Data Loss Prevention

R75.20

Administration Guide

8 December 2011

Classification: [Public]
Important Information

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>8 December 2011</td>
<td>Added procedure for enabling the DLP Portal when configuring the Exchange Security Agent</td>
</tr>
<tr>
<td>13 July 2011</td>
<td>First release of this document</td>
</tr>
</tbody>
</table>

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 R75.20 Administration Guide).
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Important Information</td>
<td>3</td>
</tr>
<tr>
<td>Introduction to Data Loss Prevention</td>
<td>8</td>
</tr>
<tr>
<td>The Need for Data Loss Prevention</td>
<td>8</td>
</tr>
<tr>
<td>DLP and Privacy</td>
<td>8</td>
</tr>
<tr>
<td>The Check Point Solution for DLP</td>
<td>9</td>
</tr>
<tr>
<td>Data Loss Prevention Terminology</td>
<td>10</td>
</tr>
<tr>
<td>How It Works</td>
<td>10</td>
</tr>
<tr>
<td>Integrated DLP Security Gateway Deployment</td>
<td>11</td>
</tr>
<tr>
<td>Dedicated DLP gateway Deployment</td>
<td>12</td>
</tr>
<tr>
<td>Alternative Gateway Deployments</td>
<td>12</td>
</tr>
<tr>
<td>What Happens on Rule Match</td>
<td>13</td>
</tr>
<tr>
<td>Role of DLP Administrator</td>
<td>14</td>
</tr>
<tr>
<td>DLP Administrator Permissions</td>
<td>14</td>
</tr>
<tr>
<td><strong>Installation and Configuration</strong></td>
<td>16</td>
</tr>
<tr>
<td>DLP Supported Platforms</td>
<td>16</td>
</tr>
<tr>
<td>Installing the DLP gateway</td>
<td>17</td>
</tr>
<tr>
<td>DLP Software Blade Trial License</td>
<td>17</td>
</tr>
<tr>
<td>Configuring a DLP Gateway or Security Cluster</td>
<td>17</td>
</tr>
<tr>
<td>Integrated Deployments</td>
<td>17</td>
</tr>
<tr>
<td>Dedicated Deployments</td>
<td>18</td>
</tr>
<tr>
<td>DLP-1 Security Cluster Wizard</td>
<td>19</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>19</td>
</tr>
<tr>
<td>Configuring a Locally Managed DLP-1 Security Cluster</td>
<td>20</td>
</tr>
<tr>
<td>Data Loss Prevention Wizard</td>
<td>20</td>
</tr>
<tr>
<td>DLP Blade Wizard Options</td>
<td>20</td>
</tr>
<tr>
<td>Completing the Wizard</td>
<td>20</td>
</tr>
<tr>
<td>Configuring a Dedicated DLP Gateway in Bridge Mode</td>
<td>20</td>
</tr>
<tr>
<td>Required Routing in Bridge Mode</td>
<td>21</td>
</tr>
<tr>
<td>Configuring Bridge IP Address</td>
<td>21</td>
</tr>
<tr>
<td>Required VLAN Trunk Interfaces</td>
<td>21</td>
</tr>
<tr>
<td>Configuring Active Directory and LDAP for DLP</td>
<td>21</td>
</tr>
<tr>
<td>Rerunning the Data Loss Prevention Wizard</td>
<td>22</td>
</tr>
<tr>
<td>Configuring a DLP Gateway for a Web Proxy</td>
<td>23</td>
</tr>
<tr>
<td>Configuring for a Web Proxy</td>
<td>23</td>
</tr>
<tr>
<td>Configuring for an Internal Web Proxy</td>
<td>24</td>
</tr>
<tr>
<td>Configuring Proxy Settings After Management Upgrade</td>
<td>24</td>
</tr>
<tr>
<td>Mail Relay Required Configuration</td>
<td>25</td>
</tr>
<tr>
<td>Configuring the Mail Relay</td>
<td>25</td>
</tr>
<tr>
<td>Configuring a Dedicated DLP gateway and Relay on DMZ</td>
<td>26</td>
</tr>
<tr>
<td>Recommended Deployments of a DLP Gateway with a Mail Relay</td>
<td>27</td>
</tr>
<tr>
<td>Workarounds for a Non-Recommended Mail Relay</td>
<td>27</td>
</tr>
<tr>
<td>TLS-Encrypted SMTP Connections</td>
<td>29</td>
</tr>
<tr>
<td>UserCheck Client</td>
<td>30</td>
</tr>
<tr>
<td>Server Discovery and Trust</td>
<td>31</td>
</tr>
<tr>
<td>Server Discovery and Trust Options</td>
<td>32</td>
</tr>
<tr>
<td>Option Comparison</td>
<td>32</td>
</tr>
<tr>
<td>Renaming the MSI</td>
<td>37</td>
</tr>
<tr>
<td>Setting CPMSI_TOOL Parameters</td>
<td>37</td>
</tr>
<tr>
<td>Installing, Connecting, Verifying Clients</td>
<td>38</td>
</tr>
<tr>
<td>Upgrading UserCheck Client</td>
<td>39</td>
</tr>
<tr>
<td>Providing Assistance</td>
<td>40</td>
</tr>
<tr>
<td>Configuring Incident Log Handling</td>
<td>40</td>
</tr>
</tbody>
</table>
Regular Expressions .......................................................... 137
Metacharacters ............................................................... 137
Square Brackets .............................................................. 138
Parentheses ................................................................. 138
Hyphen ................................................................. 138
Dot ................................................................. 138
Vertical Bar ............................................................ 138
Backslash ............................................................. 138
Escaping Symbols ..................................................... 138
Encoding Non-Printable Characters ......................... 139
Specifying Character Types ...................................... 139
Quantifiers ............................................................... 139
Curly Brackets .......................................................... 140
Question Marks .......................................................... 140
Asterisk ................................................................. 140
Plus ................................................................. 140
Supported Character Sets ........................................... 141
Character Set Aliases .................................................. 142
Index ................................................................. 145
Chapter 1

Introduction to Data Loss Prevention

In This Chapter

The Need for Data Loss Prevention 8
DLP and Privacy 8
The Check Point Solution for DLP 9
Role of DLP Administrator 14

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. We recommend that you 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.

5. Explain that captured transmissions will be logged and saved, and that some may be reported to managers (Data Owners).

6. Explain that captured emails, attachments, web posts, etc. will be available for review by security personnel.

7. 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.

8. 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.


### 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 SmartDashboard, 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 strong monitoring tools - Check Point SmartEvent.

### Data Loss Prevention Terminology

In this Administration Guide, **DLP gateway** means a Check Point Security Gateway with the Data Loss Prevention Software Blade enabled.

The DLP gateway can be deployed as a:

- **Integrated Security Gateway**: The Data Loss Prevention Software Blade is enabled on a Security Gateway, making it the DLP gateway. The firewall Software Blade, and optionally, other Network Security Software Blades, are also enabled on the gateway.

- **Dedicated Security Gateway**: The Data Loss Prevention Software Blade is enabled on a gateway, making it the DLP gateway. No other Network Security Software Blade is enabled.

### How It Works

1. The Data Loss Prevention Software Blade is enabled on a Security Gateway (1) (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 SmartDashboard and the Security Management Server (3) to install the DLP Policy on the DLP gateway.

3. The DLP gateway (1) 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. SmartView Tracker and SmartEvent (7) provide 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 an R75 or higher SecurePlatform 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 (1) (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 (2).

When setting up a dedicated DLP gateway (1), Check Point recommends that you 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 that is defined and managed by a Security Management Server on a different machine.

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.

**Figure 1-1** DLP Gateway Protecting Data Between Departments

You could put the DLP gateway between the users and the switch, to directly protect a subnet.

**Figure 1-2** DLP Gateway Protecting 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 the Domain Log Server or Security Management Server that stores DLP logs.
   - The DLP gateway logs an incident with SmartView Tracker and with SmartEvent.
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.
Role of DLP Administrator

DLP provides various auditing tools: automatic notifications to data owners when transmission of protected data has been attempted; user notifications and self-handling portal; tracking and logging with SmartView Tracker; event details, charts, graphs, filtered lists from SmartEvent; and reports from SmartReporter.

Before you begin auditing, set up your DLP policy and develop it for your needs. This is done first through the Data Types.

Data Type - A representation of data assets that you want to protect, provides building blocks of the DLP policy. Data Types can be combined for complex and flexible data recognition and preventative DLP.

The process of creating and refining 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 in SmartView Tracker. 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 SmartView Tracker provides and make sure the DLP policy works smoothly and prevents transmission of protected data.

DLP Administrator Permissions

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 SmartView Tracker.
- See the captured data (the actual email, FTP files and HTTP posts).
- Send or discard quarantined user emails from SmartView Tracker.

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/discard quarantined emails.
To configure full permissions:
1. From the Manage menu, select Users and Administrators.
2. Select the administrator account or click New > Administrator to create a new administrator user account.
   The Administrator Properties window opens, displaying General Properties.
3. Click New next to the Permissions Profile field.
   The Permissions Profile Properties window opens.
4. Make sure Read/Write All is selected.
5. Select Read DLP logs including confidential fields and incidents.
6. Click OK.

To configure a subset of permissions:
1. From the Manage menu, select Users and Administrators.
2. Select the administrator account or click New > Administrator to create a new administrator user account.
   The Administrator Properties window opens, displaying General Properties.
3. Click New next to the Permissions Profile field.
   The Permissions Profile Properties window opens.
4. Select Customized and click Edit.
   The Administrator Permission Configuration window opens.
5. Select Monitoring and Logging.
6. Select the permission(s) to give:
   - DLP Logs including confidential fields - Permissions to view all fields of DLP logs in SmartView Tracker. 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 SmartView Tracker and SmartReporter. With this permission, administrators can also release (send) or discard quarantined emails from within SmartView Tracker.
     Note - If you select both checkboxes, you are giving full DLP permissions.
7. Click OK.
Chapter 2

Installation and Configuration

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

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 R75.20 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=12414).

In This Chapter

- DLP Supported Platforms 16
- Installing the DLP gateway 16
- DLP Software Blade Trial License 16
- Configuring a DLP Gateway or Security Cluster 17
- DLP-1 Security Cluster Wizard 19
- Data Loss Prevention Wizard 20
- Configuring a Dedicated DLP Gateway in Bridge Mode 20
- Configuring Active Directory and LDAP for DLP 21
- Configuring a DLP Gateway for a Web Proxy 22
- Mail Relay Required Configuration 24
- UserCheck Client 30
- Configuring Incident Log Handling 40
- Configuring the Exchange Security Agent 41
- HTTPS Inspection 46

DLP Supported Platforms

Before installing or configuring your DLP gateway, make sure that it agrees with the platform requirements for your deployment in the R75.20 Release Notes (http://supportcontent.checkpoint.com/documentation_download?ID=12414).

Installing the DLP gateway

For instructions on how to install and do the initial configuration of the DLP gateway, refer to the R75.20 Installation and Upgrade Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12269).
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 SmartDashboard, in the gateway object.
2. Install the 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. 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 only use the Detect action ("Rule Actions" on page 65). Other DLP actions are 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.

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 SmartDashboard.
2. Edit the Security Gateway or Security Cluster object.
3. For a Security Cluster:
   - In the ClusterXL page, select High Availability New mode or Load Sharing. Note that you can use Load Sharing if the DLP rules only use the Detect action.
4. In the General Properties page, in the Software Blades area, enable 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.

5. Complete the Data Loss Prevention Wizard (on page 20).

To configure a new DLP gateway or Security Cluster:

1. Open SmartDashboard.
2. To configure a Security Gateway:
   a) Open the General Properties page of the gateway.
   b) For a new gateway object only: Click Communication and initialize SIC.
3. To configure a Security Cluster:
   a) Edit the Security Cluster object
   b) Configure the Security Cluster.
   c) In the ClusterXL page, select High Availability New mode or Load Sharing. Note that you can use Load Sharing if the DLP rules only use the Detect action.
4. In the General Properties page, in the Platform area, select the Hardware, Version and OS. Make sure the selections comply with the platform requirements for your deployment in the R75.20 Release Notes.
5. In the Software Blades area, enable 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.


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.

3. Confirm your selection.

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

1. Open SmartDashboard.
   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 20) or DLP-1 Cluster Wizard ("DLP-1 Security Cluster Wizard" on page 19).

To configure a dedicated DLP gateway or cluster on a centrally managed DLP-1 appliance:
1. Open SmartDashboard on the Security Management Server that manages the DLP-1 appliance.
2. Create a new DLP-1 Security Gateway or Security Cluster object from Network Objects > Check Point > DLP-1 > Gateway or 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 SmartDashboard 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 SmartDashboard 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.

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 21).

- **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 that are used to identify your organization.

- **Protocols** - Select protocols to which the DLP policy applies.

Completing the Wizard

After completing the wizard, do these steps for a DLP gateway of any platform.

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 SmartDashboard.
3. Do **Install Policy** on the DLP gateway only:
   a) From the menu of SmartDashboard, click **Policy** and select **Install**.
   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 Dedicated DLP Gateway in Bridge Mode

When setting 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.

• 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.

• If the DLP gateway in bridge mode is behind a cluster, the cluster must be in HA mode.

• If the bridge interface is connected to a VLAN trunk, all VLANs will be scanned by DLP. You cannot exclude specific VLANs.

• 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.

### 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 using Active Directory credentials
- Authenticate to UserCheck using 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 will ask for your Active Directory credentials to create the LDAP account unit automatically. Otherwise, you can
run the wizard again later from a computer in the Active Directory domain to create the LDAP account unit. (*"Rerunning the Data Loss Prevention Wizard" on page 22)

**To configure DLP to use Active Directory LDAP:**

1. Create the DLP gateway object in SmartDashboard from a computer that is a member of the Active Directory domain.
2. Enter your Active Directory credentials in the Active Directory page.
   You are not required to enter credentials with administrator privileges. We recommend that you 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.

   **Note** - The DLP Wizard will ask for Active Directory credentials only if no LDAP account unit exists.
   If you already have an LDAP account unit, the wizard will 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.

If you need more LDAP account units, you can create the LDAP account unit manually. To do this, refer to the R75.20 Security Management Administration Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12277).

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

---

**Rerunning the Data Loss Prevention Wizard**

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

**To run the Data Loss Prevention Wizard again:**

1. Open SmartDashboard.
2. Edit the DLP gateway object.
3. In the **General Properties page**, deselect the **Data Loss Prevention** Software Blade.
4. 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 ("HTTPS Inspection" on page 46).

Configuring for a Web Proxy

Use these procedures if the proxy or proxies are between the DLP gateway and the Internet, or in a DMZ. If a proxy is in a DMZ, we recommend that you use the DLP gateway to scan the HTTP traffic between the user network and the proxy in the DMZ.

**Configuring an R75 or higher DLP Gateway for Web Proxies**

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

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

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

**Procedure 1**

1. In SmartDashboard, edit the DLP gateway object and then open the Data Loss Prevention > Protocols page.
2. Select HTTP. Either for the gateway, or on the default protocols.
3. Select Use Proxy.
4. In the Host IP field, enter the IP address of the Web proxy server.
5. In the Port field, enter the listening port of the Web proxy server.
6. Click OK.

DLP only scans traffic to the specified web proxy.

