

15 May 2017

DATA LOSS PREVENTION

R80.10

Administration Guide

© 2017 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the Copyright page <http://www.checkpoint.com/copyright.html> for a list of our trademarks.

Refer to the Third Party copyright notices http://www.checkpoint.com/3rd_party_copyright.html for a list of relevant copyrights and third-party licenses.

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.



Check Point R80.10

For more about this release, see the R80.10 home page
<http://supportcontent.checkpoint.com/solutions?id=sk111841>.



Latest Version of this Document

Download the latest version of this document
http://supportcontent.checkpoint.com/documentation_download?ID=54805.

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



Feedback

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

Please help us by sending your comments
mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Data Loss Prevention R80.10 Administration Guide.



Searching in Multiple PDFs

To search for text in all the R80.10 PDF documents, download and extract the complete R80.10 documentation package

<http://downloads.checkpoint.com/dc/download.htm?ID=54846>.

Use **Shift-Control-F** in Adobe Reader or Foxit reader.




Revision History

Date	Description
15 May 2017	First release of this document

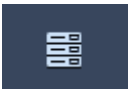



SmartConsole Toolbars

For a guided tour of SmartConsole, click **What's New** in the left bottom corner of SmartConsole.


Global Toolbar (top left of SmartConsole)

	Description and Keyboard Shortcut
	The main SmartConsole Menu
	The Objects menu. Also leads to the Object Explorer Ctrl+E
	Install policy on managed gateways Ctrl+Shift+Enter


Navigation Toolbar (left side of SmartConsole)

	Description and Keyboard Shortcut
	Gateways & Servers configuration view Ctrl+1
	Security Policies Access Control view Security Policies Threat Prevention view Ctrl+2
	Logs & Monitor view Ctrl+3
	Manage & Settings view - review and configure the Security Management Server settings Ctrl+4

Command Line Interface Button (left bottom corner of SmartConsole)

	Description and Keyboard Shortcut
	Open a command line interface for management scripting and API F9

What's New Button (left bottom corner of SmartConsole)

	Description and Keyboard Shortcut
	Open a tour of the SmartConsole

Objects and Validations Tabs (right side of SmartConsole)

	Description
Objects	Manage security and network objects
Validations	Validation warnings and errors

System Information Area (bottom of SmartConsole)

	Description
Task List	Management activities, such as policy installation tasks
Server Details	The IP address of the Security Management Server
Connected Users	The administrators that are connected to the Security Management Server

Contents

Important Information.....	3
SmartConsole Toolbars	4
Terms.....	11
Introduction to Data Loss Prevention.....	12
The Need for Data Loss Prevention.....	12
DLP and Privacy	12
The Check Point Solution for DLP	13
Content Awareness Software Blade	14
How DLP Works.....	15
Integrated DLP Security Gateway Deployment	16
Dedicated DLP gateway Deployment	17
Alternative Gateway Deployments.....	18
What Happens on Rule Match.....	19
Role of DLP Administrator	19
DLP Permissions for Administrator Accounts	20
Configuring Full DLP Permissions	21
Configuring a Subset of Permissions.....	21
Installation and Configuration.....	22
Installing the DLP gateway	22
DLP Software Blade Trial License.....	22
Configuring a DLP Gateway or Security Cluster.....	23
Configuring Integrated Deployments.....	23
Configuring Dedicated Deployments	24
DLP-1 Security Cluster Wizard	24
Prerequisites.....	24
Configuring a Locally Managed DLP-1 Security Cluster	25
Data Loss Prevention Wizard	26
DLP Blade Wizard Options	26
Completing the Wizard	26
Configuring a DLP Gateway in Bridge Mode	26
Required Routing in Bridge Mode	27
Configuring Bridge IP Address	27
Required VLAN Trunk Interfaces.....	27
Configuring Active Directory and LDAP for DLP	28
Rerunning the Data Loss Prevention Wizard	28
Configuring a DLP Gateway for a Web Proxy.....	29
Configuring DLP for a Web Proxy	29
Configuring DLP for an Internal Web Proxy.....	30
Configuring Proxy Settings after Management Upgrade.....	30
Mail Server Required Configuration	31
Configuring the Mail Relay	32
Configuring a Dedicated DLP gateway and Relay on DMZ.....	32
Recommended Deployment - DLP Gateway with Mail Relay.....	33
Workarounds for a Non-Recommended Mail Relay Deployment.....	34
Untrusted Mail Relays and Microsoft Outlook.....	36
TLS-Encrypted SMTP Connections	36
Configuring Incident Log Handling.....	36

Configuring the Exchange Security Agent.....	37
Configuring SmartConsole for the Exchange Security Agent.....	38
Exchange Server Configuration	39
Configuring SMTP Mirror Port Mode.....	42
How it works.....	42
Enabling Mirror Port Mode scanning of SMTP and HTTP Traffic.....	43
Configuring HTTPS Inspection	43
Inspecting HTTPS Packets.....	44
Configuring Gateways to inspect outbound and inbound HTTPS.....	45
UserCheck Interaction Objects.....	54
Configuring UserCheck	54
Configuring the Security Gateway for UserCheck.....	54
UserCheck CLI.....	55
Kerberos Single Sign On	56
AD Configuration	57
Configuring SmartConsole for DLP SSO	59
UserCheck Page.....	60
Creating UserCheck Interaction Objects.....	61
Plain Text Email Notifications.....	62
More UserCheck Interaction Options	62
Localizing and Customizing the UserCheck Portal	63
UserCheck Client	64
UserCheck Client Overview.....	64
UserCheck Requirements	64
Enabling UserCheck Client	65
Client and Gateway Communication.....	65
Option Comparison.....	66
File Name Based Server Discovery.....	66
Active Directory Based Configuration	67
DNS Based Configuration	68
Getting the MSI File.....	70
Distributing and Connecting Clients	70
UserCheck and Check Point Password Authentication	72
Helping Users	72
Out of the Box.....	73
Default Deployment	73
Data Loss Prevention in SmartDashboard	73
Defining My Organization	75
Adding Email Addresses and Domains to My Organization	75
Defining Internal Users	76
Defining Internal User Groups.....	76
Excluding Users from My Organization.....	76
Defining Internal Networks	77
Excluding Networks from My Organization.....	77
Defining Internal VPNs	77
Excluding VPNs from My Organization.....	78
Data Loss Prevention Policies.....	79
Overview of DLP Rules.....	79
Rule Actions	83
Managing Rules in Detect	84
Setting Rule Tracking	85

Setting a Time Restriction	87
Supported Archive Types	88
Selective Deployment - Gateways.....	88
Selective Deployment - Protocols.....	89
Auditing and Analysis.....	90
Using the Logs & Monitor Logs View	90
Event Analysis Views Available in SmartConsole.....	93
Data Owner and User Notifications	94
Defining Data Owners	94
Preparing Corporate Guidelines	94
Communicating with Data Owners	95
Communicating with Users	96
Notifying Data Owners	97
Notifying Users	97
Customizing Notifications for Users	98
Customizing Notifications to Data Owners.....	99
Customizing Notifications for Self-Handling.....	99
Setting Rules to Ask User	99
DLP Portal.....	100
What Users See and Do	100
Unhandled UserCheck Incidents.....	101
Managing Incidents by Replying to Emails.....	101
UserCheck Notifications	101
Managing Rules in Ask User	102
Learning Mode	102
Data Loss Prevention by Scenario.....	103
Analytical Deployment	103
Creating New Rules	103
Internal DLP Policy Rules.....	104
More Options for Rules.....	106
Rule Exceptions.....	107
Fine Tuning	110
Customized Deployment	110
Setting Rules to Prevent	111
Multi-Realm Authentication Support	111
Troubleshooting DLP Related Authentication Issues.....	112
Defining Data Types	113
Protecting Data By Keyword	113
Protecting Documents by Template.....	114
Protecting Files by Attributes.....	115
Protecting Data by Pattern	116
Defining Compound Data Types.....	116
Protecting Data by Fingerprint	117
Advanced Data Types.....	122
Enhancing Accuracy through Statistical Analysis	126
Adding Data Types to Rules.....	127
Focusing on Data	127
The Compliance Data Category.....	127
Editing Data Types	128
Defining Data Type Groups	133
Defining Advanced Matching for Keyword Data Types	133

Defining Post Match CPcode for a Data Type	134
Recommendation - Testing Data Types	134
Exporting Data Types.....	135
Importing Data Types	135
Repositories	136
Creating a Fingerprint Repository	136
Creating a Whitelist Repository	137
Whitelist Policy	138
Defining Email Addresses	138
Configuring the DLP Watermark.....	139
Previewing Watermarks	142
Viewing Watermarks in MS Office Documents	142
Resolving Watermark Conflicts	142
Turning Watermarking On and Off.....	146
Using the DLP Watermark Viewing Tool	146
Fine Tuning Source and Destination	147
Creating Different Rules for Different Departments.....	147
Isolating the DMZ.....	149
Defining Strictest Security.....	149
Defining Protocols of DLP Rules	150
Fine Tuning for Protocol.....	151
Configuring More HTTP Ports.....	151
Advanced Configuration and Troubleshooting	152
Configuring User Access to an Integrated DLP Gateway	152
Internal Firewall Policy for a Dedicated DLP Gateway.....	153
Advanced Expiration Handling	154
Advanced SMTP Quotas.....	155
Advanced FTP and HTTP Quotas	156
Advanced User Notifications	156
Troubleshooting: Incidents Do Not Expire	157
Troubleshooting: Mail Server Full	157
Gateway Cleanup of Expired Data	158
Gateway Cleanup of All Captured Data	158
Customizing DLP User-Related Notifications	160
Localizing DLP User-Related Notifications.....	162
Supporting LDAP Servers with UTF-8 Records.....	162
Editing Extreme Condition Values.....	162
Editing Exchange Security Agent Values.....	164
Configuring HTTP Inspection on All Ports.....	166
Defining New File Types.....	166
Server Certificates	184
Obtaining and Installing a Trusted Server Certificate	184
Viewing the Certificate.....	185
Advanced Options for Data Types.....	186
Case Sensitivity	186
Ordered Match for Names.....	187
Proximity of Matched Words	187
Match Multiple Occurrences	187
Match Whole Word Only	188
Regular Expressions and Character Sets	189

Regular Expression Syntax	189
Using Non-Printable Characters	190
Using Character Types	190
Supported Character Sets.....	191
Character Set Aliases	192

Terms

Bridge

A device that uses layer-2 connections to handle traffic between networks or systems of equivalent architectures on one logical link. Compare with layer-3 connections that use IP address routing, and with a gateway, that connections networks or systems of different architectures.

Data Type

A classification of data. The Firewall classifies incoming and outgoing traffic according to Data Types, and enforce the Policy accordingly.

DBedit

A CLI tool that lets administrators make changes to objects in the Check Point databases. We recommend the **GuiDBedit** tool instead of **dbedit** when not using scripts.

Dedicated Security Gateway

One Software Blade is enabled on a Security Gateway and the gateway is dedicated to the services of this Software Blade.

DLP

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

External Network

Computers and networks that are outside of the protected network.

Gateway

A computer or appliance that controls communication between different networks.

Integrated Security Gateway

More than one Software Blade is enabled on a Security Gateway.

Internal Network

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

Rule

A set of traffic parameters and other conditions that cause specified actions to be taken for a communication session.

Security Gateway

A computer or an appliance that inspects traffic and enforces Security Policies for connected network resources.

Security Management Server

The server that manages, creates, stores, and distributes the security policy to Security Gateways.

Security Policy

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

SmartConsole

A Check Point GUI application used to manage security policies, monitor products and events, install updates, provision new devices and appliances, and manage a multi-domain environment and each domain.

SmartDashboard

A legacy Check Point client used to create and manage the security policy.

Traffic

The flow of data between network resources.

Introduction to Data Loss Prevention

In This Section:

The Need for Data Loss Prevention.....	12
DLP and Privacy.....	12
The Check Point Solution for DLP	13
Role of DLP Administrator	19

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 various 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 is dependent upon its remaining confidential - consider intellectual property and competition.

Leakage of your data could be embarrassing or worse, cost you industrial edge or loss of accounts. Allowing your organization to act in non-compliance with privacy acts and other laws 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 taking 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 will catch 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 transfer 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.

DLP 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 deployment works. Tell users that transmissions that violate the data security guidelines of your organization will be stored and may be read by security personnel.

Information disclosure recommendations:

1. Disclose the privacy policy BEFORE deploying DLP.
2. Translate the most important DLP rules into guidelines and tell your users what is not allowed and will result in captured transmissions.
3. Explain that DLP scans only transmissions originating 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 popup from the UserCheck client (for SMTP, HTTP, FTP, etc).

If the incident of the notification is in Ask User mode, the user can click the **Send** or **Discard** link in the popup 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 popup.

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

1. Explain that captured transmissions will be logged and saved, and that some may be reported to managers (Data Owners).
2. Explain that captured emails, attachments, web posts, etc. will be available for review by security personnel.
3. Explain that review of original transmissions is for organization data security alone - you are not collecting personal information. Therefore, your users do not have, nor require, the option to not have their transmissions scanned.
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 deploy realistic out-of-the-box detection capabilities based on expert heuristics.

However, optimal DLP must take time. To define data that should be prevented from transmission, you must take into account many variables, each changing in the context of the particular transmission: 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 transfer 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-defined 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 define how data is to be matched by DLP, with the greatest flexibility possible. See the *R77 CPcode DLP Reference Guide*
http://supportcontent.checkpoint.com/documentation_download?ID=24804.

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.

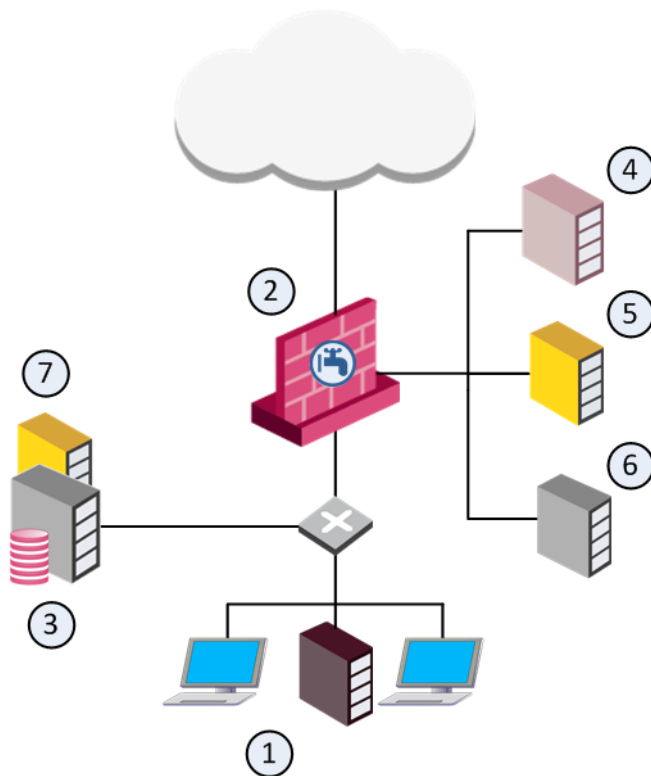
All of this functionality is easy to manage through the SmartConsole, in an interface similar to other Software Blades. You are not expected to be a DLP expert from the day of deployment. Check Point Data Loss Prevention guides you on how to customize and improve your DLP policy - with the Improve Accuracy 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 *R80.10 Next Generation Security Gateway Guide* <http://downloads.checkpoint.com/dc/download.htm?ID=54806>.

How DLP Works



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

1. The Data Loss Prevention Software Blade is enabled on a Security Gateway (2) (or a ClusterXL Security Cluster). This makes it a DLP gateway (or a DLP Security Cluster). Alternatively, a dedicated DLP gateway can sit behind a protecting Security Gateway.
2. You use the SmartConsole and the Security Management Server (3) 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 containing data and being sent through supported protocols. Thus, 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 leaves the organization.

It scans the traffic, including email attachments, for data that should be protected from being sent outside the organization. This data is recognized by protocol, source, destination, and complex Data Type representations.

It can also scan internal traffic between Microsoft Exchange clients within the organization. This requires installation of the Exchange Security Agent on the Microsoft Exchange server. 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. The **Logs & Monitor** view (7) provides effective logging, tracking, event analysis, and reporting of incidents captured by the DLP gateway.

Integrated DLP Security Gateway Deployment

In an *Integrated DLP Security Gateway* deployment, the Data Loss Prevention Software Blade is enabled on a Security Gateway (or a ClusterXL Security 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 gateway.

