Repositories** page.
3. Click **Next**.
4. In the **Fingerprint** window:
   a. Click the **Gateways** arrow button to select Security Gateways with the **Data Loss Prevention** Software Blade enabled.

      By default, the **DLP Blades** object appears.

      This object represents all DLP Gateways.

      Only Security Gateways selected here scan the repository and enforce the fingerprint data type.
   b. Define a network path to the repository
   c. If the repository defined in the network path requires a username and password to access it, enter the relevant authentication credentials.
5. Click **Test Connectivity**.

   This tests that DLP Gateways defined in the list with Security Gateways (step 4a) can access the repository using the (optional) assigned authentication credentials.
6. Click the **Match Similarity** arrow.

   This option matches similarity between the document in the repository and the document being examined by the DLP Gateway.

   You can specify an exact match with a document in the repository, or a partial match based on one of these:

   - A percentage value
   - Number of matched text segments.
7. Click **Next**.

   Select **Configure additional Data Type Properties after clicking Finish** if you want to configure more properties.
8. Click **Finish**.

   The **New data type** wizard closes.

   The data type appears in the list of data types and also on the **Repositories** page.
9. Install the Access Control policy.

Configuring more fingerprint properties

In the **Data Types** window or **Repositories** window, double-click fingerprint object to open it for editing. These properties can be configured:

Parameter	Description	
General	Change the data entered in the Data Type wizard.	
Data Owners	Add users or user groups that own the data. Data owners can be notified when the fingerprint data type is matched by a rule in the DLP policy.	
Advanced Matching	Add CPcode scripts to apply more match criteria after the fingerprint data type is matched by a rule.	
Scan Scheduling	Configure when the document repository is scanned to update the fingerprint data type. The default time object (**Every-Day**) has no time restrictions configured. This means that a scan runs without time restrictions after the fingerprint data type is added to a policy rule. If the DLP Gateway's resources and network bandwidth are an issue, limit the scan to off-peak hours.	

Parameter	Description	
Repository Scan Filter	This page offers more scanning criteria:	
	Scan files matching the following data types	This property lets you scan documents in the repository according to more data types, for example credit card numbers. If you add **Credit Card Numbers** as the data type, all the files in the repository that contain credit card numbers are fingerprinted. If "spreadsheet files" are selected as the data type, only spreadsheet files in the repository are fingerprinted.
	Scan files according to size	Only files of the specified maximum and minimum size are included in the fingerprint.
	Scan files according to modification date	Only files that match the specified modification dates are included in the fingerprint.
	Note - After a change to the filters (adding or removing a data type, selecting a different file size or modification date) the DLP Gateway regards all files in the repository as *new*. In a large repository, this results in a long scan. The fingerprint is only enforced after the end of this scan.	

Parameter	Description	
Data locations	Use the Data Locations tree to include or not include repository sub-folders. If you want the fingerprint data type to prevent only one document type from leaving the organization, put that document in a folder that contains no other document. Select only that folder as the data location.	

Using the Fingerprint Data Type

To use the fingerprint Data Type, you must:

1. Add the fingerprint Data Type to a DLP rule
2. Install the Access Control policy on the DLP Gateway.

   After the fingerprint Data Type is included in a policy, a scheduled scan occurs.

   After the scan successfully finishes, the fingerprint Data Type is enforced.

   If you want to manually start a scan of the repository:

   - In the **Repositories** window, select the fingerprint Data Type.
   - In the summary pane for the Data Type, click **Start**.

NFS Repository scanning in NATed Environments

NAT (for example in a clustered environment where each member's connections are translated to the Virtual IP address of the cluster), prevents repository scanning when the repository is located on an NFS server.

To enable repository scanning you must disable Hide NAT on all NFS services.

The members of a cluster must be configured to send NFS related traffic using the member's IP address in the Source field of the packet, and not the Virtual IP of the cluster.

Disabling Hide NAT on NFS services in a cluster

1. On the Security Management Server, edit the required `table.def` file (see the *R81.20 Security Management Administration Guide*).
2. Search for the line:

   ```
   no_hide_services_ports
   ```

   These are the services and ports not included in Hide NAT.
3. Enter the required ports and protocols:

   ```
   no_hide_services_ports = { <111, 17>, <111, 6>, <4046, 17>,
   <4046, 6> }
   ```

   Notes:
   - If a list of services and ports already exists, add these numbers to the end of the list.
   - New settings in the `table.def` file apply globally to all Security Gateways and clusters of the applicable version.
4. Save the changes in the file and exit the editor.
5. Install the Access Control policy on the ClusterXL object.

Protecting Files by Attributes

Create a data type that protects files based on file type, file name, and file size. Transmissions that contain a file that matches the parameters are matched.

To create a data type representation of files:

1. In the **Data Type Wizard**, select **Files**.
2. Click **Next**.
3. Select the appropriate parameters:

   Note - A file must match all the parameters that you define here, for it to be matched to the rule. The more parameters you set here with assurance, the more accurate the results are.

   - **The file type is any of these types** - Click the add button to select from the **Add File Types** window.
   - **The file name contains** - Enter a string or regular expression to match against file names.
   - **The file size is larger than** - Enter the threshold size in KB.
4. Click **Next**.
5. Click **Finish**
6. (Optional) To add more parameters to the Data Type, select the checkbox. Click **Finish**.

Defining Compound Data Types

You can create a complex data type representation. A compound data type includes multiple Data Types, which are matched either on AND (a number of Data Types are matched), or NOT (necessary Data Types are not present), or both.

For example, you can look for files or emails that contain patient records. You could create a data type that combines documents that match a patient record template, with a dictionary data type that contains a group of patient names who have not signed release forms. Now you have a single data type that matches emails or FTP that contain patient records of patients who have not signed a release form.

To create a compound data type representation:

1. In the **Data Type Wizard**, select **Compound**.
2. Click **Next**.
3. In the first section, click **Add** and select Data Types to match on AND.
4. In the second section, click **Add** and select Data Types to match on NOT.

   If a transmission is sent that matches all the Data Types of the first section and none of the Data Types in the second section, the data of the transmission is matched to the compound Data Types.
5. Click **Next**.
6. Click **Finish**.
7. (Optional) To add more parameters to the Data Type, select the checkbox. Click **Finish**.

Advanced Data Types

The Data Type Wizard has four advanced Data Types:

Protecting Data by Weighted Keywords

If you begin by creating a Data Type for keyword or pattern, and realize that it is not ALL or ANY, but that one word is a sign of protected data in itself, and other word would be a suspicious sign only if it appeared numerous times, you can define this complex data representation as a Weighted Keyword rather than a simple keyword or pattern.

Transmissions that contain this list of words, in the weight-sum that you define in their data, are handled based on the action of the rules that use this Data Type.

To create a Data Type representation of weighted keywords:

1. In SmartConsole, from the left navigation panel, click **Manage & Settings**.
2. In the top left section, click **Blades**.
3. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
4. SmartDashboard opens the **Data Loss Prevention** tab.
5. In the left pane, click **Data Types**.
6. From the top toolbar, click **New**.
7. The **Data Type Wizard** opens.
8. On the **Data Representation** page:
    a. Enter a name for the new data type.
    b. At the bottom, select **Advanced** and from the drop-down list, select **Weighted keywords**.
    c. Click **Next**.
9. On the **Specify Weighted Keywords** page:
    a. From the top toolbar, click **Add**.
    b. Enter the weighted keyword, phrase, or regular expression.

c. In the **Weight** section:

   Each occurrence of matching data content counts as **1** (default) or more, and the weight has limits or has no limits.

   - **Each appearance of this word contributes the following weight** - set to **1** for the lowest weight, **2** for the double-weight (one instance of this string is counted as though two), and so on.
   - **The weight of this word is limited to** - set to **0** for no limit, or set to a number greater than the weight in the field above. In this way, you set a maximum count (a ceiling) for this one weighted string.

d. In the **Regular Expression** section:

   If the string you entered in the top field is a regular expression, then select **This keyword is a Regular Expression**.

e. Click **OK**.

f. In the **Threshold** field, enter the applicable value.

   If data content matches any of the words in this Data Type, with a total weight that is greater than this value, the data is matched to the Data Loss Prevention rule.

g. Click **Next**.

10. On the **Finished Data Type Wizard** page:

    a. If you want to open this Data Type object to configure more settings, select the checkbox **Configure additional Data Type properties after clicking Finish**.

    b. Click **Finish**.

11. In the left pane, click **Policy** and configure the applicable rules that use this Data Type.
12. Save the changes in SmartDashboard (in the top left corner, click the diskette icon).
13. Close SmartDashboard.
14. In SmartConsole, install the Access Control Policy.

Protecting Data by Keywords from a Static Dictionary

If you have a list of the keywords that flag data as protected, you do not need to enter them one by one in a keyword data representation. Instead, you can upload the list as a static dictionary. You decide how many of the items in the list have to be matched to have the data match a DLP rule.

Best Practice - Dictionary files must contain one word or phrase on each line. If the dictionary file must contain non-English words, we recommend that it be a Word document (***.doc**).
Dictionaries that are simple text files (***.txt**) must be in the UTF-8 format.

To create a Data Type representation of a static dictionary:

1. In SmartConsole, from the left navigation panel, click **Manage & Settings**.
2. In the top left section, click **Blades**.
3. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
4. SmartDashboard opens the **Data Loss Prevention** tab.
5. In the left pane, click **Data Types**.
6. From the top toolbar, click **New**.
7. The **Data Type Wizard** opens.
8. On the **Data Representation** page:
    a. Enter a name for the new data type.
    b. At the bottom, select **Advanced** and from the drop-down list, select **Words from a dictionary**.
    c. Click **Next**.
9. On the **Dictionary** page:
    a. In the **Upload a dictionary** field, browse to and select the file that contains the list of terms.

b. In the **Threshold** section, configure the number of terms that must be in the content for the DLP Gateway to match the Data Type to a DLP rule.

Best Practice - First, set this to the highest reasonable value, and then lower it after you audit the **Logs & Events** logs.

For example, if the dictionary is a list of employee names, do not set the threshold to **1** because it catches every email that has a signature. Instead, set the threshold value to half the number of users and the corresponding DLP rule to **Detect**. If after about a week the rule catches no data, lower the threshold and check again. When the rule begins to detect this information that is sent out, set it to **Ask User** to make the users explain why they send this information outside before they do so. With this information, you can create a usable, reasonable, and accurate enforcement of the corporate policy.

c. Click **Next**.

10. On the **Finished Data Type Wizard** page:

a. If you want to open this Data Type object to configure more settings, select the checkbox **Configure additional Data Type properties after clicking Finish**.

b. Click **Finish**.

11. In the left pane, click **Policy** and configure the applicable rules that use this Data Type.
12. Save the changes in SmartDashboard (in the top left corner, click the diskette icon).
13. Close SmartDashboard.
14. In SmartConsole, install the Access Control Policy.

Protecting Data by Keywords from a Dynamic Dictionary

With Dynamic Dictionaries, an administrator can automatically update the DLP dictionaries without the need to manually upload the dictionaries files to the Management Server after each change and install the Access Control Policy on all DLP Gateways.

To use Dynamic Dictionaries, the administrator places dynamic dictionary files on a web server that is accessible from the DLP Gateways and configures a dictionary Data Type that contains the full address of the file on this web server. The DLP Gateways download this file every 60 minutes (default interval that can be changed) and starts to enforce it immediately.

SmartConsole and SmartView show a log entry for each downloaded dynamic dictionary.

Supported Items:

- Supported data file types: `txt` (must be in the UTF-8 format), `doc`, `docx`
- Maximum dictionary file size: 10 megabytes
- Maximum number of lines in a dictionary file: 500,000

To create a Data Type representation of a dynamic dictionary:

1. Create a data file and upload it to your web server:
   a. Create a file that contains the required data.

      Example:

      ```
      customers.txt
      ```

      Best Practice - Dictionary files must contain one word or phrase on each line. If the dictionary file must contain non-English words, we recommend that it be a Word document (***.doc** or ***.docx**).

   b. Upload this file to your web server.
2. Create a dynamic dictionary file:
   a. In a plain-text editor, create a dynamic dictionary file with the file extension ***.dyn_dict** (`<Name_of_File>.dyn_dict`).

      Example:

      ```
      customer_info.dyn_dict
      ```

b. The first line of the dynamic dictionary file must contain the URL (`http` or `https`) of the data file on your server.

   Example:

   ```
   http://192.168.22.33/public/customers.txt
   ```

c. The second line and the third lines are optional.

   If the server requires authentication, enter the username in the second line and enter the password in the third line.

   Example:

   ```
   http://192.168.22.33/public/customers.txt
   serveruser
   ServerP@ssword#
   ```

d. Save the changes in the file and close it.

3. Create the Data Type in SmartDashboard:

   a. In SmartConsole, from the left navigation panel, click **Manage & Settings**.

   b. In the top left section, click **Blades**.

   c. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.

   d. SmartDashboard opens the **Data Loss Prevention** tab.

   e. In the left pane, click **Data Types**.

   f. From the top toolbar, click **New**.

   g. The **Data Type Wizard** opens.

   h. On the **Data Representation** page:

      i. Enter a name for the new data type.

      ii. At the bottom, select **Advanced** and from the drop-down list, select **Words from a dictionary**.

      iii. Click **Next**.

i. On the **Dictionary** page:

i. In the **Upload a dictionary** field, browse to and select the ***.dyn_dict** file.

ii. In the **Threshold** section, configure the number of terms that must be in the content for the DLP Gateway to match the Data Type to a DLP rule.

Best Practice - First, set this to the highest reasonable value, and then lower it after you audit the **Logs & Events** logs.

For example, if the dictionary is a list of employee names, do not set the threshold to **1** because it catches every email that has a signature. Instead, set the threshold value to half the number of users and the corresponding DLP rule to **Detect**. If after about a week the rule catches no data, lower the threshold and check again. When the rule begins to detect this information that is sent out, set it to **Ask User** to make the users explain why they send this information outside before they do so. With this information, you can create a usable, reasonable, and accurate enforcement of the corporate policy.

iii. Click **Next**.

j. On the **Finished Data Type Wizard** page:

i. If you want to open this Data Type object to configure more settings, select the checkbox **Configure additional Data Type properties after clicking Finish**.

ii. Click **Finish**.

k. In the left pane, click **Policy** and configure the applicable rules that use this Data Type.

l. Save the changes in SmartDashboard (in the top left corner, click the diskette icon).

m. Close SmartDashboard.

4. Configure the parameters in the `$DLPDIR/config/dlp.conf` file:

a. Connect to the command line on the DLP Gateway / **each** DLP Cluster Member.

b. Log in to the Expert mode.

c. Back up the current `$DLPDIR/config/dlp.conf` file:

```
cp -v $DLPDIR/config/dlp.conf{,_BKP}
```

d. Edit the current `$DLPDIR/config/dlp.conf` file:

```
vi $DLPDIR/config/dlp.conf
```

e. Go to this section:

```
:engine (
```

f. Go to this sub-section:

```
:dynamic_dt (
```

g. Configure the values for these parameters:

```
:dynamic_dt (
        ...
        :enable_dynamic_updates (1)
        :update_interval_in_min (60)
        :passwords_are_obscured (0)
        ...
)
```

Parameters:

Parameter	Description
`enable_dynamic_updates`	Enables or disables the feature: ■ `1` - enabled ■ `0` - disabled
`update_interval_in_min`	Specifies the timeout (in minutes) for running the agents. The default is 60 minutes. The DLP Gateway runs agents periodically to create the file marking files (a file with file names and their sizes) based on the value of the "`update_interval_in_min`" parameter. To run the agents manually, run the "`fwdlp -run_agents`" command in the Expert mode on the DLP Gateway / **each** DLP Cluster Member. The agents run one time, 5 minutes after each policy installation. The next run time is based on the value of the `update_interval_in_min` parameter. To make sure the DLP Gateway / **each** DLP Cluster Member uses the configured interval, you can examine the `$DLPDIR/log/dlpe.log` file.
`passwords_are_obscured`	Enables or disables the support for obscured passwords: ■ `1` - enabled ■ `0` - disabled (default) If it is necessary to configure obscured passwords, contact *Check Point Support*.

h. Save the changes in the file and exit the editor.

5. In SmartConsole, install the Access Control Policy.

Protecting Data by Keywords from a Dynamic Dictionary using Exact Data Match (EDM)

Important - This feature requires:

- Management Server R81.20 and higher.
- DLP Gateway / DLP Cluster R81.20 and higher.

The Exact Data Match (EDM) feature extends the Dynamic Dictionary functionality.

An administrator can use a table file as a data source and configure data match based on a number of fields (table columns) in each record (table row), and a number of matched records in this table file.

Supported Items for Exact Data Match (EDM):

- Supported file types: `csv` (must be in the UTF-8 format)
- Maximum dictionary file size: 10 megabytes
- Maximum number of lines in a dictionary file: 500,000

Known Limitations for Exact Data Match (EDM):

- You can create only **one** Data Type object for Exact Data Match (EDM).
- Data Type identifier is not supported (used as a two-tier detection).
- Proximity of records is not supported.
- A Data Loss Prevention incident generates the "Detect" and "Prevent" logs.

To create a Data Type representation of a dynamic dictionary using Exact Data Match (EDM):

1. Create a CSV file and upload it to your web server:
   a. Create a plain-text file in the CSV format that contains the required table data.

      Example:

      ```
      customersInfo.csv
      ```

   b. Upload this file to your web server.
2. Create a dynamic dictionary file:

a. In a plain-text editor, create a dynamic dictionary file with the file extension ***.dyn_dict** (`<Name_of_File>.dyn_dict`).

   Example:

   ```
   customer_info_table.dyn_dict
   ```

b. The first line of the dynamic dictionary file must contain the URL (`http` or `https`) of the data file on your server.

   Example:

   ```
   http://192.168.22.33/public/customersInfo.csv
   ```

c. The second line and the third lines are optional.

   If the server requires authentication, enter the username in the second line and enter the password in the third line.

   Example:

   ```
   http://192.168.22.33/public/customersInfo.csv
   serveruser
   ServerP@ssword#
   ```

d. Save the changes in the file and close it.

3. Create the Data Type in SmartDashboard:

   a. In SmartConsole, from the left navigation panel, click **Manage & Settings**.

   b. In the top left section, click **Blades**.

   c. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.

   d. SmartDashboard opens the **Data Loss Prevention** tab.

   e. In the left pane, click **Data Types**.

   f. From the top toolbar, click **New**.

   g. The **Data Type Wizard** opens.

h. On the **Data Representation** page:

   i. Enter a name for the new data type.

   ii. At the bottom, select **Advanced** and from the drop-down list, select **Words from a dictionary**.

   iii. Click **Next**.

i. On the **Dictionary** page:

   i. In the **Upload a dictionary** field, browse to and select the ***.dyn_dict** file.

   ii. In the **Threshold** section, configure the number of terms that must be in the content for the DLP Gateway to match the Data Type to a DLP rule.

   Best Practice - First, set this to the highest reasonable value, and then lower it after you audit the **Logs & Events** logs.

   For example, if the dictionary is a list of employee names, do not set the threshold to **1** because it catches every email that has a signature. Instead, set the threshold value to half the number of users and the corresponding DLP rule to **Detect**. If after about a week the rule catches no data, lower the threshold and check again. When the rule begins to detect this information that is sent out, set it to **Ask User** to make the users explain why they send this information outside before they do so. With this information, you can create a usable, reasonable, and accurate enforcement of the corporate policy.

   iii. Click **Next**.

j. On the **Finished Data Type Wizard** page:

   i. If you want to open this Data Type object to configure more settings, select the checkbox **Configure additional Data Type properties after clicking Finish**.

   ii. Click **Finish**.

k. In the left pane, click **Policy** and configure the applicable rules that use this Data Type.

l. Save the changes in SmartDashboard (in the top left corner, click the diskette icon).

m. Close SmartDashboard.