**Procedure 2**

1. In SmartDashboard, go to the Objects Tree and select the Services tab
2. Edit the TCP service: HTTP_and_HTTPS_proxy
3. Click Advanced.
4. Select Protocol Type, and choose HTTP.
5. Click OK.
6. In the DLP gateway object, select the Data Loss Prevention > Protocols page
7. Select HTTP. Either for the gateway, or on the default protocols.
8. Make sure that Use Proxy is not selected.
9. Click OK.

**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 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 SmartDashboard, edit the DLP gateway object and open the Data Loss Prevention > Protocols page.
2. Select HTTP. Either for the gateway, or on the default protocols.
3. Click OK.
4. In the Data Loss Prevention tab, open the My Organization page.
5. In the Networks section, make sure that the Web Proxy and the user networks are included in My Organization.

Configuring the Proxy Server to Allow UserCheck Notifications

If the DLP gateway is between the Web proxy server or servers and the Internet, all packets through the DLP gateway have the source IP address of the proxy server. Therefore, the DLP gateway cannot know the real IP address of the client that opens the original connection to the proxy server. This means that the DLP gateway cannot identify the user, and therefore cannot:

- Send UserCheck client notifications to users about incidents.
- Log the source IP address of the user.

To make it possible for the DLP gateway to identify the user, you must configure the proxy server to reveal the IP address of the client. The proxy server does this by adding the x-forwarded-for header to the HTTP header. For details, see the proxy server vendor documentation.

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 R75 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 SmartDashboard computer, run:
   C:\Program Files\CheckPoint\SmartConsole\R75\PROGRAM\GuiDBEdit.exe
2. Log in with your SmartDashboard 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 Relay Required Configuration

DLP rules have different action settings.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect</td>
<td>The data transmission event is logged in SmartView Tracker. Administrators with permission can view the data that was sent. The traffic is passed.</td>
</tr>
<tr>
<td>Inform User</td>
<td>The transmission is passed, but the incident is logged and the user is notified.</td>
</tr>
<tr>
<td>Ask User</td>
<td>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 <strong>User Actions</strong> category in SmartView Tracker. Administrators that have full permissions or the View/Release/Discard DLP messages permission can also decide if to send or discard the message.</td>
</tr>
<tr>
<td>Prevent</td>
<td>The data transmission is blocked.</td>
</tr>
</tbody>
</table>

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.

In addition, 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

#### Configuring the Mail Relay for Anonymous SMTP Connections

1. In SmartDashboard:
   - Configure the mail server without authentication in the Data Loss Prevention Wizard. Alternatively:
     a) In the **Data Loss Prevention** tab, expand **Additional Settings** and click **Mail Relay**.
     b) Select **Send emails using this mail relay**.
     c) Select the mail relay. If the mail relay object does not exist, create it.

2. On your mail relay server:
   - 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 the Mail Relay for Authenticated SMTP Connections

1. In SmartDashboard:
   - Configure the mail server with authentication in the Data Loss Prevention Wizard. Alternatively:
     a) In the **Data Loss Prevention** tab, expand **Additional Settings** and click **Mail Relay**.
     b) Select **Send emails using this mail relay**.
     c) Select the mail relay. If the mail relay object does not exist, create it.
     d) Select **Authentication**.
     e) Enter the authentication credentials.
2. On your mail relay server:
   Configure the mail relay to accept authenticated connections from the DLP gateway. For details, consult the vendor documentation. For example, on Microsoft Exchange Servers, configure the default receive connector (or other relevant connector that handles SMTP traffic) for basic authentication.

### Configuring a Dedicated DLP gateway and Relay on DMZ

A specific configuration is required for a dedicated DLP gateway if these are all true:

- The DLP gateway and the mail relay that handles SMTP traffic leaving the organization are in the DMZ zone.
- Use of this mail relay is one of the following:
  - There is a mail server inside the internal network, such as Exchange, that relays its outgoing SMTP traffic through the mail relay.
  - Users email clients are configured to work directly with the mail relay.
- The DLP Policy works only on SMTP.

If this is true, configure the DLP gateway to recognize the mail server as internal to My Organization and the relay in the DMZ as external.

**To configure the DLP and Relay in the DMZ:**

1. Open the Data Loss Prevention tab in SmartDashboard.
2. Open My Organization.
3. In the Networks area, select These networks and hosts only and click Edit.
   The Networks and Hosts window opens.
4. Click Add.
   If the Internal Mail Server is already defined as a Check Point network object, select it from the list. Otherwise, click New and define it as a Host.
5. Click OK.
6. Repeat steps to add other Internal Mail Servers.
7. If users email clients are configured to work directly with the mail relay that is located in the DMZ using SMTP, add their networks. Select user networks from the list (or click New to define these networks) and then click OK.
8. Do Install Policy on the DLP gateway.
Recommended Deployments of a DLP Gateway with a Mail Relay

In the recommended deployment of a DLP gateway with a mail relay, the DLP gateway scans mails once, as they are sent from an internal mail server (such as Microsoft Exchange) (1) to a mail relay in the DMZ (2). Make sure that the DLP gateway does not scan mails as they pass from the mail relay to the target mail server in the Internet.

If you can deploy the internal mail relay behind a DMZ interface of the DLP gateway:

1. Ensure that mails from the internal mail server (e.g. Microsoft Exchange) (1) arrive at the gateway via an internal Gateway interface:
   - In the Topology page of the DLP gateway object, define the gateway interface that leads to the internal mail server as Internal.
2. 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.
3. 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

If you cannot deploy the internal mail relay behind a DMZ interface of the DLP gateway:

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 the Networks section of the My Organization page, select These networks and hosts only.
2. Select the networks that include the internal mail server, but not including the relay server.

Workarounds for a Non-Recommended Mail Relay Deployment

A non-recommended deployment is to have the DLP gateway scan mails 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 as McAfee IronMail, postfix 2.0 or earlier, and qmail) will not try the next DNS MX record, and so will not try to resend the mail to another SMTP mail server in the same domain.
- The internal mail server (1) and the internal relay (2) are in My Organization

- The internal mail server (1)(2) 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 mail.

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 mail 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 26).

- If you cannot apply these workarounds, see sk58960 (http://supportcontent.checkpoint.com/solutions?id=sk58960).

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 41) to inspect them.
UserCheck Client

Notifications to users 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).

Figure 2-3 UserCheck Example

![UserCheck Example](image)

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 to handle the incident in real-time.

**Note** - Administrators with full permissions or the View/Release/Discard DLP messages permission can also send or discard incidents from SmartView Tracker.

**Important** - Make your users 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.

Use the **Check_Point_UserCheck.MSI** file to install the client on user machines. Each UserCheck client must be configured to connect to the DLP gateway and to use the port needed for notifications (default is 443).

**Important** - The UserCheck client is not compatible with Abra or Secure Workspace.

If a UserCheck client is installed on a machine and a DLP violation occurs, the UserCheck client notification shows outside the Abra or Secure Workspace environment. We recommend that you not install the UserCheck Client on a machine that usually runs the Abra or Secure Workspace environment.

The UserCheck client must connect to a DLP gateway. For this to happen, it must discover the server and trust it.
Server Discovery and Trust

Server discovery refers to the process of deciding which server the client should connect to. We offer several methods for configuring server discovery – from a very basic method of simply configuring one server to a method of deploying a domain wide policy of connecting to a server based on your current location. This section describes these options.

Server trust refers to the process of validating that the server the end user connects to is indeed a genuine one. It also makes sure that communication between the client and the server was not tampered with by a Man In The Middle (MITM) attack.

The trust process compares the server fingerprint calculated during the SSL handshake with the expected fingerprint. If the client does not have the expected fingerprint configured, it will ask the user to verify that it is correct manually. This section describes the methods that allow the expected fingerprint to be known, without user intervention.
Server Discovery and Trust Options

These are the options that the client has for discovering a server and trusting it:

- **File name based server configuration** – If no other method is configured (default, out-of-the-box situation), any UserCheck client downloaded from the portal will be renamed to have the portal machine IP in it. During installation, the client uses this IP to represent the DLP gateway. Note that the user has to manually trust the server (the trust dialog box opens).

- **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** – It is possible to configure the server addresses in the DNS server. Note that as DNS isn’t secure, the trust data cannot be configured in that way and the user will have to authorize it manually in a trust dialog box that opens.

- **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 from first run.

### Option Comparison

<table>
<thead>
<tr>
<th></th>
<th>Requires AD</th>
<th>Manual User Trust Required?</th>
<th>Multi-Site</th>
<th>Client Remains Signed?</th>
<th>Allows Ongoing Changes</th>
<th>Level</th>
<th>Recommended for...</th>
</tr>
</thead>
<tbody>
<tr>
<td>File name based</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Very Simple</td>
<td>Single gateway deployments</td>
</tr>
<tr>
<td>AD based</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Simple</td>
<td>Deployments with AD that you can modify</td>
</tr>
<tr>
<td>DNS based</td>
<td>No</td>
<td>Yes</td>
<td>Partially (per DNS server)</td>
<td>Yes</td>
<td>Yes</td>
<td>Simple</td>
<td>Deployments without AD or with an AD you cannot modify, but the DNS can be changed</td>
</tr>
<tr>
<td>Remote registry</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Moderate</td>
<td>Where remote registry is used for other purposes</td>
</tr>
</tbody>
</table>

**File Name Based Server Discovery**

This option is the easiest to deploy, and works out-of-the-box. If your deployment consists of one DLP gateway and it is OK with you that the user must verify the server fingerprint and trust it once, you can use this option, which works with no configuration.
How does it work?

When a user downloads the UserCheck client from the DLP Portal, the address of the DLP gateway is embedded into the file name. During the installation sequence, the client checks if there is any other discovery method configured (AD based, DNS based or local registry). If no method is configured and the server can be reached, it will be used as the DLP gateway. You can make sure that this is the case by looking at the client settings and seeing that the server that is shown in the file name is present in the UserCheck dialog box.

Why can't we use this for trust data?

As the file name can be changed, we cannot be sure that the file name wasn't modified by an attacker along the way. Therefore, we cannot trust data passed in the file name as authentic, and we need to verify the trust data by another means.

AD 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 consists of three windows:

- Welcome - This window describes the tool and lets you to enter alternate credentials that are used to access the AD.
- Server configuration – This window lets you configure which DLP gateway the client should use, depending on its source location.
- Trusted gateways – This window lets you view and change the list of fingerprints that the DLP gateways consider secure.

To enable use of Active Directory to configure the client:

1. From a command line, run the client configuration tool with the AD utility:
   ```
   C:\Documents and Settings\<user name>\Local Settings\Application Data\Checkpoint\UserCheck\UserCheck.exe -adtool
   ```
2. In the Welcome page, enter the credentials of an Active Directory 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 for the DLP gateway.
6. Click OK.
   The identity of the gateway, as a server for the UserCheck client, is written in the Active Directory and given
to all clients.

**Server Configuration Rules**

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

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

For example:

This configuration 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 isn’t
   available, try BAK-GS2 (it will be used only if US-GW1 is not available, as its priority is higher).
2. Otherwise, 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. Otherwise, connect to BAK-GS2 (the default rule is always matched when it is encountered).

**Trusted Gateways**
The trusted gateways window shows the list of servers considered trusted – no popups will open when
trying to 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 by entering its address and clicking ‘Fetch Fingerprint’. Otherwise, you should enter the same name and fingerprint that is shown when connecting to that server.

**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 won’t have any affect on other AD based applications or features.

**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 ‘CHECKPOINT_DLP._tcp’ (the DNS suffix is added automatically). You can configure the address in your DNS server.

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 address of the DLP gateway.
9. Click **OK**.

**Note** - DLP gateway load sharing can be achieved by creating several SRV records with the same priority and High Availability can be achieved by creating several 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 - Displaying SRV Record Stored in the DNS Server

Run the following commands:

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
   srv hostname = dlpserver.company.com

dlpserver.company.com internet address = 192.168.1.212
>

Remote Registry

If you have another way to deploy registry entries to your client computers (i.e. Active Directory GPO updates), you can deploy the DLP gateway addresses and trust parameters before installing the clients. That way, they will use the already deployed settings immediately after installation.
To use the remote registry option:
1. Install the client on one of your computers. The agent installs itself to the users 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 it manually to connect to the requested servers (use the settings dialog box).
4. Export the following registry keys (from HKEY_CURRENT_USER):
   a) SOFTWARE\CheckPoint\UserCheck\TrustedGateways (the entire tree)
   b) SOFTWARE\CheckPoint\UserCheck
      (i) DefaultGateway
      (ii) DefaultGatewayEnabled
5. Deploy the exported keys to the workstations before installing the client on your workstations.

Renaming the MSI

You can rename the MSI file so that its connection to the DLP gateway is given automatically.

To rename the MSI file:
1. Make sure the DLP gateway has a DNS name.
2. Rename the MSI using this syntax: UserCheck_~dlpGWname.msi
   Where dlpGWname - is the DNS name of the DLP gateway.
   Optionally, you can use UserCheck_~dlpGWname-port.msi
   Where port is the port number of notifications.

Example:
UserCheck_~mydlpgw-18300.msi

Notes - You can use any prefix name; it does not have to be "UserCheck". The important part of the syntax is underscore tilde (_~), which indicate that the following 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 following string is the port number.

Setting CPMSI_TOOL Parameters

You can configure the parameters of the MSI client using the CPMSI_TOOL utility and its ini file.

Note - If you do not have ..\DLPClient\cpmsi_tool.exe in the Check Point DVD, consult with your vendor.

To configure the UserCheck parameters with the CPMSI_TOOL utility:
1. Open ..\DLPClient\params.ini in a text editor.
2. Change the value of DlpRegDefaultGateway to the DNS name (recommended) or the IP address of the DLP gateway.
3. Save and close params.ini.
4. Run the utility with this syntax:
cpmsi_tool.exe Check_Point_dlp_client.msi readini params.ini
   If you have multiple DLP gateways, you can save the different configurations as different ini files, and call each ini file in a different execution. For example:
cpmsi_tool.exe Check_Point_dlp_client_n.msi readini params_n.ini
Installing, Connecting, Verifying Clients

After configuring the clients to connect to the DLP 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 your users an email with a link to install the client. When the user clicks the link, the MSI installs the client on the computer.

Alternatively, users can download the installation package from the regular notification emails.

**To enable users to download UserCheck from notifications:**
1. Open SmartDashboard > DLP gateway properties.
2. Open the Data Loss Prevention page.
3. Select the UserCheck options.

Check Point UserCheck installations are silent and generally, no reboot is required.

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

The first time that the client connects to the DLP gateway, it asks for verification from the user that it should be connecting to the DLP gateway and approval of the footprint.

**Figure 2-4** UserCheck First Contact

![UserCheck First Contact](image)

It is recommended that you let the users know this will happen and suggest that they perform the following procedure.

**Example of message to users on UserCheck install:**

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 a message to let you know that a message or post you asked to be sent has protected data; and it may enable 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 UserCheck is not connected to the gateway, the behavior is as if the client were never installed. Email notifications will be sent for SMTP incidents and the Portal will be used for HTTP incidents.
Using UserCheck with Check Point Password Authentication

By default, a UserCheck client always authenticates with the credentials of the user that is currently logged in to the AD Domain. Authenticating with another domain user is not supported. You can configure the UserCheck client to be able to authenticate with a user account that was manually defined by the administrator in SmartDashboard. You can see and edit those users in the Data Loss Prevention tab, Additional Settings > Users page.