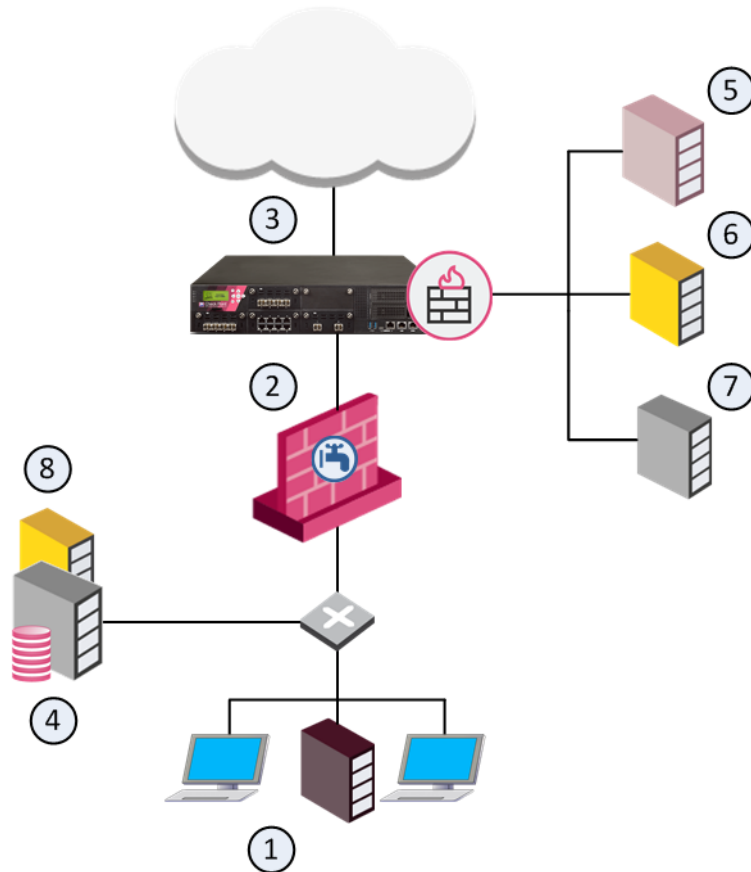
If the DLP gateway is on the perimeter, the SMTP server forwards only transmissions with destinations outside of the organization to DLP. Internal and external transmissions can be inspected by DLP if they are forwarded to DLP by the Exchange Security Agent on the Exchange Server. For external transmissions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

This deployment is supported on one of these:

- An R75 or higher SecurePlatform or Gaia Security Gateway or cluster
- An open server Security Gateway or cluster

Dedicated DLP gateway Deployment

In a *Dedicated DLP gateway*, the Data Loss Prevention Software Blade is enabled on a gateway (2) (or a ClusterXL Security Cluster). This makes it a DLP gateway (or DLP Security Cluster). No other Network Security Software Blade, is enabled. For example, the firewall Software Blade is *not* enabled on the gateway, so the gateway does not enforce the Security Policy. The DLP gateway can sit behind a protecting Security Gateway (3).



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

Best Practice - When you set up a dedicated DLP gateway (2), configure the DLP gateway as a bridge. The bridge is transparent to network routing.

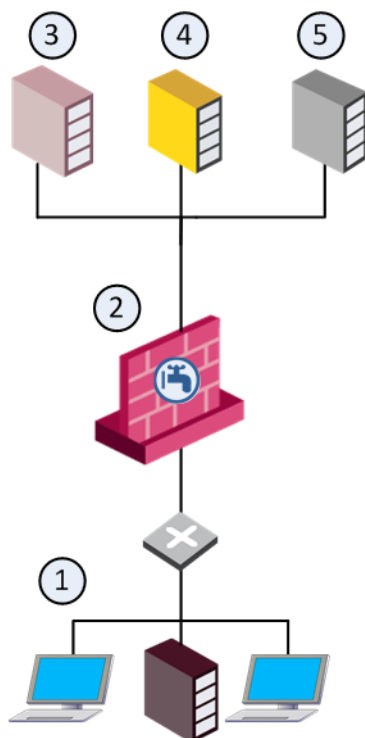
A dedicated DLP gateway deployment is supported on:

- R75 or higher UTM-1 or Power-1 appliance
- R75 or higher ClusterXL Security Cluster - running either on a UTM-1 or Power-1 Appliance, or on an open server.
- R71 or higher open server Security Gateway.
- R71 or higher DLP-1 appliance - This deployment supports two management modes:
 - **Locally Managed** - The DLP-1 appliance combines a DLP enforcement gateway together with some Security Management Server functionality. A locally managed DLP-1 appliance is responsible only for the management of its own DLP Security Policy.
 - **Centrally Managed** - The DLP-1 appliance only enforces the DLP Security Policy which a Security Management Server on a different machine defines and manages.

Alternative Gateway Deployments

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 deployment is the necessary configuration if you want to use a DLP rule that inspects data transmissions between departments.

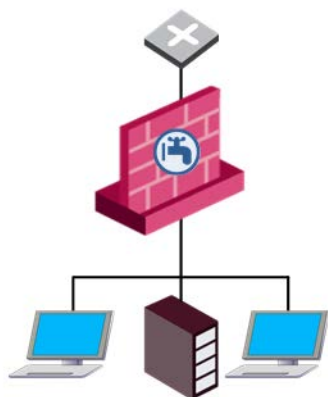
For example, you can create a DLP rule that checks emails between internal groups: **Source** is a specific network, **Destination** is **Outside Source** (anything outside of this **Source**). Such a rule would be applied only if this deployment was used.



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

Item	Description
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.
 - 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 set to be notified, will get notification about the incident.

Role of DLP Administrator

DLP provides various auditing tools: automatic notifications to data owners when transmission of protected data was attempted; user notifications and self-handling portal; tracking and logging, event details, charts, graphs, filtered lists, and reports from the Logs & Monitor view.

Before you begin your audit, configure your DLP policy. First, define Data Types.

To create and refine the DLP policy:

- Deploy out-of-the-box Data Loss Prevention with a basic policy. This policy provides strong detection capabilities from Day-1.
- You can 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.
- Choose 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.
- 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.
- 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 will decide, with the Data Owners, what incidents also require notification to the Data Owners. As you monitor the incidents, create guidelines to fine tune the DLP policy.
- 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.
- 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 and publish the changes.

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 and publish the changes.

Installation and Configuration

In This Section:

Installing the DLP gateway	22
DLP Software Blade Trial License	22
Configuring a DLP Gateway or Security Cluster	23
DLP-1 Security Cluster Wizard	24
Data Loss Prevention Wizard	26
Configuring a DLP Gateway in Bridge Mode	26
Configuring Active Directory and LDAP for DLP	28
Configuring a DLP Gateway for a Web Proxy	29
Mail Server Required Configuration	31
Configuring Incident Log Handling	36
Configuring the Exchange Security Agent	37
Configuring SMTP Mirror Port Mode	42
Configuring HTTPS Inspection	43

Check Point Data Loss Prevention is a Software Blade. It needs connectivity to a Security Management Server and a SmartConsole. A Check Point gateway or a DLP-1 appliance is necessary for DLP.

Best Practice - In a dedicated DLP gateway deployment, Check Point recommends that you have a protecting Security Gateway in front of the DLP gateway.

The environment must include a DNS.

Important - Before installing DLP, we recommend that you review the requirements and supported platforms for DLP in the *R80.10 Release Notes*
<http://downloads.checkpoint.com/dc/download.htm?ID=54802>.

Installing the DLP gateway

For instructions on how to install and do the initial configuration of the DLP gateway, see the *R80.10 Installation and Upgrade Guide*
<http://downloads.checkpoint.com/dc/download.htm?ID=54829>.

DLP Software Blade Trial License

The DLP Software Blade has a 30 day trial license.

To activate the trial license:

1. Select the **DLP Software Blade** in **SmartConsole**, in the gateway object.
2. From **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 remain 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 stops working, and a policy cannot be installed on the DLP gateway. You must unselect the DLP Software Blade, and then you can install a policy on the gateway.

Configuring a DLP Gateway or Security Cluster

You can enable the DLP Software Blade as one of the Software Blades on a Security Gateway. This is known as an integrated DLP deployment. In R75 and higher, you can also enable a DLP Software Blade on a ClusterXL in High Availability mode or Full High Availability mode on a UTM-1 appliance or 2012 Appliance models. In a *dedicated* DLP gateway, the Data Loss Prevention Software Blade is enabled on a gateway (or a ClusterXL Security Cluster) and no other Network Security Software Blade is enabled.

Note - The DLP Software Blade (as a dedicated gateway or in an integrated Security Gateway) can work as part of a ClusterXL Load Sharing cluster only when the policy contains DLP rules that use the Detect, Inform, or Prevent actions ("[Rule Actions](#)" on page 83). The Ask DLP action is not supported for ClusterXL Load Sharing.

In version R75.20 and higher, you can also configure a ClusterXL High Availability cluster of dedicated DLP-1 appliances.

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.

In a DLP gateway cluster, synchronization happens every two minutes. Therefore, if there is a failover, the new active member may not be aware of DLP incidents that happened in the two minutes since the failover.

To configure a DLP-1 appliance, see the *DLP-1 Getting Started Guide*.

Configuring Integrated Deployments

In an integrated deployment you can:

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

To enable DLP on an existing Security Gateway or cluster:

1. Open SmartConsole, click **Gateways & Servers** and double-click the Security Gateway or Security Cluster object.

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

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

You can use Load Sharing if the DLP rules use the Detect, Prevent, or Inform actions.

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** (on page 26).

Configuring Dedicated Deployments

These are the configuration options in a dedicated deployment environment:

- Dedicated DLP gateway or cluster on an existing Security Gateway or Security Cluster.
- Dedicated DLP gateway or cluster on a locally managed DLP-1 appliance.
- Dedicated DLP gateway or cluster on a centrally managed DLP-1 appliance.

To configure a dedicated DLP gateway on an existing Security Gateway or Security Cluster:

1. Configure an existing Security Gateway or cluster as a DLP gateway or Security Cluster.
2. Deselect the Firewall Software Blade, if it is selected.

When you clear the Firewall Software Blade, a warning message shows.

You are about to turn off the Firewall blade, with only the DLP blade left on.

Therefore, this Security Gateway will not enforce the security policy.

It is recommended to place this Security Gateway behind a firewall.

Are you sure you want to continue?

3. Click **Yes**.

To configure a dedicated DLP gateway or cluster on a locally managed DLP-1 appliance:

1. Open SmartConsole.
For a locally managed gateway, the Data Loss Prevention Wizard opens.
For a locally managed cluster, the DLP-1 Cluster Wizard opens.
2. Complete the Data Loss Prevention Wizard (on page 26) or DLP-1 Cluster Wizard ("DLP-1 Security Cluster Wizard" on page 24).

To configure a dedicated DLP gateway or cluster on a centrally managed DLP-1 appliance:

1. Open SmartConsole and log in to the Security Management Server that manages the DLP-1 appliance.
2. Click **Gateways & Servers** and create a new gateway or cluster object.
 - For a DLP-1 Security Gateway, click **New > Gateway**
 - For a Security Cluster, click **New > Cluster > Cluster**.
3. Complete the wizard.

DLP-1 Security Cluster Wizard

Prerequisites

Before you define a DLP Security Cluster:

- Make sure you have defined all of the network interfaces in use for each of the DLP-1 appliances. The interfaces must be defined within the same subnet. To make sure they are defined correctly, use the appliance WebUI.

- Make sure a cable is connected between the two SYNC ports on the appliances. It is not necessary to assign them IP addresses. If you do assign IP addresses, make sure the SYNC interfaces use the same subnet.
- Make sure you have the activation key that was set for appliance defined as the secondary member during initial configuration. This key is used to establish trust between the primary member and secondary member.

Configuring a Locally Managed DLP-1 Security Cluster

Use the Security Cluster wizard in SmartConsole to create a cluster for two DLP-1 gateways. With the wizard you set the name of the cluster object, the name and IP address of the secondary cluster member and configure the topology for the gateways' interfaces.

There is a Cluster Topology page for each of the network interfaces that have been configured for the cluster members. In this page you define whether a network interface participates in the cluster. If the interface is part of the cluster, you must define a virtual IP address for the cluster. This IP address is visible to the network and makes sure that failover events are transparent to all hosts in the network. If the interface is not part of the cluster, the interface is a **not-monitored private** interface.

To configure a locally managed DLP-1 Security Cluster:

1. Log in to SmartConsole using your Security Management credentials.
The Security Cluster wizard opens.
2. Click **Next**.
The Cluster General Properties page opens.
3. Enter a name for the cluster.
4. Click **Next**.
The Cluster Secondary Member page opens.
5. In **Secondary Member Name** and **Secondary Member IP Address**, enter a name and the IP address of the appliance you configured as the secondary member.
6. In **Activation Key**, enter the same activation key that was set for the secondary member in the configuration wizard and confirm it. The activation key is used by the primary member to establish initial trust with the secondary member. Once established, trust is based on security certificates.
7. To create a Security Cluster with only a primary member, select **Define the Secondary Cluster member later**.
8. Click **Next**.
The Cluster Topology page opens.
9. To set the interface to be part of the cluster, select **Interface part of the cluster** and enter a **Virtual IP Address** and **Net Mask**. If you do not want the interface to be part of the cluster, make sure the checkbox is cleared.
10. Click **Next**.
11. Repeat steps 9-10 for each defined interface.
12. In the Cluster Definition Wizard Complete page, click **Finish**.
The Data Loss Prevention Wizard opens.
13. Complete the Data Loss Prevention Wizard (on page 26).

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 LDAP for DLP ("[Configuring Active Directory and LDAP for DLP](#)" on page 28).
- **Activate DLP Portal for Self Incident Handling** - Select to activate the port. The default URL is `https://<Gateway IP>/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 requires 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) **Install Policy**.
 - b) In the **Install Policy** window, select the DLP Gateways.

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 - 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 deploy 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 will be scanned by DLP. You cannot exclude 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.

Required Routing in Bridge Mode

There must be routes between the DLP gateway and the required servers:

- Security Management Server
- DNS server
- Mail server, if an SMTP Relay server is configured to work with the gateway
- Active Directory or LDAP server, if configured to work with the 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 gateway that will be used to reach 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.

Required 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 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 required 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. ("Rerunning the Data Loss Prevention Wizard" on page 28)

To configure DLP to use Active Directory LDAP:

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.

You are not required 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 appropriate priorities to the remaining 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 *R80.10 Security Management Administration Guide*

<http://downloads.checkpoint.com/dc/download.htm?ID=54842>.

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 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 gateway to scan HTTPS connections.

Configuring 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**.

To configure DLP for Procedure 1:

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

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 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 **SmartConsole**.
8. From **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 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 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.

To use 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\R80.10\PROGRAM\GuidBedit.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

DLP rules have different 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 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 the Mail Relay

You can use the Data Loss Prevention Wizard to configure the settings for the mail relay. Use these procedures to configure these settings without the Wizard.

To open the DLP tab in SmartDashboard:

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 > Mail Server**.

To 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**.

To 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**.

To complete configuring the Mail Relay:

1. Click **Save** and then close SmartDashboard.
2. From **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

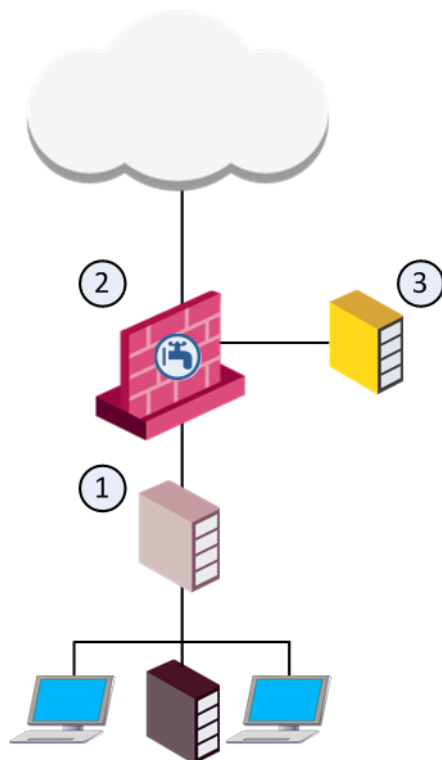
To configure the DLP and mail relay in the DMZ:

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 **My Organization**.
3. In the **Networks** area, click **Select specific networks and hosts** and click **Edit**.

The **Networks and Hosts** window opens.

4. Click **Add**.
5. If the Internal Mail Server is already defined as a Check Point network object, select it from the list.
Otherwise, click **New > Host**.
6. Enter the settings for the Internal Mail Server Host and then click **OK**.
7. Click **OK**.
8. Repeat steps to add other Internal Mail Servers.
9. If users email clients are configured to work directly with the mail relay that is located in the DMZ using SMTP, add their networks.
10. Select user networks from the list (or click **New** to define these networks) and then click **OK**.
11. Click **Save** and then close SmartConsole.
12. From **SmartConsole**, **Install Policy**.

Recommended Deployment - 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.

To deploy 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 gateway window opens and shows the **General Properties** page.
2. Make sure that mails from the internal mail server (e.g. Microsoft Exchange) (1) arrive at the gateway using an internal Gateway interface.
 - a) From the navigation tree, click **Network Management**.
 - b) Double-click the 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. Deploy the internal mail relay (2) behind a DMZ interface of the DLP gateway:
In the **Topology** page of the DLP gateway object, define the 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**

To configure the internal mail relay that is not behind a DMZ interface of the DLP gateway:

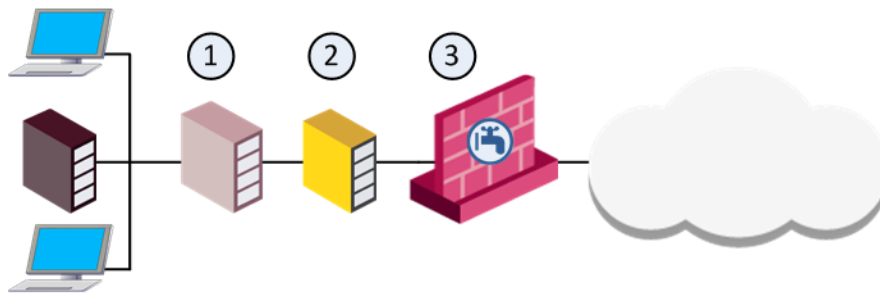
Note - If the DLP gateway interface leading to the internal mail relay is internal, and you cannot deploy the internal mail relay behind a DMZ interface of the DLP gateway.

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. From **SmartConsole**, **Install Policy**.