4. Configure the parameters in the `$FWDIR/conf/dlpe_edm_config.C` file:

a. Connect to the command line on the DLP Gateway / **each** DLP Cluster Member.

b. Log in to the Expert mode.

c. Create the `$FWDIR/conf/dlpe_edm_config.C` file (it does not exist by default):

```
touch $FWDIR/conf/dlpe_edm_config.C
```

d. Edit the `$FWDIR/conf/dlpe_edm_config.C` file:

```
vi $FWDIR/conf/dlpe_edm_config.C
```

e. Prepare the required syntax in a plain text editor (like Notepad++):

```
(
    :edm (
        :enabled (NUMBER)
        :edm_columns_to_inspect ("Col_index_1,Col_
index_2,...,Col_index_N")
        :edm_column_threshold (NUMBER)
        :edm_required_match_columns ("Col_index_1,Col_
index_2,...,Col_index_N")
    )
)
```

Parameters:

Parameter	Type	Description
`enabled`	Mandatory	Enables or disables the EDM feature: ■ `1` - enabled ■ `0` - disabled
`edm_columns_to_inspect`	Mandatory	Specifies the indexes of all columns to inspect, separated by commas, without spaces.
`edm_column_threshold`	Mandatory	Specifies how many columns must match in each record (row).
`edm_required_match_columns`	Optional	Out of all inspected columns, specifies the indexes of all columns that must match in each record (row).

Example syntax in the $FWDIR/conf/dlpe_edm_config.C file

The table data is:

1	2	3	4	5
First Name	Last Name	Email	Phone	Username
John	Doe	john.doe@example.com	123	jdoe
Bill	Smith	bill.smith@example.com	456	bsmith

1	2	3	4	5
First Name	Last Name	Email	Phone	Username
Kate	Lee	kate.lee@example.com	789	klee

These are the data loss prevention requirements:

i. Inspect only columns with the indexes from 1 to 4.

ii. Inspect two columns in each record.

This means the threshold is 2, and the possible combinations of two columns that the DLP Gateway must inspect are:

1+2, 1+3, 1+4, 2+3, 2+4, 3+4

iii. Optional: The column with the index 3 must match in each record.

This means the possible combinations of two columns that the DLP Gateway must inspect are now limited to:

1+3, 2+3, 4+3

Therefore, the required syntax is:

```
(
     :edm (
          :enabled (1)
          :edm_columns_to_inspect ("1,2,3,4")
          :edm_column_threshold (2)
          :edm_required_match_columns ("3")
     )
)
```

f. Paste the required syntax into the `$FWDIR/conf/dlpe_edm_config.C` file.

g. Save the changes in the file and exit the editor.

5. In SmartConsole, install the Access Control Policy.

Protecting Data by Message Attributes

Message attributes refer to these properties of the message:

- The total message size, in kilobytes
- Number of attachments
- Total number of words in the message

To create a Data Type for message attributes:

1. In SmartConsole, from the left navigation panel, click **Manage & Settings**.
2. In the top left section, click **Blades**.
3. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
4. SmartDashboard opens the **Data Loss Prevention** tab.
5. In the left pane, click **Data Types**.
6. From the top toolbar, click **New**.
7. The **Data Type Wizard** opens.
8. On the **Data Representation** page:
   a. Enter a name for the new data type.
   b. At the bottom, select **Advanced** and from the drop-down list, select **Message Attributes**.
   c. Click **Next**.
9. On the **Specify Message Attributes** page:

Note - For a message to match this Data Type, it must match all the criteria - the size *and* the number of attachments *and* the number of words. If the message fails to match one of the criteria, it fails to match this Data Type.

a. Configure the **Message Size**:

Define the size a message can have.

Minimum value	Maximum value	Meaning
Configured	Configured	Matches all messages whose size is within the specified range.
Configured	Not Configured	Matches all messages whose size is greater than the minimum value.
Not Configured	Configured	Matches all messages whose size is smaller than the maximum value.

b. Configure the **Number of Attachments**:

Define the number of attachments a message can have.

Minimum value	Maximum value	Meaning
Yes	Yes	Matches all messages with number of attachments that falls within the specified range.
Yes	Not Configured	Matches all messages with more attachments than the specified minimum value.
Not Configured	Yes	Matches all messages with fewer attachments than the specified maximum value.

c. Configure the **Total Number of Words in t he Message**:

Scan for a significant amount of text. If an email has a large binary file attached such as a graphic, and the email contains the words "your picture" the email might match the *Size* attribute but contain no text worth scanning. You need the email to match a DLP rule only if the email contains enough text that can conceivably result in data loss.

Minimum value	Maximum value	Meaning
Configured	Configured	Matches all messages whose word count falls within the specified range.
Configured	Not Configured	Matches all messages whose word count is greater than the specified minimum value.
Not Configured	Configured	Matches all messages whose word count is lower than the specified maximum value.

d. Click **Next**.

10. On the **Finished Data Type Wizard** page:

a. If you want to open this Data Type object to configure more settings, select the checkbox **Configure additional Data Type properties after clicking Finish**.

b. Click **Finish**.

11. Save the changes in SmartDashboard (in the top left corner, click the diskette icon).
12. Close SmartDashboard.
13. In SmartConsole, install the Access Control Policy.

Protecting Data by CPCode

CPCode is a scripting language, similar to C or Perl, specifically for Intrusion Prevention Systems. If you are familiar with this language, you can create your own complex rules. Use CPCode data types to create dynamic definitions of data to protect, or to create data type representations with custom parameters.

For example, you can create a CPCode that checks for a date that is before a public release, allowing you to create rules that stop price list releases before that date, but pass them afterwards. Other common uses of CPCode include relations between rule parameters, such as recipients (match rule to email if sent to too many domains) and protocols (match rule to HTTP if it looks like a web mail).

Best Practice - If you write a CPCode function yourself, make sure it works it before you put it in production.

Example of a CPcode function:

```
func rule_1 {
  foreach $recipient inside global:DESTS {
    foreach $comp inside CPMPETITORS_DOMAIN {
      if( casesuffix( $recipient , $comp ) ) {
        set_message_to_user(cat("The mail is sent to " ,
        $recipient ,
        "which is a competitor's mail address."));
        set_track(TRACK_LOG);
        return quarantine();
      }
    }
  }
}
```

To create a Data Type representation of CPCode:

1. Create a CPCode script file ***.cpc**.

   See the *R77 versions CPcode DLP Reference Guide*.
2. In SmartConsole, from the left navigation panel, click **Manage & Settings**.
3. In the top left section, click **Blades**.
4. In the **Data Loss Prevention** section, click **Configure in SmartDashboard**.
5. SmartDashboard opens the **Data Loss Prevention** tab.
6. In the left pane, click **Data Types**.
7. From the top toolbar, click **New**.
8. The **Data Type Wizard** opens.
9. On the **Data Representation** page:

a. Enter a name for the new data type.

b. At the bottom, select **Advanced** and from the drop-down list, select **Custom CPcode match**.

c. Click **Next**.

10. On the **Upload CPcode files** page:

a. Click **Add**.

b. Select the CPCode script file (`*.cpc`).

c. Click **Next**.

11. On the **Finished Data Type Wizard** page:

a. If you want to open this Data Type object to configure more settings, select the checkbox **Configure additional Data Type properties after clicking Finish**.

b. Click **Finish**.

12. In the left pane, click **Policy** and configure the applicable rules that use this Data Type.
13. Save the changes in SmartDashboard (in the top left corner, click the diskette icon).
14. Close SmartDashboard.
15. In SmartConsole, install the Access Control Policy.

Enhancing Accuracy through Statistical Analysis

A number of Data Types, such as credit card numbers, have an **Enhance accuracy through statistical analysis** option on their **General Properties** page.

Credit cards like Visa and Mastercard have sixteen digit numbers arranged in four groups of four. While you scan for this Data Type, all sixteen digit numbers in the data that match the Luhn algorithm are identified as credit card numbers.

The sixteen digits can represent not a credit card number. The sixteen digits can represent spare part numbers, an ordering or sales code. The **Enhance accuracy** option applies statistical analysis to increase the accuracy of identifying specified Data Types, for example credit card numbers.

To enhance accuracy through statistical analysis:

1. In **Data Loss Prevention > Data Types** select a Data Type that represents numerical data.
2. Open the Data Type to edit it.
3. On the **General Properties** page, select **Enhance accuracy through statistical analysis**.
4. Click **OK**.

Note - Enabling statistical analysis does not impact Security Gateway performance.

Adding Data Types to Rules

The data types are the building blocks of the Data Loss Prevention rule base, and the basis of the DLP policy that you install on DLP Gateways - the basis of DLP functionality. Each data type specifies a data asset to protect.

Data Owners must know about the types of data that are under their responsibility and be able to tell you to what type of data they allow to go outside of the organization, and what data must be protected.

For example, a team leader of a programming team must know that lines of code are not allowed to move outside the organization, and demand its protection. A hospital administrator must have an example of a court order to release patient records to authorized domains.

Important:

- Focus on the Data Types, not on the full rules. Enable and customize Data Types to recognize data to match.
- Start with the obvious - with the data that you know by experience should be kept inside the organization - lines of code, employee contact information, passwords, price lists, and so on. Then create more complex Data Types according to the organization confidentiality and integrity procedures, after communicating with Data Owners.
- After you have a Data Type, add it to a rule, and install the policy rule base on the DLP Gateway.

Procedure:

1. **Specify the Compliance Data Type**

   The compliance category contains built-in data types that represent accepted standards and regulatory requirements. For example, according to Payment Card Industry (PCI) compliance standards, credit card numbers of customers must not be sent to outside sources in clear text.

   In the **Data Loss Prevention Data Types** window, data types are sorted according to category. An important category is the compliance category. The **Data Types** window lets you create data types that enforce compliance in accordance with regulatory standards.

   Create Data Types

   The **Data Loss Prevention Overview** window > **DLP Featured Data types** toolbox lists the data types for:

- Compliance

  Click the **Compliance** button to the data types in this category and how many are activated.
- Business information
- Personally identifiable information
- Best Practice
- Intellectual Property
- Human Resources
- Financial

In the **Featured Data Types** area of the toolbox, two actions are available:

Action	Use
View rule	Click **View rule** to see how the compliance data type is used in the DLP policy.
Add to policy	Click **Add to policy** to add the compliance data type to the DLP policy.

Clicking **Compliance** on the tool bar in the **Data Types** window filters out those data types which do not belong to the Compliance category. Check Point regularly adds to the number of built-in data types, but if none of the types is applicable to your needs - you can create a new data type and add it to the compliance category.

Built-in data types exist for:

- EU Data Protection Directive
- FERPA - Confidential Educational Records
- GLBA - Personal Financial Information
- HIPAA - Protected Health Information
- ITAR - International Traffic in Arms Regulations
- PCI DSS - Cardholder Data
- PCI - Credit Card Numbers
- PCI - Sensitive Authentication Data

- U.S. State Laws - Personally Identifiable Information
- UK Data Protection Act

To add a new data type to the compliance category

a. In the **Data Loss Prevention Data Types** window, click **New**.

   The **Data Type Wizard** opens.

b. Select criteria such as keywords or a corporate template

c. On the last page of the wizard open, select **Configure additional Data Type properties after clicking Finish**.

d. Click **Finish**.

e. The data type properties window opens on the **General Properties** page.

f. Set the category to **Compliance**.

   Note - You cannot change the category of a built-in data type, only add new data types to one of the pre-existing categories.

Edit Data Types

After you specify Data Types with the Data Type Wizard, you can fine-tune them if necessary. Each Data Type in the General Properties window shows only its applicable fields. You only see the options that apply to the currently selected data type.

To edit Data Types:

a. In SmartDashboard, click the **Data Loss Prevention** tab.

b. Open **Data Types**, select a Data Type and click **Edit**.

c. In the **General Properties** window, edit/fill-in the fields that apply to the Data Type.

d. Click **Finish**.

The existing Data Types

Section	Description
General Properties	■ **Name** - Name of the data type representation. ■ **Comment** - Optional comments and notes. ■ **Categories** - Optional assigned category tags, for grouping data types. ■ **Flag** - Optional custom flag to help management of a large Data Types list. • **Follow Up** - Use this flag as a reminder to check the tracking logs SmartView Tracker and analysis in SmartEvent to see if your changes are catching the expected incidents and otherwise to follow up on maintenance and fine-tuning. • **Improve Accuracy** - After enabling a built-in data type, use this flag as a reminder to replace placeholder data types with real dictionary files or lists or to otherwise make built-in data types more relevant to your organization. After replacing the file with real data, remember to set this flag to **Follow Up**, to monitor its related incidents, or to **No Flag**. ■ **Description** - For built-in data types, the description explains the purpose of this type of data representation. For custom-made data types, you can use this field to provide more details.
Custom CPcode	■ **Add** - Click to add CPcode scripts. The default file type is **cpc**. See the *R77 versions CPcode DLP Reference Guide*. . ■ **View** - Click to view a CPcode script in a text editor. ■ **Remove** - Click to remove CPcode scripts.

Section	Description
Compound	■ **Each one of these data types must be matched** - All items in this list must be matched in the data, for the compound data type to match. ■ **None of these data types must be matched** - If the data matches any item in this list, the compound data type does not match. ■ **Add** - Add items to a list. ■ **Edit** - Modify the selected item. (Changes made from here affect all compound data types and rules that use the edited data type). ■ **Remove** - Remove items from a list.
Dictionary	■ **Replace** - Click to browse to a different file. ■ **View** - Click to view the file. Note that any changes you make here do not affect the file that is used by the data type. ■ **Save a Copy** - Click to save the file under another name. ■ This data is matched only if it contains at least - Set the threshold to an integer between 1 and the number of entries in the dictionary. Traffic that contains at least this many names from the dictionary is matched. **Note** - If the items in the dictionary are in a language other than English, use a Word document as the dictionary file. Any text file must be in UTF-8 format.

Section	Description
Documents Based on a Corporate Template	■ **Replace** - Click to browse to a different file. ■ **View** - Click to view the file. Note that any changes you make here do not affect the file that is used by the data type. ■ **Save a Copy** - Click to save the file under another name. ■ **Match empty templates** - Select this option if you want DLP to match the data type on an empty template. An empty template is a template that is identical to the uploaded corporate template. If the option is not selected, an empty template is detected but the data type is not matched. The template is not considered confidential until it contains inserted private data. Note the rule is bypassed for this document, but the document may still be matched by another DLP rule in the policy. ■ **Consider templates images** - Incorporates a template's graphic images into the matching process. Including template images increases the similarity score calculated between the template and the examined document. The higher the score, the more accurate the match. Select this option if the graphic images used in a template document suggest that the document is confidential. ■ **Similarity** - Move the slider to determine how closely a document must match the given template or form to be recognized as matching the data type. This matches header and footer content, as well as boiler-plate text.
File	Select the conditions that should be checked on files in data transmissions (including zipped email attachments, as well as other transmissions). A transmitted file must match all selected conditions for the File data type to be matched. ■ **The file belongs to one of these file groups** - Click **+**, and select a files type from the list. ■ **The file name contains** - Enter a string or regular expression to match against file names. ■ **The file size is larger than** - Enter the threshold size in KB.

Section	Description
Group Members	■ **Add** - Add data types to the group. If any of the members are matched, the data is recognized as matching the group data type. In the list that opens, you can click **New** to create a new data type. ■ **Edit** - Open the properties window of the selected data type. When you click **OK** or **Cancel**, the Data Type Group window is still open. ■ **Remove** - Remove the selected data type from the group. The data type is not deleted.
Keywords or Phrases	■ **Specify keywords or phrases to search for** - Enter the words to match data content. ■ **Add** - Click to add the keywords to the data type. ■ **Search List** - Keywords in the data type. ■ **Edit** - Modify the selected word or phrase in the list. ■ **Remove** - Remove the selected word or phrase from the list. ■ **All keywords and phrases must appear** - Select to match data only if all the items in the Search List are found. ■ **At least** *number* **words must appear** - Enter an integer to indicate number of items in Search List to match the Keyword data type.
Pattern	■ **Type a pattern (regular expression)** - Enter the regular expression to match data content. ■ **Add** - Click to add the regular expression to the data type. ■ **Pattern List** - Regular expressions in the data type. ■ **Edit** - Modify the selected regular expression in the list. ■ **Remove** - Remove the selected regular expression from the list. ■ **Number of occurrences** - Enter an integer to set how many matches between any of the patterns and the data are needed to recognize the data as matching the data type.

Section	Description
Similarity	■ **Similarity** - Move the slider to determine how closely a document must match the given template or form to be recognized as matching the data type. This matches header and footer content, as well as boiler-plate text.
Threshold (dictionary)	■ This data is matched only if it contains at least - Enter an integer to set how many matches in the data are needed to recognize the data as matching the data type.
Threshold (occurrences)	■ **Number of occurrences** - Enter an integer to set how many matches in the data are needed to recognize the data as matching the data type.
Threshold (keywords)	**This data is matched only if it contains:** ■ **All keywords and phrases** - Select to match data only if all the items in the Search List are found. ■ **At least** *number* **keywords or phrases** - Enter an integer to indicate number of items in Search List to match the Keyword data type.
Threshold (recipients)	This data is matched only if the email contains: ■ **At least** ***number*** **internal recipients** - Enter the minimum number of email addresses that are specified inside of My Organization that, along with external addresses, should cause the email to be regarded as suspicious of containing confidential information. ■ **and no more than** ***number*** **external recipients** - If an email is sent to a large distribution list, even if it contains numerous internal recipients, it should be recognized as an email meant for people outside the organization. In this field, enter maximum number of email addresses external to My Organization, that if more external recipients are included, the email matches a rule.

Section	Description
Threshold (External BCC)	This data is matched only if the email contains at least: ■ **Internal recipients** - Enter the minimum number of email addresses that are specified inside of My Organization that, along with external addresses, should cause the email to be regarded as suspicious of containing confidential information. ■ **External recipients** - Enter the minimum number of email addresses external to My Organization, that would cause such an email to be suspicious.
Weighted Keywords or Phrases	■ **Keyword Text** - List of current keywords or regular expressions in the list of weighted keywords. To add more, click **New**. To change the selected keyword or regular expression, click **Edit**. The Edit Word window opens. ■ **Weight** - The number that represents the importance of this item in recognizing a transmission that should be matched. The higher the number, the more weight/importance the item has. ■ **Max. Weight** - The number that represents the ceiling for this item. If content of a transmission matches the item (by keyword or by regular expression) to a total of this weight, no more counts of the item are added to the total weight of the transmission. (Zero means there is no maximum weight.) ■ **RegEx?** - Whether the item is a regular expression. ■ **Threshold** - When the weights of all items in the list are added together, if they pass this threshold, the transmission is matched.

Specify Data Type Groups

You can create a Data Type representation that is a group of existing Data Types.

To create a Data Type group:

a. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

SmartDashboard opens and shows the **DLP** tab.

b. From the navigation tree, click **Policy**.

c. Click **New** > **Data Type Group**.

   The **Group Data Type** window opens.

d. Enter a **Name** for the group.

e. In the Group Members section, click **Add**.

f. Select the Data Types that are included in this Data Type group.

g. If necessary, add **Data Owners** to the group.

h. Click **OK**.

i. Click **Save** and then close **SmartDashboard**.

j. In SmartConsole, install the policy.

2. **Create more complex Data Types per Organization**

   After you communicate with the organization Data Owners, you can specify Advanced Matching for Keyword Data Types, according to the organization confidentiality and integrity procedures.

   You can add CPcode script files for more advanced match criteria to improve accuracy after a keyword, pattern, weighted keyword, or words from a dictionary are matched. If the CPcode script file has a corresponding value file (for constants values) or CSV file, add it here.

   Note - You can add more than one CPcode script. All of the scripts must match the keywords or phrases to be recognized as matching the data type.

   To add advanced matching Data Type CPcode script:

   a. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

      SmartDashboard opens and shows the **DLP** tab.

   b. From the navigation tree, click **Data Types** .

   c. Select a **Data Type** and click **Edit**.

      The **Data Type** window opens.

   d. Click the **Advanced Matching** node.

e. In **Run these CPcode for each matched keyword to apply additional match criteria**, add the CPcode scripts to run on each of the Data Type matches.