To configure the UserCheck client to be able to authenticate with a user account that was manually defined by the administrator in SmartDashboard:

SmartDashboard Configuration
1. Open SmartDashboard.
2. For each user, edit the user object. You can do this in the Data Loss Prevention tab in the Additional Settings > Users page.
3. In the General Properties page of the User, make sure that an email address is defined.

UserCheck Client Configuration
Ask your users to:
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. Enable Allow authentication with alternate user account.

Upgrading UserCheck Client
You can upgrade the UserCheck client installation package without affecting any other component.

To upgrade the UserCheck installation package:
1. On the DLP gateway, replace the $DLPDIR/thin_client_pkg/Check_Point_UserCheck.msi file with the new file.
   The new package filename must be identical to the previous file.
2. Delete all the files under $DLPDIR/portal/apache/htdocs/SecureRepository/client that start with Check_Point_UserCheck.

For example:
If you put the new package on the gateway at /home/admin/new_package.msi, run these commands:

```bash
cd $DLPDIR/thin_client_pkg
cp Check_Point_UserCheck.msi Check_Point_UserCheck.msi.old
cp /home/admin/new_package.msi ./Check_Point_UserCheck.msi
rm -rf $DLPDIR/portal/apache/htdocs/SecureRepository/client/Check_Point_UserCheck*
```
Providing Assistance

If your users need troubleshooting assistance with the UserCheck client, you can ask them to send you the logs.

**To log UserCheck actions:**
1. Right-click the UserCheck tray icon and select **Settings**.
   The **Settings** window opens.
2. Click **Log to** and browse to a pathname for the logs to be made.
3. Click **OK**.

**To send UserCheck logs:**
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.

Configuring Incident Log Handling

In version R75 and higher, DLP incident data is stored on the remote Domain Log Server or Security Management Server that stores the DLP gateway logs. DLP incidents are only stored permanently (that is, until they expire) on the DLP gateway if no Domain Log Server or Security Management Server is configured for the DLP gateway.

**Incidents are stored at $FWDIR\log\blob.**

Because DLP incident data is stored on the Domain Log Server, Check Point recommends that you tune your Domain Log Server disk management setting for DLP incidents.

**To configure disk management for DLP incidents:**
1. In SmartDashboard, edit the Domain Log Server or Security Management Server that manages DLP logs.
2. In the **Logs and Masters** page, select **Required Free Disk Space** and enter a value.
   This setting applies to DLP incidents and logs, and to all other logs. The default setting is 45 MBytes or 15%. 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.
3. Open GuiDBedit:
   a) On the SmartDashboard computer, run
      
      ```
      C:\Program Files\CheckPoint\SmartConsole\R75.20\PROGRAM\GuiDBEdit.exe
      ```
   b) Log in with your SmartDashboard credentials.
4. In the left pane, select **Table > Network Objects > network_objects**.
5. In the right pane, select the Domain Log Server or Security Management Server that manages DLP logs.
6. In the bottom pane, in the **Field Name** column, find **log_policy**.
7. Configure these fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dlp_blob_delete_above_value_percentage</td>
<td>The maximum % of disk space that incidents are allowed to occupy.</td>
<td>20%</td>
</tr>
<tr>
<td>dlp_blob_delete_on_above</td>
<td>Whether or not to delete incidents if the incidents take up more disk space than dlp_blob_delete_above_value_percentage</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• true — Delete incidents. However, logs that are associated with the incidents are not deleted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• false — Do not delete incidents. Incidents are only deleted if free disk space becomes less than the Required Free Disk Space that is configured in SmartDashboard, in the Logs and Masters page of the Domain Log Server or Security Management Server that manages DLP logs.</td>
<td></td>
</tr>
<tr>
<td>dlp_blob_delete_on_run_script</td>
<td>Whether or not to run a script before deleting incidents. For example, to copy the logs to a different computer before they are deleted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• true — Run the script that is defined in SmartDashboard, in the Domain Log Server or Security Management Server that manages DLP logs, in the Logs and Masters &gt; Advanced page.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• false — Do not run a script.</td>
<td>false</td>
</tr>
</tbody>
</table>

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 SmartDashboard 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 SmartDashboard 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 80).
SmartDashboard Configuration

SmartDashboard configuration includes:

- Defining the Exchange Security Agent object in SmartDashboard.
- Using a wizard to:
  - Set a one-time password that will be used to initiate trusted communication between the DLP gateway and the Exchange Security Agent
  - Set the users/groups for which to send emails.
- Enable the DLP Portal (Required for the Exchange Agent).
- Preparing and installing the securing policy.

**To define the Exchange Security Agent:**

1. In SmartDashboard, open the Data Loss Prevention tab.
2. Click **Gateways**.
3. Click **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

**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 SmartDashboard 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.

Click Next.

**Exchange Security Agent - Configuration Summary**

The Exchange Agent Wizard is Completed window opens. Click Finish.

**Enable the DLP Portal:**
1. Open Data Loss Prevention > Gateways.
2. Double-click the DLP gateway related to the Exchange Agent and click Edit.
3. In the Check Point Gateways, click Data Loss Prevention.
4. In the DLP Portal section, select Activate DLP Portal for Self Incident Handling.
5. Click OK.

The next steps include:
- Installing the policy on the DLP gateway.
- Downloading, installing and configuring the Exchange Security Agent on the Exchange server.

**Exchange Server Configuration**

After the Exchange Security Agent has been installed on the Exchange server, you must:
- 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 SmartDashboard.
- **Exchange agent object name** - The same name that is set for the Exchange agent object in SmartDashboard.

- **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 SmartDashboard.

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 42).

**To start the Exchange Security Agent:**

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

**Statistics**


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.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive</td>
<td>Empty - indicates that the message is being handled by the Exchange Security Agent</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Scanned by gateway</td>
</tr>
<tr>
<td></td>
<td>Timeout</td>
</tr>
<tr>
<td>Drop</td>
<td>Dropped by gateway - after Security Gateway inspection the message matched an ask or prevent rule</td>
</tr>
<tr>
<td>Bypass</td>
<td>DLP scanning is disabled - when DLP inspection is not enabled on the Security Gateway</td>
</tr>
<tr>
<td></td>
<td>Fail open active - if one of the bypass settings in the Advanced window is matched</td>
</tr>
<tr>
<td></td>
<td>Message is too big</td>
</tr>
<tr>
<td></td>
<td>Incoming message scanning is disabled</td>
</tr>
<tr>
<td></td>
<td>Internal message scanning is disabled</td>
</tr>
<tr>
<td></td>
<td>Incoming message scanning from other domains is disabled</td>
</tr>
<tr>
<td></td>
<td>Sender is included in the Inspection Scope exceptions</td>
</tr>
<tr>
<td></td>
<td>Sender is not included in Inspection Scope settings</td>
</tr>
</tbody>
</table>

**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.
HTTPS Inspection

You can enable HTTPS traffic inspection on Security Gateways to prevent security risks related to the Secure Sockets Layer (SSL) protocol. SSL secures communication between internet browser clients and web servers. It also supplies data privacy and integrity by encrypting the traffic, based on standard encryption ciphers.

However, SSL has a potential security gap. It can hide illegal user activity and malicious traffic from the content inspection of Security Gateways. One example of a threat is when an employee uses HTTPS (SSL based) to connect from the corporate network to internet web servers. Security Gateways without HTTPS Inspection are unaware of the content passed through the SSL encrypted tunnel. This makes the company vulnerable to security attacks and sensitive data leakage.

The SSL protocol is widely implemented in public resources that include: banking, web mail, user forums, and corporate web resources.

For HTTPS traffic inspection, Security Gateways must examine the data as clear text. Encrypted data sent by a client to a web server is:

- Intercepted by the Security Gateway and decrypted.
- Inspected by the blades set in the policy.
- Encrypted again and sent to the designated web server.

The Security Gateway acts as an intermediary between the client computer and the secure web site. The Security Gateway behaves as the client with the server and as the server with the client using certificates.

All data is kept private in HTTPS Inspection logs. This is controlled by administrator permissions. Only administrators with HTTPS Inspection permissions can see all the fields in a log. Without these permissions, some data is hidden.

How it Operates

When a client computer initiates an HTTPS connection to a secure site, the Security Gateway:

1. Intercepts the request.
2. Establishes a secure connection (an SSL tunnel) to the requested web site and validates the site’s server certificate.
3. Creates a new SSL certificate for the communication between the Security Gateway and the client, sends the client the new certificate and establishes a different SSL tunnel with it.
4. Using the two tunnels:
   a) It decrypts the encrypted data from the client.
   b) Inspects the clear text content for all blades set in the policy.
   c) Encrypts the data again to keep client privacy as the data travels to the destination web server resource.
Configuring HTTPS Inspection

To enable HTTPS traffic inspection, you must do these steps:

- Set the Security Gateway for HTTPS Inspection.
- Create a generated CA on the Security Management Server or import a CA certificate already deployed in your organization.
- If you created a CA certificate, you must deploy it in the Trusted Root Certification Authorities Certificate Store on the client computers. This lets the client computers trust all certificates signed by this certificate.
- Generate an HTTPS inspection policy by defining relevant rules in the HTTPS inspection Rule Base.
- Update the trusted CA list in the Security Gateway (if necessary).
- Configure the conditions for dropping traffic from a web site server.

Enabling HTTPS Inspection on a Gateway

You must enable HTTPS inspection on each gateway. The first time you enable HTTPS inspection on one of the gateways, you must create a CA certificate for HTTPS inspection or import a CA certificate already deployed in your organization. This certificate is used by all gateways managed on the Security Management Server.

Creating a CA Certificate

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

After you create a CA certificate, you must export it so it can be distributed to clients. If you do not deploy the generated 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 ("Troubleshooting" on page 55).

To create a CA certificate:

1. In SmartDashboard, right-click the gateway object and select Edit. The Gateway Properties window opens.
2. In the navigation tree, select HTTPS Inspection.
3. In the HTTPS Inspection page, click Create.
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 48).

Importing a 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.

Important - If you are importing a CA certificate created on another Security Management Server, make sure the initial certificate was exported ("Exporting a Certificate from the Security Management Server" on page 48) from the Security Management Server on which it was created.
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. This password is only used when you import the certificate to a new Security Management Server.

**Important**: After you import a certificate from another Security Management Server, make sure to export the certificate and deploy it ("Exporting and Deploying the Generated CA" on page 48) on the client machines.

**To import a CA certificate:**

1. In SmartDashboard, right-click a gateway object, select Edit > HTTPS Inspection > Import
   Or
   From the HTTPS Inspection > Gateways pane of a supported blade, click the arrow next to Create Certificate and select Import certificate from file.
   The Import Certificate window opens.
2. Browse to the certificate file.
3. Enter the private key password.
4. Click OK.

**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 using 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.

Usage:

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

When users do 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
   Or
   From the HTTPS Inspection > Gateways pane in a supported blade, click Export.
2. Save the CA certificate file.
3. Use the Group Policy Management Console ("Deploying Certificates by Using Group Policy" on page 49) to add the certificate to the Trusted Root Certification Authorities certificate store.
4. Push the policy to the client machines in the organization.
Note - Make sure that the CA certificate is pushed to the client machines' 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 by using Active Directory Domain Services and a Group Policy object (GPO). A GPO can contain multiple configuration options, and is applied to all computers that are within 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. 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 current contents of the policy object.
5. Click Action > Export.
6. Do the instructions in the Certificate Import Wizard to find and import the certificate you exported from SmartDashboard.
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.

The HTTPS Inspection Policy

The HTTPS inspection policy determines which traffic is inspected. The primary component of the policy is the Rule Base. The rules use the categories defined in the Application Database, network objects and custom objects (if defined).

The HTTPS Rule Base lets you inspect the traffic on other network blades. The blades that HTTPS can operate on are based on the blade contracts and licenses in your organization and can include:

- Application Control
- URL Filtering
- IPS
- DLP
- Anti-Virus

If you enable Identity Awareness on your gateways, you can also use Access Role objects as the source in a rule. This lets you easily make rules for individuals or different groups of users.

To access the HTTPS inspection Rule Base:

- In SmartDashboard, open the Policy page:
  - For Application and URL Filtering and IPS - Select Advanced > HTTPS Inspection > Policy.
  - For DLP - Select Additional Settings > HTTPS Inspection > Policy.
Predefined Rule

When you enable HTTPS inspection, a predefined rule is added to the HTTPS Rule Base. This rule defines that all HTTPS and HTTPS proxy traffic from any source to the internet is inspected on all blades enabled in the Blade column. By default, there are no logs.

<table>
<thead>
<tr>
<th>Name</th>
<th>Source</th>
<th>Destination</th>
<th>Services</th>
<th>Site Category</th>
<th>Action</th>
<th>Track</th>
<th>Blade</th>
<th>Install On</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined</td>
<td>Any</td>
<td>Internet</td>
<td>HTTPS</td>
<td>Any</td>
<td>Inspect</td>
<td>None</td>
<td>All</td>
<td>All</td>
</tr>
</tbody>
</table>

Parts of the Rule

The columns of a rule define the traffic that it matches and if that traffic is inspected or bypassed. When traffic is bypassed or if there is no rule match, the traffic continues to be examined by other blades in the gateway.

Number (No.)

The sequence of rules is important because the first rule that matches is applied.

For example, if the predefined rule inspects all HTTPS traffic from any category and the next rule bypasses traffic from a specified category, the first rule that inspects the traffic is applied.

Name

Give the rule a descriptive name. The name can include spaces.

Double-click in the Name column of the rule to add or change a name.

Source

The source is where the traffic originates. The default is Any.

Important - A rule that blocks traffic, with the Source and Destination parameters defined as Any, also blocks traffic to and from the Captive Portal.

Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of network objects and select one or multiple sources. The source can be an Access Role object, which you can define when Identity Awareness is enabled.

Destination

Choose the destination for the traffic. The default is the Internet, which includes all traffic with the destination of DMZ or external. If you delete the destination value, the rule changes to Any, which applies to traffic going to all destinations.

Important - A rule that blocks traffic, with the Source and Destination parameters defined as Any, also blocks traffic to and from the Captive Portal.

To choose other destinations, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of network objects and select one or multiple destinations.

Services

By default, HTTPS traffic on port 443 and HTTP and HTTPS proxy on port 8080 is inspected. You can include more services and ports in the inspection by adding them to the services list.

To select other HTTPS/HTTP services, put your mouse in the column and a plus sign shows. Click the plus sign to open the list of services and select a service. Other services, such as SSH are not supported.

Site Category

The Site Category column contains the categories for sites and applications that users browse to and you choose to include. One rule can include multiple categories of different types.
Important - A valid URL Filtering blade contract and license are necessary on the relevant Security Gateways to use the Site Category column.

Important - To perform categorization correctly, a single connection to a site must be inspected in some cases regardless of the HTTPS inspection policy. This maps the IP address of a site to the relevant domain name.

You can also include custom applications, sites, and hosts. You can select a custom defined application or site object with the Custom button or create a new host or site with the New button at the bottom of the page.