Workarounds for a Non-Recommended Mail Relay Deployment

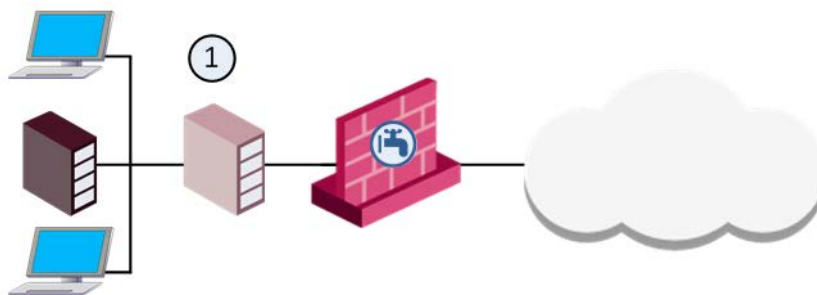
A non-recommended deployment is to have the DLP gateway scan emails as they are sent from an internal mail relay that is in My Organization to the target mail server in the Internet. In this deployment, the DLP gateway communicates with the target mail servers on behalf of the mail relay. If the target mail server does not respond, some mail relays (such Mcafee IronMail, postfix 2.0 or earlier and gmail) will not try the next DNS MX record, and so will 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 Will Not Resend Emails

If the mail relay does not succeed in sending 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 does this by sending the mail to the next DNS MX record.

Most mail relays try the next MX record if the target is unreachable, 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 try the next MX if the target server returns a 4xx error. They will therefore not send the email.

In these deployments, 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, the email will not be sent.

Workarounds for the Non-Recommended Deployments

- 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, deploy the DLP gateway between two internal mail servers. For example, put the DLP gateway in the DMZ with the relay server ("[Configuring a Dedicated DLP gateway and Relay on DMZ](#)" on page 32).
- If you cannot apply these workarounds, see sk58960 <http://supportcontent.checkpoint.com/solutions?id=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 ("[Configuring the Exchange Security Agent](#)" on page 37) to inspect them.

Configuring Incident Log Handling

To 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** and publish the changes.
5. Open GuiDBedit:
 - a) On the SmartConsole computer, run
C:\Program Files\CheckPoint\SmartConsole\R80.10\PROGRAM\GuiDBedit.exe
 - b) Log in with your SmartConsole credentials.
6. In the left pane, select **Table > Network Objects > network_objects**.
7. In the right pane, select the Log server or Security Management Server that manages DLP logs.
8. In the bottom pane, in the **Field Name** column, find **log_policy**.

9. Configure these fields:

Field Name	Description	Default value
<code>dlp_blob_delete_above_value_percentage</code>	The maximum % of disk space that incidents are allowed to occupy.	20%
<code>dlp_blob_delete_on_above</code>	Whether or not to delete incidents if the incidents take up more disk space than <code>dlp_blob_delete_above_value_percentage</code> <ul style="list-style-type: none"> <code>true</code> — Delete incidents. However, logs that are associated with the incidents are not deleted. <code>false</code> — 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
<code>dlp_blob_delete_on_run_script</code>	Whether or not to run a script before deleting incidents. For example, to copy the logs to a different computer before they are deleted. <ul style="list-style-type: none"> <code>true</code> — 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. <code>false</code> — 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. This requires 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 ("[Internal DLP Policy Rules](#)" on page 104).

Configuring SmartConsole for the Exchange Security Agent

To define 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
 - Trusted Communication
 - Inspection Scope
 - Configuration Summary
5. After you complete the wizard, click **Save** and then close SmartDashboard.
6. From **SmartConsole**, **Install Policy**.

Exchange Security Agent - General

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

- **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 the Exchange Security Agent will send emails to for inspection. 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.

Click **Next**.

Exchange Security Agent - Trusted Communication

Use the Trusted Communication page to 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.

- **One-time password** - 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**.

Click **Next**.

Exchange Security Agent - Inspection Scope

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.

- **Inspect emails sent only by these users or user groups** - Define the Active directory, internal or LDAP users whose emails will be inspected.



Note - You can define users or groups for whom emails will not be sent 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 all emails - All emails will be sent from the Exchange Security Agent to the enforcing DLP gateway for inspection.

Note - You can define users or groups for whom emails will not be sent 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.

Click **Next**.

Exchange Security Agent - Configuration Summary

The **Exchange Agent Wizard is Completed** window opens.

The next steps include:

- Installing the policy on the DLP gateway.
- Installing and configuring the Exchange Security Agent on the Exchange server.

Installing the Exchange Security Agent

To install the Exchange Security Agent:

1. On the Exchange Server, download the DLP Exchange agent MSI from the R80.10 Home Page <http://supportcontent.checkpoint.com/solutions?id=sk111841>:
 - a) From the Table of Contents, select **Tools**.
 - b) Click **Show / Hide the download matrix**.
 - c) In the **Agents** section, download the DLP Exchange agent MSI.
2. Do the steps of the installation wizard.

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.
- Start or stop the Exchange Security Agent that runs as an extension of the Microsoft Exchange Transport service.
- See Exchange Security Agent statistics.
- Monitor message status with the Message Tracking log.

- Configure when to bypass inspection of messages.

Initializing Trusted Communication

There are two possible communication states:

- **Uninitialized** is where trusted communication has not been established.
- **Trust established** is where the Exchange Security Agent has received the security certificate and can receive 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.

Starting the Exchange Security Agent

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 ("**Exchange Security Agent - Inspection Scope**" on page 38).

To start the Exchange Security Agent:

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

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.

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:

- **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.
- **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.

This table describes 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 gateway
	Timeout
Drop	Dropped by 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

Event ID	Reason
	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

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 deployment risk.

How it works

When the DLP Security Gateway is connected to a SPAN port of the switch, the 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 gateway.

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

Monitor Mode lets the 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

(<http://supportcontent.checkpoint.com/solutions?id=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
<code>status</code>	Shows the status, whether mirror port mode is enabled or disabled.
<code>enable</code>	Enables Mirror Port Mode
<code>disable</code>	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 remains enabled after a 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.

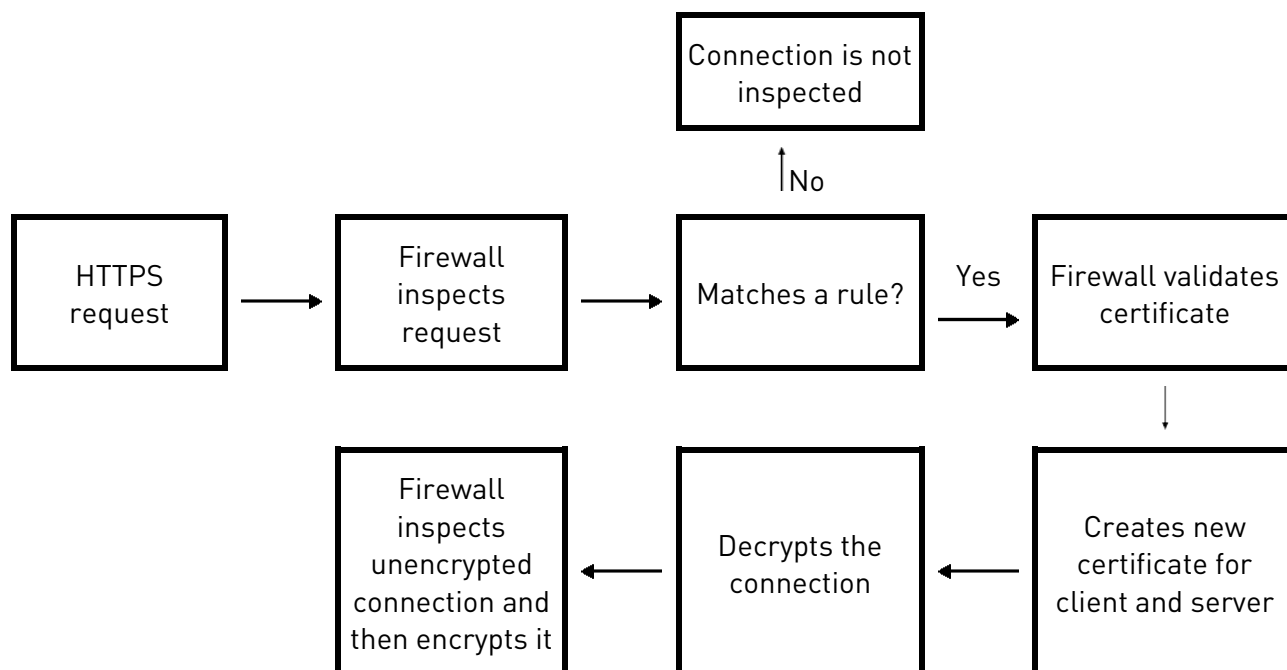
A Security Gateway uses certificates and becomes an intermediary between the client computer and the secure web site. All data is kept private in HTTPS Inspection logs. Only administrators with HTTPS Inspection permissions can see all the fields in such a log.

Inspecting HTTPS Packets

Outbound Connections

Outbound connections are HTTPS connections that arrive from an internal client and connect to the Internet. The Security Gateway compares the HTTPS request to the rules in the HTTPS Inspection Rule Base. If the request does not match any rule, the packet is not inspected and the connection is allowed.

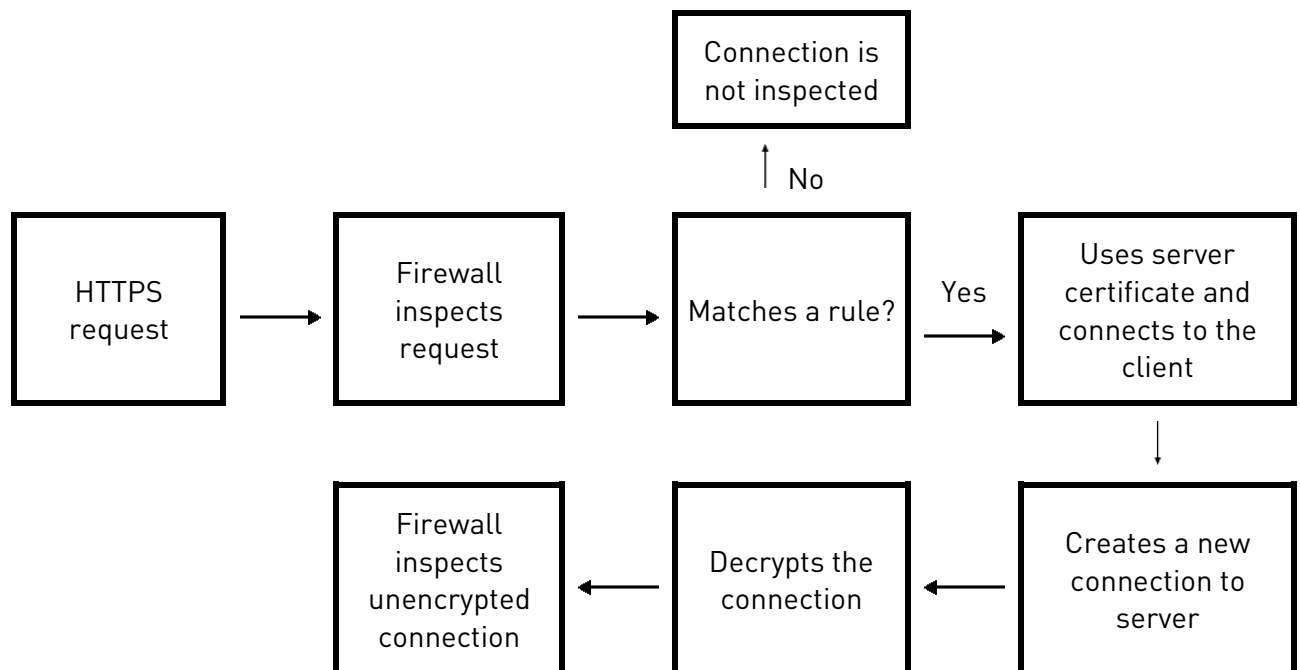
If the request matches an HTTPS Inspection rule, the Security Gateway validates the certificate from the server (on the Internet). The Security Gateway validates the certificate using the Online Certificate Status Protocol (OCSP) standard. OCSP is faster and uses much less memory than CRL Validation, which is used for certificate validation in releases lower than R80.10. For a new HTTPS connection to the server, the Security Gateway creates and uses a new certificate. There are two HTTPS connections, one to the internal client and one to the external server. It can then decrypt and inspect the packets according to the security policy. The packets are encrypted again and sent to the destination.



Inbound Connections

Inbound connections are HTTPS connections that arrive from an external client and connect to a server in the DMZ or the internal network. The Security Gateway compares the HTTPS request to the rules in the HTTPS Inspection Rule Base. If the request does not match any rule, the packet is not inspected and the connection is allowed.

If the request matches an HTTPS Inspection rule, the Security Gateway uses the certificate for the internal server to create an HTTPS connection with the external client. The Security Gateway creates a new HTTPS connection with the internal server. Since the Security Gateway has a secure connection with the external client, it can decrypt the HTTPS traffic. The decrypted traffic is inspected according to the security policy.



Configuring Gateways to inspect outbound and inbound HTTPS

This section gives an example of how to configure a Gateways 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.
 - 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.

Enabling HTTPS Inspection

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 deployed in your organization. This outbound certificate is used by all Security Gateways managed on the Security Management Server.

Creating an Outbound CA Certificate

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 deploy the generated outbound CA certificate on clients, users will 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.

To create an outbound CA certificate:

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 deploy the CA certificate ("[Exporting and Deploying the Generated CA](#)" on page 47).

Importing an Outbound CA Certificate

You can import a CA certificate that is already deployed 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 ("[Exporting a Certificate from the Security Management Server](#)" on page 47).
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, deploy it to clients ("[Exporting and Deploying the Generated CA](#)" on page 47).

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
```

Exporting and Deploying 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 will be in the CA list and they will 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 ("[Deploying Certificates by Using Group Policy](#)" on page 48) 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.

Deploying Certificates by Using Group Policy

You can use this procedure to deploy 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 deploy 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.

Configuring 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 ("[Assigning a Server Certificate for Inbound HTTPS Inspection](#)" on page 49).
5. Define an HTTPS inspection policy:
 - Create rules
 - Add a server certificate to the **Certificate** column of each rule.

Assigning 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 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

These are 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.
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 will 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. <ul style="list-style-type: none"> • 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	WebCalendarServer 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.

Managing Certificates by Gateway

The **Gateways** pane lists the gateways with HTTPS Inspection enabled. Select a gateway and click **Edit** to edit the 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 deployed in your organization.

- You can import a CA certificate from another Security Management Server. Before you can import it, you must first export ("[Exporting a Certificate from the Security Management Server](#)" on page 47) it from the Security Management Server on which it was created.

Adding 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.

Showing 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 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 Interaction Objects

In This Section:

Configuring UserCheck	54
Kerberos Single Sign On	56
UserCheck Page	60
Creating UserCheck Interaction Objects.....	61
Plain Text Email Notifications.....	62
More UserCheck Interaction Options	62
Localizing and Customizing the UserCheck Portal	63

Configuring UserCheck

Configuring the Security Gateway for UserCheck

Enable or disable UserCheck directly on the Security Gateway. If users connect to the gateway remotely, set the internal interface of the gateway (on the **Topology** page) to be the same as the **Main URL** for the UserCheck portal.

Note - The **Main URL** field must be manually updated if:

- The **Main URL** field uses an IP address and not a DNS name
- You change the IPv4 address of the gateway to IPv6 or the opposite

To configure a Security Gateway for UserCheck:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **UserCheck**.
3. Click **Enable UserCheck for active blades**.
4. In the **Main URL** field, select the primary URL for the web portal that shows the UserCheck notifications.
5. If the **Main URL** points to an external interface:
 - a) In the **Accessibility** section, click **Edit**.
 - b) In the **Accessibility** window, click the applicable setting:
 - **Through all interfaces**
 - **According to the firewall policy**
 - a) Click **OK**.
6. If necessary, click **Aliases** to add URL aliases that redirect different hostnames to the **Main URL**.
For example: `Usercheck.mycompany.com` The aliases must resolve to the portal's IP address on the corporate DNS server.
7. In the **Certificate** area, click **Import** to import a certificate that the portal uses to authenticate to the server.

8. In the **Accessibility** area, click **Edit** to configure interfaces on the gateway through which the portal can be accessed. These options are based on the topology configured for the gateway. Users are sent to the UserCheck portal if they connect:

- **According to the Firewall policy.** Select this option if there is a rule that states who can access the portal.
- **Through all interfaces**
- **Through internal interfaces** (default)
 - **Including undefined internal interfaces**
 - **Including DMZ internal interfaces**
 - **Including VPN encrypted interfaces** (default)

Note - If **Including VPN encrypted interfaces** is selected, add a Firewall rule that looks like this:

Source	Destination	VPN	Service	Action
Any	Gateway on which UserCheck client is enabled	Any Traffic	UserCheck	Accept

9. In the **UserCheck Client** area, select **Activate UserCheck Client Support**.
- The UserCheck client enables user interaction notifications.
 - Click **Download Client** to download the installation file for the UserCheck client.

Note: The link will not be active until the UserCheck portal is up.

10. Click **OK**.

11. **Install policy.**

UserCheck CLI

Usrchk

You can use the `usrchk` command in the gateway command line to show or clear the history of UserCheck objects.

Description `usrchk`

Syntax `usrchk [debug] [hits] [incidents]`

Parameters

Parameter	Description
<code>debug</code>	Controls debug messages

hits	<p>Shows user incident options:</p> <p>list - Options to list user incidents</p> <ul style="list-style-type: none"> • <code>all</code> - List all existing incidents. • <code>user <username></code> - List incidents of a specified user. • <code>uci <name of interaction object></code> - List incidents of a specified UserCheck interaction object <p>clear - Options to clear user incidents</p> <ul style="list-style-type: none"> • <code>all</code> - Clear all existing incidents • <code>user <username></code> - Clear incidents for a specified user • <code>uci <name of interaction object></code> - Clear incidents of a specified UserCheck interaction object <p>db - user hits database options</p>
incidents	<p>Operations that can be done for incidents. For example:</p> <ul style="list-style-type: none"> • <code>Expiring</code> Sends emails to users about their expiring email violations

Examples:

- To show all UserCheck interaction objects, run: `usrchk hits list all`
- To clear the incidents for a specified user, run: `usrchk hits clear user <username>`

Notes:

- You can only run a command that contains `user <username>` if:
 - Identity Awareness is enabled on the gateway.
 - Identity Awareness is used in the same policy rules as UserCheck objects.
- To run a command that contains a specified UserCheck interaction object, first run `usrchk hits list all` to see the names of the interaction objects. Use the name of the interaction object as it is shown in the list.

Kerberos Single Sign On

The UserCheck agent supports single sign on using 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 gateway.

For more detailed information on Kerberos SSO, see:

- <http://web.mit.edu/Kerberos/> <http://web.mit.edu/Kerberos/>

- <http://technet.microsoft.com/en-us/library/bb742433.aspx>
<http://technet.microsoft.com/en-us/library/bb742433.aspx>

Single Sign-On Configuration

SSO configuration has two steps:

- **AD Configuration**
Creating a user account and mapping it to a Kerberos principal name.
- **SmartConsole Configuration**
Creating an LDAP Account Unit and configuring it to support SSO.

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 choose 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 login** 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 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.

Ktpass is a command-line tool available in Windows 2000 and higher.

Retrieve 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:
 - a) Retrieve the correct executable for your service pack from the Microsoft Support site <http://support.microsoft.com/> prior to installation. It is part of the Windows 2003 support tools. For example, AD 2003 SP2 requires support tools for 2003 sp2 <http://www.microsoft.com/downloads/details.aspx?familyid=96A35011-FD83-419D-939B-9A772EA2DF90&displaylang=en>.
 - b) Download the support.cab and suptools.msi files to a new folder on your AD server.
 - c) Run the suptools.msi.
- ActiveDirectory 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 Ktpass

1. Open a command line to run the ktpass tool (**Start > Run > cmd**).

2. At the command prompt, run ktpass with this syntax:

```
C:> 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!@#

```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ktpass -princ ckp_pdp/corp.acme.com@CORP.ACME.COM -mapuse
r ckpsso@corp.acme.com -pass qwe123!@# -out unix.keytab -crypto RC4-HMAC-NT
Targeting domain controller: PrimaryDC.corp.acme.com
Using legacy password setting method
Successfully mapped ckp_pdp/corp.acme.com to ckpsso.
WARNING: ptype and account type do not match. This might cause problems.
Key created.
Output keytab to unix.keytab:
Keytab version: 0x502
keysize 70 ckp_pdp/corp.acme.com@CORP.ACME.COM ptype 0 <KRB5_NT_UNKNOWN> vno 3 e
type 0x17 <RC4-HMAC> keylength 16 <0xc377ba8a4dd52401bc404dbe49771bbc>

C:\Users\Administrator>_
```

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 will fail if you have 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:
`settspn -D ckp_pdp/corp.acme.com ckpsso`

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** and publish the changes.

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** and publish the changes.

UserCheck Page

On the **UserCheck** page, you can create, edit, and preview UserCheck interaction objects and their messages. It has these options:

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

These are the default UserCheck messages:

Name	Action Type	Description
Inform User	Inform	Shows when the action for the rule is inform . It informs users what the company policy is for that site.
Blocked Message	Block	Shows when a request is blocked.
Ask User	Ask	Shows 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.
Cancel Page	Cancel	Shows after a user gets an Inform or Ask message and clicks Cancel.
Success Page	Approve	Shows information was sent according to the user's request.
Successfully Discarded	Discard	Shows when the information was successfully discarded according to the user's request.

Ask and **Inform** pages include a **Cancel** button that users can click to cancel the request.

You can preview each message page in these views:

- **Regular view** - How the message shows in a web browser on a PC or laptop
- **Mobile Device** - How the message shows in a web browser on a mobile device
- **Email** - How the message shows in email
- **Agent** - How the message shows in the agent

Creating UserCheck Interaction Objects

Create a UserCheck Interaction object from the Rule Base or from the **UserCheck** page of the DLP tab. The procedure below shows how to create the object from the Rule Base in SmartDashboard.

Note - You can only edit DLP UserCheck objects in SmartDashboard. You cannot create or edit them in SmartConsole.

To create a UserCheck object that includes a message:

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**.

The **Action** column uses these interaction modes:

- **Inform user** - Show an informative message users. Users can continue to the application or cancel the request.
- **Ask user** - Show 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.
- **Prevent** - Show a message to users and block the application request.

3. Right-click the cell for the rule and select the interaction mode > **New**.

You can also double-click an existing interaction mode to edit it.

The **UserCheck Interaction** window opens on the **Message** page.

4. Enter a name for the UserCheck object and, optionally, a comment.
5. Select a language (English is the default) from the Languages tabs.
6. Click **Add logo** to add a graphic, such as company logo.

Note - The graphic must have a height and width of 176 x 52 pixels.

7. Click the text box adjacent to the picture and enter title text for the message.
8. In the page title, message subject, and message body text boxes, enter the message content. You can:

a) Use the formatting toolbar to change text color, alignment, add or remove bullets.

b) **Insert field** variables for:

- Username
- Original URL
- Source IP
- Incident ID
- Violation protocol
- Email subject / File name

- **Matched Rules Notifications**

Variables are replaced with applicable values when the (Prevent, Ask, Inform) action occurs and the message shows. The Username can only be displayed if the Identity Awareness blade is enabled.

c) Use the **Insert User Input** variable to add a:

- **Confirm checkbox** - Users select a checkbox to continue
- **Textual Input** - Users can enter an explanation for their activity or other text according to the instructions. Edit the default text in the Textual Input box based on your business needs.
- **Wrong report category** - Users can click a link to report that an incorrect category was included in the message. Use this field with the **Category** variable.

9. **Optional:** Click **Preview in browser** to see the results in your default browser.

10. Click **OK**.

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

12. From **SmartConsole**, **Install Policy**.

Plain Text Email Notifications

Not all email clients can handle emails in rich text or HTML format. To accommodate such clients, you can configure the gateway to send emails without images.

To configure emails without images:

1. On the DLP gateway, open this file for editing:
`$FWDIR/conf/usrchkd.conf`
2. Locate the `send_emails_with_no_images` entry.
3. Change the value to `true`.
4. Save and close the file.
5. Kill the `userchkd` process.

The process is automatically restarted by the gateway. The new configuration will survive a gateway reboot.

Email notifications are now sent in both plain text and HTML formats. The user's email client decides which format to show.

More UserCheck Interaction Options

For each UserCheck Interaction object you can configure these options from the UserCheck Interaction window:

- **Message** - Modify the message text.
- **Languages** - Select a default language for the message.
- **Fallback Action** - For DLP, the fallback action is derived from the original action. If the original action is:
 - **Ask** - The fallback is **Block**
 - **Inform** - The fallback is **Detect**
- **Conditions** - Select actions that must occur before users can access the application. Select

one or more of these options:

- **User accepted and selected the confirm checkbox** - This applies if the UserCheck message contains a checkbox (**Insert User Input > Confirm Checkbox**). Users must accept the text shown and select the checkbox before they can access the application.
- **User filled some textual input** - This applies if the UserCheck message contains a text field (**Insert User Input > Textual Input**). Users must enter text in the text field before they can access the application. For example, you might require that users enter an explanation for use of the application.

Localizing and Customizing the UserCheck Portal

After you set the UserCheck interaction object language, you can translate the Portal **OK** and **Cancel** buttons to the applicable language. For more information, see: sk83700
<http://supportcontent.checkpoint.com/solutions?id=sk83700>.

The DLP UserCheck predefined notifications are in only English by default. If necessary, you can add more languages manually.

To support more languages for UserCheck:

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 **UserCheck**.
3. Select a UserCheck interaction object and click **Edit**.
4. In the **Message** pane, click **Languages**.
5. From the list, select the applicable language.
6. Click **OK**.

A tab for the language is added.

7. Enter the necessary text and click **OK**.

UserCheck Client

In This Section:

UserCheck Client Overview	64
UserCheck Requirements	64
Enabling UserCheck Client	65
Client and Gateway Communication	65
Getting the MSI File	70
Distributing and Connecting Clients	70
Helping Users	72

UserCheck Client Overview

The UserCheck client is installed on endpoint computers to communicate with the gateway and show UserCheck interaction notifications to users.

It works with these Software Blades:

DLP - Notifications of DLP incidents can be sent by email (for SMTP traffic) or shown in a popup from the UserCheck client in the system tray (for SMTP, HTTP and FTP).

- UserCheck client adds the option to send notifications for applications that are not in a web browser, such as Skype, iTunes, or browser add-ons (such as radio toolbars). The UserCheck client can also work together with the UserCheck portal to show notifications on the computer itself when:
- The notification cannot be displayed in a browser, or
- The UserCheck engine determines that the notification will not be shown correctly in the browser.

Users select an option in the notification message to respond in real-time.

For DLP, administrators with full permissions or the View/Release/Discard DLP messages permission can also send or discard incidents from the SmartConsole **Logs & Monitor Logs** view.

Workflow for installing and configuring UserCheck clients:

1. Configure how the clients communicate with the gateway and create trust with it.
2. Enable UserCheck and the UserCheck client on the gateway.
3. Download the UserCheck client MSI file.
4. Install the UserCheck client on the endpoint computers.
5. Make sure that the UserCheck clients can connect to the gateway and receive notifications.

UserCheck Requirements

See *UserCheck Client Requirements* in the *R80.10 Release Notes*
<http://downloads.checkpoint.com/dc/download.htm?ID=54802>.

Enabling UserCheck Client

Enable UserCheck and the UserCheck client on the gateway in the Properties window of the gateway object in SmartConsole. This is necessary to let clients communicate with the gateway.

To enable UserCheck and the UserCheck client on the gateway:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **UserCheck**.
3. Select **Enable UserCheck for active blades**.
This enables UserCheck notifications from the gateway.
4. In the UserCheck Client section, select **Activate UserCheck Client support**.
This enables UserCheck notifications from the client.
5. Click **OK** and **Install Policy**.

Client and Gateway Communication

In an environment with UserCheck clients, the gateway acts as a server for the clients. Each client must be able to *discover* the server and create *trust* with it.

To create trust, the client makes sure that the server is the correct one. It compares the server fingerprint calculated during the SSL handshake with the expected fingerprint. If the server does not have the expected fingerprint, the client asks the user to manually confirm that the server is correct.

Here is a summary of the methods that you can use for clients to discover and trust the server. More details are described later in this section.

- **File name based server configuration** – If no other method is configured (default, out-of-the-box situation), all UserCheck clients downloaded from the portal are renamed to have the portal machine IP address in the filename. During installation, the client uses this IP address to connect to the gateway. Note that the user has to click **Trust** to manually trust the server.
- **AD based configuration** – If client computers are members of an Active Directory domain, you can deploy the server addresses and trust data using a dedicated tool.
- **DNS SRV record based server discovery** – Configure the server addresses in the DNS server. Note that the user has to click **Trust** to manually trust the server.
- **Remote registry** – All of the client configuration, including the server addresses and trust data reside in the registry. You can deploy the values before installing the client (by GPO, or any other system that lets you control the registry remotely). This lets you use the configuration when the client is first installed.

Option Comparison

	Requires AD	Manual User Trust (one time) Required?	Multi-Site	Client Remains Signed?	Still works after Gateway Changes	Level	Recommended for...
File name based	No	Yes	No	Yes	No	Very Simple	Single Security Gateway deployments
AD based	Yes	No	Yes	Yes	Yes	Simple	Deployments with AD that you can modify
DNS based	No	Yes	Partially (per DNS server)	Yes	Yes	Simple	Deployments without AD With an AD you cannot change, and a DNS that you can change
Remote registry	No	No	Yes	Yes	Yes	Moderate	Where remote registry is used for other purposes

File Name Based Server Discovery

This option is the easiest to deploy, and works out-of-the-box. It requires that users manually click **Trust** to trust the server the first time they connect. You can use this option if your deployment has only one Security Gateway with the relevant Software Blades.

How does it work?

When a user downloads the UserCheck client, the address of the Security Gateway is inserted in the filename. During installation, the client finds if there is a different discovery method configured (AD based, DNS based, or local registry). If no method is configured, and the gateway can be reached, it is used as the server. In the UserCheck Settings window, you can see that the server you connect to is the same as the Security Gateway in the UserCheck client filename.

Users must manually make sure that the trust data is valid, because the filename can be easily changed.

Renaming the MSI

You can manually change the name of the MSI file before it is installed on a computer. This connects the UserCheck client to a different gateway.

To rename the MSI file:

1. Make sure the gateway has a DNS name.
2. Rename the MSI using this syntax: **UserCheck_~GWname.msi**
Where *GWname* - is the DNS name of the gateway.

Optional: Use **UserCheck_~GWname-port.msi**

Where *port* is the port number of notifications. For example, UserCheck_~mygw-18300.msi.



Notes - The prefix does not have to be "UserCheck". The important part of the syntax is underscore tilde ([~]), which indicates that the next string is the DNS of the gateway.

If you want to add the port number for the notifications to the client from the gateway, the hyphen (-) indicates that the next string is the port number.

Active Directory Based Configuration

If your client computers are members of an Active Directory domain and you have administrative access to this domain, you can use the Distributed Configuration tool to configure connectivity and trust rules.

The Distributed Configuration tool has three windows:

- **Welcome** - Describes the tool and lets you enter different credentials that are used to access the AD.
- **Server configuration** - Configure which Security Gateway the client connects to, based on its location.
- **Trusted gateways** - View and change the list of fingerprints that the Security Gateways consider secure.

To enable Active Directory based configuration for clients:

1. Download and install the UserCheck client MSI on a computer.
From the command line on that computer, run the client configuration tool with the AD utility.
For example, on a Windows 7 computer:
`"C:\Users\<user name>\Local Settings\Application Data\Checkpoint\UserCheck\UserCheck.exe" -adtool`
The Check Point UserCheck - Distributed Configuration tool opens.
2. In the **Welcome** page, enter the credentials of an AD administrator.
By default, your AD username is shown. If you do not have administrator permissions, click **Change user** and enter administrator credentials.
3. In the **Server Configuration** page, click **Add**.
The **Identity Server Configuration** window opens.
4. Select **Default** and then click **Add**.
5. Enter the IP address or Fully Qualified Domain Name (FQDN) and the port of the Security Gateway.
6. Click **OK**.
The identity of the AD Server for the UserCheck client is written in the Active Directory and given to all clients.

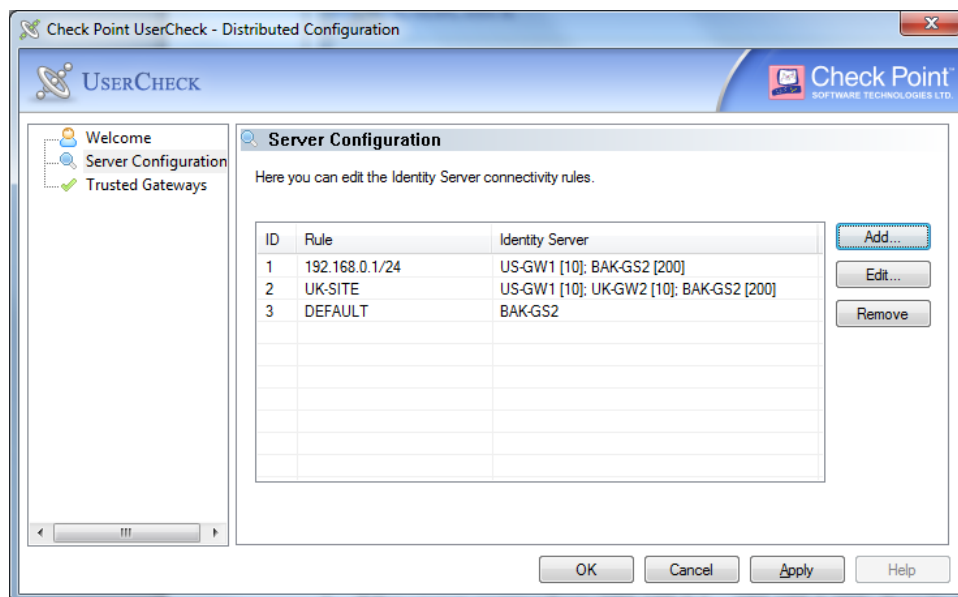


Note - The entire configuration is written under a hive named **Check Point** under the **Program Data** branch in the AD database that is added in the first run of the tool. Adding this hive does not affect other AD based applications or features.

Server Configuration Rules

If you use the Distributed Configuration tool and you configure the client to **Automatically discover** the server, the client fetches the rule lists. Each time it must connect to a server, it tries to match itself against a rule, from top to bottom.

When the tool matches a rule, it uses the servers shown in the rule, according to the priority specified.



The configuration in this example means:

1. If the user is coming from '192.168.0.1 – 192.168.0.255', then try to connect to US-GW1. If it is not available, try BAK-GS2 (it is only used if US-GW1 is not available, as its priority is higher).
2. If the user is connected from the Active Directory site 'UK-SITE', connect either to UK-GW1 or UK-GW2 (choose between them randomly, as they both have the same priority). If both of them are not available, connect to BAK-GS2.
3. If rules 1 and 2 do not apply, connect to BAK-GS2 (the default rule is always matched when it is encountered).