- **Add** - Click to add CPcode scripts. The default file type is **cpc**. See the *R77 versions CPcode DLP Reference Guide*. .
- **View** - Click to view a CPcode script in a text editor.
- **Remove** - Click to remove CPcode scripts.

f. Click **OK**.

g. Click **Save** and then close **SmartDashboard**.

h. In SmartConsole, install the policy.

3. **Add the created Data Type to a rule**

For all Data Type representations, you can add CPcode scripts that run after a data type is matched. Then you can test the Data Types.

Specifying a Post Match CPcode for a Data Type

a. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP**, and click **Open DLP Policy in SmartDashboard**.

SmartDashboard opens and shows the **DLP** tab.

b. From the navigation tree, click **Data Types**.

c. Select a Data Type and click **Edit**.

The **Data Type** window opens.

d. Click the **Advanced Matching** node.

e. In the **Run these CPcode scripts after this Data Type is matched to apply additional match criteria**, add the CPcode scripts to run on each of the Data Type matches.

- **Add** - Click to add CPcode scripts. The default file type is **CPC**.
- **View** - Click to view a CPcode script in a text editor.
- **Remove** - Click to remove CPcode scripts.

f. Click **OK**.

g. Click **Save** and then close **SmartDashboard**.

h. In **SmartConsole**, install policy.

Testing Data Types (Recommendation)

Before installing a policy that contains new Data Types, you can test them in a lab environment.

Recommendation for testing procedure:

a. Create a Data Type.

b. Create a user called Tester, with your email address.

c. Create a rule:

- Data = this Data Type
- Action = Detect
- Source = Tester
- Destination = Outside

d. Send an email (or other data transmission according to the protocols of the rule) that should be matched to the rule.

e. In SmartConsole, open the **Logs & Monitor** > **Logs** view and check that the incident was tracked with the **Event Type** value being the name of the Data Type.

- If the transmission was not caught, change the parameters of the Data Type. For example, if the Data Type is Document by Template, move the slider to a lower match-value.
- If the transmission was caught, change the parameters of the Data Type to be stricter, to ensure greater accuracy. For example, in a Document by Template Data Type, move the slider to a higher match-value.

f. After fine-tuning the parameters of the Data Type, re-send a data transmission that should be caught and check that it is.

Important - If you change the action of the rule to Ask User, to test the notifications, you must change the subject of the email if you send it a second time.
If Learning mode is active, DLP recognizes email threads. If a user answers an **Ask User** notification with **Send**, DLP does not ask again about emails in the same thread.

g. Send another transmission, as similar as possible, but that must pass. Make sure it passes.

   For example, for a Document by Template Data Type, try to send a document that is somewhat similar to the template but contains no sensitive data.

   If the acceptable transmission is not passed, adjust the Data Type parameters to increase accuracy.

Exporting Data Types

You can export to a file the Data Types that you have created or that are built-in. This allows you to share Data Types between DLP Gateways, when each is managed by a different Security Management Server.

a. In SmartConsole, click **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

b. From the navigation tree, click **Data Types**.

c. Select the Data Type to export.

d. Click **Actions** > **Export**.

e. Save it as a file with the **dlp_dt** extension.

f. Click **Save** and then close SmartDashboard.

Importing Data Types

You can share Data Types with another Security Management Server or recover a Data Type that was exported but then deleted. You can also obtain new Data Types from your value-added reseller or from Check Point and use this procedure to add the new Data Types to your local system.

Note - You can only export and then import Data Types on Security Management Servers that are the same version. For example, you can export and import Data Types on different R80.30 Security Management Servers. You cannot export Data Types from an R80 Security Management Server and then import them to an R80.30 Security Management Server.

Procedure

a. In **SmartConsole**, click **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

b. From the navigation tree, click **Data Types**.

c. Click **Actions** > **Import**.

d. Select the **dlp_dt** file holding the Data Type that you want.

e. Click **Save**.

f. Close **SmartDashboard**.

g. In SmartConsole, install the policy.

4. Install the Policy on the DLP Gateways.

Repositories

Repositories are network locations used for document storage.

DLP has two kinds of repository:

- **Fingerprint Repository**

  The fingerprint repository is used to store files from which the fingerprint Data Type is derived. A fingerprint repository is automatically created when you create the fingerprint Data Type. Files that exactly or partially match documents in the fingerprint repository are identified before they go outside of the organization.

  Creating a Fingerprint Repository:

  1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

     SmartDashboard opens and shows the **DLP** tab.
  2. From the navigation tree, click **Repositories**.
  3. Click **New** > **Fingerprint**.

     The Data Type wizard opens with Fingerprint selected as the Data Type.
  4. Enter a name for the Data Type.
  5. Click **Next**.
  6. In the **Fingerprint** window:
     a. Click the Gateways arrow button to select Security Gateways with the DLP blade enabled.

        By default, The **DLP Blades** object shows. This object represents all Security Gateways that have the DLP blade enabled. Only Security Gateways selected here scan the repository and enforce the fingerprint data type.

     b. Define a network path to the repository.

     c. If the repository defined in the network path requires a username and password to access it, enter the relevant authentication credentials.

7. Click **Test Connectivity**.

   This tests that DLP Gateways defined in the Security Gateways list (step 4a) can access the repository using the (optional) assigned authentication credentials.

8. Click the **Match Similarity** arrow.

   This option matches similarity between the document in the repository and the document being examined by the DLP Gateway. You can specify an exact match with a document in the repository, or a partial match based on:

   - A percentage value or
   - Number of matched text segments.

9. Click **Next**.
10. (Optional) To configure more properties, select **Configure additional Data Type Properties after clicking Finish** .
11. Click **Finish**.

    The **New data type** wizard closes. The data type shows in the list of data types and also on the **Repositories** page.

12. Click **Save** and then close **SmartDashboard**.
13. In **SmartConsole**, install policy.

- **Whitelist Repository**

  The Whitelist repository is a store of documents that are *allowed* to go outside of the organization. The Whitelist repository can be used to improve the accuracy of the DLP policy.

  Note - For a file not to be included in the DLP match, it must exactly match a file in the whitelist repository.

  Creating a Whitelist Repository:

  1. In SmartConsole, select **Security Policies > Shared Policies > DLP** and click **Open DLP Policy in SmartDashboard**.

     SmartDashboard opens and shows the **DLP** tab.

  2. From the navigation tree, click **Repositories**

3. Click **New > Whitelist Repository**.

   The **Whitelist Repository** window opens.

   Enter a name and informative comments for the repository type.

4. In the **Whitelist Repository** section:

   a. Click the **Gateways** arrow button to select Security Gateways with the DLP blade enabled.

      By default, The **DLP Blades** object shows. This object represents all Security Gateways that have the DLP blade enabled. Only Security Gateways selected here scan the repository.

   b. Define a **Network Path** to the repository.

   c. If the repository defined in the network path requires a username and password to access it, enter the related authentication credentials. (Domain/Username).

5. Click **Test Connectivity**.

   This tests that DLP Gateways defined in the Security Gateways list can access the repository using the (optional) assigned authentication credentials.

6. To ignore text segments that are in the whitelist and fingerprint repository, click **Do not include a text segment in the fingerprint match if the segment is in both the fingerprint and whitelist repositories**.

7. Click **OK**.

   The Whitelist shows in the list of repositories.

   To manually start a scan of the whitelist repository, click **Start** in the **Scan now** area on the summary pane.

8. Click **Save** and then close SmartDashboard.

9. In SmartConsole, install policy.

Whitelist Policy

There are two ways to create a list of files that the DLP Rule Base never matches:

- Manually add the files to the **Whitelist Policy** window in SmartConsole.

  Files in the list are uploaded to the Security Management Server and not matched against DLP rules.

  Best Practice - We recommend it if you have a small number of files.

- Place the files in a Whitelist Repository on the network.

  Files in this repository are not included in the match.

To add files to the Whitelist:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.
2. From the navigation tree, click **Whitelist Policy**.
3. In the **Whitelist Files** section, click **Add**.
4. Browse to the file.
5. Click **Open**.

   The file is uploaded to a folder on the Security Management Server.

   Note - For a file that is not in the DLP match, it must exactly duplicatea file in the whitelist.
6. Click **Save** and then close SmartDashboard.
7. In SmartConsole, install policy.

Defining Email Addresses

To define email addresses and domains for use in rules:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Additional Settings** > **Email Addresses**.

3. Click **New**.

   The **Email Addresses** window opens.

4. Enter a **Name** for this group of email addresses (even if it includes only one address) or domain.

5. Enter the email address or domain.

6. Click **Add**.

   Add the necessary email addresses and domains for this object.

7. Click **OK**.

8. Click **Save** and then close SmartDashboard.

9. In SmartConsole, install policy.

Configuring the DLP Watermark

You apply watermarks when you introduce custom XML files that contain the watermarking data. Only documents in these Office Open XML formats can have a watermark:

- DOCX
- PPTX
- XLSX

Important - Older formats supported in Office 2007 and above for backward compatibility (such as DOC, PPT, and XLS, cannot be watermarked). If you change the file extension from doc to docx , it does not make the document eligible for watermarks.
If the DLP Gateway scans the Data Type, and this Data Type occurs in the body of the email and not the document, the document is not be watermarked. For example, when you scan for credit card numbers, if the credit card number shows in the body of an email with a document attached, the document is not watermarked. The Data Type must occur in the document.

Watermarking Documents

Procedure:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy** in SmartDashboard.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Policy**.
3. For the Data Type, right-click the **Action** cell, and select a restrictive **Action** such as **Ask**, **Inform User** or **Detect**.
4. Right-click the Action cell and select the Watermark profile.

   DLP has 3 built-in profiles:

   - **Classified** - places the word **Classified** in the center of the page.
   - **Invisible only** - contains only hidden text.
   - **Restricted** - places the word **Restricted** at the bottom of the page, and these inserted fields: **sender**, **recipient**, and **send date**.

5. If there are no exiting watermark profiles, click **New** and create one.

   Note - You can also modify a built-in profile.

6. Click **Save** and then close **SmartDashboard**.
7. In SmartConsole, install the policy.

Creating a New Watermark Profile

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy** in **SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **Additional Settings** > **Watermarks**.

3. Click **New**.

   The **Watermark Profiles** window opens.

4. In the **General** page, enter the **Name** for the watermark profile.

5. Click **Advanced**.

   The **Advanced Settings** window opens.

6. Clear the **Use the same configuration for all supported file types** option to create different watermarks for Word, Excel, or PowerPoint files.

   Note - A watermark in Excel cannot exceed 255 characters. The 255 character limit includes the visible watermark text and formatting data. If you exceed the 255 character limit, the watermark feature makes a best effort to show as much text as possible.
   The 255 limit is per document.

7. **Add the sets of watermarks to these options**

   - **All pages**

Section Break	In Word 2007	In Word 2010
Yes	All pages get watermark	All pages get watermark
No	All pages get watermark	All pages get watermark

   - **First page only**

Section Break	In Word 2007	In Word 2010
Yes	*All pages get watermark*	First page only gets watermark
No	*All pages get watermark*	First page only gets watermark

- **Even pages only**

Section Break	In Word 2007	In Word 2010
Yes	*All pages get watermark*	*All pages get watermark*
No	Only even pages get watermark	Only even pages get watermark

- **Odd pages only**

Section Break	In Word 2007	In Word 2010
Yes	*All pages get watermark*	*All pages get watermark*
No	Only odd pages get watermark	Only odd pages get watermark

Note - The actual placement of watermarks depends on:
- If the document contains Section Breaks on the page.
- The version of MS Word used to create the document.

8. Click **OK**.

Adding a Shadow Behind Watermark Text in Word and PowerPoint

1. On the Security Gateway, run: `cpstop`
2. On the Security Gateway, open for editing: `$DLPDIR/config/dlp.conf`.
3. Search for the attribute: `watermark_add_shadow_text(0)`.
4. Change the value of the attribute from 0 to 1.
5. Set percentages for watermark transparency and size, for DOCX and PPTX files.

   Change the `watermark_text_opacity_percentage` property from 30 (70% transparency) to the new value.
6. Save and close the file.
7. Run: `cpstart`

   Note - Before the changes to `dlp.conf` take effect, you must run `cpstop` and `cpstart`.

Configuring Watermark Settings on the General Page

1. To configure the location of the watermark:
   a. Click the watermark graphic.

      The **Select text location on page** window opens.

   b. Click the location for the watermark.
2. To configure the watermark text:
   a. Click the field with the watermark text.

      To create a new watermark, click **Add watermark text to another location**.

      The text formatting tools are shown.

   b. Click **Insert Field** to add a dynamic field to the watermark.

   c. Click the Diagonal button, to show the text on a 45 degree diagonal.

      Note - Watermark rotation is only available for:
      - PowerPoint presentations in MS Office 2007 and 2010
      - Word documents in MS Office 2010

   d. To change the text to seventy-percent transparency, click the **Transparency** button.
3. Click **OK**.

Configuring Watermark Settings on the Hidden Text Page

1. Select **Add the following hidden text to the document**.
2. Click **Add**, and select which fields should be inserted as encrypted hidden text into the document.
3. For the purpose of forensic tracking, hidden text can be viewed using the DLP watermark viewing tool (see *"Using the DLP Watermark Viewing Tool" on page 233*).
4. Click **OK**.

   If Microsoft Office 2007 (or higher) is installed on the same computer as SmartConsole, a preview of the watermark shows on a sample file in the preview pane.

   Note - The preview pane is not available if you create or edit a watermark from the DLP policy rule base. To see a preview, create a watermark from **Additional Settings > Advanced > Watermarks > New**.

5. In **Additional Settings** > **Advanced** > **Watermarks** section:

   a. Make sure **Apply watermarks on Data Loss Prevention rules** is selected.

   b. Set how existing watermarks are handled on documents that pass repeatedly through DLP Gateways. You can keep or replace the current watermarks.

   Note - Hidden encrypted text is not removed, only added to by each DLP Gateway. Hidden text can later be used for forensic tracking.

Completing the Watermark Profile

- Click **Save** and then close **SmartDashboard**.
- In SmartConsole, install the policy.

Previewing Watermarks

In **SmartConsole > Data Loss Prevention tab > Additional Settings > Watermarks**, Watermarks are previewed in the right-hand pane on sample documents.

To preview watermarks:

1. Download sample Office files from the Security Management Server.
2. Apply the watermark to these files.

   The sample preview files are named:

   - example.docx
   - example.pptx
   - example.xlsx

To open a document or preview it, you must install Microsoft Office 2007 (or higher) and SmartConsole on your computer.

You can also preview watermarks on *User-Added Files*.

To view watermarks on user-added files:

1. Open the drop-down box in the preview pane.

   The **Select File** window opens.
2. Click **Add** and browse to your Word, Excel, or PowerPoint file.

   The **Select File** window is now divided into **User Added Files** and **Sample Files**.
3. Select your user added file to see it previewed with the watermark.

   Note - When you preview a user-added file, the file is uploaded to the Security Management Server and stays on the server. To remove this file, select it in the **Select File** window and click the red X in the top right-hand corner.

Viewing Watermarks in MS Office Documents

For Office documents that have been watermarked by a DLP Gateway, view the watermarks in this way:

Office document	Go to:
Word	**View > Print Layout** or **Full Screen Reading**
Excel	**View > Page layout > Print Layout**
PowerPoint	PowerPoint has a number of built-in layers. The DLP watermark sits above the slide layout layer but below the slide content layer. This means that the watermark always shows below the content of a slide.

Resolving Watermark Conflicts

When scanned by the DLP Gateway, an email with a document attached might match one or more DLP rules. If the rules have different and conflicting watermark profiles, then the conflict must be resolved for visible watermarks and resolved for hidden text.

- **Resolving Visible Watermark Conflicts**

  An outgoing document may match one or more rules in the DLP policy. If each rule specifies different watermarking profiles, then a conflict arises. For example if different profiles specify dissimilar text in the center, the conflict must be resolved by merging the different watermark profiles according to rule precedence. Rule precedence is decided based on **ACTION** and **SEVERITY** priorities.

  After rule precedence is decided, a merged watermark profile is built according to this criteria:

  - All the Visible watermarks from the rule with the highest precedence are added to the document.
  - Visible watermarks from the rule with the second highest precedence are added to the document only if they do not conflict with watermarks from the first.
  - Visible watermarks from the rule with the third highest precedence are added to the document only if they do not conflict with watermarks added by the two rules before.

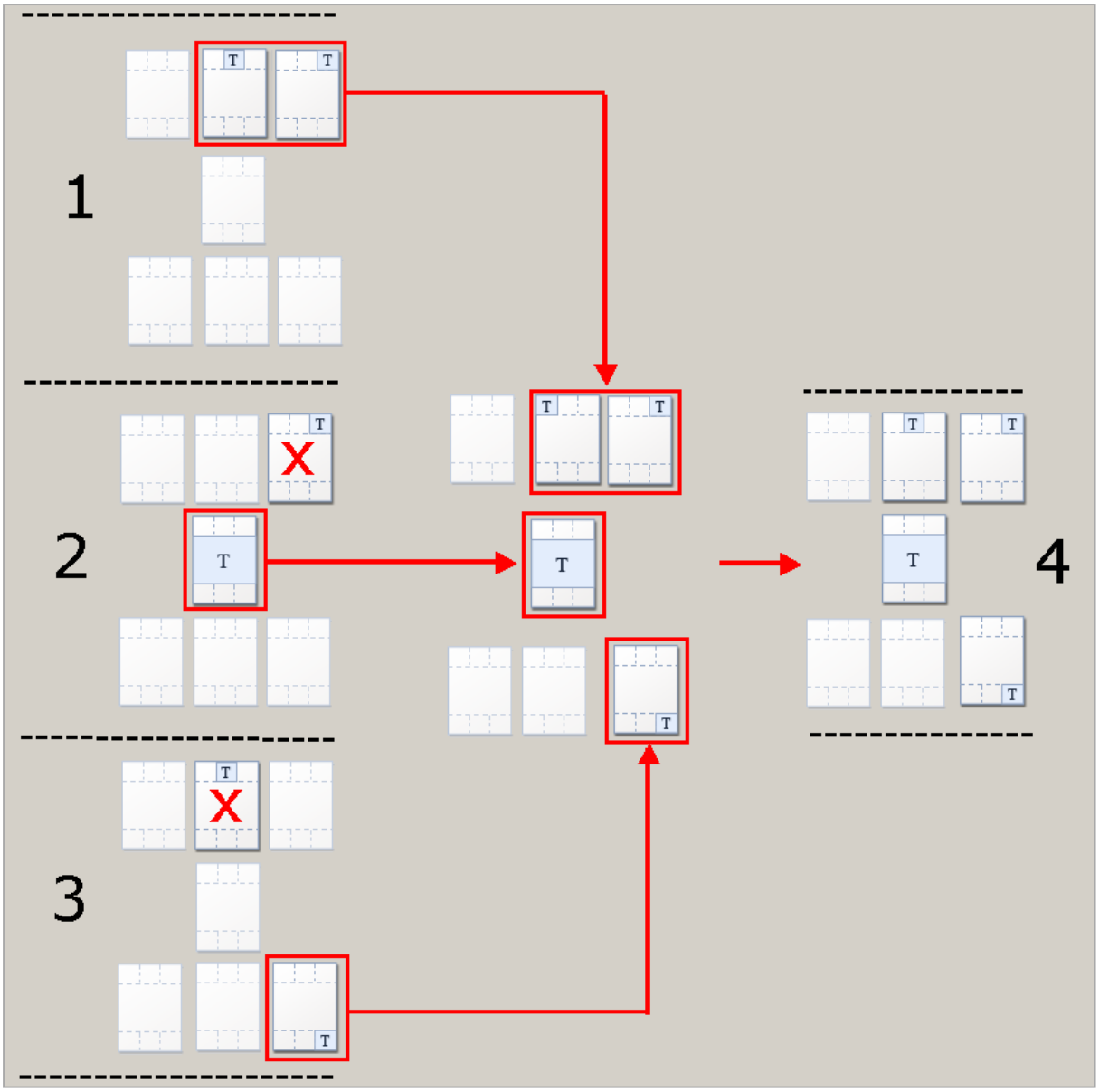
    The procedure repeats until all watermarks are added to the merged profile. For example, if you have three DLP rules, each with a custom Watermark Profile, and an email matches all three of these rules:

DLP Data Rule	Precedence	Watermark Profile Name	In graphic
Rule_A	1	W1	1
Rule_B	2	W2	2
Rule_C	3	W3	3

  - Rule_1 has greater precedence than Rule_2 and Rule_3
  - Rule_2 has greater precedence than Rule_3

  The Merged Profile

  The merged profile (4) is built by taking elements from all the profiles.