Note - You can only use custom objects that specify the domain name or host part of a URL. URLs that contain paths are not supported. For example, you can use an object defined as www.gmail.com but not www.gmail.com/myaccount.

To add site categories to a rule:
Put your mouse in the column and a plus sign shows. Click the plus sign to open the Category viewer. For each category, the viewer shows a description and if there are applications or sites related with it.

- To filter the Available list by categories or custom-defined sites, click the specified button in the toolbar of the viewer. The Available list opens in the left column and then you can add items to the rule.
- To add a category object to the rule, click the checkbox in the Available list.
- To see the details of category without adding it to the rule, click the name of the item in the Available list.
- You can only select a category to add to the rule from the Available list.
- If a category is already in a rule, it will not show in the Category viewer.
- If you know the name of a category, you can search for it. The results will show in the Available list.
- You can add a new host site with the New button.

Adding a New Host Site
You can create a new host site object to use in the HTTPS Rule Base if there is no corresponding existing category. Only the domain name part or hosts part of the URL is supported.

To create a new host site:
1. Click the plus icon in the Site Category column.
2. In the Category viewer, select New. The Hosts/Sites window opens.
3. Enter a name for the host site.
4. Set a color for the host site icon (optional).
5. Enter a comment for the host site (optional).
6. In Hosts List, enter a valid URL and click Add.
7. If you used a regular expression in the URL, click Hosts are defined as regular expressions.
8. Click OK.
   The new host site is added to the Selected list and can be added to the Rule Base.

Action
The action is what is done to the traffic. Click in the column to see the options and select one to add to the rule.

- Inspect - The traffic is inspected on the blades set in the Blades column.
- Bypass - The traffic of source and destination traffic in rules that include the bypass action are not decrypted and inspected. You can bypass HTTPS inspection for all Check Point objects. This is recommended for URL Filtering and IPS updates. Other HTTPS protections that already operate on traffic will continue to work even when the HTTPS traffic is not decrypted for inspection.
Track
Choose if the traffic is logged in SmartView Tracker or if it triggers other notifications. Click in the column and the options open. The options include:

- **None** - Does not record the event
- **Log** - Records the event's details in SmartView Tracker. This option is useful for obtaining general information on your network's traffic. There is one or more log for each session depending on the suppression option.
- **Alert** - Logs the event and executes a command, such as display a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in Policy > Global Properties > Log and Alert > Alert Commands
- **Mail** - Sends an email to the administrator, or runs the mail alert script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **SNMP Trap** - Sends a SNMP alert to the SNMP GUI, or runs the script defined in Policy > Global Properties > Log and Alert > Alert Commands
- **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in Policy > Global Properties > Log and Alert > Alert Commands

Blade
Choose the blades that will inspect the traffic. Click in the column and the options open. The options include:

- Application Control
- Data Loss Prevention
- IPS
- URL Filtering
- Anti-Virus

⚠️ **Important** - The blade options you see are based on the blade contracts and licenses in your organization.

Install On
Choose which gateways the rule will be installed on. The default is **All**, which means all gateways that have HTTPS inspection enabled. Put your mouse in the column and a plus sign shows. Click the plus sign to open the list of available gateways and select.

Bypassing HTTPS Inspection to 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 to software updates:**
1. In the HTTPS Inspection > Policy pane, select **Bypass HTTPS Inspection of traffic to well known software update services (list is dynamically updated)**. This option is selected by default.
2. Click **list** to see the list of approved domain names.

Gateways Pane
The **Gateways** pane lists the gateways with HTTPS Inspection enabled. Select a gateway and click **Edit** to edit the gateway properties. You can also search, add and remove gateways from here.

For each gateway, you see the gateway name, IP address and comments.

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

If the Security Management Server managing the selected gateway does not have a generated CA certificate installed on it, you can add it with **Import certificate from file**. There are two options:
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 48) it from the Security Management Server on which it was created.

**Adding Trusted CAs**

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 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's server certificate.

R75.20 contains a preconfigured list of trusted CAs. This list is updated by Check Point, see sk64521 (https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsoultiondetails=&solutionid=sk64521). 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's security certificate, but lets the user continue to the website.

You can change the default setting to block untrusted server certificates ("Server Validation" on page 54).


To add a trusted CA to the Security Gateway, you must export the necessary certificate from a non-trusted web site and then import it into SmartDashboard.

**To export a CA certificate to add to the trusted CAs list:**
2. Install the security policy.
3. Browse to the site to get the certificate issued by the CA.
4. Go to the Certification Path of the certificate.
5. Select the root certificate (the top most certificate in the list).
6. In Internet Explorer and Chrome:
   a) Click View Certificate.
   b) From the Details tab, click Copy to File.
   c) Follow the wizard steps.
7. In Firefox, export the certificate.

**To import a CA certificate to the Trusted CAs list:**
1. In SmartDashboard, open HTTPS Inspection > Trusted CAs.
2. Click Actions > Import certificate, browse to the location of the saved certificate and click Open.
   The certificate is added to the trusted CAs list.
3. Install the security policy on gateways enabled with HTTPS Inspection.

**Saving a CA Certificate**

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

**To export a selected certificate:**
1. In SmartDashboard, 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.

**Updating the Trusted CAs List**

Updates for the trusted CAs list will be published periodically on the Check Point web site in a ZIP file.

**To update the Trusted CAs list:**
1. In SmartDashboard, open HTTPS Inspection > Trusted CAs.
2. Click **Actions > Update certificate list**.
3. Browse to the ZIP file and click **Open**.
   You see the certificates that will be added or removed to the list and the validity date range of the certificates.
4. Click **Proceed** to confirm the update.
   The certificates will be added or removed respectively from the list.

**HTTPS Validation**

**Server Validation**

When a Security Gateway receives an untrusted certificate from a web site server, the settings in this section define when to drop the connection.

- **Untrusted server certificate**
  - When selected, traffic from a site with an untrusted server certificate is immediately dropped. The user gets an error page that states that the browser cannot display the webpage.
  - When cleared, a self-signed certificate shows on the client machine when there is traffic from an untrusted server. The user is notified that there is a problem with the website's security certificate, but lets the user to continue to the website (default).

- **Revoked server certificate (validate CRL)**
  - When selected, the Security Gateway validates that each server site certificate is not in the Certificate Revocation List (CRL). To validate the CRL, the Security Gateway must have access to the internet. For example, if a proxy server is used in the organization's environment, you must configure the proxy for the Security Gateway.
    To configure the proxy:
    a) From the **Firewall** tab, double-click the Security Gateway that requires proxy configuration.
    b) Select **Topology > Proxy**.
    c) Select **Use custom proxy settings for this network object** and **Use proxy server** and enter the proxy IP address.
    d) Optionally, you can use the default proxy settings.
    e) Click **OK**.

    ! Important - Make sure that there is a rule in the Rule Base that allows outgoing HTTP from the Security Gateway.

  - When cleared, the Security Gateway does not check for revocations of server site certificates (default).

- **Expired server certificate**
  - When selected, the Security Gateway drops the connection if the server certificate has expired.
  - When cleared, the Security Gateway creates a certificate with the expired date. The user can continue to the website (default).

- **Track validation errors**
  Choose if the server validation traffic is logged in SmartView Tracker or if it triggers other notifications. The options include:
  - **None** - Does not record the event.
  - **Log** - Records the event's details in SmartView Tracker
  - **Alert** - Logs the event and executes a command, such as shows a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in **Policy > Global Properties > Log and Alert > Alert Commands**
  - **Mail** - Sends an email to the administrator, or runs the mail alert script defined in **Policy > Global Properties > Log and Alert > Alert Commands**
  - **SNMP Trap** - Sends an SNMP alert to the SNMP GUI, or runs the script defined in **Policy > Global Properties > Log and Alert > Alert Commands**
  - **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in **Policy > Global Properties > Log and Alert > Alert Commands**
HTTPS Inspection

Installation and Configuration

- **Automatically retrieve intermediate CA certificates**
  - When selected, intermediate CA certificates issued by trusted root CA certificates that are not part of the certificate chain are automatically retrieved using the information on the certificate.
  - When cleared, a web server certificate signed by an intermediate CA certificate which is not sent as part of the certificate chain, will be considered untrusted.

Certificate Blacklisting

You can create a list of certificates that are blocked. Traffic from servers using the certificates in the blacklist will be dropped. If a certificate in the blacklist is also in the Trusted CAs list, the blacklist setting overrides the Trusted CAs list.

- **Add** - Lets you add a certificate. Enter the certificate’s serial number (in hexadecimal format HH:HH) and a comment that describes the certificate.
- **Edit** - Lets you change a certificate in the blacklist.
- **Remove** - lets you delete a certificate in the blacklist.
- **Search** - Lets you search for a certificate in the blacklist.

- **Track dropped traffic**
  Choose if the dropped traffic is logged in SmartView Tracker or if it triggers other notifications. The options include:
  - **None** - Does not record the event.
  - **Log** - Records the event's details in SmartView Tracker
  - **Alert** - Logs the event and executes a command, such as shows a popup window, send an email alert or an SNMP trap alert, or run a user-defined script as defined in Policy > Global Properties > Log and Alert > Alert Commands
  - **Mail** - Sends an email to the administrator, or runs the mail alert script defined in Policy > Global Properties > Log and Alert > Alert Commands
  - **SNMP Trap** - Sends an SNMP alert to the SNMP GUI, or runs the script defined in Policy > Global Properties > Log and Alert > Alert Commands
  - **User Defined Alert** - Sends one of three possible customized alerts. The alerts are defined by the scripts specified in Policy > Global Properties > Log and Alert > Alert Commands

Troubleshooting

Secure connections between a client and server with no traffic create logs in SmartView Tracker labeled as "Client has not installed CA certificate". This can happen when an application or client browser fails to validate the server certificate. Possible reasons include:

- The generated CA was not deployed on clients ("Exporting and Deploying the Generated CA" on page 48).
- The DN in the certificate does not match the actual URL (for example, when you browse to https://www.gmail.com, the DN in the certificate states mail.google.com).
- Applications (such as FireFox and anti-viruses) that use an internal trusted CAs list (other than Windows). Adding the CA certificate to the Windows repository does not solve the problem.

The option in the HTTPS Validation pane:

- **Log connections of clients that have not installed the CA certificate**
  - When selected, logs are recorded for secure connections between a client and server with no traffic in SmartView Tracker (default). Logs are recorded only when a server certificate is trusted by the Security Gateway. If the server certificate is untrusted, a self-signed certificate is created and always results in a log labeled as "Client has not installed CA certificate".
  - When cleared, logs are not recorded for secure connections without traffic that can be caused by not installing the CA certificate on clients or one of the above mentioned reasons.
HTTPS Inspection in SmartView Tracker

Logs from HTTPS Inspection are shown in SmartView Tracker. There are two types of predefined queries for HTTPS Inspection logs in SmartView Tracker:

- HTTPS Inspection queries
- Blade queries - HTTPS Inspection can be applied to these blades:
  - Application Control
  - URL Filtering
  - IPS
  - DLP
  - Anti-Virus

To open SmartView Tracker do one of these:

- From the SmartDashboard toolbar, select Window > SmartView Tracker.
- Press Control + Shift + T.

HTTPS Inspection Queries

These are the predefined queries in Predefined > Network Security Blades > HTTPS Inspection.

- **All** - Shows all HTTPS traffic that matched the HTTPS Inspection policy and was configured to be logged.
- **HTTPS Validations** - Shows traffic with connection problems.
  - Action values include rejected or detected. The actions are determined by the SSL validation settings ("HTTPS Validation" on page 54) for HTTPS Inspection.
  - HTTPS Validation values include:
    - Untrusted Server Certificate
    - Server Certificate Expired
    - Revoked Certificate or Invalid CRL
    - SSL Protocol Error - For general SSL protocol problems

Blade Queries

When applying HTTPS Inspection to a specified blade:

- There is an HTTPS Inspection predefined query for each of the blades that can operate with HTTPS Inspection. The query shows all traffic of the specified blade that passed through HTTPS inspection.
- The log in the blade's queries includes an HTTP Inspection field. The field value can be inspect or bypass. If the traffic did not go through HTTPS inspection, the field does not show in the log.

Permissions for HTTPS Logs

An administrator must have HTTPS inspection permissions to see classified data in HTTPS inspected traffic.

To set permissions for an administrator in a new profile:

1. In the Users and Administrators tree, select an administrator > Edit.
2. In the Administrator Properties > General Properties page in the Permissions Profile field, click New.
3. In the Permissions Profile Properties window:
   - Enter a Name for the profile.
   - Select Customized and click Edit.
   The Permissions Profile Custom Properties window opens.
4. In the Monitoring and Logging tab, select HTTPS Inspection logs for permission to see the classified information in the HTTPS Inspection logs.
5. Click OK on all of the open windows.
To edit an existing permissions profile:
1. From the SmartDashboard toolbar, select Manage > Permissions Profiles.
2. Select a profile and click Edit.
3. Follow the instructions above from step 3.

HTTPS Inspection in SmartEvent

Events from HTTPS Inspection are shown in SmartEvent. There are two types of predefined queries for HTTPS Inspection events in SmartEvent:

- HTTPS Inspection queries for HTTPS validations
- Blade queries - HTTPS Inspection can be applied to these blades:
  - Application Control
  - URL Filtering
  - IPS
  - DLP
  - Anti-Virus

To open SmartEvent do one of these:
- From the SmartDashboard toolbar, select Window > SmartEvent.
- Press Control +Shift +T.

Event Analysis in SmartEvent

SmartEvent supplies advanced analysis tools with filtering, charts, reporting, statistics, and more, of all events that pass through enabled Security Gateways. SmartEvent shows all HTTPS Inspection events.

You can filter the HTTPS Inspection information for fast monitoring on HTTPS Inspection traffic.

- Real-time and history graphs of HTTPS Inspection traffic.
- Graphical incident timelines for fast data retrieval.
- Easily configured custom views to quickly view specified queries.
- Incident management workflow.

SmartEvent shows information for all Software Blades in the environment.

Viewing Information in SmartEvent

There are two types of predefined queries for HTTPS Inspection events in SmartEvent:

- HTTPS Inspection queries
- Blade queries

HTTPS Inspection Queries

- Go to Events > Predefined > HTTPS Inspection > HTTPS Validation to shows the SSL validation events that occurred.
- The Details and Summary tabs in the event record show if the traffic was detected or rejected due to SSL Validation settings.

Blade Queries

- There is an HTTPS Inspection predefined query for each of the blades that can operate with HTTPS Inspection. The query shows all traffic of the specified blade that passed through HTTPS inspection.
- The Summary tab in the event record in the blade's queries includes an HTTPS Inspection field. The field value can be inspect or bypass. If the traffic did not go through HTTPS inspection, the field does not show in the event record.
Chapter 3

Out of the Box

In This Chapter

- Default Deployment
- Data Loss Prevention in SmartDashboard
- Defining My Organization
- Data Loss Prevention Policies
- Auditing and Analysis

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 SmartView Tracker tracking to find the key data leaks.

Data Loss Prevention in SmartDashboard

When you open the SmartDashboard to the Data Loss Prevention tab, these views are available.