Use the **Add**, **Edit** and **Remove** buttons to change the server connectivity rules.

Trusted Gateways

The **Trusted Gateways** window shows the list of servers that are trusted - no messages open when users connect to them.

You can add, edit or delete a server. If you have connectivity to the server, you can get the name and fingerprint. Enter its IP address and click **Fetch Fingerprint** in the **Server Trust Configuration** window. If you do not have connectivity to the server, enter the same name and fingerprint that is shown when you connect to that server.

DNS Based Configuration

If you configure the client to **Automatic Discovery** (the default), it looks for a server by issuing a DNS SRV query for the address of the gateway (the DNS suffix is added automatically). You can configure the address in your DNS server.

To configure DNS based configuration on the DNS server:

1. Go to **Start > All Programs > Administrative Tools > DNS**.
2. Go to **Forward lookup zones** and select the applicable domain.
3. Go to the **_tcp** subdomain.
4. Right click and select **Other new record**.
5. Select **Service Location, Create Record**.
6. In the **Service** field, enter **CHECKPOINT_DLP**.
7. Set the **Port number** to 443.
8. In **Host offering this server**, enter the IP address of the Security Gateway.
9. Click **OK**.

To configure Load Sharing for the Security Gateway, create multiple SRV records with the same priority.

To configure High Availability, create multiple SRV records with different priorities.



Note - If you configure AD based and DNS based configuration, the results are combined according to the specified priority (from the lowest to highest).

Troubleshooting DNS Based Configuration

To troubleshoot issues in DNS based configuration, you can see the SRV records that are stored on the DNS server.

To see SRV records on the DNS server:

Run:

```
C:\> nslookup
> set type=srv
> checkpoint_dlp._tcp
```

The result is:

```
C:\> nslookup
> set type=srv
> checkpoint_dlp._tcp

Server:  dns.company.com
Address:  192.168.0.17

checkpoint_dlp._tcp.ad.company.com    SRV service location:
    priority      = 0
    weight        = 0
    port          = 443
    svr hostname  = dlpserver.company.com

dlpserver.company.com internet address = 192.168.1.212
>
```

Remote Registry

If you have a way to deploy registry entries to your client computers, for example, Active Directory or GPO updates, you can deploy the Security Gateway addresses and trust parameters before you install the clients. Clients can then use the deployed settings immediately after installation.

To configure the remote registry option:

1. Install the client on one of your computers. The agent installs itself in the user directory, and saves its configuration to HKEY_CURRENT_USER.
2. Connect manually to all of the servers that are configured, verify their fingerprints, and click **Trust** on the fingerprint verification dialog box.
3. Configure the client to manually connect to the requested servers (use the **Settings** window).
4. Export these registry keys (from HKEY_CURRENT_USER):
 - a) SOFTWARE\CheckPoint\UserCheck\TrustedGateways (the entire tree)
 - b) SOFTWARE\CheckPoint\UserCheck\
 - (i) DefaultGateway
 - (ii) DefaultGatewayEnabled
5. Import the exported keys to the endpoint computers before you install the UserCheck client.

Getting the MSI File

To get the MSI file:

1. In SmartConsole, in the **Gateways & Servers** view, open the **General Properties** window of the gateway object.
2. From the navigation tree, select **UserCheck**.
3. In the **UserCheck Client** section, click **Download Client**.



Important - Before you can download the client msi file, the UserCheck portal must be up. The portal is up only after a Policy installation.

Distributing and Connecting Clients

After configuring the clients to connect to the gateway, install the clients on the user machines. You can use any method of MSI or EXE mass deployment and installation that you choose. For example, you can send users an email with a link to install the client. When a user clicks the link, the MSI file automatically installs the client on the computer.

Alternatively, users can download the installation package from the regular DLP UserCheck notifications.

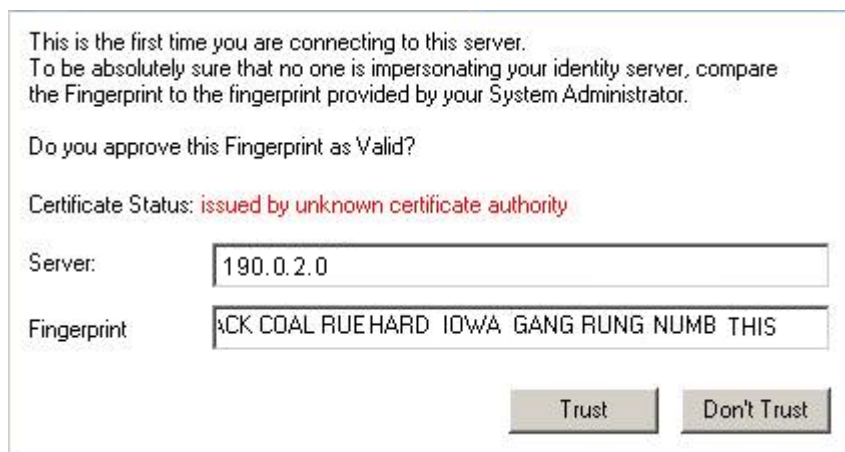
To install the client for all user accounts on a Windows computer, see sk96107

<http://supportcontent.checkpoint.com/solutions?id=sk96107>.

The installation is silent and generally, no reboot is required.

When the client is first installed, the tray icon indicates that it is not connected. When the client connects to the gateway, the tray icon shows that the client is active.

The first time that the client connects to the gateway, it asks for verification from the user and approval of the fingerprint.



Best Practices:

- Let the users know this will happen.
- Use a server certificate that is trusted by the certificate authority installed on users' computers. Then users do *not* see a message that says: **Issued by unknown certificate authority**.

If UserCheck for DLP is enabled on the gateway, users are required to enter their username and password after the client installs.

Example of message to users about the UserCheck client installation (for DLP):

Dear Users,

Our company has implemented a Data Loss Prevention automation to protect our confidential data from unintentional leakage. Soon you will be asked to verify the connection between a small client that we will install on your computer and the computer that will send you notifications.

This client will pop up notifications if you try to send a message that contains protected data. It might let you to send the data anyway, if you are sure that it does not violate our data-security guidelines.

When the client is installed, you will see a window that asks if you trust the DLP server. Check that the server is SERVER NAME and then click Trust.

In the next window, enter your username and password, and then click OK.



Note - If the UserCheck client is not connected to the gateway, the behavior is as if the client was never installed. Email notifications are sent for SMTP incidents and the Portal is used for HTTP incidents.

UserCheck and Check Point Password Authentication

You can see and edit Check Point users from **Users and Administrators** in the navigation tree.

To enable Check Point password authentication:

SmartConsole Configuration

1. Open SmartConsole and open the **Manage & Settings** view.
2. Click **Permissions & Administrators > Administrators**, and select an existing user or create a new user.
3. In the **General Properties** page of the user, make sure that an email address is defined.
4. In the **Authentication Properties** page of the user, set **Authentication Scheme** to **Check Point Password** and enter the password and password confirmation.
5. Click **OK**.

UserCheck Client Configuration

Ask your users to configure their UserCheck client:

1. On the UserCheck client computer, right click the UserCheck icon in the Notification Area (next to the system clock).
2. Select **Settings**.
3. Click **Advanced**.
4. Select **Authentication with Check Point user accounts defined internally in SmartConsole**.

Helping Users

If users require assistance to troubleshoot issues with the UserCheck client, you can ask them to send you the logs.

To configure the client to generate logs:

1. Right-click the UserCheck tray icon and select **Settings**.
The **Settings** window opens.
2. Click **Log to** and browse to a pathname where the logs are saved.
3. Click **OK**.

To send UserCheck logs from the client:

1. Right-click the UserCheck tray icon and select **Status**.
The **Status** window opens.
2. Click **Advanced** and then click the **Collect information for technical support** link.
The default email client opens, with an archive of the collected logs attached.

Out of the Box

In This Section:

Default Deployment	73
Data Loss Prevention in SmartDashboard	73
Defining My Organization	75
Data Loss Prevention Policies	79
Auditing and Analysis	90

Default Deployment

The first stage of DLP deployment 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 will transmit data as a part of their daily tasks. DLP will catch incidents that match rules of the policy. Rules in this stage will be set to **Detect**, allowing you to monitor usage and understand the specific needs of your organization without disrupting your users.
- You will audit the data, using experience-driven severity ratings, and the Logs & Monitor tracking 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.

Page	Function
Policy	Manage the rule base for Data Loss Prevention policy.
Whitelist Policy	Manage files that will never be matched by the DLP Rule Base.
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 gateways and Exchange Agents. You can see a graphical representation of this information in SmartView Monitor.
UserCheck	<p>Manage UserCheck objects that are used in a Rule Base to:</p> <ul style="list-style-type: none"> • 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:	
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).
Advanced	<ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • CPU load levels are more than the high CPU load watermark • Other extreme conditions including: <ul style="list-style-type: none"> ▪ 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 <p>If necessary, you can change the default values ("Editing Extreme Condition Values" on page 162).</p> • 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.

Adding Email Addresses and Domains to My Organization

You define 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 about Domains:

- 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 defined in My Organization **and** if the IP address of the sender is an interface/network defined 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 defined. If you do not have the domain defined (either by Email Address Domain or LDAP Account Unit) for My Organization, DLP will 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**.

Defining Internal Users

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

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. Expand **Additional Settings > Users**.
2. Click **New > User**.

The **User Properties** window opens.

3. 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 **Additional Settings > Users**.
2. Click **New > User Group**.

The **Group Properties** 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. Open **Data Loss Prevention > My Organization**.
2. In the **Users** area, click **Exclusions**.

The **User groups and Users** window opens.

3. Select the listed items that you want to exclude from **My Organization**.

4. Click **Add**.
5. Click **OK**.

Defining Internal Networks

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

If you choose to define My Organization by naming specific networks or hosts, any internal networks or hosts that you did not name will not be considered internal by DLP.



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

To define specific networks and hosts:

1. In SmartConsole, open the **Data Loss Prevention** tab.
2. Click **My Organization**.
3. In the **Networks** area, select **These networks and hosts only**.
4. Click **Edit**.
5. In the **Networks and Hosts** window, select items from the list of defined networks and hosts and then click **Add**.
6. Add as many items as needed to define **My Organization**.
7. Click **OK**.

Excluding Networks from My Organization

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

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

Any network, network group, or host that you define as an exclusion will be recognized by Data Loss Prevention as **Outside My Org**. 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. Open **Data Loss Prevention > My Organization**.
2. In the **Networks** area, click **Exclusions**.
The **Networks and Hosts** window opens.
3. Select the listed items that you want to exclude from **My Organization**.
4. Click **Add**.
5. Click **OK**.

Defining Internal VPNs

Remote Access communities in **VPN** of **My Organization** are supported only in Office Mode.

To configure Office Mode for support of Remote Access communities:

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

To include 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. From **SmartConsole**, **Install Policy**.

Excluding VPNs from My Organization

To discover VPNs known to DLP:

1. In SmartConsole, click **Gateways & Servers**, and find the VPN gateway that protects the DLP gateway.
For an integrated DLP deployment, this is the DLP gateway itself. The protecting VPN gateway includes the IP address of the DLP gateway in its encryption domain.
2. Double-click the VPN gateway.
The 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.

To exclude 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 navigation 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 gateway; they are excluded by default.
5. Click **Save** and then close SmartDashboard.
6. From **SmartConsole**, **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.

Overview of DLP Rules

A Data Loss Prevention rule is made up 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 will check 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 choose to make the destination any network object defined in the SmartConsole to protect data transfer 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 choose 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 any place of the policy, it will not be checked further.
- **An action to take** - DLP response 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, 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 using 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

In addition to 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 these notifications, you must:

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 handle a DLP incident and apply the same decision for subsequent messages ("**Learning Mode**" on page 102).

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 any 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 match those of the HTTP connection being examined by the DLP gateway.

2. The **Source** column of the DLP rule contains an access role.

Redirecting to the Captive Portal lets DLP:

- Identify unknown users and log their FTP and HTTP activity
Once known, these users can be matched against access roles in the policy.
- Send notification emails for FTP and HTTP violations



Note - Captive Portal redirection occurs:

- Regardless of the 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 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 gateway, the identities of users behind the proxy will remain hidden unless 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 showing internal IP addresses in requests to the internet, select **Hide X Forward-For header in outgoing traffic**.
4. Install the policy.

Example DLP rule 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 will prevent a known user in the Finance department from sending credit numbers outside of the organization. Known users that are not listed in the access role will not be prevented from sending credit card numbers outside of the organization.

- An unknown user (a computer with an IP address that is not mapped to any user in the Active Directory) attempting to send credit card numbers outside of the organization will not be stopped by this rule.
- A user that is known but not part of the access role will not be prevented from sending credit card numbers.
- There is also no redirect to the Captive Portal so that the unknown sender cannot be identified.

Rule 2

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

In this rule:

- Known users inside the organization will be prevented from sending out credit card data, and receive email notification of the policy violation.
- Unknown users inside the organization sending out all types of data will be directed to the Captive Portal for identification. Once identified, DLP scans the data for a possible violation.



Note - Enabling Identity Captive Portal on this rule means that HTTP or HTTPS connections passing from inside to outside of the organization must be identified 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 Portal

In this rule:

- A known user in the Finance department will be prevented from sending credit numbers outside of the organization.
- An access role in the Source (plus Captive Portal in the Action column) means that for HTTP connections there is a redirect if the source user is unknown and the destination matches the destination specified by the policy
- A user that is known but not part of the access role will *not be*:
 - Prevented from sending out credit card numbers
 - Redirected to the Captive Portal.

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 will be 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 will also inform the Marketing and Technical Communications manager that the PDF was released from the company to an external destination.

In this case:

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

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	<p>The transmission is passed. The event is logged and is available for your review and analysis 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.</p> <p>You can choose to notify Data Owners of the event. This is true for all the following actions as well.</p>
Inform User	The transmission is passed, but the incident is logged and the user is notified.

Action	Description
Ask User	<p>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.</p> <p>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.</p>
Prevent	<p>The data transmission is blocked.</p> <p>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.</p>
Watermark	<p>Tracks outgoing Microsoft Office documents (Word, Excel, or PowerPoint files from Office 2007 and higher) by adding visible watermarks or invisible encrypted text.</p> <ul style="list-style-type: none"> • 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 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 fw process, to run the <code>internal_snmp_trap</code> 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: <ul style="list-style-type: none"> • 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). These options are available:

Store Option	Meaning
Yes	<ul style="list-style-type: none"> • Email data is stored as an .eml file • FTP data is stored in the .zip format • HTTP <ul style="list-style-type: none"> • 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 <p>Note: For FTP and HTTP, only those elements of the message that violate DLP rules are stored.</p>

Store Option	Meaning
Only as Text	<ul style="list-style-type: none"> 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. <p>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.</p>
Don't Store	<p>When the rule is matched, the incident is logged and the data deleted so that it cannot be viewed in the Logs & Monitor view.</p> <p>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:</p> <ul style="list-style-type: none"> Delete - Priority 1 Yes - Priority 2 Only as Text - Priority 3 Don't Store - Priority 4
Delete	<p>Logs the incident and immediately deletes the data. Select this example for sensitive data such as credit card numbers.</p> <p>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.</p>

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 data will be stored 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 gateway, open: `$DLPPDIR/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 will not be enforced once the time object expires.
- Time objects are not supported for UTM-1 Edge appliances and QoS. Installing a DLP policy that contains a time object in a rule will result in failure.
- An object that does not have an activation or expiration date is always active.

To create 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**.

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.

To create a time group 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 **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**.

Supported Archive Types

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

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

Selective Deployment - Gateways

For any rule in the policy, you can choose that it be deployed on specific Enforcing Gateways.

To deploy a rule on specific Enforcing DLP Gateways:

1. In SmartConsole, open **Data Loss Prevention > Policy**.
2. In the rule you want, click in the plus in the **Install On** column.
Defined DLP Gateways appear in a menu.

3. Select the Gateways on which you want this rule to be deployed.
4. **Install Policy** on the DLP gateway.

Selective Deployment - Protocols

Check Point Data Loss Prevention supports various data transmission protocols.

It is recommended that you enable protocols as needed in your deployment. 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 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 Agent emails ("[Configuring the Exchange Security Agent](#)" on page 37) and the HTTPS protocol.

To select protocol deployment for all gateways:

1. In SmartConsole, open **Data Loss Prevention**.
2. Expand **Additional Settings** and click **Protocols**.
3. 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 will have no effect.

To select protocol deployment per gateway:

1. In SmartConsole, open the **Firewall** tab.
2. In the **Network Objects** list, double-click the gateway.
The properties window of the gateway opens.
3. In **General Properties** > **Software Blades** > **Network Security**, make sure **Data Loss Prevention** is selected.
4. Open the **Data Loss Prevention** page.
5. In the **Protocols** area, select one of the following:
 - **Apply the DLP policy on the default protocols** - as selected in the Data Loss Prevention tab, according to the previous procedure.
 - **Apply the DLP policy to these protocols only** - select the protocols that you want this gateway to check for the Data Loss Prevention policy.

Auditing and Analysis

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, displaying 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.

From the log of a specific incident you can open the actual data that caused the incident. You should not have to review most of the incidents manually, but the original transmission (for example, the email or its attachment) is kept for you if there is a question from the sender or the data owners.

Because personal emails and web posts may be captured and stored for viewing, **you must let the users know** that this may happen. Failure to do so may cause your organization 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 required. DLP incidents may not show if the incidents (which are in EML file format) are associated with any other application.

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.