- All the watermarks from W1 are added to the merged profile (4)
- Only the center watermark from W2 is added to the merged profile.

  (The watermark in the top right corner does not overwrite the watermarks placed there by W1, which has higher precedence.)
- Only the bottom right corner watermark from W3 is added to the merged profile.

  (The watermark for the top center location is already taken by W1, which has greater precedence.)

Naming the Merged Profile

If the merged profile takes elements from existing profiles (hidden text or visible watermarks) then the name of those profiles are integrated into the name of the merged profile. In the above example, the name of the merged profile is **W1;W2;W3**, with a semi-colon which separates the individual profile names. This is the name that shows in the **DLP Watermark Profile** column in the **Logs & Monitor** view.

- **Resolving Hidden Text Watermark Conflicts**

  If different watermark profiles specify invisible text, the text is taken from the profile attached to the DLP rule that has the highest precedence. Rule precedence is derived from the **ACTION** and **SEVERITY** priorities in the DLP Rule Base.

Action	Priority
Ask User	1
Inform User	2
Detect	3

  Hidden text is taken from the watermark profile belonging to the rule that has the highest **ACTION** priority. If the two rules have the **Ask User** setting, the same priority, then **SEVERITY** is considered:

Severity	Priority
Critical	1
High	2
Medium	3
Low	4

  For example, if an email with a document attached matches these two rules:

Data	Action	Severity	Watermark Profile
Rule 1	Ask User	Low	W1
Rule 2	Detect	Critical	W2

The **ACTION** setting for Rule 1 has a greater priority than the **ACTION** setting defined for Rule 2. Rule 1 takes precedence. The hidden text configured for the W1 profile applies even though Rule 2 has a greater **SEVERITY**. If the rule is changed to:

Data	Action	Severity	Watermark Profile
Rule 1	Inform User	Low	W1
Rule 2	Inform User	Medium	W2

The rules have the same **ACTION** priority, so **SEVERITY** is considered. In this case **Medium** has a higher priority than **Low**. Hidden text from the W2 profile is added to the document. Rule 2 has precedence.

If the rules have the same priority for **ACTION** and **SEVERITY**, for example:

Data	Action	Severity	Watermark Profile
Rule 1	Inform User	Low	W1
Rule 2	Inform User	Low	W2

Rule precedence is decided according to an internal calculation based on the name of the rule in the data column.

Turning Watermark Feature On and Off

You can turn the watermark option off in a number of ways:

- In Database Tool (GuiDBEdit Tool):
  - Search for the `enable_watermarking_feature` property.
  - Set the value of the property to FALSE.
- In **DLP > Additional Settings > Advanced > Watermarks** section clear **Apply watermarks on DLP rules**

  In the DLP rule base, the warning **Watermarks are not applied on the DLP policy** shows at the bottom of the policy table.

  Clicking **Apply** opens the **Advanced Settings** Window where you can once more add watermarks in the DLP rules.

Using the DLP Watermark Viewing Tool

For forensic tracking, hidden text can be decrypted and read using the DLP watermark viewing tool.

To view hidden text on a watermarked document:

1. Copy the document, or a folder of documents, to the DLP Gateway.
2. On the Security Gateway, run: `dlp_watermark_viewer`

   Enter the name of one file or the path to a directory that contains a number of files.
3. The output shows the hidden fields included in the profile.

   Note - Only the hidden text is shown by the tool, not the document's content.

Keys used for decrypting hidden text are stored on the Security Management Server and downloaded to the Security Gateway. DLP Gateways managed by the same Security Management Server share the same keys and a common (random) ID. The random ID identifies the Security Management Server that installed the DLP policy on the Security Gateway. The viewing tool only shows text added by Security Gateways managed by the same Security Management Server. For example, for a document that has passed through three DLP Gateways, each managed by a different Security Management Server, you must copy the file to each Security Gateway and run the tool on each. The tool only shows the hidden text added by that Security Gateway, and not the text added by Security Gateways managed by other Security Management Servers.

Important - If you reinstall a Security Gateway, the keys and random ID are downloaded again from the server. The new Security Gateway can be used to decrypt hidden text added by the old one. But if you reinstall the Security Management Server the random ID is lost. The random ID that the Security Gateway adds to the document does not match the ID of the new Security Management Server. The DLP viewer does not show the document's hidden text.

Fine Tuning Source and Destination

In the Rule Base, you can change the default Source (My Organization) and the default Destination (Outside My Org) to any network object, user, or group that is defined in SmartConsole, and you can fine tune user definitions specifically for DLP.

To create a domain object:

1. In SmartConsole, click **Objects** > **Object Explorer** (CTRL+E).
2. Click **New** > **Network Object** > **More** > **Domain**.

   The **New Domain** window opens.
3. In **Enter Object Name**, enter the URL of the domain.
4. Clear **FQDN**.
5. Click **OK**.
6. Publish the SmartConsole session.

Creating Different Rules for Different Departments

You can set the Source of a rule to be any specified user, group, host, network, or VPN. You can then set the Destination to be Outside. The rule inspects data transmissions from the source to any destination outside of the source. This creates DLP rules specific to one group of users.

Note - There is a difference between **Outside Source** (external to a source that is a subset of My Organization) and **Outside of My Org** (external to My Organization).
To enable use of Outside Source, the DLP Gateway must be functioning in front of the servers that handle the data transmission protocols. For example, to use Outside on SMTP transmissions, the DLP Gateway must inspect the emails before the Mail Server does.

Alternatively, the Destination of the rule could be another user, group, host, and so on. This would create DLP rules to inspect and control the data transmissions between two groups of users.

Examples:

1. DLP rule to prevent the Finance Department from leaking salary information to employees.
   - **Source** = **Finance** (specify a group to include users, groups, or network that specifies the Finance Department)
   - **Destination** = **Outside Source** (any destination outside of Finance, internal or external to My Organization)
   - **Data Type** = **Salary Reports** (specify a Data Type Group that matches spreadsheets OR regular expressions for salaries in dollars - ([0-9]*),[0-9][0-9][0-9].[0-9][0-9] and employee names)

Data	Source	Destination	Action
Salary Reports	Finance	Outside Source	Prevent

2. DLP rule to prevent permanent employees from sending customer lists to temporary employees.
   - **Source** = **My Organization**
   - **Destination** = **Temps** (specify a group of temporary employee user accounts)

- **Data Type** = **Customer Names** (built-in Data Type customized with your dictionary of customer names)

Data	Source	Destination	Action
Customer Names	My Organization	Temps	Prevent

3. Different DLP rules for different departments.

   The Legal Department sends confidential legal documents to your legal firm. They need to be able to send to that firm, but never to leak to anyone else, either inside the organization or outside.

   HR needs to send legal contracts to all employees, but not to leak to anyone outside the organization.

   All other departments should have no reason to send legal documents based on your corporate template to anyone, with the exception of sending back the contracts to HR.

   The first rule would be:

   - **Source** = **Legal** (a group that you specify to include your Legal Department)
   - **Destination** = **Outside Source** (to prevent these documents from being leaked to other departments as well as outside the organization)
   - **Data** = built-in **Legal Documents**
   - **Exception** = allow the data to be sent to your lawyers email address
   - **Action** = **Ask User**

   The second rule would be:

   - **Source** = **HR**
   - **Destination** = **Outside My Org**
   - **Data** = built-in **Legal Documents**
   - **Action** = **Ask User**

   The third rule would be:

   - **Source** = selection of all groups excluding Legal and HR
   - **Destination** = **Outside Source** (to prevent users from sharing confidential contracts)
   - **Data** = built-in **Legal Documents**
   - **Exception** = allow the data to be sent to HR
   - **Action** = **Ask User**

Note - In this rule, you would have to exclude the two groups if you want to ensure that other rules that applied before. If you select My Organization as the source of the third rule, it applies to the users in Legal and HR, and thus negate the other rules.

Isolating the DMZ

To make sure that Data Loss Prevention checks data transmissions to the DMZ, configure the DMZ as external to **My Organization**.

For example, the PCI DSS (Payment Card Industry Data Security Standard - Copyright of PCI Security Standards Council, LLC). Requirement 1.4.1 requires to include a DMZ in the environment to prevent direct Internet traffic to and from secured internal data access points.

To make sure traffic from My Organization to the DMZ is checked for Data Loss Prevention:

1. Make sure that the DLP Gateway configuration includes a definition of the DMZ hosts and networks.
2. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.
3. From the navigation tree, click **My Organization**.
4. In the **Networks** section, make sure that:
   - **Anything behind the internal interfaces of my DLP Gateways** is selected.
   - **Anything behind interfaces which are marked as leading to the DMZ** is NOT selected.
5. Click **Save** and then close **SmartDashboard**.
6. In **SmartConsole**, install policy.

Defining Strictest Security

You may select to define the strictest environment possible. Using these settings ensures that data transmissions are always checked for Data Loss Prevention, even if the transmission is from and within your secured environment.

Important - You must ensure that legitimate transmissions are not blocked and that Data Owners are not overwhelmed with numerous email notifications. If you do use the settings explained here, set the actions of rules to **Detect** until you are *sure* that you have included all legitimate destinations in this strict definition of what is the internal **My Organization**.

To define a strict My Organization:

1. In SmartConsole, select **Security Policies** > **Shared Policies** > **DLP** and click **Open DLP Policy in SmartDashboard**.

   SmartDashboard opens and shows the **DLP** tab.

2. From the navigation tree, click **My Organization**.
3. In the **Email Addresses** section, remove the defined items.
4. Configure the VPN settings:
   a. In the **VPN** section, click **All VPN traffic**.
   b. Click **Exclusions**.
   c. In the **VPN Communities** window, add the communities that are NOT checked by DLP.
   d. Click **OK**.
5. Configure the Networks settings:
   a. In the **Networks** section, click **Select specific networks and hosts**.
   b. Click **Edit**.
   c. In the **Networks and Hosts** window, select the defined Check Point network objects to include in **My Organization**.
   d. Click **OK**.
6. Configure the Users settings:
   a. In the **Users** section, click **These users, user groups and LDAP groups only**.
   b. Click **Edit**.

c. In the **User Groups and Users** window, select the defined users, user groups, and LDAP groups that you want to include in **My Organization**.

d. Click **OK**.

7. Click **Save** and then close **SmartDashboard**.

8. In SmartConsole, install policy.

Specifying Protocols of DLP Rules

Each rule in the Data Loss Prevention policy has a definition for the protocols of the data transmission. The default setting for **Protocols** is **Any**: DLP scans transmissions over all enabled protocols.

You can control which protocols are supported by DLP in general, or by each Security Gateway, or for each rule.

To specify supported protocols for DLP:

1. Open **Additional Settings** > **Protocols**.
2. Select the protocols to give them the DLP support, in general.

   For example, if performance becomes an issue, you could clean the HTTP checkbox here, without making any other change in the policy. HTTP posts and web mail would go through without Data Loss Prevention inspection.

To specify supported protocols for individual DLP Gateways:

1. Open **Additional Settings > Protocols**.
2. In the **Protocol Settings on DLP Blades** area, select a DLP Gateway.
3. Click **Edit**.

   The properties window of the Security Gateway opens.
4. Open the **Data Loss Prevention** page of the Security Gateway properties.
5. Select **Apply the DLP policy to these protocols only** and select the protocols that get support on this DLP Gateway.

To specify supported protocols for a rule:

1. In the **Policy** view, click the **Protocol** column plus button.

   If this column is not in view, right-click a column header. From the list of possible columns that shows, select **Protocols**.
2. Select the protocols for this rule.

   Traffic that matches the other parameters of the rule, but is sent over another protocol, is not inspected.

Fine Tuning for Protocol

When you select a specific source or destination for a DLP rule, you can optimize the rule for the selected protocol.

By default, rules use all supported protocols, or the default protocols selected for the Security Gateway (in the Check Point Security Gateway window).

If you specify that a rule should use only mail sending protocols, such as SMTP, the source and destination can be users (including user groups and LDAP Account Units) or email addresses (including specific email or domains).

If you specify that a rule must use only HTTP or FTP or both, the rule ignores any source or destination that is not recognized by IP address.

If the rule uses all supported protocols, HTTP and FTP recognize only source and destinations that IP address can specify. SMTP recognizes and enforce the rule for sources and destinations based on users and emails.

Configuring More HTTP Ports

To scan transmissions on HTTP running on any port other the standard HTTP ports (80, 8080), you must define the non-standard ports to be included in the HTTP protocol.

To add ports to HTTP:

1. In **SmartConsole**, click **Objects** > **Object Explorer** (Ctrl+E).
2. Click **New** > **Service** > **TCP**.
3. Enter the name for the TCP object.
4. In **Protocol**, select **HTTP**.
5. If necessary, click **Customize** and enter the port or port range.
6. Click **OK**.
7. Install the Access Control policy.

Advanced Configuration

These sections explain how to keep maintenance for the DLP Gateway and captured files.

Configuring User Access to an Integrated DLP Gateway

To use the DLP Portal , and UserCheck, users must be allowed to access the DLP Gateway. By default, users can only access the DLP Gateway through its internal interfaces, but not through its external interfaces.

You can configure user access to the DLP Gateway in SmartConsole in the **Accessibility** section of the **Data Loss Prevention** page of the DLP Gateway object.

The options are:

- **Through all interfaces** - Lets users access the DLP Gateway through all interfaces, including external interfaces.

  Note - We do not recommend that you use "Through all interfaces" when you configure the DLP Gateway at the perimeter.

  - **Through internal interfaces** - Lets users to access the DLP Gateway through interfaces that are defined as *Internal* in the Topology page of the DLP Gateway object. If an interface is configured in the Topology page as *Not Defined* or as *Interface leads to DMZ*, it is not counted as an internal interface with respect to DLP Accessibility options.

    This is the default option. This option is recommended to prevent unauthorized access to the DLP Gateway from the external Security Gateway interfaces. To make this option meaningful, make sure the topology of the internal and external interfaces of the DLP Gateway are correctly defined.

  - **Including VPN encrypted interfaces** - Interfaces used for establishing route-based VPN tunnels (VTIs)

- **According to the Firewall policy** - Allow access according to Firewall Rule Base rules defined by the SmartConsole administrator. Use this option if you want to decide which ports to open for DLP. The applicable ports are:

Feature	Service	TCP Port
DLP Portal	**TCP HTTP**	80
	TCP HTTPS	443
UserCheck	**TCP**	18300
	TCP HTTPS	443
Reply-to-email	**TCP HTTPS**	25

For example, to allow access from remote sites and/or remote users to the DLP Gateway, add rules that allow access to the UserCheck service (port 18300) and HTTPS (port 443) from those VPN Communities to the DLP Gateway. You can also define the source IP address from which SMTP communication is allowed. This would normally be the mail server that receives emails from users.

Internal Firewall Policy for a Dedicated DLP Gateway

A dedicated DLP Gateway enforces a predefined, fixed *Internal firewall policy.* This policy gives users access to the DLP Gateway for the UserCheck services: DLP Portal, UserCheck, and SMTP. The policy is made up of implied rules.

The Internal Firewall Policy on a dedicated DLP Gateway is not related to the Data Loss Prevention (DLP) Policy that is defined by the administrator in the Policy page of the Data Loss Prevention tab of SmartConsole. It is also not related to the Access Control Policy which is explicitly defined by the administrator in SmartConsole.

If you do an **Install Policy:**

- An integrated DLP Security Gateway enforces the *Firewall Policy* and the Data Loss Prevention (DLP) Policy.
- A dedicated DLP Gateway enforces the *Internal Firewall Policy* and the Data Loss Prevention (DLP) Policy.

Important - A dedicated DLP Gateway does not enforce the Firewall Policy, Stateful Inspection, anti-spoofing or NAT. Check Point recommends that you place it behind a protecting Security Gateway or firewall.

The Internal Firewall Policy lets users access these services and ports (and no others) on the DLP Gateway:

Feature	Service	TCP Port
DLP Portal	**TCP HTTP**	**80**
	TCP HTTPS	**443**
UserCheck	**TCP**	**18300**
	TCP HTTPS	**443**
WebUI	**TCP**	**4434**
Reply-to-email	**SMTP**	**25**
Secure Shell	**SSH**	**22**
ICMP	**ICMP requests**	

Advanced Expiration Handling

You can change the time to expire for unhandled UserCheck incidents. This is done in the DLP configuration files. You must make sure that the expiration of incidents is greater than the expiration time for learning user actions, to ensure that you do not nullify the feature that learns user actions.

To change expiration time:

1. On the DLP Gateway, open the **$FWDIR/dlp/config/dlp.conf** file.
2. Find the expiration for quarantine parameter:

   ```
   :backend (
   :expiration (
   :quarantine (604800)
   ```

   The default value is `604800`. This is the number of seconds that the DLP Gateway holds a DLP Ask User incident in, until the user decides to send or discard it.
3. Find the expiration for learning user actions (called `thread_caching`) in the same `backend` section.

   ```
   :backend (
   .(
   .
   .
   )
   :thread_caching (
   :cache_expiration_in_days (7)
   ```

   The value of `backend:expiration:quarantine`, when converted from seconds to days, must be greater than or equal to the value of `backend:thread_caching:cache_expiration_in_days`.
4. Change the value of quarantine as needed.

   By default, incident data is held in the Security Gateway for 21 days after the incident actually expired. This extra time enables you to retrieve data for users who were on vacation, for example. You can change the removal interval.
5. Change the value (in days) of `backend:expiration:db` as needed.

   ```
   :backend (
   :expiration (
   :db (21)
   ```
6. Save **dlp.conf** and install the policy on the DLP Gateway.

Advanced SMTP Quotas

The DLP quota check ensures that users are not overloading the file system with unhandled UserCheck incidents. If a user has so many captured emails, or emails with large attachments, that the quota per user is exceeded, DLP handles the issue.

The email quota threshold has two values - minimum and maximum. If a user exceeds the maximum email quota, DLP deletes older emails until the user's file system folder size is lower than the minimum quota threshold.

To change quota behavior:

1. On the DLP Gateway, open the **$FWDIR/conf/mail_security_config** file.
2. Find the quota parameters:

```
#is quota for mail repository active value can be 0 or 1
user_quota_active=1
#quota size per user in Mega Byte currently set to 100 mb per
user
quota_size_per_user=100
#quota size per user upper and lower limit in percentage
values can range between 0 to 100 and upper can't be smaller
than lower
user_quota_upper_limit=90
user_quota_lower_limit=50
```

To deactivate quota checks and deletes:

Set `user_quota_active` to **0**.

The other options are relevant only if `user_quota_active=1`.

To change the folder size allowed to each user for DLP incidents and data:

Change the value of `quota_size_per_user` (MB).

To set the threshold (percent of quota size) to delete older emails:

Change the value of `user_quota_upper_limit`.

By default, if 90% of the quota size is exceeded, DLP begins to delete older emails.

To set the lower limit (percent of quota size) to change the value of `user_quota_lower_limit`:

By default, quota cleanup stops when enough emails are deleted to bring the user folder size to 50% of the quota size, or lower.

3. Save the **mail_security_config** and install the policy on the DLP Gateway.

Advanced FTP and HTTP Quotas

This quota check ensures that users are not overloading the file system with unhandled UserCheck incidents using FTP or HTTP transmissions. If a user has so many captured HTTP posts, or large FTP upload attempts, that the quota per user is exceeded, DLP handles the issue.

To change quota behavior:

1. On the DLP Gateway, open the **$FWDIR/dlp/conf/dlp.conf** file.
2. Find the HTTP or the FTP section, and this parameter: **save_incident_quota_percentage**

   The default value is `85`. This is 85% of the file system, for this type of transmission. The value range is 0 to 100. If zero, no quota is enforced.
3. Change this value to change the threshold that initiates the cleanup.