<table>
<thead>
<tr>
<th>Page</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>Quick access to urgent tasks, commonly used features, and overview statistics.</td>
</tr>
<tr>
<td>Policy</td>
<td>Manage the rule base for Data Loss Prevention policy.</td>
</tr>
<tr>
<td>Gateways</td>
<td>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.</td>
</tr>
<tr>
<td>Data Types</td>
<td>Define representations of data assets to protect.</td>
</tr>
<tr>
<td>My Organization</td>
<td>Define the internal environment: networks, users, email addresses, and VPN communities.</td>
</tr>
<tr>
<td>Additional Settings:</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td>Define users, user groups, and AD/LDAP groups as network objects, to use in DLP and other Software Blades.</td>
</tr>
<tr>
<td><strong>Network and Resources</strong></td>
<td>Manage networks, hosts, servers, LDAP Account Units, and other network objects for use in DLP. Manage DLP and SmartDashboard administrators.</td>
</tr>
<tr>
<td><strong>Protocols</strong></td>
<td>Enable the protocols to be checked on individual DLP gateways.</td>
</tr>
<tr>
<td><strong>Mail Relay</strong></td>
<td>Configure the mail server for DLP to send notification emails.</td>
</tr>
<tr>
<td><strong>Email Addresses or Domains</strong></td>
<td>Manage email address lists and domains for use in DLP rules and data types.</td>
</tr>
<tr>
<td><strong>Advanced</strong></td>
<td>• Incident Tracking - Define whether to log all emails (to calculate ratio of incidents) or just DLP incidents.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Extreme Conditions - Lets you define if to bypass DLP SMTP, FTP and HTTP inspection and prefer connectivity under these extreme conditions:</td>
</tr>
<tr>
<td></td>
<td>▪ CPU load levels are more than the high CPU load watermark</td>
</tr>
<tr>
<td></td>
<td>▪ Other extreme conditions including:</td>
</tr>
<tr>
<td></td>
<td>▪ Internal errors</td>
</tr>
<tr>
<td></td>
<td>▪ Protocol message sizes are more than the default value</td>
</tr>
<tr>
<td></td>
<td>▪ File attachments are more than the default value</td>
</tr>
<tr>
<td></td>
<td>▪ Archive depth level is more than the default value</td>
</tr>
<tr>
<td></td>
<td>If necessary, you can change the default values (&quot;Editing Extreme Condition Values&quot; on page 114).</td>
</tr>
</tbody>
</table>
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 SmartDashboard must be in the Active Directory domain to take advantage of the LDAP User List features.

My Organization Definitions:

- Adding Email Addresses and Domains to My Organization
- Defining Internal Users
- Defining Internal User Groups
- Excluding Users from My Organization
- Defining Internal Networks
- Excluding Networks from My Organization
- Defining Internal VPNs
- Excluding VPNs from My Organization

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 adding domains, do not use the @ sign. A valid domain example is: example.com
- If you add a domain, it will catch all sub domains as well. For example, if the domain is example.com, email addresses such as jsmith@uk.example.com are also considered as 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 SmartDashboard, open the Data Loss Prevention tab.
2. Click My Organization.
Defining 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 SmartDashboard.

**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 SmartDashboard.

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 SmartDashboard.

To define specific networks and hosts:
1. In SmartDashboard, 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

If your Check Point deployment includes Virtual Private Networks, allow dynamic VPN traffic to be included in your My Organization definition.

A DLP gateway is aware of the VPN communities in which it participates. A dedicated DLP gateway for example, is aware of the VPN communities in which its protecting Security Gateway participates. Even if other VPNs are configured in your SmartDashboard, only those that are relevant to the DLP gateway are included in the DLP My Organization.

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

To configure Office Mode for support of Remote Access communities:
- If Office Mode IP addresses are assigned from IP pool, nothing further is required.
- If addresses are assigned from RADIUS, DHCP, or ipassignment.conf:
1. Open the properties of the gateway > IPSec VPN.
2. Open Office Mode.
3. Select Perform Anti spoofing on Office Mode addresses.
4. Enter the IP address range.

**To include VPN traffic in My Organization:**
1. In SmartDashboard, open the Data Loss Prevention tab.
2. Click My Organization.
3. In the VPN area, make sure the All VPN traffic checkbox is selected.

### Excluding VPNs from My Organization

VPN traffic is an encrypted tunnel between sites. If you have multiple VPNs in your deployment, you might want to exclude some from the My Organization definition.

For example, if you have a VPN with a third party, such as a business partner, you can configure a VPN community that joins the organizations together. All traffic between the two organizations would be seen as internal by the VPN gateway of each office. However, if you want DLP to prevent confidential data being passed to the business partner, you could exclude the VPN from My Organization and thus control the type of data that is passed.

Before you make this decision, you should know which VPNs defined in your SmartDashboard are relevant to the DLP gateway.

DLP can see only the VPNs in which its protecting VPN gateway participates. All defined gateways are listed in the VPN Communities window in which you define exclusions; but only the relevant VPNs can be manually excluded. The others are always excluded and cannot be included.

**Figure 3-5** Known and Unknown VPNs

The organization behind the DLP gateway is protected by a VPN gateway (1). This gateway participates in a VPN community (2). Therefore, DLP sees the remote hosts in the VPN (3) as part of My Organization.

The protecting VPN gateway does not participate in the VPN community between the other sites (3 and 5), and is not aware of the VPN between them (4). Therefore, DLP considers the hosts in site 5 as external to My Organization.

**To discover VPNs known to DLP:**
1. Find the protecting VPN gateway of 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 in the Network Objects tree, to open the gateway properties.
3. Open the IPSec VPN page.
   - The DLP gateway is aware of the VPN communities that are listed in the IPSec VPN page of the protecting VPN gateway.
To exclude VPNs from My Organization:
1. Open the Data Loss Prevention tab > My Organization.
2. In the VPN area, click Exclusions.
   The VPN Communities window opens.
3. 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.

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

Each Data Loss Prevention rule defines the following:

- **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.
- **Source of the transmission** - 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. It is recommended that you 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.
- **Destination** - by default, anything that is outside of the internal organization. You may choose to make the destination any network object defined in the SmartDashboard 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.
- **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.
- **Action** - 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.
- **Track** - when data transmissions match Data Loss Prevention rules, they are logged as incidents in SmartView Tracker by default. You can add email notifications here and other tracking methods.
- **Severity** - set the severity of the rules in your policy, to help in filtering and reporting while auditing Data Loss Prevention incidents through SmartEvent. 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.

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 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. An administrator with full permissions or the View/Release/Discard DLP messages permission can also send/discard this mail from SmartView Tracker. 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:

a) The email is quarantined.

b) The user gets a notification and has to make a decision relating to what to do.

c) The data owner gets a notification.

d) The rule violations (one for **Detect** and one for **Ask User**) are logged.

e) An administrator can send/discard this email from SmartView Tracker. Notification is sent to the user.
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.

Table 3-2 Data Loss Prevention Rule Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect</td>
<td>The transmission is passed. The event is logged in SmartView Tracker and is available for your review and analysis in SmartReporter and SmartEvent. The data and the email itself, or the properties of the transmission if not email, are saved in storage for future reference. You can choose to notify Data Owners of the event. This is true for all the following actions as well.</td>
</tr>
<tr>
<td>Inform User</td>
<td>The transmission is passed, but the incident is logged and the user is notified.</td>
</tr>
<tr>
<td>Ask User</td>
<td>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 SmartView Tracker under the User Actions category. Administrators with full permissions or with the View/Release/Discard DLP messages permission can also decide whether the transmission should be completed or not from SmartView Tracker. This can be useful in the event that a user is not available to make sure if it should be sent.</td>
</tr>
<tr>
<td>Prevent</td>
<td>The data transmission is blocked. Note: Check Point does not recommend using the Prevent action at first because it may be disruptive. To improve the accuracy of the rule matches, set rules to prevent only when you have tested them with the less strict actions over a reasonable amount of time.</td>
</tr>
</tbody>
</table>

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 SmartView Tracker 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 Up Rule Tracking

A major consideration for any Data Loss Prevention rule is how to audit incidents.

In the rule base of the Data Loss Prevention policy, the Track column offers the same options as in the rule base of the Firewall:

- **Log** - Records the incident in SmartView Tracker (default); all the options (except None) also log an incident.
- **Alert** - Sends a popup window to the SmartView Monitor desktop.
• **SNMP Trap** - Sends an SNMP alert to the SNMP GUI. This uses the `fwd` process, to run the `internal_snmp_trap` script that sends an ID, the trap type, source port, community, and host name.

• **User Defined Alert** - Sends one of three possible customized alerts that you provide with your own scripts. The alerts are defined by the scripts specified in **Policy > Global Properties > Log and Alert > Alert Commands**. The alert process on the Log server executes the scripts.

### 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 SmartDashboard, 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. Do **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 actions 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 41) and the HTTPS protocol.

**To select protocol deployment for all gateways:**

1. In SmartDashboard, 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 SmartDashboard, 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 with SmartView Tracker and SmartEvent, 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.

The Overview page of Data Loss Prevention in SmartDashboard provides a quick link to data types and rules that are marked for Follow Up.

Using SmartView Tracker

The DLP gateway issues logs for various events.

To open SmartView Tracker:
1. In SmartDashboard, select Window > SmartView Tracker.
2. In the Network & Endpoint tab, expand Predefined > Data Loss Prevention Blade.
   The Data Loss Prevention logs are categorized for filtering.

To see more information:
1. Double-click an item in the log window.
   The Record Details window opens.
2. Click DLP Log.
   The DLP Record 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 SmartDashboard 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 SmartView Tracker 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

SmartView Tracker actions for DLP incidents include:

<table>
<thead>
<tr>
<th>DLP Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ask User</td>
<td>DLP incident captured and put in Quarantine, user asked to decide what to do.</td>
</tr>
<tr>
<td>Do not Send</td>
<td>User decided to drop transmission that was captured by DLP. An administrator with full permissions or with the View/Release/Discard DLP messages permission can also drop these transmissions. Email notification is sent to the user.</td>
</tr>
<tr>
<td>Send</td>
<td>User decided to continue transmission after DLP notified that it may contain sensitive data. 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.</td>
</tr>
</tbody>
</table>
### DLP General Columns

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

<table>
<thead>
<tr>
<th>DLP Columns</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident UID</td>
<td>Unique ID of the incident.</td>
</tr>
<tr>
<td>DLP Action Reason</td>
<td>Reason for the action. Possible values: Rulebase, Internal Error, Prior User Decision</td>
</tr>
<tr>
<td>Related Incident</td>
<td>Internal incident ID related to the current log.</td>
</tr>
<tr>
<td>DLP Transport</td>
<td>Protocol of the traffic of the incident: HTTP, FTP, Email.</td>
</tr>
</tbody>
</table>

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 actions (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.

<table>
<thead>
<tr>
<th>Restricted Filters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Rule Name</td>
<td>Name of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Rule UID</td>
<td>Internal rule ID of the DLP rule on which the incident was matched.</td>
</tr>
<tr>
<td>Data Type UID</td>
<td>Internal ID of the data type on which the incident was matched.</td>
</tr>
<tr>
<td>Data Type Name</td>
<td>Name of the matched data type.</td>
</tr>
<tr>
<td><strong>Restricted Filters</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>User Action Comment</td>
<td>Comment given by user when releasing the incident from the Portal.</td>
</tr>
<tr>
<td>DLP Recipients</td>
<td>For SMTP traffic, list of recipients of captured email.</td>
</tr>
<tr>
<td>Scanned Data Fragment</td>
<td>Captured data itself: email and attachment of SMTP, file of FTP, or HTTP traffic.</td>
</tr>
<tr>
<td>Message to User</td>
<td>Message sent, as configured by administrator, for the rule on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Categories</td>
<td>Category of data type on which the incident was matched.</td>
</tr>
<tr>
<td>DLP Words List</td>
<td>If the data type on which the incident was matched included a word list (keywords, dictionary, and so on), the list of matched words.</td>
</tr>
<tr>
<td>Mail Subject</td>
<td>For SMTP traffic, the subject of captured email.</td>
</tr>
</tbody>
</table>

### Using SmartEvent

SmartEvent provides advanced analysis tools with filtering, charts, reporting, statistics, and more, of all events that pass through enabled Security Gateways. SmartEvent combines all DLP logs of the same incident (all matching rules and data types and user action if applicable) to a single event.

You can filter out the specific Data Loss Prevention information for efficient monitoring and relevant reporting on DLP incidents.

- Real-time and history graphs and reports of Data Loss Prevention incidents
- Graphical incident timelines for rapid information retrieval
- Easily configured custom views to quickly answer specific queries
- Incident management workflow
- Reports to data owners on a scheduled basis

To open SmartEvent:

1. In SmartDashboard, select Window > SmartEvent.
2. When SmartEvent is open, open Events.
3. Select Predefined > DLP or any of the analysis data categories under DLP.
Chapter 4

Data Owner and User Notifications

In This Chapter

Data Owners 71
Preparing Corporate Guidelines 72
Communicating with Data Owners 72
Communicating with Users 73
Notifying Data Owners 73
Notifying Users 74
Customizing Notifications 74
Setting Rules to Ask User 75
DLP Portal 76
UserCheck Notifications 77
Managing Rules in Ask User 77
Learning Mode 77

Data Owners

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

For example, according to heuristics, it might seem logical that no source code be sent outside of your organization; but a Data Owner explains that her team needs to send code snippets to outside technical support for troubleshooting. Add this information to the list of data types that this Data Owner controls, and create an Exception to the Rule for this type of data, coming from this team, and being sent to the technical support domain.

When DLP incidents are logged, the DLP gateway can send automatic notifications to the Data Owners. For example, configure Data Owner notification for rules that have a critical severity. Automatic notifications ensure that the Data Owner knows about relevant incidents and can respond rapidly to issues under their responsibility.

To define data owners:

1. On the SmartDashboard, open the Data Loss Prevention tab > Data Types.
2. Double-click a data type in the list.
   The properties window of the data type opens.
3. Click Data Owners.
4. Click Add.
   The Add Data Owners window opens.
5. Select the user or group who is responsible for this data and click Add.
   If the data owner is not in the list, click New. In the Email Addresses window, enter the name and email address of the data owner (or name a list of email addresses).
6. Add as many data owners as needed.
7. Click OK.
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: $DLPDIR/config/dlp.conf
2. Find the corporate_info_link parameter and change the value to be the URL of your corporate guidelines (format = http://www.example.com).
3. Save the file and close it.
4. Do 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.

Table 4-3 Recommended Data Owner Notification

<table>
<thead>
<tr>
<th>Rule Action</th>
<th>Recommendation for Data Owner Notification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detect</td>
<td>In general, you should not notify Data Owners for Detect rules.</td>
</tr>
<tr>
<td>Inform User</td>
<td>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.</td>
</tr>
<tr>
<td>Ask User</td>
<td>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.</td>
</tr>
<tr>
<td>Prevent</td>
<td>Any rule that is severe enough to justify the immediate block of a transmission, is often enough to justify the Data Owner being notified.</td>
</tr>
</tbody>
</table>
Communicating with Users

It is recommended that before you install the first policy, you 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 unallowed 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.