DLP Action	Description
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 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 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 logs that are generated will show Prevent as the action. The action implemented will be Prevent. The log of the Detect rule will show **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 will always be 100%.
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.

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

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.

Data Owner and User Notifications

In This Section:

Defining Data Owners	94
Preparing Corporate Guidelines	94
Communicating with Data Owners	95
Communicating with Users	96
Notifying Data Owners	97
Notifying Users	97
Customizing Notifications for Users	98
Setting Rules to Ask User	99
DLP Portal	100
Managing Incidents by Replying to Emails	101
UserCheck Notifications	101
Managing Rules in Ask User	102
Learning Mode	102

Defining Data Owners

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. From **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 any email that violates a DLP rule will be captured and may be reviewed, you have fulfilled the requirements of the law.

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 gateway, open: **\$DLPPDIR/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.

Communicating 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. Having organization-wide guidelines should prevent conflicts if a Data Owner makes a request that is not good business practice; you can direct the Data Owner to the guidelines, rather than rejecting the request personally.

You are responsible for finding a balance between notifying the Data Owner every time an incident occurs - which may overwhelm the person and reduce the effectiveness of the system - and failing to notify the Data Owner enough. 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.

Communicating with Users

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

- Declare the date that the policy was or will start to operate.
- Let them know that the policy operates 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 will be notified by email when this occurs.
- Give a link to the corporate policy.
- Let them know that not abiding to specific rules will cause in result in notification to managers, containing the user's name and the type of data that was leaked.
- Give the expiration time (default is 7 days) for incidents to be handled.

After installing 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 is happening and why, when this data is related.

When a user performs an action that matches a rule, DLP handles the communication and logging 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.
Prevent	<p>An email for this type of rule does not offer handling options, but does provide necessary information.</p> <p>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.</p>

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.

To configure 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. Define the data owners of the Data Type ("[Defining Data Owners](#)" on page 94).
3. From the navigation tree, click **Policy**.
4. Right-click the **Track** column of the rule and select **Email**.
The **Email Notification** window opens.
5. Click **When data is matched, send an email to the following recipients**.
Data Owners is selected by default.
6. For additional email recipients, click Add and select the user.
7. 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
8. Click **OK**.
9. Click **Save** and then close **SmartDashboard**.
10. From **SmartConsole**, **Install Policy**.

Notifying Users

While users are becoming familiar with 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 should significantly improve user leaks over a relatively short amount of time.

You can set 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.

You can also set rules to ask the user what should be done about captured data - send it on or delete it.

To configure user notification:

1. Open **Data Loss Prevention > Policy**.
2. In the **Action** column of the rule to change, right-click and select **Inform User** or **Ask User**.

Customizing Notifications for Users

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

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

In the notification, the user may see:

- 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 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 DLP Policy 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. From **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 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 a rule and select **Edit Rule Notification**.
To notify the user and pass the data, change the action to **Inform User**.
4. In the window that opens, change the text with your own message to fit the rule. You can use text or variables.
5. Click **OK**.
6. Click **Save** and then close **SmartDashboard**.
7. From **SmartConsole**, **Install Policy**.

Setting 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 ("[Configuring the Mail Relay](#)" on page 32).

To set a rule 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. From **SmartConsole**, **Install Policy**.

To set up the gateway for Ask User rules:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
The gateway 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 will use to send notification emails.
6. Click **OK**.
7. **Install Policy**.

DLP 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, choose 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://<Gateway IP>/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 Portal explains that decisions are logged.

- If the user chooses to continue the transmission, they have the opportunity to explain why it should be sent before the action is completed.
- If the user chooses to discard the transmission, DLP deletes the transmission immediately.
- If the user wants to review the transmission before deciding, they will see the reasons why it was captured and have 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://<Gateway IP>/dlp`
- Right-click the UserCheck agent icon in the Task Bar notification area and select **Review DLP notifications**.

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**.

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 gateway 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. **Install 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.

If the incident is in 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.

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 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.

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 previous post 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 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

In This Section:

Analytical Deployment.....	103
Creating New Rules.....	103

Analytical Deployment

After auditing incidents identified by heuristic-driven rules, you begin to 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 choose to combine provided Data Types to make your policy stricter, or to create Exceptions to allow specific conditions.
- Rules in this stage will be set to **Ask User**, allowing your users to 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 will 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, choose one of the following:
 - 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 - Used as 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 going from Network_A to any address outside of Network_A. In comparison, if the destination was Outside My Org, the rule would inspect only data transmissions going 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 the following:
 - Leave **Detect** - To have a matching incident logged without disrupting the data transmission
 - Right-click and select **Inform User** - To pass the transmission but send notification to user
 - Right-click and select **Ask User** - To wait for user decision on whether 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.
 You can add a notification to the Data Owners: select **Email** and customize the notification that the Data Owners will see if this rule is matched.
9. In the **Install On** column, leave **DLP Blades**, to have this rule applied to all DLP Gateways, or click the plus 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 past that time frame, it is allowed to continue. The relevant time zone is that of the Check Point Security Gateway enforcing 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** and then close **SmartDashboard**.
14. From **SmartConsole**, **Install 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 ("[Configuring the Exchange Security Agent](#)" on page 37).

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

While this rule covers the scenario example, an organization may want 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 (including 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 ("[Creating Exceptions](#)" on page 108).

Without an exception, if a Finance department user sends a financial report to anyone, it will match 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 will be blocked based on the Prevent action in the second rule and there will be 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 will be applied for financial reports sent by Finance department users to all internal users other than Finance users.
- The *Ask User* action will be applied for financial reports sent by Finance department users to all external users.
- The *Prevent* action will be applied for financial reports sent by any user not in the Finance department to any external or internal user.

Scenario 3: Financial reports can only be sent within the Finance department. Any user that sends a financial report from outside the Finance department will get a notification and has to make a decision relating 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 setting up the basics of a rule, you can do more.

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 are following 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, right-click the rule base headers and select **Name**.

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

To see the protocols of rules, right-click the rule base headers and 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: in the **Severity** column, leave **Medium**, or 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 work on this rule or the Data Types used by it.

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

For example, you create a new rule using the built-in Data Type **Employee Names**. You know that this is a placeholder Data Type - you are going to have to supply the list of names of employees in your organization. You flag this rule for **Improve Accuracy** and continue working on the rule base. Later you can find the rule for Employee Names easily, by grouping the rules by flags or by the **Overview** link. Then you can edit the Data Type, starting 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 Follow up 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 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. From **SmartConsole**, **Install Policy**.

Rule Exceptions

Sometimes you may want to 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), should 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, allowing this data type to be sent to the specific email address. You could make this case even better: in the exception, include a secondary data type is a Dictionary of patient names who have signed a waiver for the social worker to see their records. Thus, with one rule, you ensure that only records that the social worker is allowed to see are sent to the social worker's office. DLP prevents anyone from sending records to an unauthorized email address. It ensures that no employee of the clinic has to deal personal requests to have the records sent to unauthorized destination - it simply cannot be done.

Creating Exceptions

To create an exception to a DLP rule:

1. In SmartConsole, select **Security 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. From **SmartConsole**, **Install 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, 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, 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

In This Section:

Customized Deployment	110
Setting Rules to Prevent	111
Multi-Realm Authentication Support	111
Defining Data Types	113
Adding Data Types to Rules	127
Repositories	136
Whitelist Policy	138
Defining Email Addresses	138
Configuring the DLP Watermark	139
Fine Tuning Source and Destination	147
Defining Protocols of DLP Rules	150

Customized Deployment

Check Point DLP provides the **MultiSpect** set of features. These features provide the flexibility you need to monitor and ensure accuracy of your DLP deployment. 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 will 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 will match 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. From **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 DLPportal or UserCheck agent
- DLP looks up an email address extracted from SMTP traffic to identify a user

To define AD servers Using GuiDBedit:

1. Open **GuiDBedit**.
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 **GuiDBedit**.
8. Install the updated policy on the DLP enabled gateway.

Troubleshooting DLP Related Authentication Issues

The Check Point database tool, **GuiDBedit**, 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: **GuiDBedit > Tables > Other > authentication_objects**:

Object	Description
DLPSEnderRealm	<p>Controls authentication for the DLP portal and the UserCheck agent. This object contains:</p> <ul style="list-style-type: none"> 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. <p>Use DLPSEnderRealm to solve authentication problems.</p>
dlp_ldap_auth_settings	<p>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.</p> <p>The CustomLoginAttr string lets you enter a custom LDAP query with a specified email address. The default query is: (mail=<>>) (proxyAddresses=smtp:<>>)</p> <p>By default, it searches for the user with the specified email address.</p> <p>To refine the query, you can add other AD attributes to the query or change existing ones.</p> <p>WARNING: Changing this default query might affect DLP rules that enforce a policy according to users or user groups defined by access roles. <i>Known</i> users may become <i>Unknown</i> and the data they send allowed to leave the organization.</p>
dlp_internal_auth_settings	<p>This object controls how DLP identifies users by querying the email address attribute in the database of internal users defined in SmartConsole.</p>

Defining 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. Choose an option that defines the type of traffic that will be checked against a rule containing this data type.
6. Fill in the properties as required in the next step (each step is relevant to the option selected in the previous step).
7. Click **Finish**.
8. Click **Save** and then close **SmartDashboard**.
9. From **SmartConsole**, **Install Policy**.

Protecting Data By Keyword

You can create a list of keywords that will be matched against data transmissions. Transmissions that contain this list of words in their data are matched. You define whether it should match it on an ALL or ANY basis.

To create a data type representation of specified keywords:

1. In the **Data Type Wizard**, select **Keywords**.
2. Click **Next**.
The next step is the **Specify Keywords** window.
3. Enter a keyword to protect.
4. Click **Add**.
5. Enter as many keywords or phrases as you want in this data type.
6. Decide whether data should be matched if all the keywords in this list are matched, if only one match is necessary, or a specific number should be matched.

For example, if you want to ensure that no one can send an email that contains any of the names of congressmen in a committee, their names would be the keywords and you would set the **Threshold** to **At least 1**. (Note that the higher the threshold, the more precise the results will be.)

If you wanted to allow emails mentioning the congressmen, but decided that all of their names in one email would be suspicious, then set **Threshold** to **All words must appear**.

7. Click **Next**.
8. Click **Finish**; or if you want to add more parameters to the data type, select the checkbox and then click **Finish**.

Protecting Documents by Template

Confidential and sensitive documents are often based on templates. A template defines 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 will 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.

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 Type Wizard**, 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. Choose 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 will catch. 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 will be different for each template.

5. Click **Next**.
6. Click **Finish**.

To configure additional properties for the Data Type, select **Configure additional Data Type properties** clicking **Finish**.

Property	Description
Match empty templates	<ul style="list-style-type: none"> • 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. <p>Note: the rule is bypassed for this document, but the document may still be matched by another DLP rule in the policy.</p>
Consider template's images	<ul style="list-style-type: none"> • 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.

Alternative to slider testing:

If you want to catch documents that match on different levels with different actions, you may try this procedure:

1. Create the Data Type for the template, setting the slider to 10%.
2. In the **Policy** window, create a Detect rule that tracks matching documents but does not stop them.
3. Create another Data Type, just like the first, but set the slider to 50%.
4. Create an Ask User rule that tracks matching documents and holds the transmission until the user decides whether it should be sent or is too sensitive and should be deleted.
5. Create a third Data Type, with the slider set to 90%.
6. Create a Prevent rule that tracks matching documents and blocks the transmission.

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. Thus, the more parameters you can set here with assurance, the more accurate the results will be.

- **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**, or if you want to add more parameters to the data type, select the checkbox and then click **Finish**.

Protecting Data by Pattern

You can create a regular expression that will be matched against content in data transmissions. Transmissions that contain strings that match the pattern in their data are 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.
6. Decide whether data should match the data type if the pattern is matched even once, or if it should be allowed 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, you would set the pattern to `^[0-9]+\.[0-9]{2}?$` and you would set the **Number of occurrences** to **5**.
7. Click **Next**.
8. Click **Finish**; or if you want to add more parameters to the data type, select the checkbox and then 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 will match 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**; or if you want to add more parameters to the Data Type, select the checkbox and then click **Finish**.

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 will accurately match 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 DLP 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.
- The signature of the file passing through the DLP gateway is compared against the signatures of files in the repository. If there is a signature match, the file scanned by the gateway is prevented from going 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 will not be updated until the next scheduled scan occurs.

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 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 will be 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


Large repositories might cause a scan to 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 will recommence where it stopped when the next scheduled scan occurs.

Logging

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.

Logs are generated when:

- 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, you will only see the start and finish logs.

Log Details

- **Fingerprint**

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.

- **Fingerprint scan details**

Repository root path The upper level repository

Current directory Current directory being scanned

Directories The total number of directories in the repository selected in data locations.

Repository size (MB) The size of the repository

Repository Files The number of files in the repository

Directories scanned The number of directories scanned so far

Scanned size (MB) The number MBs scanned so far

Scanned files The number of files scanned so far

Unreachable directories Number of sub directories in the repositories that could not be opened during the scan.

Fingerprinted files	The number of files with a fingerprint signature
Filtered files	The number of files that were not scanned because they did not meet the criteria set on the Repository Scan Filter page. For example file size, modification date, or Data Type.
Scan speed (KBs)	The speed of the scan
Progress	Percentage of the repository so far scanned
Remaining time	Estimated time to scan completion

To create 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 will show on the **Data Loss Prevention > Repositories** page.
3. Click **Next**.
4. In the **Fingerprint** window:
 - a) Click the Gateways arrow button to select gateways with the DLP blade enabled.
By default, The **DLP Blades** object shows. This object represents all gateways that have the DLP blade enabled. Only 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 gateways list (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:
 - A percentage value or
 - 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 shows in the list of data types and also on the **Repositories** page.

To configure 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:

- **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 gateway resources and network bandwidth are an issue, limit the scan to off-peak hours.

- **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 will result in a long scan. The fingerprint will only be enforced after this scan has ended.

- **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 a policy on the DLP enabled 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:

- a) On the **Repositories** window, select the fingerprint Data Type.
- b) In the summary pane for the Data Type, click **Start**.

NFS Repository scanning in NATed Environments

NATing, *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.

To disable Hide NAT on NFS services:

1. On the Security Management Server, open `$FWDIR/lib/table.def` for editing.
2. Search for the line: `no_hide_services_ports`.
These are the services and ports not included in Hide NAT.
3. Enter:
`no_hide_services_ports = { <111, 17>, <111, 6>, <4046, 17>, <4046, 6> }`
If a list of services and ports already exists, add these numbers to the end of the list.
4. Save and close the file.
5. Install the policy onto the ClusterXL object.

Note:

- New settings in `table.def` globally to all gateways.
- For more, see sk31832 (<http://supportcontent.checkpoint.com/solutions?id=sk31832>).

Advanced Data Types

The Data Type Wizard has four advanced Data Types:

- Weight Keywords
- Words from a dictionary
- Custom CP code match
- Message attributes

Protecting Data by Weighted Keyword

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 according to the action of the rules that use this Data Type.

To create a Data Type representation of weighted keywords:

1. In the **Data Type Wizard**, select **Advanced** and from the drop-down list, select **Weighted Keywords**.
2. Click **Next**.

3. Click the arrow of the **Add** button and select either **Word or Phrase** or **Regular Expression**.
(If you click the **Add** button instead of its sub-menu, the item will be a keyword, not a pattern.)
The **Edit Word** window opens, for both types of item.
4. Enter the keyword, phrase, or regular expression.
5. In the **Weight** area, set whether each occurrence of matching data content should be counted as **1** (default) or more, and if there is a ceiling to the weight.
 - **Each appearance of this word contributes the following weight** - set to 1 for lowest weight, 2 for double-weight (one instance of this string will be 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 higher than the weight in the previous value to set a maximum count (a ceiling) for this one word.
6. Click **OK**.
7. In the **Specify Weighted Keywords** step, set the **Threshold**. If data content matches any of the words in this Data Type, with a total weight surpassing this value, the data is matched to the Data Loss Prevention rule.
8. Click **Next**.
9. Click **Finish**; or if you want to add more parameters to the Data Type, select the checkbox and then click **Finish**.

Providing Keywords by Dictionary

If you pre-planned the keywords that should 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 dictionary. You decide how many of the items in the list have to be matched to have the data match the rule.

Best Practice - Dictionary files should be one word or phrase per line. If the file contains non-English words, it is recommended that it be a Word document (*.doc). Dictionaries that are simple text files must be in UTF-8 format.

To create a Data Type representation of dictionary:

1. In the **Data Type Wizard**, select **Advanced** and from the drop-down list, select **words from a Dictionary**.
2. Click **Next**.
3. Browse to the file containing the list of terms.
4. In the **Threshold** area, set the number of terms in this list that must be in the content to have the data matched to the rule.

Best Practice - Set this to the highest reasonable value first, and then lower it after you audit the Logs & Monitor logs.

For example, if the dictionary is a list of employee names, you should not set the threshold to **1**, which would catch every email that has a signature. You could set an Employee Name Dictionary Data Type to a threshold of half the number of users and its rule to **Detect**. If no data is caught by the rule after about a week, lower the threshold and check again. When the rule begins to detect this information being sent out, set it to **Ask User**, so that users have to explain why they are sending this information outside before it will be sent. With this information on hand, you can create a usable, reasonable and accurate enforcement of corporate policy.

5. Click **Next**.
6. Click **Finish**; or if you want to add more parameters to the Data Type, select the checkbox and then click **Finish**.

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).



Note - See the *R77 CPcode DLP Reference Guide*

http://supportcontent.checkpoint.com/documentation_download?ID=24804.

If you write a CPcode function yourself, you should test it first before putting it in production.