   When disk usage is greater than this value, incidents are not saved.

   Best Practice
   If you decrease this value, decrease the age of FTP and HTTP incidents before deletion, to ensure that you have enough disk space to save incidents: **$FWDIR/conf/mail_security_config** file > `dlp_delete_redundant_files_age_group1_files` parameter
4. Save **dlp.conf** and install the policy on the DLP Gateway.

Advanced User Notifications

You can enable or disable email notifications that are sent to users when their captured DLP incidents or incident data are deleted from the Security Gateway.

Notifications are especially important if incidents and data are deleted because of exceeding quota (may occur if the user's email storage exceeds the user-allowed limit), because:

- DLP may delete UserCheck incidents and data for which the user expected to have more handling time.
- DLP deletes the data; there is no way to undo this action.

On the other hand, if a user gets a notification that an incident expired because it wasn't handled in time, you can still retrieve the data of the incident (if needed). DLP deletes the data of expired incidents a number of days after the data expired.

You can configure, which DLP automatic actions fire the notifications.

To activate or de-activate user notifications of DLP deletion:

1. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
2. In the top left pane, go to **Table** > **Other** > **dlp_data_tbl**.
3. In the top right pane, click **dlp_general_settings_object**.
4. In the bottom pane, in the Field Name column, scroll down to the **notification** object.

   You see different types of notifications (see the text in the **Field description** column).
5. To enable a notification, set the value of its **active** attribute to **true**.
6. Save the changes (**File** menu > **Save All**).
7. Close the Database Tool (GuiDBEdit Tool).
8. In SmartConsole, install the policy.

Gateway Cleanup of Data

The complete data of UserCheck incidents are held in quarantine on the DLP Gateway. Thus, if an email is caught, and it contains a large attachment, it takes up the necessary space on the Security Gateway until the incident is handled or expires.

Gateway Cleanup of Expired Data

The DLP Gateway automatically cleans itself of expired incident data. Incident data that is held for the `backend:expiration:db` number of days gets deleted.

Changing How Often and When the Gateway Checks for Data to Delete

1. On the DLP Gateway, open the **$FWDIR/conf/mail_security_config** file.
2. Find the expiration interval parameter:

```
#A check for expired email items is executed every
'expiration_interval' minutes
expiration_interval=1440
#the first time of execution for the expiration feature set to
begin at 3:30 in the morning when there is no traffic on the
system
expiration_execution_time=3:45
```

3. Change the value of `expiration_interval` (minutes), to have the Security Gateway search for expired data on a different interval. The default is 1440 minutes, which is one day.
4. Change the value of `expiration_execution_time` (24 hour clock), to change the time of day that the Security Gateway is cleaned. Be default, this is 3:45 AM, to ensure that Security Gateway maintenance does affect performance during usual working hours.
5. Save **mail_security_config** and install the policy on the DLP Gateway.

Gateway Cleanup of All Captured Data

DLP automatically cleans its Security Gateway periodically of temporary files, to make sure that disk use does not unduly build over time. But sometimes unnecessary files are left on the disk.

You can customize the cleanup with these configuration files:

- `$FWDIR/conf/mail_security_config`
- `$DLPDIR/config/dlp_cleanup_files_list.conf`

Important - It is not recommended to de-activate the cleanup. If you must do so, set the value of `dlp_delete_redundant_files_active` to 0.

mail_security_config File Parameters

mail_security_config Parameters	Description
dlp_delete_redundant_files_interval	How often (in minutes) cleanup runs. Default = 1440 (24 hours)
dlp_delete_redundant_files_execution_time	Exact time (on 24 hour clock) when cleanup runs. Default = 4:45 (when Security Gateway load is low)
dlp_delete_redundant_files_age_group1_files	Minimum age of UserCheck data files, which should be maintained on the disk until their handling expiration arrives. Default = 0 (use the expiration_time_in_days value) Note: This value does not change the expiration of incidents; it changes when data of expired incidents is removed.
dlp_delete_redundant_files_age_group2_files	Minimum age of files in **/proc** Default = 15 minutes
dlp_delete_redundant_files_age_group3_files	Minimum age of files in **$FWDIR/tmp/dlp** Default = 15 minutes

The dlp_cleanup_files_list.conf file is a list of scan commands with this syntax

`scan[ CHECK_DB | - ] path mask scale age`

Parameter	Description
CHECK_DB or -	Tests files to see if they are in the DLP database, to prevent accidental deletion of UserCheck incident data: `scan CHECK_DB` To clean up everything, even user captured data, change the flag to a dash (-): `scan -`
path	Path to look for files to delete. May include shortcuts such as $DLPDIR or $FWDIR, but cannot contain spaces.
mask	Regular expressions for files to match: * = all files Default masks used include: `*.eml`, `*.result`, `*.meta`
scale	Unit of measure for age parameter: `minutes_back` or `days_back`
age	Minimal time since creation the file must have before it can be deleted

Best Practice - Contents of this file explain more options, such as how to use macros for file age. It is recommended that you read the file comments before changing anything here.

The default age values of scan commands in the file are macros that pull values from **mail_security_config**. You can use numeric values instead of macros.

age Macros	Description
$2	group1 age (in days): UserCheck data files, value taken from `dlp_delete_redundant_files_age_group1_files`
$3	group2 age (in minutes): **/proc** files, value taken from `dlp_delete_redundant_files_age_group2_files`
$4	group3 age (in minutes): **/tmp/dlp** files, value taken from `dlp_delete_redundant_files_age_group3_files`

Customizing DLP User-Related Notifications

These procedures tell how to customize backend files to change the text of user-related notifications.

It is also possible to localize the files to a language other than US English.

Customizing the DLP notification emails

1. On the Security Gateway in the **$DLPDIR/backend/conf/** directory, edit these files:

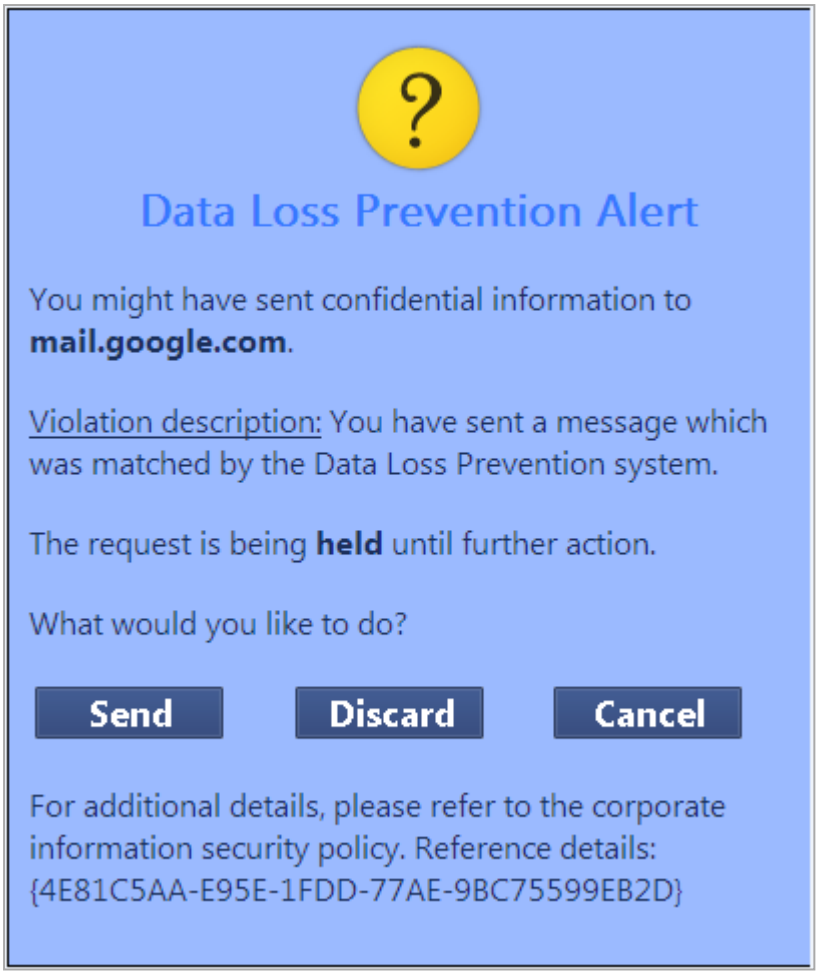
File	Function
dictionary_en_us.conf	Basic dictionary
about_to_expire_notification_tmplt_en_us.html data_owners_mail_notification_tmplt_en_us.html detect_mail_notification_tmplt_en_us.html expired_owners_mail_tmplt_en_us.html expired_sender_mail_tmplt_en_us.html failure_mail_notification_en_us.html prevent_mail_notification_tmplt_en_us.html quarantine_mail_notification_tmplt_en_us.html quota_deleted_notification_tmplt_en_us.html released_mail_notification_tmplt_en_us.html	Email notifications

2. Install the policy on the DLP Gateway.

Customizing the UserCheck DLP notifications

You can edit files to customize UserCheck notifications. For example, to edit the notification in the screenshot, you edit `quarantine_smtp_uc_notification_tmplt_en_us.html`

Example:


Data Loss Prevention Alert
You might have sent confidential information to mail.google.com.
Violation description: You have sent a message which was matched by the Data Loss Prevention system.
The request is being held until further action.
What would you like to do?
Send
Discard
Cancel
For additional details, please refer to the corporate information security policy. Reference details: {4E81C5AA-E95E-1FDD-77AE-9BC75599EB2D}

1. On the Security Gateway in the `$DLPDIR/backend/conf` directory, edit these UserCheck notification files:

File	Function
inform_ftp_uc_notification_tmplt_en_us.html	ftp protocol when the action is inform
inform_http_uc_notification_tmplt_en_us.html	http protocol when the action is inform
inform_smtp_uc_notification_tmplt_en_us.html	smtp protocol when the action is inform
prevent_ftp_uc_notification_tmplt_en_us.html	ftp protocol when the action is prevent
prevent_http_uc_notification_tmplt_en_us.html	http protocol when the action is prevent
prevent_smtp_uc_notification_tmplt_en_us.html	smtp protocol when the action is prevent
quarantine_ftp_uc_notification_tmplt_en_us.html	ftp protocol when the action is ask
quarantine_http_uc_notification_tmplt_en_us.html	http protocol when the action is ask
quarantine_smtp_uc_notification_tmplt_en_us.html	smtp protocol when the action is ask

2. Install the policy on the DLP Gateway.

Customizing the DLP Portal

Note - Do not change the key because you can use it in more than one place, and a call for a nonexistent key can possibly cause a runtime error. Change only the textual content. Use these rules:

- Keep only HTML
- Must not contain double quotes, dollar sign or backslash symbols
- Can possibly contain HTML entities.
  For example: `&quot;` (double quote), `&#36;` (dollar sign), `&#92;` (backslash)

1. On the Security Gateway, customize the file **$DLPDIR/portal/apache/phpincs/conf/L10N/portal_en_US.php**.
2. To apply the changes, run the `cpstop` and `cpstart` commands on the Security Gateway.

Customizing notification text in SmartConsole???Should this be SMARTDASHBOARD variable instead of the SMARTCONSOLE variable???

1. Open SmartConsole???Should this be SMARTDASHBOARD variable instead of the SMARTCONSOLE variable??? > **Data Loss Prevention** .
2. From the categories on the left, select **Policy**.
3. In a rule that has notification as part of the **Action**, right-click **Action** and select **Edit Notification**.
4. Change the notification text.
5. Install the policy on the DLP Gateway.

Important - You loose changes in the files when you upgrade to the higher version. We recommend you keep a copy of the all changes in files, to overwrite upgraded files.

Localizing DLP User-Related Notifications

You can localize the text of all user-related notifications to a language other than US English.

Change notification text in email, UserCheck, and portal backend files, and in SmartConsole to the same language.

Note - DLP can detect Data Types in all languages.

Supporting LDAP Servers with UTF-8 Records

By default, DLP supports LDAP users with English-language ASCII encoding only.

To support LDAP servers with UTF-8 user records:

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. On the left, select **Managed Objects** > **Servers**.
4. For each LDAP Account Unit named <*ldap_au_name*> that stores credentials in UTF-8, change the value of the **SupportUnicode** attribute to `true`.
5. Save the changes.
6. Close Database Tool (GuiDBEdit Tool).
7. In SmartConsole, install policy on the DLP Gateway.

Configuring the Corporate Guidelines Link

You can set up a link to your corporate Data Loss Prevention guidelines. It is embedded in notification emails. Your guidelines help the user to decide whether it is safe to send a message matched on the Ask User rules.

By default there is no link defined for corporate guidelines. You define this link for each DLP Gateway.

To configure a link to your corporate guidelines:

1. Open a command line on the DLP Gateway.
2. Open the **$DLPDIR/config/dlp.conf** file.
3. In the **backend** section, **corporate_info_link** parameter, add your link.
4. Do **Install Policy** on the DLP Gateway.

Editing Extreme Condition Values

You can configure two options for extreme conditions in SmartConsole that determine when to prefer connectivity:

- **When the Gateway is under heavy CPU load** - Select this option to keep connectivity when the CPU load is more than the permitted high watermark. This option is cleared by default.
  - When you select this checkbox and there is a heavy load condition - FTP and HTTP traffic is bypassed and not inspected. By default, only SMTP traffic is continuously inspected. Full DLP inspection resumes when the CPU load returns to a value below the low watermark.
  - When you clear this checkbox and there is a heavy load condition - FTP, HTTP and SMTP traffic is continuously inspected.
- **Under all other extreme conditions** - Select this option to keep connectivity under extreme conditions (internal errors or too large message sizes). This option is selected by default.
  - When you select this checkbox and there is an internal error or a message exceeds the maximum size - all traffic is allowed.
  - When you clear this checkbox and there is an internal error or a message exceeds the maximum size - all traffic is blocked.

These options are configured in **SmartConsole** in the **Data Loss Prevention** tab > **Additional Settings** > **Advanced** > **Extreme Conditions** section.

You can see the default values for **extreme conditions** in the Database Tool (GuiDBEdit Tool). With Database Tool (GuiDBEdit Tool), you can edit the default values for parameters related to **extreme conditions** (see fields below).

To edit Extreme Condition field values:

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. In the left pane, select **Table > Other > dlp_data_tbl**.
4. In the right pane, select **dlp_general_settings_object**.
5. In the bottom pane, in the **Field Name** column, find **engine_settings**.
6. You can configure these fields if the **When the Gateway is under heavy CPU load** checkbox is selected:

Field Name	Description	Default Value
`cpu_high_watermark`	Threshold for stopping inspection on heavy load. When CPU load is more than the defined threshold, DLP bypasses the protocols set to True.	90%
`cpu_low_watermark`	Threshold for resuming inspection after the `cpu_high_watermark` was reached. When CPU load is less than the defined threshold, DLP inspects the protocols set to True.	70%
`prefer_connectivity_on_heavy_load_protocols > ftp_inspection`	By default, DLP **bypasses** FTP traffic on heavy load. If you change this to false, FTP is inspected on heavy load.	true
`prefer_connectivity_on_heavy_load_protocols > http_inspection`	By default, DLP **bypasses** HTTP traffic on heavy load. If you change this to false, HTTP is inspected on heavy load.	true
`prefer_connectivity_on_heavy_load_protocols > smtp_inspection`	By default, DLP **inspects** SMTP traffic on heavy load. If you change this to true, SMTP is bypassed on heavy load.	false

7. You can configure these fields if the **Under all other extreme conditions** checkbox is selected:

Field Name	Description	Default Value

`ftp_max_files`
`http_max_files`
`smtp_max_files`
	The maximum number of files (attachments) in an FTP/HTTP/SMTP message.	100

Field Name	Description	Default Value

`ftp_max_message_size_in_mega`
`http_max_message_size_in_mega`
`smtp_max_message_size_in_mega`
	The maximum size in MB of an FTP/HTTP/SMTP message.	150

`max_recursion_level`	How many recursion levels deep can be done for archived messages.	6

8. Save the changes and close Database Tool (GuiDBEdit Tool).
9. In SmartConsole, install policy.

Note - It is possible to either prefer connectivity or security upon cluster failover. You can set this in **Gateway Cluster Properties** > **IPS** > **Upon Cluster Failover**.

Editing Exchange Security Agent Values

You can edit default values for parameters related to the Exchange Security Agent (see *"Configuring the Exchange Security Agent" on page 51*) with the *Database Tool (GuiDBEdit Tool)* or dbedit (see sk13301).

To edit Exchange Security Agent values:

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. In the left pane, go to **Table > Other > dlp_data_tbl**.
4. In the right pane, select the **Exchange Agent object** that represents the SmartConsole Exchange Security Agent object.
5. In the bottom pane, in the **Field Name** column, you can configure these fields:

Field Name	Description	Default Value
`is_tap_mode`	The Exchange Security Agent sends messages to the Security Gateway but does not wait for a response from the Security Gateway. For all rules with the detect or inform action, the Exchange Security Agent is automatically configured to work in tap mode. For other rules, the default is to not work in tap mode. If you want the system to always work in tap mode, change the value from false to true.	False
`scan_mails_ received_from_ sender_out_of_ my_organization`	If to scan SMTP messages from a domain that is not in the organization's Exchange. By default this value is false. This means that it only scans messages from your organization's Exchange. To scan messages from senders outside of the domain, change the value to true.	False
`scan_mails_ send_to_ recipient _ from_my_ organization`	If to scan internal traffic.	True

Field Name	Description	Default Value
scan_mails_ send_to_ recipient _out_my_ organization	If to scan messages sent outside of the organization.	True
dont_scan_smtp	Scans messages received by the Exchange server in SMTP. This means that messages in SMTP that come from the same domain get scanned.	False

6. In the right pane, select **dlp_general_settings_objects** to configure this field:

Field Name	Description	Default Value
exchange_send_ status_to_gw _frequency	The time interval that the Exchange Security Agent sends statuses to the Security Gateway.	10
user_dlp_logs_ customization _settings > send_log_for_ each _skipped_ email_with_ allow_status	If to send logs about messages that are not sent to the Security Gateway because of the Inspection Scope settings.	False

7. In the left pane, select **Network Objects** > < **Network Objects** > **<Security Gateway object>** > **data_loss_prevention_blade_settings** to configure this field:

Field Name	Description	Default Value
encrypt_ exchange_ traffic	The Exchange Security Agent sends traffic to the Security Gateway encrypted in TLS.	True

8. Save the changes.
9. Close Database Tool (GuiDBEdit Tool).
10. In SmartConsole, install policy.

Configuring HTTP Inspection on All Ports

You can configure inspection of HTTP transmissions on all ports (standard HTTP ports 80, 8080, and other non-standard ports you might have configured).

To enable HTTP inspection on all ports:

1. In **SmartConsole**, click **Gateways & Servers** and double-click the **Security Gateway**.

   The Security Gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Data Loss Prevention** > **Protocols**.
3. Click **default protocols**.

   The **Default Protocols** window opens.
4. Click **Enable HTTP inspection on nonstandard ports**.
5. Click **OK**.

   Note - When you set HTTP inspection on all ports there is a performance impact.
6. Close the Security Gateway window.
7. Install Policy.

Defining New File Types

You can define a Data Type based on a file type with the "File Attributes" Data Type. This Data Type offers several file type families.

To add a new file type to the File Data Type options:

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. Under **Other** > **dlp_data_tbl** create a new object of **file_type** type.
4. Name the object **file_type_*<ID>***. For the full list of IDs see the table below.
5. Enter a name for the file type in the **visual_string** field.
6. (Optional) Enter a description for the file type in the **description** field.
7. Save the new changes and close Database Tool (GuiDBEdit Tool).
8. In SmartConsole, install policy.