<table>
<thead>
<tr>
<th>Table 4-4 Recommended User Notifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Action</td>
</tr>
<tr>
<td>Detect</td>
</tr>
<tr>
<td>Inform User</td>
</tr>
<tr>
<td>Ask User</td>
</tr>
<tr>
<td>Prevent</td>
</tr>
</tbody>
</table>

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 Data Loss Prevention > Data Types, define the data owners of the data type.
2. Open Data Loss Prevention > Policy.
3. Right-click the Track column of the rule and select Email. The Email window opens.
4. Select the checkbox. **Data Owners** is provided by default.
   If you want the notification to be sent to others as well, click the plus button and select users or groups in the **Add Recipients** window.

5. Provide the text to appear in the email.
   **Default text is:** The Data Loss Prevention blade has found traffic which matches a rule

6. Click **OK**.

**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**

Customize notifications sent to users to match your organization culture and needs. Maintain an impersonal and nonjudgmental format. Focus on the issue and on helping users to change their future behavior, while handling this specific incident.

The user may see any of the following information:

- The sender is your corporate Mail Delivery address.
- 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.
  It is recommended that you explain that the data may be read by others, for the purpose of protecting 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 Prevention system determined that it may contain confidential information.

You can change this text by entering the message that you want.

You can include the following variables to provide specific information.
### Setting Rules to Ask User

The Ask User rule action provides UserCheck, distributing unintentional data security checks to the user. This action provides automated education to users. When a user attempts to transmit protected data, DLP captures the data and notifies the user. The notification (by email or by popup of the UserCheck client on user machines) explains the policy about transmitting this data and provides links to handle the incident.

**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 25).

---

**Table 4-5 Notification Variables**

<table>
<thead>
<tr>
<th>Variable Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%_part_name_%</code></td>
<td>Location of the data in violation: Email's Body or the name of the attachment</td>
</tr>
<tr>
<td><code>%_rule_name_%</code></td>
<td>Name of the rule that matched the transmission</td>
</tr>
<tr>
<td><code>%_data_objects_%</code></td>
<td>Name of the data types that represent matched data in the transmission</td>
</tr>
</tbody>
</table>

The following variables are applied to emails that match Unintentional Recipient or External BCC rules.

**Table 4-6 More Notification Variables**

<table>
<thead>
<tr>
<th>Variable Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>%_internal_recipients_num_%</code></td>
<td>Number of intended destinations inside My Organization</td>
</tr>
<tr>
<td><code>%_external_recipient_%</code></td>
<td>List of external addresses (<a href="mailto:user@domain.com">user@domain.com</a>) in the destination</td>
</tr>
</tbody>
</table>

**Example:**

You sent an email that is in violation of `%_rule_name_%` because it contains `%_data_objects_%` and is to be sent to an address outside of the organization: `%_external_recipient_%`.

---

**Customizing Notifications to Data Owners**

To change the text of a notification to Data Owners:

1. Open Data Loss Prevention > Policy.
2. Right-click in the Track column of a rule and select Email.
   - The Email window opens.
3. Change the text with your own message to fit the rule.

**Customizing Notifications for Self-Handling**

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

1. Open Data Loss Prevention > Policy.
2. Right-click in the Action column of a rule and select Edit Properties.
   - This option is available for all actions except Detect, because users are not to be informed of rules that match on this action. Change the action to Inform User if you want to notify the user and still pass the data.
3. In the window that opens, change the text with your own message to fit the rule. You can use text or variables.
To set a rule to ask user:
1. Open Data Loss Prevention > Policy.
2. 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 doing Install Policy with new Ask User rules, make sure the DLP gateway is set up for Ask User options.

To set up the gateway for Ask User rules:
1. Open Data Loss Prevention > Gateways.
2. Select the DLP gateway and click Edit.
   The properties window of the gateway opens.
3. In the left pane list of pages, click Data Loss Prevention.
4. In the DLP Portal area, select Activate DLP Portal for Self Incident Handling.
5. In the left pane list of pages, click Data Loss Prevention > Mail Relay.
6. Select the mail server that the DLP gateway will use to send notification emails.
7. Click OK.

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 SmartDashboard 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:

- Clicking a link in the DLP notification email
- Clicking a link in the UserCheck Client notification
- Browsing directly to the DLP Portal URL. The default URL is: https://<Gateway IP>/dlp
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 SmartView Tracker 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 SmartView Tracker. See DLP Blade > User Actions, where the Action of logged incidents is Quarantine Expired.

UserCheck Notifications

If you configure and install the UserCheck client on user machines, notifications will appear in popups from the system tray. These notifications will display the same information as the email notifications.

If the incident is in Ask User mode, the popups will have Send and Discard links. The users can handle the incidents directly from UserCheck, without having to go to the DLP 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 SmartDashboard, select Window > SmartView Tracker.
2. In the Network & Endpoint tab, expand Predefined > Data Loss Prevention Blade.
3. Click User Actions.

Learning Mode

DLP can recognize email threads or HTTP posts and adapt the policy, rather than asking users to manage each email or HTTP post.

Emails

For example, an Ask User rule is matched. The user gets a notification that an email has been captured by DLP. The user decides to send the email and gives a description why.

DLP caches the subject and recipient list of the email. While the user sends emails in the same thread, DLP will allow the emails. The user gives one explanation why the thread must be allowed if each message contains the content of messages from before. The explanation is given one time for each email thread, for each rule. The explanation is applicable for a week. After a week, the user is notified again.

If a user sends a new violation in the same thread, DLP sends a new notification to the user.

By default, learning mode for Emails is not active.

If DLP scans Exchange traffic, then learning mode is also applied to Exchange emails.

HTTP Posts

Learning mode for HTTP posts operates like learning mode for emails. The user gives one explanation why a post to a site must be allowed if a post contains the content of a post from before. The explanation is given
one time for each HTTP post to a site, for each rule. The explanation is applicable for an hour. After an hour, the user is notified again.

If a user posts a new violation to the same site, DLP notifies the user and asks again.

By default, learning mode for HTTP is not active.

If HTTPS Inspection is enabled, then learning mode is also applied to HTTPS posts.

**To configure learning mode for email threads and HTTP posts:**


2. Select the relevant 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 an hour. 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 cleared by default. When HTTPS Inspection is enabled, learning mode is also applied to HTTPS posts.
Chapter 5

Data Loss Prevention by Scenario

In This Chapter

Analytical Deployment 79
Creating New Rules 79

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 SmartView Tracker, you will review the self-handling actions and the explanations of users.

Creating New Rules

Create the rules that make up the DLP policy. At this stage, before creating your own data types, you can use any of the numerous built-in data types.

To create DLP rules:
1. In SmartDashboard, open the Data Loss Prevention tab > Policy.
2. 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.
3. 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.
4. 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.
5. 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.

6. 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.

7. In the **Track** column, leave **Log** (to log the incident and have it in SmartView Tracker 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.

8. 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.

9. In the **Category** column, right-click and select a defined category.

10. In the **Comment** column, right-click and select **Edit** to enter a comment for the rule.

**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 41).

**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

<table>
<thead>
<tr>
<th>Data</th>
<th>Source</th>
<th>Destination</th>
<th>Exceptions</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Reports</td>
<td>Finance Dept</td>
<td>Outside Source</td>
<td>None</td>
<td>Ask User</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Data</th>
<th>Source</th>
<th>Destination</th>
<th>Exceptions</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial Reports</td>
<td>Finance Dept</td>
<td>Outside Source</td>
<td>None</td>
<td>Ask User</td>
</tr>
<tr>
<td>Financial Reports</td>
<td>My Organization</td>
<td>Any</td>
<td>1</td>
<td>Prevent</td>
</tr>
</tbody>
</table>

2. To make sure there are no double matches in regards to reports sent by Finance department users, add an exception to the rule.
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.

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

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

---

**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 in SmartEvent and provide more relevant reports with SmartReporter. 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**.

It is recommended that if you import data types from Check Point or your vendor, that you flag rules using these data types as **Follow up**, and check the results of these rules in SmartView Tracker and SmartEvent 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 generated by Follow up rules:**
1. Open SmartView Tracker.
2. In the **Network & Endpoint** tab, open **Predefined > DLP Blade > Follow Up**.

**To see events generated by Follow up rules:**
1. Open SmartEvent.
2. In the **Events** tab, open **Predefined > DLP > DLP Follow Up Events**.

**Predefining Rules**

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

**To disable rules:**
1. Open **Data Loss Prevention > Policy**.
2. Right-click the rule to disable and select **Disable Rule**.
3. If this changes the install policy, re-install the policy on DLP gateways.

**To enable rules:**
1. Open **Data Loss Prevention > Policy**.
2. Right-click the disabled rule.
   - It is marked with a red X in the rule base.
3. Click **Disable Rule** to clear the selection.

**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
Creating New Rules

Data Loss Prevention by Scenario
Page 83

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. Open Data Loss Prevention > Policy.
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. Install the policy on the DLP gateway.

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”. This could be both the original data type and another data type - such as patient record + patient name who signed.

To specify complex data types for Exceptions:
1. In the Data column of the exception, click the plus button.
2. In the drop-down list, select the data types to add to the Exception.
3. Select the data types to add to the Exception.
4. Click Add.

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.
   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.

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.
Chapter 6

Fine Tuning

In This Chapter

Customized Deployment 85
Setting Rules to Prevent 86
Adding Data Types to Rules 86
Defining Email Addresses 97
Fine Tuning Source and Destination 98
Defining Protocols of DLP Rules 101

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. (It is recommended that such rules include notification to data owner and to user.)
Setting Rules to Prevent

To have full Data Loss Prevention, you might think that data transmissions with protected data should all be prevented from leaving the organization. However, putting all your rules to Prevent from the start will surely cause so many disruptions in mission-critical work of your organization, that the protection will become worse than meaningless. The best practice is to set rules to Prevent only after users have become familiar with the Organization Guidelines and audits of your logs have shown that automated prevention of user initiated actions is necessary - and then, only for specific data types, users, or other parameters.

Note - This is one reason why you might want to create a user group for new employees, so that they can learn from the UserCheck stage before having their transmissions automatically prevented.

Another user group you will probably find useful is one for terminating employees.

It is recommended that for rules set to Prevent that also have a High or Critical severity, you also set Email in the Track parameter. This will ensure that the data owners are notified by email as soon as such an incident is prevented.

To set a rule to Prevent:
1. Open Data Loss Prevention > Policy.
2. In the Action column of the rule to change, right-click and select Prevent.

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 heuristics - 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.

Defining Data Types

The optimal method for defining new data type representations is to use the Data Type Wizard.

First, review the predefined data types: you might not need to add more. If the data assets that you want to protect from leakage are not represented in the Data Types page, open the Data Type Wizard.

To add a new data type:
1. On the SmartDashboard, open the Data Loss Prevention tab.
2. Open Data Types and click New; or in Policy > Data column, double-click and in the Add Data Types window, click New.
   The Data Type Wizard opens.
3. Enter a name for the new data type.
4. Choose an option that defines the type of traffic that will be checked against a rule containing this data type.
5. Fill in the properties as required in the next step (each step is relevant to the option selected in the previous step).
6. Click **Finish**.

### 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, for example: patient records, credit history, court orders, utility bills, and customer account records. A template defines the headers, footers, seals, and formatting of associated documents; this is what makes all court orders, for example, look the same.
Create a data type that protects documents based on a specific template. Transmissions that contain a document that was based on the template are matched.

**Figure 6-6** Example of Template for Documents to be Protected by PCI

![Example of Template](image)

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.
   - It is recommended that you first set this slider quite low; the higher it is, the less the rule will catch. After completing the wizard, send a test email with such a document, and check the SmartView Tracker logs to see if the document was caught. Slowly increase the Similarity level until the rule is catching the documents you want. This will be different for each template.
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.

**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**

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 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 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.

Note - 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.
   
   It is recommended that you first set this to the highest reasonable value, and then lower it after auditing the SmartView Tracker 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 [R75.20 CPcode DLP Reference Guide](http://supportcontent.checkpoint.com/documentation_download?ID=12381).

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:**

```cpp
func rule_1 {
    foreach $recipient inside global:DESTS {
        foreach $comp inside CPMPETITORS_DOMAIN {
            if( casesuffix( $recipient, $comp ) ) {
                set_message_to_user(cat("The mail is sent to ", $recipient, "which is a competitor's mail address.")));
                set_track(TRACK_LOG);
                return quarantine();
            }
        }
    }
}
```
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.

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Properties</td>
<td>• <strong>Name</strong> - Name of the data type representation.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Comment</strong> - Optional comments and notes.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Categories</strong> - Optional assigned category tags, for grouping data types.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Flag</strong> - Optional custom flag to help management of a large Data Types list.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Follow Up</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Improve Accuracy</strong> - 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 <strong>Follow Up</strong>, to monitor its related incidents, or to <strong>No Flag</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Description</strong> - 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.</td>
</tr>
<tr>
<td>Custom CPcode</td>
<td>• <strong>Add</strong> - Click to add CPcode scripts. The default file type is <strong>cpc</strong>. See the R75.20 CPcode DLP Reference Guide (<a href="http://supportcontent.checkpoint.com/documentation_download?ID=12381">http://supportcontent.checkpoint.com/documentation_download?ID=12381</a>).</td>
</tr>
<tr>
<td></td>
<td>• <strong>View</strong> - Click to view a CPcode script in a text editor.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove</strong> - Click to remove CPcode scripts.</td>
</tr>
<tr>
<td>Compound</td>
<td>• <strong>Each one of these data types must be matched</strong> - All items in this list must be matched in the data, for the compound data type to match.</td>
</tr>
<tr>
<td></td>
<td>• <strong>None of these data types must be matched</strong> - If the data matches any item in this list, the compound data type does not match.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> items to a list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> selected item. (Changes made from here affect all compound data types and rules that use the edited data type).</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove</strong> items from a list.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Dictionary</td>
<td>• <strong>Replace</strong> - Click to browse to a different file.</td>
</tr>
<tr>
<td></td>
<td>• <strong>View</strong> - Click to view the file. Note that any changes you make here do not affect the file that is used by the data type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Save a Copy</strong> - Click to save the file under another name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>This data will be matched only if it contains at least</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> - 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.</td>
</tr>
<tr>
<td>Documents Based on a Corporate Template</td>
<td>• <strong>Replace</strong> - Click to browse to a different file.</td>
</tr>
<tr>
<td></td>
<td>• <strong>View</strong> - Click to view the file. Note that any changes you make here do not affect the file that is used by the data type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Save a Copy</strong> - Click to save the file under another name.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Similarity</strong> - 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.</td>
</tr>
<tr>
<td>File</td>
<td>• <strong>File</strong> - 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.</td>
</tr>
<tr>
<td></td>
<td>• <strong>The file type is any of these types</strong> - Click <strong>Add</strong>, and select a files type from the list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>The file name contains</strong> - Enter a string or regular expression to match against file names.</td>
</tr>
<tr>
<td></td>
<td>• <strong>The file size is larger than</strong> - Enter the threshold size in KB.</td>
</tr>
<tr>
<td>Group Members</td>
<td>• <strong>Add</strong> - 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 <strong>New</strong> to create a new data type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> - Open the properties window of the selected data type. When you click <strong>OK</strong> or <strong>Cancel</strong>, the Data Type Group window is still open.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove</strong> - Remove the selected data type from the group. The data type is not deleted.</td>
</tr>
<tr>
<td>Keywords or Phrases</td>
<td>• <strong>Specify keywords or phrases to search for</strong> - Enter the words to match data content.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Add</strong> - Click to add the keywords to the data type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Search List</strong> - Keywords in the data type.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Edit</strong> - Modify the selected word or phrase in the list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove</strong> - Remove the selected word or phrase from the list.</td>
</tr>
<tr>
<td></td>
<td>• <strong>All keywords and phrases must appear</strong> - Select to match data only if all the items in the Search List are found.</td>
</tr>
<tr>
<td></td>
<td>• <strong>At least number words must appear</strong> - Enter an integer to indicate number of items in Search List to match the Keyword data type.</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Pattern          | - **Type a pattern (regular expression)** - Enter the regular expression to match data content.  
|                  | - **Add** - Click to add the regular expression to the data type.          
|                  | - **Pattern List** - Regular expressions in the data type.                 
|                  | - **Edit** - Modify the selected regular expression in the list.           
|                  | - **Remove** - Remove the selected regular expression from the list.       
|                  | - **Number of occurrences** - Enter an integer to set how many matches between any of the patterns and the data are needed to recognize the data as matching the data type. |
| Similarity       | - **Similarity** - Move the slider to determine how closely a document must match the given template or form to be recognized as matching the data type. This will match header and footer content, as well as boiler-plate text. |
| Threshold (dictionary) | - **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) | - **Number of occurrences** - Enter an integer to set how many matches in the data are needed to recognize the data as matching the data type. |
| Threshold (keywords) | This data will be matched only if it contains:  
|                  | - **All keywords and phrases** - Select to match data only if all the items in the Search List are found.  
|                  | - **At least number keywords or phrases** - Enter an integer to indicate number of items in Search List to match the Keyword data type. |
| Threshold (recipients) | This data will be matched only if the email contains:  
|                  | - **At least number 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 number external recipients** - If an email is sent to a large distribution list, even if it contains numerous internal recipients, it should be recognized as an email meant for people outside the organization. In this field, enter maximum number of email addresses external to My Organization, that if more external recipients are included, the email will match a rule. |
| Threshold (External BCC) | This data will be matched only if the email contains at least:  
|                  | - **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. |
Adding Data Types to Rules