To create a Data Type representation of CPcode:

1. In the **Data Type Wizard**, select **Advanced** and from the drop-down list, select **a Custom CPcode**.
2. Click **Next**.
3. Browse to the CPcode script file.
4. Click **Next**.
5. Click **Finish**; or if you want to add more parameters to the Data Type, select the checkbox and then click **Finish**.

Example of CPcode function:

```
func rule_1 {
    foreach $recipient inside global:DESTS {
        foreach $comp inside CPMPEITORS_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();
            }
        }
    }
}
```

Defining the Message Attribute Data Type

In DLP, a message can be sent using the SMTP, HTTP, or FTP protocols.

Message attributes refer to 3 properties of the message:

- The total message *size* in KB
- Number of *attachments*
- Total *number of words* in the message

To create the message attribute Data Type:

1. Start the **Data Type Wizard**
2. Select **Advanced** and from the drop-down list select **Message Attributes**.

The **Specify Message Attributes** window opens.

3. Configure these message attributes:

- **Size**

The size attribute can have a:

Minimum value	Maximum value	Meaning
Yes	Yes	Messages that fall within the specified range match the message attribute.
Yes	No	A message whose size is greater than the minimum value specified here matches the attribute.
No	Yes	A message whose size is smaller than the maximum value specified here matches the attribute.

- **Attachments**

Define the number of attachments a message can have.

Minimum value	Maximum value	Meaning
Yes	Yes	A Message whose number of attachments falls within the specified range matches the message attribute.
Yes	No	A message with more than the minimum number of attachments specified here matches the attribute.
No	Yes	A message with less attachments than those shown by the maximum value specified here matches the attribute.

- **Number of words**

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 will want the email to match a DLP rule only if the email contains enough text that could conceivably result in data loss.

Minimum value	Maximum value	Meaning
Yes		Messages whose word count falls within the specified range matches the message attribute.
Yes	No	A message whose word count is greater than the minimum value specified here matches the attribute.
No	Yes	A message whose word count is lower than the maximum value specified here matches the attribute.

4. Click **Next**.

5. Click **Finish**.

If you want to add more parameters to the Data Type, select the **Configure additional Data Type properties** after clicking finish and then click **Finish**.



Note - For a message to match the Data Type attribute, it must match the criteria for size *and* the number of attachments *and* the number of words. If the message fails to match one of the criteria, it will fail to match the attribute.

Enhancing Accuracy through Statistical Analysis

A number of Data Types, such as credit card numbers, have an option called **Enhance accuracy through statistical analysis** on their **General Properties** page.

Credit cards like Visa and Mastercard have sixteen digit numbers arranged in four groups of four. While scanning for this Data Type, all sixteen digit numbers in the data that match the Luhn algorithm will be identified as credit card numbers. The sixteen digits might not represent a credit card number. The sixteen digits might 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 for editing.
3. On the **General Properties** page, select **Enhance accuracy through statistical analysis**.
4. Click **OK**.



Note - Enabling statistical analysis does not impact 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 defines a data asset that you want to protect.

Data Owners should be aware of the types of data that are under their responsibility and be able to tell you what type of data must be able to move outside of the organization and what data must be protected.

For example, a team leader of a programming team should know that lines of code should not be allowed to move outside the organization, and require that it be protected. A hospital administrator should have an example of a court order releasing patient records to authorized domains.

Focusing on Data

- 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 Gateways.

The Compliance Data Category

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.

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.

The **Data Loss Prevention Overview** window > **DLP Featured Data types** toolbox lists the data types for:

- Compliance
Clicking the **Compliance** button shows 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

1. In the **Data Loss Prevention Data Types** window, click **New**.
The **Data Type Wizard** opens.
2. Select criteria such as keywords or a corporate template
3. On the last page of the wizard open, select **Configure additional Data Type properties after clicking Finish**.
4. Click **Finish**.
5. The data type properties window opens on the **General Properties** page.
6. 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.

Editing Data Types

After you define 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.

Section	Description
General Properties	<ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • Add - Click to add CPcode scripts. The default file type is cpc. See the <i>R77 CPcode DLP Reference Guide</i> http://supportcontent.checkpoint.com/documentation_download?ID=24804. • View - Click to view a CPcode script in a text editor. • Remove - Click to remove CPcode scripts.
Compound	<ul style="list-style-type: none"> • 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 items to a list. • Edit selected item. (Changes made from here affect all compound data types and rules that use the edited data type). • Remove items from a list.

Section	Description
Dictionary	<ul style="list-style-type: none"> • 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 will be 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 will be matched. <p>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.</p>
Documents Based on a Corporate Template	<ul style="list-style-type: none"> • 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 will match header and footer content, as well as boiler-plate text.
File	<p>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.</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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 <i>number</i> words must appear - Enter an integer to indicate number of items in Search List to match the Keyword data type.
Pattern	<ul style="list-style-type: none"> • 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.
Similarity	<ul style="list-style-type: none"> • 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 will match header and footer content, as well as boiler-plate text.
Threshold (dictionary)	<ul style="list-style-type: none"> • This data will be 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)	<ul style="list-style-type: none"> • 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)	<p>This data will be matched only if it contains:</p> <ul style="list-style-type: none"> • All keywords and phrases - Select to match data only if all the items in the Search List are found. • At least <i>number</i> keywords or phrases - Enter an integer to indicate number of items in Search List to match the Keyword data type.

Section	Description
Threshold (recipients)	<p>This data will be matched only if the email contains:</p> <ul style="list-style-type: none"> • At least <i>number</i> internal recipients - Enter the minimum number of email addresses that are defined 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 <i>number</i> 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 will match a rule.
Threshold (External BCC)	<p>This data will be matched only if the email contains at least:</p> <ul style="list-style-type: none"> • Internal recipients - Enter the minimum number of email addresses that are defined 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	<ul style="list-style-type: none"> • 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.

To edit a Data Type:

1. On the SmartConsole, open the **Data Loss Prevention** tab.
2. Open **Data Types**, select a Data Type and click **Edit**.
3. In the General Properties window, edit/fill-in the fields that apply to the Data Type.
4. Click **Finish**.

Defining Data Type Groups

You can create a Data Type representation that is a group of existing Data Types.

To create a Data Type group:

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 > Data Type Group**.
The **Group Data Type** window opens.
4. Enter a **Name** for the group.
5. In the Group Members section, click **Add**.
6. Select the Data Types that are included in this Data Type group.
7. If necessary, add **Data Owners** to the group.
8. Click **OK**.
9. Click **Save** and then close **SmartDashboard**.
10. From **SmartConsole**, **Install Policy**.

Defining Advanced Matching for Keyword Data Types

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.

To add advanced matching Data Type CPcode script:

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. Select a Data Type and click **Edit**.
The **Data Type** window opens.
4. Click the **Advanced Matching** node.
5. 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 CPcode DLP Reference Guide*
http://supportcontent.checkpoint.com/documentation_download?ID=24804.
 - **View** - Click to view a CPcode script in a text editor.
 - **Remove** - Click to remove CPcode scripts.
6. Click **OK**.
7. Click **Save** and then close **SmartDashboard**.
8. From **SmartConsole**, **Install Policy**.

Defining Post Match CPcode for a Data Type

For all Data Type representations, you can add CPcode scripts that run after a data type is matched.

To add a post match Data Type CPcode script:

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. Select a Data Type and click **Edit**.
The **Data Type** window opens.
4. Click the **Advanced Matching** node.
5. In **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.
6. Click **OK**.
7. Click **Save** and then close **SmartDashboard**.
8. From **SmartConsole**, **Install Policy**.

Recommendation - Testing Data Types

Before installing a policy that contains new Data Types, you can test them in a lab environment.

Recommendation for testing procedure:

1. Create a Data Type.
2. Create a user called Tester, with your email address.
3. Create a rule:
 - Data = this Data Type
 - Action = Detect
 - Source = Tester
 - Destination = Outside
4. Send an email (or other data transmission according to the protocols of the rule) that should be matched to the rule.
5. 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.
6. 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 will not ask again about any email in the same thread.

7. Send another transmission, as similar as possible, but that should be passed; check that it is passed.

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.

To export a 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. Select the Data Type to export.
4. Click **Actions > Export**.
5. Save it as a file with the **dlp_dt** extension.
6. 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 deleted but previously exported. 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.

To import Data Types:

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 **Actions > Import**.
4. Select the **dlp_dt** file holding the Data Type that you want.
5. Click **Save** and then close **SmartDashboard**.
6. From **SmartConsole**, **Install Policy**.

Repositories

Repositories are network locations used for document storage. DLP has two kinds of repository

- Fingerprint
- Whitelist

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.

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 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 gateways with the DLP blade enabled.

By default, The **DLP Blades** object shows. This object represents all gateways that have the DLP blade enabled. Only 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 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**.
Select **Configure additional Data Type Properties after clicking Finish** if you want to configure more properties.
 10. Click **Finish**.
The New data type wizard closes. The data type shows in the list of data types and also on the **Repositories** page.
 11. Click **Save** and then close **SmartDashboard**.
 12. From **SmartConsole**, **Install Policy**.

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 gateways with the DLP blade enabled.
By default, The **DLP Blades** object shows. This object represents all gateways that have the DLP blade enabled. Only 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 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. From **SmartConsole**, **Install Policy**.

Whitelist Policy

There are two ways to create a list of files that will never be matched by the DLP Rule Base:

- 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** - This option is recommended if you only 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 not to be included in the DLP match, it must exactly match a file in the whitelist.

6. Click **Save** and then close **SmartDashboard**.
7. From **SmartConsole**, **Install Policy**.

Defining Email Addresses

In DLP administration you may need to define email addresses or domains that are outside of your network security management.

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. From **SmartConsole**, **Install Policy**.

Configuring the DLP Watermark

Watermarking works by introducing custom XML files that contain the watermarking data. Only documents in these Office Open XML formats can be watermarked:

- DOCX
- PPTX
- XLSX



Important - Older formats supported in Office 2007 and above for backward compatibility (such as DOC, PPT, and XLS, cannot be watermarked). Changing the file extension from doc to docx will not make the document eligible for watermarking.

If the Data Type scanned for by the DLP gateway occurs in the body of the email and not the document, the document will not be watermarked. For example if you are scanning for credit card numbers. If the credit card number shows in the body of an email with a document attached, the document will not be watermarked. The Data Type has to occur in the document.

To watermark documents:

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 Policy**.

To create 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. Set if watermarks are added to:

- **All pages**
- **First page only**
- **Even pages only**
- **Odd pages only**

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**.

Watermark option	Section Break	In Word 2007	In Word 2010
All pages	Yes	All pages get watermark	All pages get watermark
	No	All pages get watermark	All pages get watermark
First page only	Yes	<i>All pages get watermark</i>	First page only gets watermark
	No	<i>All pages get watermark</i>	First page only gets watermark
Even pages only	Yes	<i>All pages get watermark</i>	<i>All pages get watermark</i>
	No	Only even pages get watermark	Only even pages get watermark
Odd pages only	Yes	<i>All pages get watermark</i>	<i>All pages get watermark</i>
	No	Only odd pages get watermark	Only odd pages get watermark

To configure 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

a) To change the text to seventy-percent transparency, click the Transparency button.

3. Click **OK**.

To add a shadow behind Watermark text in Word and PowerPoint:

1. On the gateway, run: `cpstop`
2. On the gateway, open for editing: `$DLPPDIR/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`.

To configure 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 ("[Using the DLP Watermark Viewing Tool](#)" on page 146).
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. Existing watermarks can be kept, or replaced.

Note - Hidden encrypted text is not removed, only added to by each DLP gateway. Hidden text can later be used for forensic tracking.

To complete the watermark profile:

1. Click **Save** and then close **SmartDashboard**.
2. In **SmartConsole**, **Install Policy**.

Previewing Watermarks

In **SmartConsole > Data Loss Prevention tab > Additional Settings > Watermarks**, Watermarks are previewed in the right-hand pane on sample documents.

Preview works by downloading sample Office files from the Security Management Server and applying the watermark to them. 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) on the computer that has SmartConsole installed.

Watermarks can also be previewed 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. The file will stay on the server until you remove it by selecting the file in the **Select File** window and clicking 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 Hidden Text 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.

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 will arise. 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:

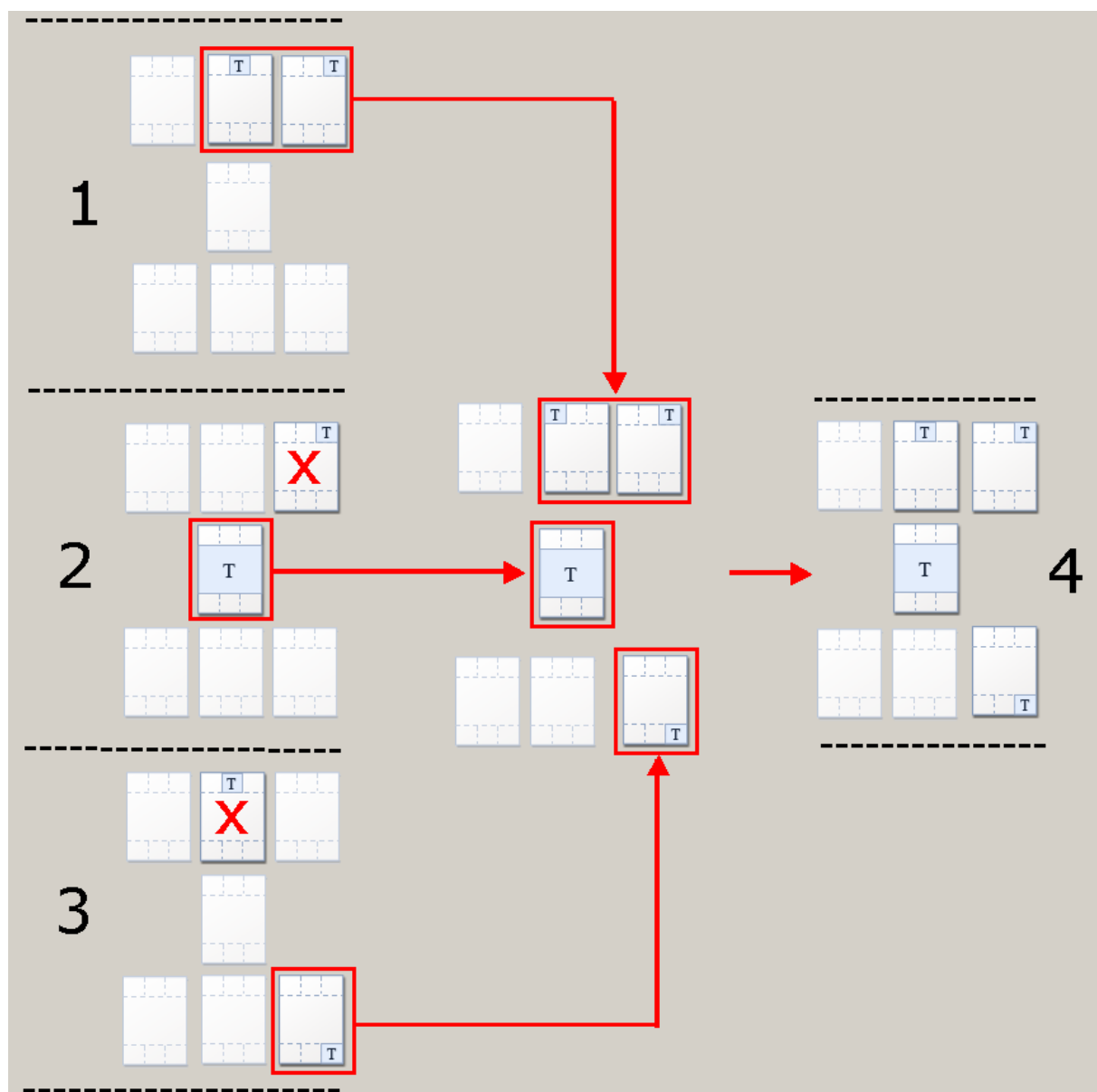
- All the Visible watermarks from the rule with the highest precedence are added to the document.
- Visible watermarks from the rule with the second highest precedence are added to the document only if they do not conflict with watermarks from the first.
- Visible watermarks from the rule with the third highest precedence are added to the document only if they do not conflict with watermarks added by the previous two rules.

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 (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 will not overwrite the watermarked 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.

Turning Watermarking On and Off

Watermarking can be turned off in a number of ways:

- In GuiDBedit:
 - 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 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 gateway. The viewing tool will only show text added by 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 gateway and run the tool on each. The tool will only show the hidden text added by that gateway, and not the text added by 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 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 added to the document by the gateway will not match the ID of the new Security Management Server. The DLP viewer will 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 changes.

Creating Different Rules for Different Departments

You can set the Source of a rule to be any defined user, group, host, network, or VPN. You can then set the Destination to be Outside. The rule will inspect data transmissions from the source to any destination outside of the source. This will create DLP rules specific to one group of users.



Note the different 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, etc. 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** (define a group to include users, groups, or network that defines the Finance Department)
 - **Destination = Outside Source** (any destination outside of Finance, internal or external to My Organization)
 - **Data Type = Salary Reports** (define 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** (define 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 define 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 the previous rules are applied. If you chose My Organization as the source of the third rule, it would apply to the users in Legal and HR and thus negate the other rules.

Isolating the DMZ

To ensure that data transmissions to the DMZ are checked by Data Loss Prevention, define the DMZ as being outside of **My Organization**.

For example, the PCI DSS¹ Requirement 1.4.1 requires that a DMZ be included in the environment to prevent direct Internet traffic to and from secured internal data access points.

To ensure 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 choose 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**.

¹ Payment Card Industry Data Security Standard - Copyright of PCI Security Standards Council, LLC.