Supported File Types

Supported File Types

Table: Supported File Types

ID	File Type	ID	File Type
1	Word for DOS 4.x	2	Word for DOS 5.x
3	Wordstar 5.0	4	Wordstar 4.0
5	Wordstar 2000	6	WordPerfect 5.0
7	MultiMate 3.6	8	MultiMate Advantage 2
9	IBM DCA/RFT	10	IBM DisplayWrite 2 or 3
11	SmartWare II	12	Samna
13	PFS: Write A	14	PFS: Write B
15	Professional Write 1	16	Professional Write 2
17	IBM Writing Assistant	18	First Choice WP
19	WordMarc	20	Navy DIF

Table: Supported File Types (continued)

ID	File Type	ID	File Type
21	Volkswriter	22	DEC DX 3.0 and below
23	Sprint	24	WordPerfect 4.2
25	Total Word	26	Wang IWP
27	Wordstar 5.5	28	Wang WPS
29	Rich Text Format (RTF)	30	Mac Word 3.0
31	Mac Word 4.0	32	Mass 11
33	MacWrite II	34	XyWrite / Nota Bene
35	IBM DCA/FFT	36	Mac WordPerfect 1.x
37	IBM DisplayWrite 4	38	Mass 11
39	WordPerfect 5.1/5.2	40	MultiMate 4.0
41	Q&A Write	42	MultiMate Note
43	PC File 5.0 Doc	44	Lotus Manuscript 1.0
45	Lotus Manuscript 2.0	46	Enable WP 3.0
47	Windows Write	48	Microsoft Works 1.0
49	Microsoft Works 2.0	50	Wordstar 6.0
51	OfficeWriter	52	Mac Word 4.x Complex
53	IBM DisplayWrite 5	54	Word for Windows 1.x
55	Word for Windows 1.x complex	56	Ami
57	Ami Pro	58	First Choice 3 WP
59	Mac WordPerfect 2.0	60	Mac Works 2.0 WP
61	Professional Write Plus	62	Legacy
63	Signature	64	Wordstar for Windows
65	Word for Windows 2.0	66	JustWrite 1.0

Table: Supported File Types (continued)

ID	File Type	ID	File Type
67	Wordstar 7.0	68	Windows Works WP
69	JustWrite 2.0	70	Ami [Clip]
71	Legacy [Clip]	72	Pro Write Plus [Clip]
73	Mac Word 5.x	74	Enable WP 4.x
75	WordPerfect 6.0	76	Word for DOS 6.x
77	DEC DX 3.1	78	WordPerfect Encrypted
79	Q&A Write 3	80	Mac WordPerfect 3.0
83	WordPerfect 5.1 Far East	84	Ichitaro 3.x
85	Ichitaro 4.x/5.x/6.x	86	Word for Windows 1.2 J
87	Word for Windows 5.0 J	88	Matsu 4
89	Matsu 5	90	P1 Japan
91	Rich Text Format Japan	92	CEO Write
93	Windows Works 3.0 WP	94	Microsoft WordPad
95	WP/Novell Unknown Format	96	Word for Windows 2.0 Object
97	WordPerfect 6.1 - 12.0 / X3	98	Fulcrum Document Format
99	Europa Fulcrum 5	100	Europa Fulcrum 6
101	Internet HTML	102	Word 7.0
103	Arehangeul	104	Hana
105	Windows Works 4.0 WP	106	PerfectWorks for Windows
107	WordPerfect 7.0/8.0/10.0	108	WordPro 96
109	HTML - Central European	110	HTML - Japanese (ShiftJIS)
111	HTML - Japanese (EUC)	112	HTML - Chinese (Big5)
113	HTML - Chinese (EUC)	114	HTML - Chinese (GB)

Table: Supported File Types (continued)

ID	File Type	ID	File Type
115	HTML - Korean (Hangul)	116	HTML - Cyrillic (ANSI 1251)
117	HTML - Cyrillic (KOI8-R)	118	Text - Cyrillic (ANSI 1251)
119	Cyrillic (KOI8-R)	120	WWRITE - Japan SJIS
121	WWRITE - Chinese GB	122	WWRITE - Hangul
123	WWRITE - Chinese BIG5	124	Digital WPS Plus
125	Mac Word 6	126	Microsoft Word 97/98
127	Rainbow	128	Interleaf 6
129	MIFF 3.0	130	MIFF 4.0
131	MIFF 5.0	132	Text Mail
133	Mac Word 97	134	Interleaf Japan
135	MIFF 3.0 Japan	136	MIFF 4.0 Japan
137	MIFF 5.0 Japan	138	MIFF 5.5
139	WordPerfect 8.0/10.0	140	Ichitaro 8.x/9.x/10.x/11.x/12.x/13.x/2004
141	vCard	142	HTML - Cascading Style Sheets
143	MS Outlook	144	Pocket Word
145	WordPro 97/Millennium	146	Microsoft Word 2000
147	Word 2000 HTML	148	Excel 2000 HTML
149	PowerPoint 2000 HTML	150	Extensible Markup Language (XML)
151	Wireless Markup Language (WML)	152	WMLB
153	HTML - Japanese (JIS)	154	WML - Chinese (Big5)
155	WML - Chinese (EUC)	156	WML - Chinese (GB)
157	WML - Cyrillic (ANSI 1251)	158	WML - Cyrillic (KOI8-R)

Table: Supported File Types (continued)

ID	File Type	ID	File Type
159	WML - Japanese (JIS)	160	WML - Japanese (ShiftJIS)
161	WML - Japanese (EUC)	162	WML - Korean (Hangul)
163	WML - Central European	164	WML - CSS
165	StarOffice 5.2 Writer	166	MIFF 6.0
167	MIFF 6.0 Japan	168	MIFF
169	Java Script	170	ASCII Text
171	Handheld Device Markup Language (HDML)	172	Compact HTML (CHTML)
173	XHTML Basic	174	AvantGo HTML
175	Web Clipping Application (WCA) HTML	176	SearchML
177	Pocket Word - Pocket PC	178	Wireless HTML
179	Hangul 97 Word Processor	180	Hangul 2002 - 2007 Word Processor
181	Internet HTML - Unicode	182	XML With Doctype HTML
184	EBCDIC encoded Text	185	Microsoft Word 2002
186	Microsoft Word 2003/2004	187	Internet Message
188	StarOffice 6 & 7 Writer	189	Microsoft Outlook PST/OST 97/2000/XP
190	XHTML	191	Microsoft Works 2000
192	Internet Mail Message	193	Internet News Message
194	Outlook Express News Message	195	Outlook Express Mail Message
196	vCalendar	197	Transport-Neutral Encapsulation Format(TNEF)
198	MHTML(Web Archive)	199	Search HTML

Table: Supported File Types (continued)

ID	File Type	ID	File Type
200	Search Text	201	PST Fields File
202	Microsoft Outlook PST/OST 2003/2007	203	Microsoft Outlook PAB
204	SearchML 20	205	SearchML 30
206	Yahoo! Messenger Archive	207	Microsoft Word XML 2003
208	MS Office 12 Word format	209	StarOffice 8/Open Office 2.x Writer
210	SearchML 31	211	Outlook Form Template
212	Microsoft Word 2007	213	Password Protected Microsoft Word 2007
214	Microsoft Word 2007 Template	215	SearchML 32
216	DRM protected Unknown	217	DRM protected Microsoft Word
218	DRM protected Microsoft Word 2007	219	File sealed by Oracle IRM
220	Extensible Metadata Platform	221	SearchML 33
222	PHTML	223	Open Office Writer 6
224	Open Office Writer 8	225	IBM Lotus Symphony Document
226	SearchML 34	227	MS Office 12 (2007) Word - Macro Enabled XML format
228	MS Office 12 (2007) Word Template - Macro Enabled XML format	229	Microsoft Word Picture
230	Smart DataBase	231	DBase III
232	DBase IV or V	233	Framework III
234	Microsoft Works DB	235	DataEase 4.x
236	Paradox 2 or 3	237	Paradox 3.5
238	Q&A Database	239	Reflex

Table: Supported File Types (continued)

ID	File Type	ID	File Type
240	R:Base System V	241	R:Base 5000
242	R:Base File 1	243	R:Base File 3
244	First Choice DB	245	Mac Works 2.0 DB
246	Windows Works DB	247	Paradox
248	Microsoft Access	249	CEO Decision Base
250	Windows Works 3.0 DB	251	Windows Works 4.0 DB
252	Microsoft Access 7	253	Microsoft Project 98
254	Microsoft Project 2000/2002/2003	255	Microsoft Project 2002
256	MS Project 2007	257	Lotus Notes database
258	Symphony	259	Lotus 1-2-3 1.0
260	Lotus 1-2-3 2.0	261	Lotus 1-2-3 3.x
262	Smart Spreadsheet	263	Microsoft Excel 2.x
264	Enable Spreadsheet	265	Microsoft Works SS
266	VP-Planner	267	Mosaic Twin
268	SuperCalc 5	269	Quattro Pro
270	Quattro	271	PFS: Plan
272	First Choice SS	273	Microsoft Excel 3.0
274	Generic WKS	275	Mac Works 2.0 SS
276	Windows Works SS	277	Microsoft Excel 4.0
278	Quattro Pro for Windows	279	Lotus 1-2-3 4.x / 5.x
280	Quattro Pro Windows Japan	281	CEO Spreadsheet
282	Microsoft Excel 5.0/7.0	283	Multiplan 4.0
284	Windows Works 3.0 SS	285	Quattro Pro 4.0

Table: Supported File Types (continued)

ID	File Type	ID	File Type
286	Quattro Pro 5.0	287	Quattro Pro Win 6.0
288	Lotus 123 Release 2 for OS/2	289	Lotus 123 for OS/2 Chart
290	Windows Works 4.0 SS	291	Quattro Pro Win 7.0/8.0
292	Quattro Pro Win 7.0/8.0 Graph	293	Lotus 1-2-3 97 Edition
294	Microsoft Mac Excel 4.0	295	Microsoft Mac Excel 5.0
296	Microsoft Excel 97/98/2004	297	MS Excel 3.0 Workbook
298	MS Excel 4.0 Workbook	299	MS Excel Mac 4.0 Workbook
300	MS Excel Mac 4.0 Workbook	301	Lotus 1-2-3 98/Millennium Edition
302	Quattro Pro 8.0	303	Quattro Pro Win 9.0 / X3
304	Microsoft Excel 2000	305	Quattro Pro Win 10.0
306	Microsoft Excel 2002	307	StarOffice 5.2 Calc
308	Quattro Pro Win 11.0	309	Microsoft Excel 2003
310	StarOffice 6 & 7 Calc	311	Quattro Pro Win 12.0
312	StarOffice 8/Open Office 2.x Calc	313	Microsoft Excel 2007
314	Password Protected Microsoft Excel 2007	315	Microsoft Excel 2007 Binary
316	DRM protected Microsoft Excel 2007	317	DRM protected Microsoft Excel 2007
318	MS Works SS6	319	Open Office Calc 6
320	Open Office Calc 8	321	IBM Lotus Symphony Spreadsheet
322	Excel Template 2007	323	Excel Macro Enabled
324	Excel Template Macro Enabled 2007	325	Windows Bitmap

Table: Supported File Types (continued)

ID	File Type	ID	File Type
326	Tagged Image File Format	327	Paintbrush
328	Compuserve GIF	329	EPS (TIFF Header)
330	CCITT Group 3 Fax	331	Mac PICT2
332	WordPerfect Graphic	333	Windows Metafile
334	Lotus PIC	335	Mac PICT
336	Ami Draw	337	Targa
338	GEM Image	339	OS/2 Bitmap
340	Windows Icon	341	Windows Cursor
342	Micrografx product	343	MacPaint
344	Corel Draw 2.0	345	Corel Draw 3.0
346	HP Graphics Language	347	Harvard 3.0 Chart
348	Harvard 2.0 Chart	349	Harvard 3.0 Presentation
350	Freelance	351	WordPerfect Graphic 2
352	CGM Graphic Metafile	353	Excel 2.x Chart
354	Excel 3.0 Chart	355	Excel 4.0 Chart
356	Candy 4	357	Hanako 1.x
358	Hanako 2.x	359	JPEG File Interchange
360	Excel 5.0/7.0 Chart	361	Corel Draw 4.0
362	PowerPoint 4.0	363	Multipage PCX
364	PowerPoint 3.0	365	Corel Draw 5.0
366	OS/2 Metafile	367	PowerPoint 7.0
368	AutoCAD DXF (ASCII)	369	AutoCAD DXF (Binary)
370	AutoCAD DXB	371	Freelance 96/97/Millennium Edition

Table: Supported File Types (continued)

ID	File Type	ID	File Type
372	Mac PowerPoint 3.0	373	Mac PowerPoint 4.0
374	WordPerfect Presentations	375	OS/2 Warp Bitmap
376	AutoCAD Drawing 12	377	AutoCAD Drawing 13
378	Adobe Illustrator	379	Corel Presentations 7.0 - 12.0 / X3
380	WordPerfect Graphic 7.0/8.0/9.0	381	Adobe Acrobat (PDF)
382	Framemaker	383	RAS - Sun Raster
384	AutoShade Rendering	385	Kodak Photo CD
386	PowerPoint 4.0 (extracted from docfile)	387	Mac PowerPoint 4.0 (extracted from docfile)
388	Enhanced Windows Metafile	389	GEM
390	Mac PowerPoint 3.0	391	Mac PowerPoint 4.0
392	Harvard Graphics for Windows	393	IGES Drawing File Format
394	IBM Picture Interchange Format	395	X-Windows Bitmap
396	X-Windows Pixmap	397	CALS Raster File Format
398	Portable Network Graphics Format	399	X-Windows Dump
400	CorelDraw ClipArt	401	HP Gallery
402	Graphics Data Format	403	Micrografx Designer
404	Post Script	405	Microsoft PowerPoint 97-2004
406	Corel Draw 6.0	407	Corel Draw 7.0
408	PDF MacBinary Header	409	AutoCAD Drawing - Unknown Version
410	Visio 4.x	411	AutoCAD Drawing 14
412	PBM (Portable Bitmap)	413	PGM (Portable Graymap)
414	PPM (Portable Pixmap)	415	Adobe Photoshop

Table: Supported File Types (continued)

ID	File Type	ID	File Type
416	Microsoft PowerPoint Dual 95/97	417	Paint Shop Pro
418	Kodak FlashPix	419	Visio 5.x
420	Corel Draw 8.0	421	Visio 6.x
422	Corel Draw 9.0	423	Progressive JPEG
424	Microsoft PowerPoint 2000/2002	425	Bentley Microstation DGN
426	Windows 98/2000 Bitmap	427	Wireless Bitmap
428	MIFF Graphic	429	Microsoft PowerPoint 2
430	WordPerfect Graphic 10.0	431	Visio 3.x
432	Micrografx Designer	433	PDF Image
434	StarOffice 5.2 Impress	435	Adobe Illustrator 9
436	AutoCAD 2000/2002 Drawing	437	AutoCAD 2.5 Drawing
438	AutoCAD 2.6 Drawing	439	AutoCAD 9 Drawing
440	AutoCAD 10 Drawing	441	QuarkXPress 3.0 For Macintosh
442	QuarkXPress 3.1 For Macintosh	443	QuarkXPress 3.2 For Macintosh
444	QuarkXPress 3.3 For Macintosh	445	QuarkXPress 4.0 For Macintosh
446	QuarkXPress 3.3 For Windows	447	QuarkXPress 4.0 For Windows
448	QuarkXPress 5.0 For Windows	449	Export Image
450	StarOffice 6 & 7 Draw	451	StarOffice 6 & 7 Impress
452	JBIG2 Bitmap	453	Corel Draw 10.0
454	Corel Draw 11.0	455	Microsoft Visio 2003
456	StarOffice 8 Draw	457	StarOffice 8/Open Office 2.x Impress
458	AutoCAD 2004/2005/2006 Drawing	459	Microsoft PowerPoint 2007

Table: Supported File Types (continued)

ID	File Type	ID	File Type
460	Microsoft XML Paper Specification	461	Password Protected Microsoft Powerpoint 2007
462	AutoCAD 2007 Drawing	463	OS/2 v.2 Bitmap
464	StarView Metafile	465	eFax Document
475	DRM protected Microsoft Powerpoint	476	DRM protected Microsoft Powerpoint 2007
477	AutoDesk DWF	478	Corel Draw 12.0
479	JPEG 2000	480	Adobe Indesign
481	JPEG 2000 jpf Extension	482	JPEG 2000 mj2 Extension
483	WordPerfect Informs 1.0	484	Lotus Screen SnapShot
485	Lotus Screen Snapshot	486	Interchange Format
487	Microsoft Escher Graphics	488	Windows Sound
489	Windows Video	490	MIDI File
491	Macromedia Director	492	Macromedia Flash
493	Macromedia Flash	494	Quicktime Movie
495	MPEG Layer3 ID3 Ver 1.x	496	MPEG Layer3 ID3 Ver 2.x
497	ID3 Ver 1.x	498	ID3 Ver 2.x
499	MPEG-1 audio - Layer 3	500	MPEG-1 audio - Layer 1
501	MPEG-1 audio - Layer 2	502	MPEG-2 audio - Layer 1
503	MPEG-2 audio - Layer 2	504	MPEG-2 audio - Layer 3
505	Advanced Systems Format	506	Windows Media Video (ASF subtype)
507	Windows Media Audio (ASF subtype)	508	Microsoft Digital Video Recording (ASF subtype)

Table: Supported File Types (continued)

ID	File Type	ID	File Type
509	Real Media (both Real Audio and Real Video)	510	MPEG-1 video
511	MPEG-2 video	512	ISO Base Media File Format
513	MPEG-4 file	514	MPEG-7 file
515	EXE / DLL File	516	.COM File
517	.ZIP File	518	Self UnZIPping .EXE
519	.ARC File	520	MS Office Binder
521	UNIX Compress	522	UNIX Tar
523	Envoy	524	QuickFinder
525	Windows Clipboard File	526	Envoy 7
527	StuffIt	528	LZH Compress
529	Self-Extracting LZH	530	UNIX GZip
531	Java Class File	532	mbox(RFC-822 mailbox)
533	Lotus Notes Database R6.x	534	Generic Password Protected Microsoft Office 2007 Document
535	Microsoft Cabinet File	536	.RAR File
537	Self extracting RAR File	538	Microsoft InfoPath
549	Flexiondoc 1 (original) schema	550	Flexiondoc 2 schema
551	Flexiondoc 3 schema	552	Flexiondoc 4 schema
553	Flexiondoc 5 schema	554	Flexiondoc 5.1 schema
555	OASIS OpenDocument v1.0	556	Flexiondoc 5.2 schema
557	Domino XML schema	558	Adobe Indesign Interchange
559	XML Visio	560	Mail archive DXL
561	Mail message DXL	562	Generic DXL

Table: Supported File Types (continued)

ID	File Type	ID	File Type
564	AutoCAD DWG 2008	565	Publisher 2003
566	Publisher 2007	567	Open Office Impress 6
568	Open Office Impress 8	569	IBM Lotus Symphony Presentations
570	Open Office Draw 6	571	Open Office Draw 8
572	PowerPoint 2007 Template	573	PowerPoint 2007 Macro Enabled
574	PowerPoint 2007 Template Macro Enabled	575	PowerPoint 2007 Slideshow file
576	PowerPoint 2007 Template Macro Enabled	577	Oracle Multimedia internal raster format
578	TK thesaurus	579	TK abbrev
580	TK dictionary	581	TK quote
582	TK written word	583	TK culturelit
584	TK grammar	585	TK thessyn
586	Text - (ASCII)	587	Text - (Hex)
588	Text - (ANSI)	589	Text - (Unicode)
590	Text - (ASCII)	591	Text - (ANSI 8)
592	Text - Unknown format	593	Text - MAC - 7bit
594	Text - MAC - 8bit	595	Text - Japanese (ShiftJIS)
596	Text - Chinese (GB)	597	Text - Korean (Hangul)
598	Text - Chinese (Big 5)	599	Code page 852 - MS DOS Slavic
600	Text - Japanese (EUC)	601	Text - Hebrew (7-bit)
602	Text - Hebrew (IBM PC8)	603	Text - Hebrew (VAX E0)
604	Text - Hebrew (Windows ANSI 1255)	605	Text - Arabic 710

Table: Supported File Types (continued)