Necessary Sections

### Section: Weighted Keywords or Phrases

<table>
<thead>
<tr>
<th>Weighted Keywords or Phrases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Keyword Text</strong> - List of current keywords or regular expressions in the list of weighted keywords. To add more, click <strong>New</strong>. To change the selected keyword or regular expression, click <strong>Edit</strong>. The Edit Word window opens.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Weight</strong> - 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.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Max. Weight</strong> - 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.)</td>
<td></td>
</tr>
<tr>
<td>• <strong>RegEx?</strong> - Whether the item is a regular expression.</td>
<td></td>
</tr>
<tr>
<td>• <strong>Threshold</strong> - When the weights of all items in the list are added together, if they pass this threshold, the transmission is matched.</td>
<td></td>
</tr>
</tbody>
</table>

**To edit a data type:**
1. On the SmartDashboard, 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.

For example, you could create a group of data types that protect your organization from leaking personal contact information, to comply with privacy laws. The data type group would include various built-in data types for personal names of different countries, last names, personal email addresses, and so on. Using the data type group, you can create and maintain rules more efficiently.

Data type groups are matched on OR. If data matches any of the data types in the group, the data type group is matched.

**To create a data type group:**
1. In **Data Types**, click the arrow of **New** and select **Data Type Group**.
   The **Group Data Type** window opens.
2. Enter a name for the group.
3. Click **Add** and select the data types that will be in this data type group.
   If relevant, add Data Owners to the group.
4. Click **OK**.

### 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.

**Note** - You can add more than one CPcode script. All of the scripts must match the keywords or phrases to be recognized as matching the data type.

**To add advanced matching data type CPcode script:**
1. In **Data Types**, select a data type and click **Edit**.
   The **Data Type** window opens.
2. Click the Advanced Matching node.

3. 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 R75.20 CPcode DLP Reference Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12381).
   - **View** - Click to view a CPcode script in a text editor.
   - **Remove** - Click to remove CPcode scripts.

4. Click OK.

### 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.

When you use CPcode scripts here as match criteria, you get a more advanced level of improved accuracy on matched data types. When you set more than one CPcode script, data types with specified CPcode scripts are matched on AND. If data matches all of the CPcode scripts, the data type is matched. If the CPCode script file has a corresponding value file (for a constant value) or csv file, add it here.

For example, you can add a CPcode script that matches data types that occur during work hours (09:00 - 17:00) on work days.

**To add a post match data type CPcode script:**

1. In Data Types, select a data type and click Edit. The Data Type window opens.
2. Click the Advanced Matching node.
3. 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. See the R75.20 CPcode DLP Reference Guide (http://supportcontent.checkpoint.com/documentation_download?ID=12381).
   - **View** - Click to view a CPcode script in a text editor.
   - **Remove** - Click to remove CPcode scripts.
4. Click OK.

### 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 SmartView Tracker or SmartEvent 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 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.

You might want to export data types as a recovery measure: recover a data type that you or another DLP administrator deleted.

**To export a data type:**
1. Open Data Loss Prevention > Data Types.
2. Select the data type to export.
3. Click Actions > Export.
4. Save it as a file with the dlp_dt extension.

**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. Open Data Loss Prevention > Data Types.
2. Click Actions > Import.
3. Select the dlp_dt file holding the data type that you want.

**Defining Email Addresses**

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

For example:
- Addresses to which data must be sent, or should never be sent.
- Domains that are external but should be considered internal for DLP.
- Domains that are internal but should be checked for unauthorized data transfer (not everyone in your organization should have access to the data of everyone else).

You can create Email Address objects. Each object holds a list of addresses or domains, or both, where the list can contain one or more items. After you create an Email Address object, you can add it to:
- Rules as the Source or Destination.
- Exceptions to rules.
  For example, the administrator of a hospital makes an exception to a rule that prevents patient records from being sent outside the organization. The exception says to allow patient records to be sent to the email address of the social worker.
Note - All the addresses in the object are a unit. You cannot choose to use some email addresses of an object and not others.

Notes about Domains:
- When adding domains, do not use the @ sign. A valid domain example is: example.com
- If you add a domain, it will catch all sub domains as well. For example, if the domain is example.com, email addresses such as jsmith@uk.example.com are also considered as part of My Organization.

To define email addresses and domains for use in rules:
1. Expand Additional Settings > Email Addresses.
2. Click New.
   The Email Addresses window opens.
3. Enter a name for this group of email addresses (even if it includes only one address) or domain.
4. Enter the address or domain.
5. Add as many email addresses and domains as needed for this list.

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 SmartDashboard, and you can fine tune user definitions specifically for DLP.

Note - SMTP only matches users, groups, and email addresses. HTTP and FTP only match Network objects. If needed, you can add a network and a user group to a rule.

From version R75.20 and higher, you can also use these objects as the Destination of the rule:
- **My Organization** - When the system is configured to work with the Exchange Security Agent, use this object to define the entire internal organization including emails from users in the Source object.
- **Any** - When the system is configured to work with the Exchange Security Agent, use this object to define any destination. This includes:
  - All users in the internal organization.
  - Any destination outside of the organization.
- **Domain** - Defines a domain used in HTTP and FTP posts. For example, to examine Facebook posts that contain company confidential source code, create a rule with:
  - Source = My Organization
  - Destination = .facebook.com (domain object)
  - Data Type = Source Code (built-in Data Type)

  Note - These objects are not enforced in rules installed on gateway versions before R75.20. In such cases, policy installation might fail with warnings and errors. To avoid such errors, make sure to specify gateway versions that are R75.20 and higher in the Install On column.

To create a domain object:
1. Open the Firewall tab > Network Objects tree > New > Domain.
2. Enter the URL of the domain and click OK.
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 difference between Outside Source (external to a source that is a subset of My Organization) and Outside of My Org (external to My Organization).

To enable use of Outside Source, the DLP gateway must be functioning in front of the servers that handle the data transmission protocols. For example, to use Outside on SMTP transmissions, the DLP gateway must inspect the emails before the Mail Server does.

Alternatively, the Destination of the rule could be another user, group, host, 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][0-9][0-9] and employee names)

   ![Figure 6-7 Prevent Finance from Leaking Salaries](image)

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)

   ![Figure 6-8 Prevent Customer Names Leaking to Temps](image)

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 DSS\(^1\) 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 SmartDashboard, open the Data Loss Prevention tab.
3. Click My Organization.
4. In the Networks area, 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 OK.

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. For example:

• If your organization includes a large number of temporary users and small number of permanent users and machines
• If system administration has been known to take time to remove terminated aliases
• If your domain is being changed

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.

\(^1\) Payment Card Industry Data Security Standard - Copyright of PCI Security Standards Council, LLC.
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 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 SmartDashboard, select Manage > Services. The Services window opens.
2. Click New > TCP. The TCP Service Properties window opens.
3. Provide a name for the web service.
4. Provide the port or port range.
5. Click Advanced. The Advanced TCP Service Properties window opens.
7. In the Protocol Type list, select HTTP.
8. Click OK.
Appendix A

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 103
Internal Firewall Policy for a Dedicated DLP Gateway 104
Advanced Expiration Handling 105
Advanced SMTP Quotas 106
Advanced FTP and HTTP Quotas 107
Advanced User Notifications 108
Troubleshooting: Incidents Do Not Expire 108
Troubleshooting: Mail Server Full 108
Gateway Cleanup of Expired Data 109
Gateway Cleanup of All Captured Data 110
Customizing DLP User-Related Notifications 111
Supporting LDAP Servers with UTF-8 Records 113
Editing Extreme Condition Values 114
Editing Exchange Security Agent Values 115
Configuring HTTP Inspection on All Ports 116
Defining New File Types 117
Server Certificates 132

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 SmartDashboard 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.
According to the Firewall policy - Allow access according to Firewall Rule Base rules defined by the SmartDashboard administrator. Use this option if you want to decide which ports to open for DLP. The applicable ports are:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Service</th>
<th>TCP Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Portal</td>
<td>TCP HTTP</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>TCP HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>UserCheck</td>
<td>TCP</td>
<td>18300</td>
</tr>
<tr>
<td></td>
<td>TCP HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>Reply-to-email</td>
<td>TCP HTTPS</td>
<td>25</td>
</tr>
</tbody>
</table>

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 SmartDashboard. It is also not related to the Firewall Policy which is explicitly defined by the administrator in the Firewall tab of SmartDashboard.

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:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Service</th>
<th>TCP Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Portal</td>
<td>TCP HTTP</td>
<td>80</td>
</tr>
<tr>
<td></td>
<td>TCP HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>UserCheck</td>
<td>TCP</td>
<td>18300</td>
</tr>
<tr>
<td></td>
<td>TCP HTTPS</td>
<td>443</td>
</tr>
<tr>
<td>WebUI</td>
<td>TCP</td>
<td>4434</td>
</tr>
<tr>
<td>Reply-to-email</td>
<td>SMTP</td>
<td>25</td>
</tr>
<tr>
<td>Secure Shell</td>
<td>SSH</td>
<td>22</td>
</tr>
<tr>
<td>ICMP</td>
<td>ICMP requests</td>
<td></td>
</tr>
</tbody>
</table>
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.
   If you decrease this value, it is recommended that you 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 SmartDashboard computer, run
      `C:\Program Files\CheckPoint\SmartConsole\R75.20\PROGRAM\GuiDBEdit.exe`
   b) Log in with your SmartDashboard 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 SmartView Tracker 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
   ```
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. By default, this is 3:45 AM, to ensure that gateway maintenance does not 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 ensure that disk usage does not unduly build up over time. However, some unnecessary files may be left on the disk. For example, if the gateway fails, large crash logs may be kept.

The cleanup process of DLP can be customized with the configuration files:

- `$FWDIR/conf/mail_security_config`
- `$DLPDIR/config/dlp_cleanup_files_list.conf`

⚠️ **Important** - It is not recommended that you de-activate the cleanup process. However, if you must do so, set the value of `dlp_delete_redundant_files_active` to 0.

<table>
<thead>
<tr>
<th><code>mail_security_config</code> Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dlp_delete_redundant_files_interval</code></td>
<td>How often (in minutes) cleanup runs. Default = 1440 (24 hours)</td>
</tr>
<tr>
<td><code>dlp_delete_redundant_files_execution_time</code></td>
<td>Exact time (on 24 hour clock) when cleanup runs. Default = 4:45 (when gateway load is low)</td>
</tr>
<tr>
<td><code>dlp_delete_redundant_files_age_group1_files</code></td>
<td>Minimum age of UserCheck data files, which should be maintained on the disk until their handling expiration arrives. Default = 0 (use the <code>expiration_time_in_days</code> value) Note: This value does not change the expiration of incidents; it changes when data of expired incidents is removed.</td>
</tr>
<tr>
<td><code>dlp_delete_redundant_files_age_group2_files</code></td>
<td>Minimum age of files in <code>/proc</code> Default = 15 minutes</td>
</tr>
<tr>
<td><code>dlp_delete_redundant_files_age_group3_files</code></td>
<td>Minimum age of files in <code>$FWDIR/tmp/dlp</code> Default = 15 minutes</td>
</tr>
</tbody>
</table>

The `dlp_cleanup_files_list.conf` file is a list of scan commands with the following syntax:

```
scan [CHECK_DB | -] path mask scale age
```
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 $DLPDIR/backend/conf/, edit these files:

<table>
<thead>
<tr>
<th>File</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>dictionary_en_us.conf</td>
<td>Basic dictionary</td>
</tr>
<tr>
<td>about_to_expire_notification_tmplt_en_us.html</td>
<td>Email notifications</td>
</tr>
<tr>
<td>data_owners_mail_notification_tmplt_en_us.html</td>
<td></td>
</tr>
<tr>
<td>detect_mail_notification_tmplt_en_us.html</td>
<td></td>
</tr>
</tbody>
</table>

Customizing DLP User-Related Notifications

These procedures explain how to customize backend files to change the text of user-related notifications.

To clean up everything, even user captured data, change the flag to a dash (-):