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**.

Defining 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 will scan transmissions over all enabled protocols.

You can control which protocols are supported by DLP in general, or by each gateway, or for each rule.

To define supported protocols for DLP:

1. Open **Additional Settings > Protocols**.
2. Select the protocols that you want DLP to be able to support, in general.

For example, if performance becomes an issue, you could clear 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 define 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 gateway opens.
4. Open the **Data Loss Prevention** page of the gateway properties.
5. Select **Apply the DLP policy to these protocols only** and select the protocols that you want this DLP gateway to support.

To define supported protocols for a rule:

1. In the **Policy** view, click the **Protocol** column plus button.
If this column is not visible, right-click a column header. In the list of possible columns that appears, 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 choose 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 gateway (in the Check Point 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 should use only HTTP or FTP or both, the rule will ignore any source or destination that is not recognized by IP address.

If the rule uses all supported protocols, HTTP and FTP will recognize only source and destinations that can be defined by IP address. SMTP will recognize 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 than 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**.
The **New TCP** window opens.
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 Policy**.

Advanced Configuration and Troubleshooting

The following sections explain how to maintain the DLP gateway and captured files.

In This Appendix

Configuring User Access to an Integrated DLP Gateway	152
Internal Firewall Policy for a Dedicated DLP Gateway	153
Advanced Expiration Handling	154
Advanced SMTP Quotas	155
Advanced FTP and HTTP Quotas	156
Advanced User Notifications	156
Troubleshooting: Incidents Do Not Expire	157
Troubleshooting: Mail Server Full	157
Gateway Cleanup of Expired Data	158
Gateway Cleanup of All Captured Data	158
Customizing DLP User-Related Notifications	160
Supporting LDAP Servers with UTF-8 Records	162
Editing Extreme Condition Values	162
Editing Exchange Security Agent Values	164
Configuring HTTP Inspection on All Ports	166
Defining New File Types	166
Server Certificates	184

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 the DLP gateway is deployed 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 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** - Select this option to let users access the DLP gateway through connections made from VPN encrypted interfaces.
- **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 Firewall Policy which is explicitly defined by the administrator in the Firewall tab of 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 a DLP Ask User incident will be held in the DLP gateway until the user decides whether it should be sent or discarded.

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 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 remaining 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) that when exceeded, older emails are deleted, 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), 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 **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 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 decide which DLP automatic actions fire notifications in GuiDBedit. **GuiDBedit**, also known as the Check Point Database Tool, enables you to change Check Point configuration files in a GUI.

To activate or de-activate user notifications of DLP deletion:

1. Open GuiDBedit:
 - a) On the SmartConsole computer, run
`C:\Program Files\CheckPoint\SmartConsole\R80.10\PROGRAM\GuiDBedit.exe`
 - b) Log in with your SmartConsole credentials.
2. Open **Table > Other > dlp_data_tbl**
3. Open **dlp_general_settings_object**
This parameter determines the types of emails that are to be sent for exceeding quotas and for expiration of incidents.

4. Set the value of the **active** field for the email notifications that you want.
5. Save the changes and install the policy.

Troubleshooting: 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 will not expire.

3. Save **mail_security_config** and install the policy on the DLP gateway.

Troubleshooting: 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, open 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**), leave `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 **dlp.conf** and 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 `global_quota_active` parameter in **\$FWDIR/conf/mail_security_config** to 0.

Gateway Cleanup of Expired 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 required space on the gateway until the incident is handled or expires.

The DLP gateway automatically cleans itself of expired incident data. Incident data that is held for the `backend:expiration:db` number of days will be deleted.

To change 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 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 gateway is cleaned. Be default, this is 3:45 AM, to ensure that 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 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 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 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 the following syntax:

```
scan [ CHECK_DB | - ] path mask scale age
```

	Description
CHECK_DB or -	Tests files to see if they are in the DLP database, to prevent accidental deletion of UserCheck incident data: <code>scan CHECK_DB</code> To clean up everything, even user captured data, change the flag to a dash (-): <code>scan -</code>
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 <code>dlp_delete_redundant_files_age_group1_files</code>
\$3	group2 age (in minutes): /proc files, value taken from <code>dlp_delete_redundant_files_age_group2_files</code>
\$4	group3 age (in minutes): /tmp/dlp files, value taken from <code>dlp_delete_redundant_files_age_group3_files</code>

Customizing DLP User-Related Notifications

These procedures explain 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.

To customize the DLP notification emails:

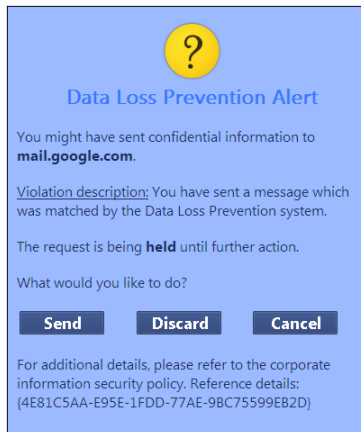
1. On the gateway in **\$DLPPDIR/backend/conf/**, edit these files:

File	Purpose
<code>dictionary_en_us.conf</code>	Basic dictionary
<code>about_to_expire_notification_tmplt_en_us.html</code>	Email notifications
<code>data_owners_mail_notification_tmplt_en_us.html</code>	
<code>detect_mail_notification_tmplt_en_us.html</code>	
<code>expired_owners_mail_tmplt_en_us.html</code>	
<code>expired_sender_mail_tmplt_en_us.html</code>	
<code>failure_mail_notification_en_us.html</code>	
<code>prevent_mail_notification_tmplt_en_us.html</code>	
<code>quarantine_mail_notification_tmplt_en_us.html</code>	
<code>quota_deleted_notification_tmplt_en_us.html</code>	
<code>released_mail_notification_tmplt_en_us.html</code>	

2. **Install Policy** on the DLP gateway.

To customize the UserCheck DLP notifications (Available from R71.10 DLP):

You can customize UserCheck notifications by editing files. For example, to edit the notification in the screenshot, you edit `quarantine_smtp_uc_notification_tmplt_en_us.html`



1. On the gateway in `$DLPDIR/backend/conf`, edit these UserCheck notification files:

File	Purpose
<code>inform_ftp_uc_notification_tmplt_en_us.html</code>	ftp protocol when the action is inform
<code>inform_http_uc_notification_tmplt_en_us.html</code>	http protocol when the action is inform
<code>inform_smtp_uc_notification_tmplt_en_us.html</code>	smtp protocol when the action is inform
<code>prevent_ftp_uc_notification_tmplt_en_us.html</code>	ftp protocol when the action is prevent
<code>prevent_http_uc_notification_tmplt_en_us.html</code>	http protocol when the action is prevent
<code>prevent_smtp_uc_notification_tmplt_en_us.html</code>	smtp protocol when the action is prevent
<code>quarantine_ftp_uc_notification_tmplt_en_us.html</code>	ftp protocol when the action is ask
<code>quarantine_http_uc_notification_tmplt_en_us.html</code>	http protocol when the action is ask
<code>quarantine_smtp_uc_notification_tmplt_en_us.html</code>	smtp protocol when the action is ask

2. **Install Policy** on the DLP gateway.

To customize the DLP Portal:



Note - Never change the key as it may be used in more than one place, and a call for a missing key may result in runtime error. You should only change the textual content. Use these rules:

- Keep only HTML
- Must not contain double quotes, dollar sign or backslash symbols.
- May contain HTML entities.
For example: `"` ; (double quote), `$` ; (dollar sign), `\` ; (backslash)

1. On the gateway, customize the file **\$DLPPDIR/portal/apache/phpincs/conf/L10N/portal_en_US.php**.
2. To apply the changes, run `cpstop` and `cpstart` on the gateway.

To customize notification text in SmartConsole:

1. Open SmartConsole > **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 Policy** on the DLP gateway.



Important - Changes in the files will be lost when you upgrade to the next version. We recommend you maintain a copy of the all changes 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. Open GuiDBedit.
2. On the left, select **Managed Objects > Servers**.
3. For each LDAP Account Unit named `<ldap_au_name>` that stores credentials in UTF-8, change the value of the **SupportUnicode** attribute to `true`.
4. Save the changes.
5. **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.

Default values for **extreme conditions** exist in the GuiDBedit application. With GuiDBedit you can edit the default values for parameters related to **extreme conditions** (see fields below).

To edit Extreme Condition field values:

1. Open GuiDBedit:
 - a) On the SmartConsole computer, run
C:\Program Files\CheckPoint\SmartConsole\R80.10\PROGRAM\GuiDBedit.exe
 - b) Log in with your SmartConsole credentials.
2. In the left pane, select **Table > Other > dlp_data_tbl**.
3. In the right pane, select **dlp_general_settings_object**.
4. In the bottom pane, in the **Field Name** column, find **engine_settings**.
5. 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

Field Name	Description	Default Value
<code>prefer_connectivity_on_heavy_load_protocols > http_inspection</code>	By default, DLP bypasses HTTP traffic on heavy load. If you change this to false, HTTP is inspected on heavy load.	true
<code>prefer_connectivity_on_heavy_load_protocols > smtp_inspection</code>	By default, DLP inspects SMTP traffic on heavy load. If you change this to true, SMTP is bypassed on heavy load.	false

6. You can configure these fields if the **Under all other extreme conditions** checkbox is selected:

Field Name	Description	Default Value
<code>ftp_max_files</code> <code>http_max_files</code> <code>smtp_max_files</code>	The maximum number of files (attachments) in an FTP/HTTP/SMTP message.	100
<code>ftp_max_message_size_in_mega</code> <code>http_max_message_size_in_mega</code> <code>smtp_max_message_size_in_mega</code>	The maximum size in MB of an FTP/HTTP/SMTP message.	150
<code>max_recursion_level</code>	How many recursion levels deep can be done for archived messages.	6

7. Install policy in SmartConsole.



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 ("[Configuring the Exchange Security Agent](#)" on page 37) in the GuiDBedit application.

To edit Exchange Security Agent values:

- Open GuiDBedit:
 - On the SmartConsole computer, run
C:\Program Files\CheckPoint\SmartConsole\R80.10\PROGRAM\GuiDBedit.exe
 - Log in with your SmartConsole credentials.
- In the left pane, select **Table > Other > dlp_data_tbl**.
- In the right pane, select the **Exchange Agent object** that represents the SmartConsole Exchange Security Agent object.

4. In the bottom pane, in the **Field Name** column, you can configure these fields:

Field Name	Description	Default Value
<code>is_tap_mode</code>	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
<code>scan_mails_received_from_sender_out_of_my_organization</code>	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 will only scan messages from your organization's Exchange. To scan messages from senders outside of the domain, change the value to true.	False
<code>scan_mails_send_to_recipient_from_my_organization</code>	If to scan internal traffic.	True
<code>scan_mails_send_to_recipient_out_my_organization</code>	If to scan messages sent outside of the organization.	True
<code>dont_scan_smtp</code>	Scans messages received by the Exchange server in SMTP. This means that messages in SMTP arriving from the same domain will be scanned.	False

5. In the right pane, select **dlp_general_settings_objects** to configure this field:

Field Name	Description	Default Value
<code>exchange_send_status_to_gw_frequency</code>	The time interval that the Exchange Security Agent sends statuses to the Security Gateway.	10
<code>user_dlp_logs_customization_settings > send_log_for_each_skipped_email_with_allow_status</code>	If to send logs about messages that are not sent to the gateway because of the Inspection Scope settings.	False

- 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

- Install policy in SmartConsole.

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:

- In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
The gateway window opens and shows the **General Properties** page.
- From the navigation tree, click **Data Loss Prevention > Protocols**.
- Click **default protocols**.
The **Default Protocols** window opens.
- Click **Enable HTTP inspection on nonstandard ports**.
- Click **OK**.
Note - When you set HTTP inspection on all ports there is a performance impact.
- Close the gateway window and **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:

- Open **GUIDBEdit**:
 - On the SmartConsole computer, run:
C:\Program Files\CheckPoint\SmartConsole\R80.10\PROGRAM\GuiDBEdit.exe
 - Log in with your SmartConsole credentials.
- Under **Other > dlp_data_tbl** create a new object of **file_type** type.
- Name the object **file_type_</D>**. For the full list of IDs see the table below.
- Enter a name for the file type in the **visual_string** field.
- Enter a description for the file type in the **description** field (optional).
- Save the new created object and close **GUIDBEdit**.
- Install Policy**.

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
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
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)
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)

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
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
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
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
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
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
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
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)
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	StuftIt	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
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
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
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)
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)
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
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
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
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
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 communication, gateways must establish trust with endpoint computers by showing a *Server Certificate*. This section discusses the procedures necessary to generate and install server certificates.

Check Point gateways, by default, 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 tries to connect to the gateway with the default certificate, certificate warning messages open in the browser. To prevent these warnings, 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 and Installing a Trusted Server Certificate

To be accepted by an endpoint computer without a warning, 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 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 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 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 gateway command line, log in to expert mode.

2. Run:

```
cpopenssl req -new -out <CSR file> -keyout <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 gateway from the CA, generate a P12 file that has the Signed Certificate and the private key.

1. Get the Signed Certificate for the 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 gateway command line, log in to expert mode.
4. Use the *.crt file to install the certificate with the *.key file that you generated.
 - a) Run:


```
cpopenssl pkcs12 -export -out <output file> -in <signed cert chain file>
-inkey <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

To install the certificate:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
The gateway window opens and shows the **General Properties** page.
2. From 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**

In the **Certificate** section, click **Import** or **Replace**.
3. **Install Policy** on the gateway.
Note - The **Repository of Certificates** on the IPsec VPN page of the gateway object is only for self-signed certificates. It does not affect the certificate installed manually using this procedure.

Viewing the Certificate

To see the new certificate from SmartConsole:

1. In SmartConsole, click **Gateways & Servers** and double-click the Security Gateway.
The gateway window opens and shows the **General Properties** page.
2. From the navigation tree, click **Data Loss Prevention**.
3. In the **Certificate** section, click **View**.

Advanced Options for Data Types

These Data Types have several advanced options you can edit only from GuiDBedit:

- Dictionary
- Keywords
- Weighted Keywords
- Patterns

To open the options for these Data Types:

1. Run: `c:\Program Files\CheckPoint\SmartConsole\R80.10\PROGRAM\GuiDBedit.exe`
2. Connect to the Security Management Server.
3. Go to **Table > Other > dlp_data_tbl** and select the Data Type that you want to change.

In This Appendix

Case Sensitivity.....	186
Ordered Match for Names	187
Proximity of Matched Words	187
Match Multiple Occurrences.....	187
Match Whole Word Only	188

Case Sensitivity

Applies to Data Types:

- **Dictionary**
- **Keywords**
- **Weighted Keywords**
- **Patterns**

By default, DLP finds text strings in uppercase or lowercase. You can choose 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 will 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 will find only "John Smith". By default, DLP will 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 will not trigger an action.

For example, if your dictionary file contains *confidential* and *information* and the proximity check is enabled, DLP will detect messages in which these words are within 3 words of each other. In this example:

The dictionary rule will match the text: This email contains *confidential* company *information*.

The dictionary rule will 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_occurrences` to `false`.
By default, this value is `true` for Patterns.

To record a match for every time a word is used:

- Set `count_occurrences` 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 choose 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 will only match patterns that do not have characters before or after the pattern. In this example:

The Data Type will match the text: confident

The Data Type will 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, will never match as whole word only.

Regular Expressions and Character Sets

In This Appendix

Regular Expression Syntax	189
Supported Character Sets	191

Regular Expression Syntax

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

Metacharacter	Name	Description
\	Backslash	escape metacharacters non-printable characters character types
[]	Square Brackets	character class definition
{ }	Parenthesis	sub-pattern, to use metacharacters on the enclosed string
{min[,max]}	Curly Brackets	min/max quantifier {n} - exactly n occurrences {n,m} - from n to m occurrences {n,} - at least n occurrences
.	Dot	match any character
?	Question Mark	zero or one occurrences (equals {0,1})
*	Asterisk	zero or more occurrences of preceding character
+	Plus Sign	one or more occurrences (equals {1,})
	Vertical Bar	alternative
^	Circumflex	anchor pattern to beginning of buffer (usually a word)
\$	Dollar	anchor pattern to end of buffer (usually a word)
-	hyphen	range in character class

Using Non-Printable Characters

To use non-printable characters in patterns, escape the reserved character set.

Character	Description
\a	alarm; the BEL character (hex 07)
\cx	"control-x", where x is any character
\e	escape (hex 1B)
\f	formfeed (hex 0C)
\n	newline (hex 0A)
\r	carriage return (hex 0D)
\t	tab (hex 09)
\ddd	character with octal code ddd
\xhh	character with hex code hh

Using Character Types

To specify types of characters in patterns, escape 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 scans texts in the UTF-8 Unicode character encoding. It therefore converts the messages and files that it scans from its initial encoding to UTF-8.

Before it can change the encoding of the message or file, the DLP gateway must identify the encoding. The DLP gateway does this using the meta data or the MIME Headers. If none of the two exist, the default gateway encoding is used.

The DLP gateway determines the encoding of the message or file it scans 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. Text files or the body of an email, for example. 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 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 file:
 - R77, R77.10, R77.20 - `$DLPDIR/config/dlp.conf`
 - R77.30 - `$FWDIR/conf/file_convert.conf`
2. In the `engine` section, search for 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 convert the message (or parts of it) to UTF-8. If that is so, the DLP gateway will not fully scan the message.

Character Set Aliases

The character sets that can be used as the default input character set of the DLP gateway are:

Name of Character Set	Alias
UTF-8Encoded 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
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

Name of Character Set	Alias
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
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