ID	File Type	ID	File Type
606	Text - Arabic 720	607	Text - Arabic (Windows ANSI 1256)
609	Text - Japanese (JIS)	610	Text - Central European
611	UTF-8 encoded Text	612	Text - U.S. English/Portuguese (EBCDIC 37)
613	Text - Austrian/German (EBCDIC 273)	614	Text - Danish/Norwegian (EBCDIC 277)
615	Text - Finnish/Swedish (EBCDIC 278)	616	Text - Italian (EBCDIC 280)
617	Text - Spanish (EBCDIC 284)	618	Text - U.K. English (EBCDIC 285)
619	Text - French (EBCDIC 297)	620	Text - Belgian/International (EBCDIC 500)
621	Text - Eastern European (EBCDIC 870)	622	Text - Icelandic (EBCDIC 871)
623	Text - Turkish (EBCDIC 1026)	624	HTML - U.S. English/Portuguese (EBCDIC 37)
625	HTML - Austrian/German (EBCDIC 273)	626	HTML - Danish/Norwegian (EBCDIC 277)
627	HTML - Finnish/Swedish (EBCDIC 278)	628	HTML - Italian (EBCDIC 280)
629	HTML - Spanish (EBCDIC 284)	630	HTML - U.K. English (EBCDIC 285)
631	HTML - French (EBCDIC 297)	632	HTML - Belgian/International (EBCDIC 500)
633	HTML - Eastern European (EBCDIC 870)	634	HTML - Icelandic (EBCDIC 871)
635	HTML - Turkish (EBCDIC 1026)	636	UUE Encoded Text
637	UUE Encoded Continued Part	638	XXE Encoded Text
639	XXE Encoded Continued Part	640	YEnc Encoded Text

Table: Supported File Types (continued)

ID	File Type	ID	File Type
641	YEnc Encoded Continued Part	642	BinHex Encoded Text
643	BinHex Encoded Continued Part	644	Text - Arabic (ASMO-708)
645	Text - Arabic (DOS OEM 720 TRANSPARENT ASMO)	646	Text - Arabic (ISO 8859-6)
647	Text - Arabic (Mac)	648	Text - Baltic (ISO 8859-4)
649	Text - Baltic (Windows ANSI 1257)	650	Text - Central European (DOS OEM 852 Latin II)
651	Text - Central European (ISO 8859-2)	652	Text - Central European (Mac)
653	Text - Central European (Windows ANSI 1250)	654	Text - Chinese Simplified (Windows ANSI 936 [GB2312])
655	Text - Chinese Traditional (Windows ANSI 950 [BIG5])	656	Text - Cyrillic (DOS OEM 855)
657	Text - Cyrillic (ISO 8859-5)	658	Text - Cyrillic (KOI8-R)
659	Text - Cyrillic (Mac)	660	Text - Cyrillic (Windows ANSI 1251)
661	Text - Greek (ISO 8859-7)	662	Text - Greek (Mac)
663	Text - Greek (Windows ANSI 1253)	664	Text - Hebrew (DOS OEM 862)
665	Text - Hebrew (ISO 8859-8)	666	Text - Japanese (Mac)
667	Text - Korean (Windows ANSI 1361 [Johab])	668	Text - Korean (Windows ANSI 949)
669	Text - Russian (DOS OEM 866)	670	Text - Thai (Windows ANSI 874)
671	Text - Turkish (DOS OEM 857)	672	Text - Turkish (ISO 8859-9)
673	Text - Turkish (Mac)	674	Text - Turkish (Windows ANSI 1254)
675	Text - Vietnamese (Windows ANSI 1258)	676	Text - Western European (ISO 8859-1)

Table: Supported File Types (continued)

ID	File Type	ID	File Type
677	Text - Western European (Mac)	678	Text - Western European (Windows ANSI 1252)
679	HTML - Arabic (ASMO-708)	680	HTML - Arabic (DOS OEM 720 TRANSPARENT ASMO)
681	HTML - Arabic (ISO 8859-6)	682	HTML - Arabic (Mac)
683	HTML - Arabic (Windows ANSI 1256)	684	HTML - Baltic (ISO 8859-4)
685	HTML - Baltic (Windows ANSI 1257)	686	HTML - Central European (DOS OEM 852 Latin II)
687	HTML - Central European (ISO 8859-2)	688	HTML - Central European (Mac)
689	HTML - Central European (Windows ANSI 1250)	690	HTML - Chinese Simplified (EUC)
691	HTML - Chinese Simplified (Windows ANSI 936 [GB2312])	692	HTML - Chinese Traditional (Windows ANSI 950 [BIG5])
693	HTML - Cyrillic (DOS OEM 855)	694	HTML - Cyrillic (ISO 8859-5)
695	HTML - Cyrillic (KOI8-R)	696	HTML - Cyrillic (Mac)
697	HTML - Cyrillic (Windows ANSI 1251)	698	HTML - Greek (ISO 8859-7)
699	HTML - Greek (Mac)	700	HTML - Greek (Windows ANSI 1253)
701	HTML - Hebrew (DOS OEM 862)	702	HTML - Hebrew (ISO 8859-8)
703	HTML - Hebrew (Windows ANSI 1255)	704	HTML - Japanese (Mac)
705	HTML - Japanese (Windows Shift-JIS ANSI 932)	706	HTML - Korean (Windows ANSI 1361 [Johab])
707	HTML - Korean (Windows ANSI 949)	708	HTML - Russian (DOS OEM 866)

Table: Supported File Types (continued)

ID	File Type	ID	File Type
709	HTML - Thai (Windows ANSI 874)	710	HTML - Turkish (DOS OEM 857)
711	HTML - Turkish (ISO 8859-9)	712	HTML - Turkish (Mac)
713	HTML - Turkish (Windows ANSI 1254)	714	HTML - Vietnamese (Windows ANSI 1258)
715	HTML - Western European (ISO 8859-1)	716	HTML - Western European (Mac)
717	HTML - Western European (Windows ANSI 1252)	718	Plugin
719	Text - Japanese (ShiftJIS)	720	Windows Metafile [5000]
721	WordPerfect Graphic [B]	722	Ami (internal bitmap)
723	Word (internal bitmap)	724	Mac PICT2 Binary
725	Windows Metafile [5005]	726	Windows Metafile [5006]
727	PerfectWorks Picture	728	WPG2 (internal bitmap)
729	Windows DIB	730	WPG1 (internal bitmap)
731	Embedded Bitmap	732	Embedded Bitmap
733	IAF (internal bitmap)	734	IAF (internal bitmap)
735	PICT (internal bitmap)	736	Export OCR data as Text, no formatting
737	Export OCR data as RTF, yes formatting	738	Export OCR data as HTML
739	EDRM export	753	Open Office 3.x Writer (ODF 1.2)
754	StarOffice 9 Writer (ODF 1.2)	755	Oracle Open Office 3.x Writer (ODF 1.2)
756	Samsung Jungum File	757	Kingsoft Office Writer File
758	Microsoft Word 2010	759	Microsoft Word 2010 Template

Table: Supported File Types (continued)

ID	File Type	ID	File Type
760	Microsoft Word 2010 Macro Enabled Document	761	Microsoft Word 2010 Macro Enabled Template
764	Microsoft Project 2010	765	Microsoft Excel XML 2003
766	Open Office 3.x Calc (ODF 1.2)	769	Microsoft Excel 2007 Excel Add-in Macro File
770	Lotus Data Interchange Format	771	StarOffice 9 Calc (ODF 1.2)
772	Oracle Open Office 3.x Calc (ODF 1.2)	773	Kingsoft Office Spreadsheet File
774	Corel Presentations X4	775	Microsoft Excel 2010 Macro Enabled Workbook
776	Microsoft Excel 2010 Template	777	Microsoft Excel 2010 Macro Enabled Template
784	Windows Media Player Playlist	786	Flexiondoc v5.4 (XML)
790	Open Office 3.x Impress (ODF 1.2)	791	Open Office 3.x Draw (ODF 1.2)
792	Corel Presentations X4	793	Microsoft Access Report Snapshot 2000 - 2003
794	StarOffice 9 Impress (ODF 1.2)	795	StarOffice 9 Draw (ODF 1.2)
796	Oracle Open Office 3.x Impress (ODF 1.2)	797	Oracle Open Office 3.x Draw (ODF 1.2)
798	Microsoft PowerPoint 2010	799	Microsoft PowerPoint 2010 Template
800	Microsoft PowerPoint 2010 Macro Enabled Template	801	Microsoft PowerPoint 2010 Slideshow
802	Microsoft PowerPoint 2010 Macro Enabled Presentation	803	Microsoft PowerPoint 2010 Macro Enabled Slideshow
805	Macromedia Flash 9	806	Macromedia Flash 10
807	Microsoft Windows Explorer Command File	808	7z Archive File

Table: Supported File Types (continued)

ID	File Type	ID	File Type
809	Trillian Text Log File	810	Trillian XML Log File
811	Microsoft Live Messenger Log File	812	AOL Messenger Log File
813	Windows Help File	814	Windows Compiled Help File
815	Windows shortcut	816	TrueType Font File
817	TrueType Font Collection File	818	TrueType (MAC) Font File
819	MS Outlook Appointment File	820	Outlook Appointment Form Template
821	MS Outlook Journal File	822	Outlook Journal Form Template
823	MS Outlook Contact File	824	Outlook Contact Form Template
825	MS Outlook Note File	826	Outlook Note Form Template
827	MS Outlook Task File	828	Outlook Task Form Template
829	Apple Mail 2.0 Message	830	Self extracting 7z Archive File
831	AutoCAD 2010/2011/2012 Drawing	832	Microsoft Access 2000/2002/2003
833	Microsoft Access 2007/2010	834	Microsoft Access Web Database
835	Microsoft Access 2007/2010 Template File	836	Outlook Non Delivery Report
837	Outlook Non Delivery Report Form Template	838	Outlook Post
839	Outlook Post Form Template	840	Outlook Distribution List
841	Outlook Distribution List Form Template	842	Outlook Clear Signed Email
843	Outlook Clear Signed Email Form Template	844	Outlook Opaque Signed Email
845	Outlook Opaque Signed Email Form Template	846	Apple iWork Pages File

Table: Supported File Types (continued)

ID	File Type	ID	File Type
847	Apple iWork Pages File Preview	848	S/MIME (Secure/MIME)
849	Clear Signed S/MIME (Secure/MIME)	850	Microsoft Word 2013
851	Microsoft Word 2013 Template	852	Microsoft Word 2013 Macro Enabled Document
853	Microsoft Word 2013 Macro Enabled Template	854	Quattro Pro Win X5
855	Apple iWork Numbers File	856	Apple iWork Numbers File Preview
857	Microsoft Excel XML 2007/2010	858	Microsoft Excel 2013 Workbook
859	Microsoft Excel 2013 Macro Enabled Workbook	860	Microsoft Excel 2013 Template
861	Microsoft Excel 2013 Macro Enabled Template	862	Microsoft Excel 2013 Excel Add-in Macro File
863	Microsoft Excel 2013 Binary	864	Microsoft OneNote Table of Contents File
865	Microsoft OneNote Package	866	Corel Presentations X5
867	Apple iWork Keynote File	868	Apple iWork Keynote File Preview
869	Scalable Vector Graphics File	870	AutoDesk DWF Archive File
871	Microsoft PowerPoint 2013	872	Microsoft PowerPoint 2013 Template
873	Microsoft PowerPoint 2013 Macro Enabled Template	874	Microsoft PowerPoint 2013 Slideshow
875	Microsoft PowerPoint 2013 Macro Enabled Presentation	876	Microsoft PowerPoint 2013 Macro Enabled Slideshow
877	Microsoft Office Theme File	878	Adobe Photoshop Large Document Format

Table: Supported File Types (continued)

ID	File Type	ID	File Type
879	Digital Imaging and Communications in Medicine (DICOM) File	913	Microsoft Word 2016
914	Microsoft Word 2016 Template	915	Microsoft Word 2016 Macro Enabled Document
916	Microsoft Word 2016 Macro Enabled Template	917	Microsoft PowerPoint 2016
918	Microsoft PowerPoint 2016 Template	919	Microsoft PowerPoint 2016 Macro Enabled Template
920	Microsoft PowerPoint 2016 Slideshow	921	Microsoft PowerPoint 2016 Macro Enabled Presentation
922	Microsoft PowerPoint 2016 Macro Enabled Slideshow	923	Microsoft Excel 2016 Workbook
924	Microsoft Excel 2016 Macro Enabled Workbook	925	Microsoft Excel 2016 Template
926	Microsoft Excel 2016 Macro Enabled Template	927	Microsoft Excel 2016 Excel Add-in Macro File
928	Microsoft Excel 2016 Binary		

Server Certificates

For secure SSL connection, Security Gateways must establish trust with endpoint computers. To do so, they show a *Server Certificate*. This section discusses the procedures necessary to generate and install server certificates.

By default, Check Point Security Gateways use a certificate created by the Internal Certificate Authority on the Security Management Server as their server certificate. Browsers do not trust this certificate. When an endpoint computer connects to the Security Gateway with the default certificate, certificate warning messages open in the browser. To prevent these warning messages, the administrator must install a server certificate signed by a trusted certificate authority.

All portals on the same Security Gateway IP address use the same certificate.

Obtaining, Installing, and Viewing a Trusted Server Certificate

To be accepted by an endpoint computer without a warning, Security Gateways must have a server certificate signed by a known certificate authority (such as Entrust, VeriSign or Thawte). This certificate can be issued directly to the Security Gateway, or be a chained certificate that has a certification path to a trusted root certificate authority (CA).

The next sections describe how to get a certificate for a Security Gateway that is signed by a known Certificate Authority (CA).

Generating the Certificate Signing Request

First, generate a *Certificate Signing Request* (CSR). The CSR is for a *server* certificate, because the Security Gateway acts as a server to the clients.

Note - This procedure creates private key files. If private key files with the same names already exist on the computer, they are overwritten without warning.

1. From the Security Gateway command line, log in to the Expert mode.
2. Run:

   ```
   cpopenssl req -new -out <Name of CSR file> -keyout <Name of
   Private Key file> -config $CPDIR/conf/openssl.cnf
   ```

   This command generates a private key. You see this output:

   ```
   Generating a 2048 bit RSA private key
   .+++
   ...+++
   writing new private key to 'server1.key'
   Enter PEM pass phrase:
   ```

3. Enter a password and confirm.

   Fill in the data.

   - The **Common Name** field is mandatory. This field must have the Fully Qualified Domain Name (FQDN). This is the site that users access. For example: `portal.example.com`.
   - All other fields are optional.

4. Send the CSR file to a trusted certificate authority. Make sure to request a *Signed Certificate* in PEM format. Keep the `.key` private key file.

Generating the P12 File

After you get the Signed Certificate for the Security Gateway from the CA, generate a P12 file that has the Signed Certificate and the private key.

1. Get the Signed Certificate for the Security Gateway from the CA.

   If the signed certificate is in P12 or P7B format, convert these files to a PEM (Base64 encoded) formatted file with a CRT extension.

2. Make sure that the CRT file has the full certificate chain up to a trusted root CA.

   Usually you get the certificate chain from the signing CA. Sometimes it split into separate files. If the signed certificate and the trust chain are in separate files, use a text editor to combine them into one file. Make sure the server certificate is at the top of the CRT file.

3. From the Security Gateway command line, log in to the Expert mode.

4. Use the `*.crt` file to install the certificate with the `*.key` file that you generated.

   a. Run:

   ```
   cpopenssl pkcs12 -export -out <Name of output file> -in
   <Name of signed certificate chain file> -inkey <Name of
   Private Key file>
   ```

   For example:

   ```
   cpopenssl pkcs12 -export -out server1.p12 -in server1.crt
   -inkey server1.key
   ```

   b. Enter the certificate password when prompted.

Installing the Signed Certificate

1. Log in to SmartConsole.
2. From the left Navigation Toolbar, click **Gateways & Servers**.
3. Open the Identity Awareness Gateway object.
4. In the navigation tree, click the appropriate Software Blade page:
   - **Mobile Access** > **Portal Settings**
   - **Platform Portal**
   - **Data Loss Prevention**
   - **Identity Awareness** > **Captive Portal** > **Settings** > **Access Settings**
5. Install the Access Control Policy on the Security Gateway.

Note - The **Repository of Certificates** on the IPsec VPN page of the Security Gateway object is only for self-signed certificates. It does not affect the certificate installed manually using this procedure.

Viewing the Certificate

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.

   The **Security Gateway Properties** window opens and shows the **General Properties** page.

2. From the navigation tree, click **Data Loss Prevention**.

3. In the **Certificate** section, click **View**.

Kerberos Single Sign On

The UserCheck agent supports single sign on through the Kerberos network authentication protocol. Kerberos is the default authentication protocol used in Windows 2000 domains and above.

The Kerberos protocol is based on the idea of *tickets*, encrypted data packets issued by a trusted authority, in this case the Active Directory (AD). When a user logs in, the user authenticates to a domain controller that provides an initial *ticket granting ticket* (TGT). This ticket vouches for the user's identity.

When the user needs to authenticate against the DLP Gateway through the UserCheck agent, the agent presents this ticket to the domain controller and requests a *service ticket* (SR) for a specific resource (the DLP Gateway). The UserCheck agent presents this service ticket to the Security Gateway.

For more detailed information on Kerberos SSO, see:

- http://web.mit.edu/Kerberos/
- http://technet.microsoft.com/en-us/library/bb742433.aspx

Single Sign-On Configuration has two steps:

- **AD Configuration**

  You create a user account and map it to a Kerberos primary name.

  Performing AD Configuration

  The AD configuration involves:

  - Creating a New User Account
  - Mapping the User Account to a Kerberos Principle Name

  Creating a new User Account

  1. In Active Directory, open **Active Directory Users and Computers** (Start > Run > dsa.msc)
  2. Add a new user account. You can select any username and password.

     For example: a user account named `ckpsso` with the password `qwe123!@#` to the domain `corp.acme.com`
  3. Clear **User must change password at next logon** and select **Password Never Expires**.

Mapping the User Account to a Kerberos Principle Name

This step uses the *ktpass* utility to create a Kerberos principal name that is used by both the Security Gateway and the AD. A Kerberos principal name consists of a service name (for the DLP Gateway that the UserCheck agent connect to) and the domain name to which the service belongs.

The *ktpass* is a command-line tool available in Windows 2000 and higher.

Retrieving the correct executable

You must install the correct ktpass.exe version on the AD. Ktpass.exe is not installed by default in Windows 2003.

- Windows 2003:

  1. Retrieve the correct executable for your service pack from the Microsoft Support site prior to installation. It is part of the Windows 2003 support tools. For example, AD 2003 SP2 requires support tools for 2003 sp2.
  2. Download the support.cab and suptools.msi files to a new folder on your AD server.
  3. Run the `suptools.msi`.

- Active Directory 2008:

  The *ktpass* utility is already installed on your server in the Windows\System32 folder and you can run the command line. You need to open the command prompt as an administrator by right clicking it and selecting "run as an Administrator".

Use the ktpass

1. Open a command line to run the *ktpass* tool (**Start** > **Run** > **cmd**).
2. At the command prompt, run *ktpass* with this syntax:

   ```
   ktpass -princ ckp_pdp/domain_name@DOMAIN_NAME -mapuser
   username@domain_name -pass password -out unix.keytab -
   crypto RC4-HMAC-NT
   ```

   Important - Enter the command exactly as shown. It is case-sensitive.

   This is an example of running ktpass with these parameters:

Parameter	Value
domain_name@DOMAIN_NAME	corp.acme.com@CORP.ACME.COM
username@domain_name	ckpsso@corp.acme.com
password	qwe123@#

The AD is ready to support Kerberos authentication for the Security Gateway.

The example above shows the *ktpass* syntax on Windows 2003. When using Windows 2008/2008 R2 Server, the *ktpass* syntax is slightly different. Parameters are introduced using a forward slash "/" instead of a hyphen "-".

Example (Windows 2008)

```
ktpass /princ ckp_pdp/corp.acme.com@CORP.ACME.COM /mapuser
ckpsso@corp.acme.com /pass qweQWE!@# /out unix.keytab
/crypto RC4-HMAC-NT
```

Authentication Failure

Authentication fails if you used the ktpass utility before for the same principal name (ckp_pdp/domain_name@DOMAIN_NAME) but with a different account.

If you have used the ktpass utility before:

1. On the AD server, run:

   ```
   ldifde -f check_SPN.txt -t 3268 -d
   "dc=corp,dc=acme,dc=com" -l servicePrincipalName -r "
   (servicePrincipalName=ckp_pdp*)" -p subtree
   ```

2. Open the `check_SPN.txt` file and verify that only one record is present.

   If multiple records exist, you must delete the different account or remove its association to the principal name.

   Remove the association with the principle name by running:

   ```
   settspn -D ckp_pkp/domain_name old_account name.
   ```

   For example:

   ```
   setspn -D ckp_pdp/corp.acme.com ckpsso
   ```

- **SmartConsole Configuration**

  You create an LDAP Account Unit and configure it to support SSO.

  Configuring SmartConsole for DLP SSO

  Configure the object in SmartConsole for an LDAP Account Unit to support SSO.

  To create a host object for the AD server:

  1. In SmartConsole, click **Objects** > **Object Explorer** (Ctrl+E).
  2. Click **New** > **Host**.
  3. Configure the settings for the host.
  4. Click **OK**.
  5. Publish the SmartConsole session.

  To configure the LDAP account unit:

  1. From the Object Explorer, click **New** > **Server** > **LDAP Account Unit**.
  2. In the **General** tab of the **LDAP Account Unit Properties** window, enter these settings:
     a. Enter the **Name**.
     b. In **Profile**, select **Microsoft_AD**.
     c. In the **Domain** field, enter the domain name.

        Best Practice - Configure this field for account units that you want to use for Identity Awareness. This setting does not affect other LDAP Account Units.

     d. Select **CRL retrieval** and **User management**.

3. Click **Active Directory SSO configuration**.
4. In the **Active Directory SSO configuration** window, configure these settings:
    a. Select **Use Kerberos Single Sign On**.
    b. Enter the **Domain Name**.
    c. Enter the **Account Name** and **Password** for the AD account.
    d. Do not change the default settings for **Ticket encryption method**.
    e. Click **OK**.
5. Configure these settings in the **Servers** tab:
    a. Click **Add**.
    b. In **Host**, select the host object for the AD server.
    c. Enter the **Login DN** of the user (added in the AD) for LDAP operations.
    d. Enter the **Password** and confirm it.
    e. In the **Check Point Gateways are allowed to** section, make sure that **Read data from this server** is selected.
6. Click the **Encryption** tab, and configure these settings:
    a. Click **Use Encryption (SSL)**.
    b. Click **Fetch**.
    c. Click **OK**.

    Note - LDAP over SSL is not supported by default. If you have not configured your domain controller to support LDAP over SSL, either skip step 6 or configure your domain controller to support LDAP over SSL.
7. Click the **Objects Management** tab, and configure these settings:
    a. In the **Manage objects on field**, select the host object for the AD server
    b. Click **Fetch Branches** to configure the branches in use.
    c. Set the number of entries supported.
8. Click the **Authentication** tab, and configure these settings:
    a. In the **Users's default values** section, click **Default authentication scheme**.
    b. Select **Check Point Password**.

9. Click **OK**.
10. Publish the SmartConsole session.

Troubleshooting

The following sections explain how to troubleshoot the DLP Gateway and captured files.

Incidents Do Not Expire

If UserCheck incidents are not expiring, or the change in value of the quarantine parameter seems to have no effect, verify that expiration is enabled.

To enable expiration of UserCheck incidents

1. On the DLP Gateway, open the **$FWDIR/conf/mail_security_config** file.
2. Find the expiration active parameter:

   ```
   [mail_repository]
   #is expiration for mail repository active value can be 0 or 1
   expiration_active=1
   ```

   The default value is `1`. If the value of expiration_active is `0`, incidents do not expire.
3. Save **mail_security_config** and install the policy on the DLP Gateway.

Mail Server Full

The **/var/spool/mail** directory may become full. This may occur if you de-activate the settings to delete incident data after expiration or on exceeding quota. It may also occur due to regular usage, depending on your environment. The quota for the DLP data to be held on the mail server is set in the configuration files.

DLP routinely checks the usage on the Mail Server **/var/spool/mail** directory against the DLP **global_quota_percentage** parameter. If usage on the Mail Server exceeds the global quota: no more emails are stored; all emails of UserCheck incidents are passed; and logs are issued.

To change the quota use percentage:

1. On the DLP Gateway, open the **$FWDIR/conf/mail_security_config** file.
2. Find the global quota parameter:

   ```
   # ... no more emails are written and a log comes out every 5
   minutes
   global_quota_percentage=80
   ```

   The default value is 80 (% of Mail Server used).
3. Change the value to the usage percent you want.
4. Save **mail_security_config** and install the policy on the DLP Gateway.

To change DLP behavior if global quota is exceeded:

1. On the DLP Gateway, edit the **$FWDIR/dlp/config/dlp.conf** file.
2. Find the SMTP parameters:

```
:smtp (
:enabled (1)
:max_scan_size (150000000)
:max_recursion_level (4)
:max_attachments (100)
:block_on_engine_error (0)
```

   - If you want UserCheck emails to be sent and logged (same behavior as **Detect**), keep the default **0**:

     ```
     block_on_engine_error (0)
     ```

   - If you want UserCheck emails to be dropped and logged (same behavior as **Prevent**), change the value to **1**:

     ```
     block_on_engine_error (1)
     ```

3. Save the changes in the file and exit the editor.
4. Install the policy on the DLP Gateway.

Important - For security and performance, it is recommended that you leave the Mail Server quota activated. However, if you do need to de-activate it, set the value of the `global_quota_active` parameter to **0** in the **$FWDIR/conf/mail_security_config** file.

Advanced Options for Data Types

These Data Types have several advanced options you can edit only with the *Database Tool (GuiDBEdit Tool)*:

- Dictionary
- Keywords
- Weighted Keywords
- Patterns

To open the options for these Data Types:

1. Close all SmartConsole windows connected to the Management Server.
2. Connect with *Database Tool (GuiDBEdit Tool)* to the Management Server.
3. Go to **Table > Other > dlp_data_tbl**.
4. Select the Data Type that you want to change:
   - **Case Sensitivity**

     Applies to Data Types:

     - **Dictionary**
     - **Keywords**
     - **Weighted Keywords**
     - **Patterns**

     By default, DLP finds text strings in uppercase or lowercase. You can select to only find text that matches the case of the words in the Data Type lists.

     To find text strings only when the case of the characters matches:

     - Set `case_sensitivity` to `true`.

       The default value is `false`.

     Note - The Case Sensitivity option applies to ASCII words. Non-ASCII words are always case sensitive..

- **Ordered Match for Names**

  Applies to Data Types:

  - **Dictionary**

  By default, DLP finds dictionary words exactly as they are listed in the dictionary file. DLP does not find the dictionary words if they are in a different order. You can configure DLP to find dictionary words even if they occur in a different order.

  This is important when DLP looks for names of people that are in a different order. For example, if your dictionary file includes the name "John Smith", DLP finds only "John Smith". By default, DLP does not find "Smith John" in sent messages.

  To find dictionary entries in any order:

  - Set `ordered_match` to `false`.

    The default value is `true`.

- **Proximity of Matched Words**

  Applies to Data Types:

  - **Dictionary**

  DLP can use the proximity of dictionary words to each other as a criteria in the DLP rules. With this option, if DLP finds the words far from each other, DLP does not trigger an action.

  For example, if your dictionary file contains *confidential* and *information* and the proximity check is enabled, DLP detects messages in which these words are within 3 words of each other. In this example:

  The dictionary rule matches the text: This email contains *confidential* company *information*.

  The dictionary rule does not match the text: This *information* about our product is not *confidential*.

  To enable DLP to check the proximity of dictionary words:

  - Set `enable_proximity_check` to `true`.

    The default value is `false`.

  To change the value of how near the dictionary words need to be to each other:

  - Set `proximity` to the number of words that are allowed to be between Dictionary words.

    The default value is `3`.

- **Match Multiple Occurrences**

  Applies to Data Types:

  - **Dictionary**
  - **Keywords**
  - **Patterns**

  DLP scans messages for words that are included in your lists. DLP can record a match for each occurrence of a word in the text, or DLP can record a match once regardless of how many times the word is used in the text.

  By default, Patterns are recorded as a match each time the pattern is used in the text, but Dictionary words and Keywords are recorded as a match only once regardless of how many times they are used in the text.

  To record a single match regardless of how many times a word is used:

  Set `count_occurences` to `false`.

  By default, this value is `true` for Patterns.

  To record a match for every time a word is used:

  Set `count_occurences` for the Data Type to `true`.

  By default, this value is `false` for Dictionary and Keywords.

- **Match Whole Word Only**

  Applies to Data Types:

  - **Weighted Keywords** - only when keyword is a regular expression
  - **Patterns**

  DLP can match text as partial or whole words. For Weighted Keywords and Patterns, you can select to match only whole words. Dictionary or Keywords Data Types are always matched when they appear as a whole word only.

  For example, if your Pattern Data Type contains **(C|c)onfident** and the whole word only option is enabled, DLP only match patterns that do not have characters before or after the pattern. In this example:

  - **The Data Type matches the text:** confident
  - **The Data Type does not match the text:** confidential

  To match whole words only:

  Set `whole_word_only` to `true`.

  By default, the value is `false`.

  Note - Languages in which words are not bounded by white spaces or punctuation symbols, such as in Japanese or Chinese, do not match as whole word only.

5. Save the changes and close Database Tool (GuiDBEdit Tool).
6. In SmartConsole, install policy.

Regular Expressions and Character Sets

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

Non-Printable Characters

To use non-printable characters in patterns, deflate the reserved character set.

Character	Description
\a	alarm the BEL character (hex code `07`)
\cX	"control-X", where X is any character
\e	escape (hex code `1B`)
\f	formfeed (hex code `0C`)
\n	newline (hex code `0A`)
\r	carriage return (hex code `0D`)
\t	tab (hex code `09`)
\ddd	character with octal code `ddd`
\xhh	character with hex code `hh`

Character Types

To specify types of characters in patterns, deflate the reserved character.

Character	Description
\d	any decimal digit [0-9]
\D	any character that is not a decimal digit
\s	any whitespace character
\S	any character that is not whitespace
\w	any word character (underscore or alphanumeric character)
\W	any non-word character (not underscore or alphanumeric)

Supported Character Sets

The DLP Gateway examines texts in the UTF-8 Unicode character encoding. It therefore changes the messages and files that it examines from its initial encoding to UTF-8.

Before the DLP Gateway can change the encoding of the message or file, the DLP Gateway must identify the encoding. To do this, the DLP Gateway uses the meta data or the MIME headers. If not, then it uses the default Security Gateway encoding.

The DLP Gateway determines the encoding of the message or file it examines as follows:

1. If the file contains meta data, the DLP Gateway reads the encoding from there. For example: Microsoft Word files contain the encoding in the file.
2. Some files have no meta data, but do have MIME headers. For example, text files or the body of an email. For those files the DLP Gateway reads the encoding from the MIME headers:

   ```
   Content-Type: text/plain; charset="iso-2022-jp"
   ```

3. Some files do not have meta data or MIME headers. For those files, the DLP Gateway assumes that the encoding of the original message or file is the default encoding of the Security Gateway. A log message is written to `$DLPDIR/log/dlpe_problem_files.log`:

   ```
   Charset for file <file name> is not provided. Using the default: <charset name>
   ```

   The out-of-the-box default encoding is `Windows Code Page 1252 (Latin I)`. This can be changed.

To change the default encoding of the DLP Gateway:

1. On the DLP Gateway, edit the `$FWDIR/conf/file_convert.conf` file.
2. In the `engine` section, find the `default_charset_for_text_files` field.

   For example:

   ```
   :default_charset_for_text_files (windows-1252)
   ```

   Use one of the supported aliases as the value of this field. Each character set has one or more optional aliases.

   For example, to make the default character set encoding `Russian KOI8-R`, change the field value as follows:

   ```
   :default_charset_for_text_files (KOI8-R)
   ```

If the DLP Gateway cannot use an encoding for a message or file, an error message shows in `$DLPDIR/log/dlpe_problem_files.log`:

```
File <file name> has unsupported charset: <charset name>. Trying to
convert anyway
```

If the DLP Gateway cannot use an encoding, it is possible that it cannot change the message (or parts of it) to UTF-8. If that is so, the DLP Gateway does not fully examine the message.

Character Set Aliases

The table below shows character sets you can use as the default input character set of the DLP Gateway.

Summary table

Table: Character Set Aliases

Name of Character Set	Alias
UTF-8 Encoded Unicode	UTF-8
UTF-7 Encoded Unicode	UTF-7
ASCII (7-bit)	ASCII
Japanese (JIS)	JIS_X0201
Japanese (EUC)	EUC-JP
Korean Standard	KSC_5601
Simplified Chinese	GB2312
EBCDIC Code Page 37 (United States)	IBM037
EBCDIC Code Page 273 (Germany)	IBM273
EBCDIC Code Page 274 (Belgium)	IBM274
EBCDIC Code Page 277 (Denmark, Norway)	IBM277
EBCDIC Code Page 278 (Finland, Sweden)	IBM278
EBCDIC Code Page 280 (Italy)	IBM280
EBCDIC Code Page 284 (Latin America, Spain)	IBM284
EBCDIC Code Page 285 (Ireland, UK)	IBM285
EBCDIC Code Page 297 (France)	IBM297
EBCDIC Code Page 500 (International)	IBM500

Table: Character Set Aliases (continued)

Name of Character Set	Alias
EBCDIC Code Page 1026 (Turkey)	IBM1026
DOS Code Page 850 (Multilingual Latin I)	IBM850
DOS Code Page 852 (Latin II)	IBM852
DOS Code Page 855 (Cyrillic)	IBM855
DOS Code Page 857 (Turkish)	IBM857
DOS Code Page 860 (Portuguese)	IBM860
DOS Code Page 861 (Icelandic)	IBM861
DOS Code Page 863 (French)	IBM863
DOS Code Page 865 (Danish, Norwegian)	IBM865
DOS Code Page 869 (Greek)	IBM869
Windows Code Page 932 (Japanese Shift-JIS)	Shift_JIS
Windows Code Page 874 (Thai)	ibm874
Windows Code Page 949 (Korean)	KS_C_5601-1987
Windows Code Page 950 (Traditional Chinese Big 5)	csBig5
Windows Code Page 1250 (Central Europe)	windows-1250
Windows Code Page 1251 (Cyrillic)	windows-1251
Windows Code Page 1252 (Latin I)	windows-1252
Windows Code Page 1253 (Greek)	windows-1253
Windows Code Page 1254 (Turkish)	windows-1254
Windows Code Page 1255 (Hebrew)	windows-1255
Windows Code Page 1256 (Arabic)	windows-1256
Windows Code Page 1257 (Baltic)	windows-1257
ISO-8859-1 (Latin 1)	ISO-8859-1

Table: Character Set Aliases (continued)

Name of Character Set	Alias
ISO-8859-2 (Latin 2)	ISO-8859-2
ISO-8859-3 (Latin 3)	ISO-8859-3
ISO-8859-4 (Baltic)	ISO-8859-4
ISO-8859-5 (Cyrillic)	ISO-8859-5
ISO-8859-6 (Arabic)	ISO-8859-6
ISO-8859-7 (Greek)	ISO-8859-7
ISO-8859-8 (Hebrew)	ISO-8859-8
ISO-8859-9 (Turkish)	ISO-8859-9
Mac OS Roman	csMacintosh
Russian KOI8-R	KOI8-R

Command Line Reference

See the *R81.20 CLI Reference Guide*.

Syntax Legend

Whenever possible, this guide lists commands, parameters and options in the alphabetical order.

This guide uses this convention in the Command Line Interface (CLI) syntax:

Character	Description

TAB	Shows the available nested subcommands:
	`main command`
	`→ nested subcommand 1`
	`→ → nested subsubcommand 1-1`
	`→ → nested subsubcommand 1-2`
	`→ nested subcommand 2`
	Example:
	`cpwd_admin`
	`config`
	`-a <options>`
	`-d <options>`
	`-p`
	`-r`
	`del <options>`
	Meaning, you can run only **one** of these commands:
	■ This command: `cpwd_admin config -a <options>`
	■ Or this command: `cpwd_admin config -d <options>`
	■ Or this command: `cpwd_admin config -p`
	■ Or this command: `cpwd_admin config -r`
	■ Or this command: `cpwd_admin del <options>`

Character	Description
Curly brackets or braces **{ }**	Enclose a list of available commands or parameters, separated by the vertical bar **|**. User can enter only one of the available commands or parameters.
Angle brackets **< >**	Enclose a variable. User must explicitly specify a supported value.
Square brackets or brackets **[ ]**	Enclose an optional command or parameter, which user can also enter.

dlpcmd

Description

Control the Data Loss Prevention Engine on a Security Gateway.

Syntax

```
dlpcmd [-s]
      action_by_admin <options>
      getquarantined
      getquarantinedcount
      getquarantinedsize
      ramdisk <options>
```

Important:

- In a Cluster, you must configure all the Cluster Members in the same way.
- On Scalable Platforms (Maestro and Chassis), you must run the applicable commands in the Expert mode on the applicable Security Group.

Parameters

Parameter	Description
`-s`	Silent mode - does not print failure messages on the screen.

`action_by_admin <options>`	Sends or deletes the specified quarantined email by its public GUID from quarantine.
	The available options are:
	■ Send (Release) the specified quarantined email:
	`dlpcmd action_by_admin 1 {Public GUID of the Quarantined Email} ["Justification for Sending or Deleting"] ["Administrator Name"]`
	■ Delete (Discard) the specified quarantined email:
	`dlpcmd action_by_admin 2 {Public GUID of the Quarantined Email} ["Justification for Sending or Deleting"] ["Administrator Name"]`
	Notes:
	■ You must enclose the email ID in curly brackets `{}`.
	■ You can see this action in Audit Logs in SmartConsole. For example, see sk117753.

`getquarantined`	Shows the list of all quarantined emails.
`getquarantinedcount`	Shows the number of all quarantined emails.
`getquarantinedsize`	Shows the total size of all emails in quarantine.
`ramdisk <options>`	Shows and controls the DLP RAM Disk. The available options are: ■ `off` - Disables the DLP RAM Disk ■ `on` - Enables the DLP RAM Disk ■ `size <Size in MBytes>` - Configures the size of the DLP RAM Disk ■ `status` - Shows the DLP RAM Disk information **Important** - All operations except "`status`" require a restart of all services (`cpstop` and `cpstart`).

Example

```
[Expert@MyGW:0]# dlpcmd getquarantined
Printing quarantined mails:
Mail GUID: {8698E6EC-340C-9115-0AB6-F6CA9986147F}; Arrival date: Sun Dec  1 13:38:32 2019; exp
date: Sun Dec  8 13:38:32 2019; sender: dataowner-JOHNDOE;
... ... ...
[Expert@MyGW:0]#
[Expert@MyGW:0]# dlpcmd action_by_admin 1 {8698E6EC-340C-9115-0AB6-F6CA9986147F} "Released an
Email" "Main Admin"
[Expert@MyGW:0]#
[Expert@MyGW:0]# dlpcmd getquarantined
No quarantined mails
[Expert@MyGW:0]#
```

Working with Kernel Parameters

See the *R81.20 Quantum Security Gateway Guide* > Chapter "Working with Kernel Parameters".

Kernel Debug

See the *R81.20 Quantum Security Gateway Guide* > Chapter "Kernel Debug on Security Gateway".

Glossary

A

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

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

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

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

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

B

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

C

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

Cluster Member
Security Gateway that is part of a cluster.

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

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

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

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

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

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

D

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

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

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

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

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

E

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

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

G

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

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

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

H

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

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

I

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

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

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

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

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

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

J

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

K

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

L

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

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

M

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

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

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

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

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

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

N

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

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

O

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

P

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

Q

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

R

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

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

S

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

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

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

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

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

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

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

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

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

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

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

T

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

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

U

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

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

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

V

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

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

Z

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