```
scan -
```

**Note** - 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.

<table>
<thead>
<tr>
<th>age Macros</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2</td>
<td>group1 age (in days): UserCheck data files, value taken from dlp_delete_redundant_files_age_group1_files</td>
</tr>
<tr>
<td>$3</td>
<td>group2 age (in minutes): /proc files, value taken from dlp_delete_redundant_files_age_group2_files</td>
</tr>
<tr>
<td>$4</td>
<td>group3 age (in minutes): /tmp/dlp files, value taken from dlp_delete_redundant_files_age_group3_files</td>
</tr>
</tbody>
</table>
Customizing DLP User-Related Notifications

2. To apply the changes, do 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

**Figure 6-9** UserCheck Example

<table>
<thead>
<tr>
<th>File</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>expired_owners_mail_tmplt_en_us.html</td>
<td></td>
</tr>
<tr>
<td>expired_sender_mail_tmplt_en_us.html</td>
<td></td>
</tr>
<tr>
<td>failure_mail_notification_en_us.html</td>
<td></td>
</tr>
<tr>
<td>prevent_mail_notification_tmplt_en_us.html</td>
<td></td>
</tr>
<tr>
<td>quarantine_mail_notification_tmplt_en_us.html</td>
<td></td>
</tr>
<tr>
<td>quota_deleted_notification_tmplt_en_us.html</td>
<td></td>
</tr>
<tr>
<td>released_mail_notification_tmplt_en_us.html</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>File</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>inform_ftp_uc_notification_tmplt_en_us.html</td>
<td>ftp protocol when the action is inform</td>
</tr>
<tr>
<td>inform_http_uc_notification_tmplt_en_us.html</td>
<td>http protocol when the action is inform</td>
</tr>
<tr>
<td>inform_smtp_uc_notification_tmplt_en_us.html</td>
<td>smtp protocol when the action is inform</td>
</tr>
<tr>
<td>prevent_ftp_uc_notification_tmplt_en_us.html</td>
<td>ftp protocol when the action is prevent</td>
</tr>
<tr>
<td>prevent_http_uc_notification_tmplt_en_us.html</td>
<td>http protocol when the action is prevent</td>
</tr>
<tr>
<td>prevent_smtp_uc_notification_tmplt_en_us.html</td>
<td>smtp protocol when the action is prevent</td>
</tr>
<tr>
<td>quarantine_ftp_uc_notification_tmplt_en_us.html</td>
<td>ftp protocol when the action is ask</td>
</tr>
</tbody>
</table>
To apply the changes, do **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: `&quot;` (double quote), `&$36;` (dollar sign), `&#$92;` (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 SmartDashboard:**

1. Open SmartDashboard > 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. To apply the changes, do **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 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 SmartDashboard 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. Do Install Policy on the DLP gateway.
Editing Extreme Condition Values

You can configure two options for extreme conditions in SmartDashboard 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 SmartDashboard 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 SmartDashboard computer, run
      C:\Program Files\CheckPoint\SmartConsole\R75.20\PROGRAM\GuiDBEdit.exe
   b) Log in with your SmartDashboard 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:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_high_watermark</td>
<td>Threshold for stopping inspection on heavy load. When CPU load is more than the defined threshold, DLP bypasses the protocols set to True.</td>
<td>90%</td>
</tr>
<tr>
<td>cpu_low_watermark</td>
<td>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.</td>
<td>70%</td>
</tr>
<tr>
<td>prefer_connectivity_on_heavy_load_protocols &gt; ftp_inspection</td>
<td>By default, DLP bypasses FTP traffic on heavy load. If you change this to false, FTP is inspected on heavy load.</td>
<td>true</td>
</tr>
</tbody>
</table>
## 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 41) in the GuiDBEdit application.

### To edit Exchange Security Agent values:

1. Open GuiDBedit:
   a) On the SmartDashboard computer, run `C:\Program Files\CheckPoint\SmartConsole\R75.20\PROGRAM\GuiDBEdit.exe`
   b) Log in with your SmartDashboard credentials.
2. In the left pane, select **Table > Other > dlp_data_tbl**.
3. In the right pane, select the **Exchange Agent object** that represents the SmartDashboard Exchange Security Agent object.
4. In the bottom pane, in the **Field Name** column, you can configure these fields:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefer_connectivity_on_heavy_load_protocols &gt; http_inspection</td>
<td>By default, DLP <strong>bypasses</strong> HTTP traffic on heavy load. If you change this to false, HTTP is inspected on heavy load.</td>
<td>true</td>
</tr>
<tr>
<td>prefer_connectivity_on_heavy_load_protocols &gt; smtp_inspection</td>
<td>By default, DLP <strong>inspects</strong> SMTP traffic on heavy load. If you change this to true, SMTP is bypassed on heavy load.</td>
<td>false</td>
</tr>
</tbody>
</table>

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

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

7. Install policy in SmartDashboard.

**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.

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).

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>is_tap_mode</td>
<td>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.</td>
<td>False</td>
</tr>
<tr>
<td>scan_mails_received_from_sender_out_of_my_organ</td>
<td>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.</td>
<td>False</td>
</tr>
<tr>
<td>scan_mails_send_to_recipient_from_my_organ</td>
<td>If to scan internal traffic.</td>
<td>True</td>
</tr>
<tr>
<td>scan_mails_send_to_recipient_out_my_organ</td>
<td>If to scan messages sent outside of the organization.</td>
<td>True</td>
</tr>
<tr>
<td>dont_scan_smtp</td>
<td>Scans messages received by the Exchange server in SMTP. This means that messages in SMTP arriving from the same domain will be scanned.</td>
<td>False</td>
</tr>
</tbody>
</table>

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

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

6. In the left pane, select Network Objects > Network Objects > <Security Gateway object > > data_loss_prevention_blade_settings to configure this field:

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>encrypt_exchange_traffic</td>
<td>The Exchange Security Agent sends traffic to the Security Gateway encrypted in TLS.</td>
<td>True</td>
</tr>
</tbody>
</table>

7. Install policy in SmartDashboard.

Configuring HTTP Inspection on All Ports
To enable HTTP inspection on all ports:
1. Open SmartDashboard.
2. In the DLP gateway object, open Data Loss Prevention > Protocols > default protocols.
3. Select Enable HTTP inspection on nonstandard ports.
4. Click OK.

Note - When you set HTTP inspection on all ports there is a performance impact.

Defining New File Types

You can define a Data Type based on a file type with the "File Attributes" Data Type. This Data Type offers several file type families.

To add a new file type to the File Data Type options:
1. Open GUIDBEdit:
   a) On the SmartDashboard computer, run
      \Program Files\CheckPoint\SmartConsole\R75.20\PROGRAM\GuiDBEdit.exe
   b) Log in with your SmartDashboard credentials.
2. Under Other > dlp_data_tbl create a new object of file_type type.
3. Name the object file_type_<ID>. For the full list of IDs see the table below.
4. Enter a name for the file type in the visual_string field.
5. Enter a description for the file type in the description field (optional).
6. Save the new created object and close GUIDBEdit.
7. Install the policy.

<table>
<thead>
<tr>
<th>ID</th>
<th>File Type</th>
<th>ID</th>
<th>File Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Word for DOS 4.x</td>
<td>2</td>
<td>Word for DOS 5.x</td>
</tr>
<tr>
<td>3</td>
<td>Wordstar 5.0</td>
<td>4</td>
<td>Wordstar 4.0</td>
</tr>
<tr>
<td>5</td>
<td>Wordstar 2000</td>
<td>6</td>
<td>WordPerfect 5.0</td>
</tr>
<tr>
<td>7</td>
<td>MultiMate 3.6</td>
<td>8</td>
<td>MultiMate Advantage 2</td>
</tr>
<tr>
<td>9</td>
<td>IBM DCA/RFT</td>
<td>10</td>
<td>IBM DisplayWrite 2 or 3</td>
</tr>
<tr>
<td>11</td>
<td>SmartWare II</td>
<td>12</td>
<td>Samna</td>
</tr>
<tr>
<td>13</td>
<td>PFS: Write A</td>
<td>14</td>
<td>PFS: Write B</td>
</tr>
<tr>
<td>15</td>
<td>Professional Write 1</td>
<td>16</td>
<td>Professional Write 2</td>
</tr>
<tr>
<td>17</td>
<td>IBM Writing Assistant</td>
<td>18</td>
<td>First Choice WP</td>
</tr>
<tr>
<td>19</td>
<td>WordMarc</td>
<td>20</td>
<td>Navy DIF</td>
</tr>
<tr>
<td>21</td>
<td>Volkswriter</td>
<td>22</td>
<td>DEC DX 3.0 and below</td>
</tr>
<tr>
<td>23</td>
<td>Sprint</td>
<td>24</td>
<td>WordPerfect 4.2</td>
</tr>
<tr>
<td>25</td>
<td>Total Word</td>
<td>26</td>
<td>Wang IWP</td>
</tr>
<tr>
<td>27</td>
<td>Wordstar 5.5</td>
<td>28</td>
<td>Wang WPS</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>----</td>
<td>------------------------------------</td>
<td>----</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>29</td>
<td>Rich Text Format (RTF)</td>
<td>30</td>
<td>Mac Word 3.0</td>
</tr>
<tr>
<td>31</td>
<td>Mac Word 4.0</td>
<td>32</td>
<td>Mass 11</td>
</tr>
<tr>
<td>33</td>
<td>MacWrite II</td>
<td>34</td>
<td>XyWrite / Nota Bene</td>
</tr>
<tr>
<td>35</td>
<td>IBM DCA/FFT</td>
<td>36</td>
<td>Mac WordPerfect 1.x</td>
</tr>
<tr>
<td>37</td>
<td>IBM DisplayWrite 4</td>
<td>38</td>
<td>Mass 11</td>
</tr>
<tr>
<td>39</td>
<td>WordPerfect 5.1/5.2</td>
<td>40</td>
<td>MultiMate 4.0</td>
</tr>
<tr>
<td>41</td>
<td>Q&amp;A Write</td>
<td>42</td>
<td>MultiMate Note</td>
</tr>
<tr>
<td>43</td>
<td>PC File 5.0 Doc</td>
<td>44</td>
<td>Lotus Manuscript 1.0</td>
</tr>
<tr>
<td>45</td>
<td>Lotus Manuscript 2.0</td>
<td>46</td>
<td>Enable WP 3.0</td>
</tr>
<tr>
<td>47</td>
<td>Windows Write</td>
<td>48</td>
<td>Microsoft Works 1.0</td>
</tr>
<tr>
<td>49</td>
<td>Microsoft Works 2.0</td>
<td>50</td>
<td>Wordstar 6.0</td>
</tr>
<tr>
<td>51</td>
<td>OfficeWriter</td>
<td>52</td>
<td>Mac Word 4.x Complex</td>
</tr>
<tr>
<td>53</td>
<td>IBM DisplayWrite 5</td>
<td>54</td>
<td>Word for Windows 1.x</td>
</tr>
<tr>
<td>55</td>
<td>Word for Windows 1.x complex</td>
<td>56</td>
<td>Ami</td>
</tr>
<tr>
<td>57</td>
<td>Ami Pro</td>
<td>58</td>
<td>First Choice 3 WP</td>
</tr>
<tr>
<td>59</td>
<td>Mac WordPerfect 2.0</td>
<td>60</td>
<td>Mac Works 2.0 WP</td>
</tr>
<tr>
<td>61</td>
<td>Professional Write Plus</td>
<td>62</td>
<td>Legacy</td>
</tr>
<tr>
<td>63</td>
<td>Signature</td>
<td>64</td>
<td>Wordstar for Windows</td>
</tr>
<tr>
<td>65</td>
<td>Word for Windows 2.0</td>
<td>66</td>
<td>JustWrite 1.0</td>
</tr>
<tr>
<td>67</td>
<td>Wordstar 7.0</td>
<td>68</td>
<td>Windows Works WP</td>
</tr>
<tr>
<td>69</td>
<td>JustWrite 2.0</td>
<td>70</td>
<td>Ami [Clip]</td>
</tr>
<tr>
<td>71</td>
<td>Legacy [Clip]</td>
<td>72</td>
<td>Pro Write Plus [Clip]</td>
</tr>
<tr>
<td>73</td>
<td>Mac Word 5.x</td>
<td>74</td>
<td>Enable WP 4.x</td>
</tr>
<tr>
<td>75</td>
<td>WordPerfect 6.0</td>
<td>76</td>
<td>Word for DOS 6.x</td>
</tr>
<tr>
<td>77</td>
<td>DEC DX 3.1</td>
<td>78</td>
<td>WordPerfect Encrypted</td>
</tr>
<tr>
<td>79</td>
<td>Q&amp;A Write 3</td>
<td>80</td>
<td>Mac WordPerfect 3.0</td>
</tr>
<tr>
<td>81</td>
<td>CEO Word</td>
<td>82</td>
<td>Word 6.0 or 7.0</td>
</tr>
<tr>
<td>83</td>
<td>WordPerfect 5.1 Far East</td>
<td>84</td>
<td>Ichitaro 3.x</td>
</tr>
<tr>
<td>85</td>
<td>Ichitaro 4.x/5.x/6.x</td>
<td>86</td>
<td>Word for Windows 1.2 J</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------</td>
<td>-----</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>87</td>
<td>Word for Windows 5.0 J</td>
<td>88</td>
<td>Matsu 4</td>
</tr>
<tr>
<td>89</td>
<td>Matsu 5</td>
<td>90</td>
<td>P1 Japan</td>
</tr>
<tr>
<td>91</td>
<td>Rich Text Format Japan</td>
<td>92</td>
<td>CEO Write</td>
</tr>
<tr>
<td>93</td>
<td>Windows Works 3.0 WP</td>
<td>94</td>
<td>Microsoft WordPad</td>
</tr>
<tr>
<td>95</td>
<td>WP/Novell Unknown Format</td>
<td>96</td>
<td>Word for Windows 2.0 Object</td>
</tr>
<tr>
<td>97</td>
<td>WordPerfect 6.1 - 12.0 / X3</td>
<td>98</td>
<td>Fulcrum Document Format</td>
</tr>
<tr>
<td>99</td>
<td>Europa Fulcrum 5</td>
<td>100</td>
<td>Europa Fulcrum 6</td>
</tr>
<tr>
<td>101</td>
<td>Internet HTML</td>
<td>102</td>
<td>Word 7.0</td>
</tr>
<tr>
<td>103</td>
<td>Arehangeul</td>
<td>104</td>
<td>Hana</td>
</tr>
<tr>
<td>105</td>
<td>Windows Works 4.0 WP</td>
<td>106</td>
<td>PerfectWorks for Windows</td>
</tr>
<tr>
<td>107</td>
<td>WordPerfect 7.0/8.0/10.0</td>
<td>108</td>
<td>WordPro 96</td>
</tr>
<tr>
<td>109</td>
<td>HTML - Central European</td>
<td>110</td>
<td>HTML - Japanese (ShiftJIS)</td>
</tr>
<tr>
<td>111</td>
<td>HTML - Japanese (EUC)</td>
<td>112</td>
<td>HTML - Chinese (Big5)</td>
</tr>
<tr>
<td>113</td>
<td>HTML - Chinese (EUC)</td>
<td>114</td>
<td>HTML - Chinese (GB)</td>
</tr>
<tr>
<td>115</td>
<td>HTML - Korean (Hangul)</td>
<td>116</td>
<td>HTML - Cyrillic (ANSI 1251)</td>
</tr>
<tr>
<td>117</td>
<td>HTML - Cyrillic (KOI8-R)</td>
<td>118</td>
<td>Text - Cyrillic (ANSI 1251)</td>
</tr>
<tr>
<td>119</td>
<td>Cyrillic (KOI8-R)</td>
<td>120</td>
<td>WWRITE - Japan SJIS</td>
</tr>
<tr>
<td>121</td>
<td>WWRITE - Chinese GB</td>
<td>122</td>
<td>WWRITE - Hangul</td>
</tr>
<tr>
<td>123</td>
<td>WWRITE - Chinese BIG5</td>
<td>124</td>
<td>Digital WPS Plus</td>
</tr>
<tr>
<td>125</td>
<td>Mac Word 6</td>
<td>126</td>
<td>Microsoft Word 97/98</td>
</tr>
<tr>
<td>127</td>
<td>Rainbow</td>
<td>128</td>
<td>Interleaf 6</td>
</tr>
<tr>
<td>129</td>
<td>MIFF 3.0</td>
<td>130</td>
<td>MIFF 4.0</td>
</tr>
<tr>
<td>131</td>
<td>MIFF 5.0</td>
<td>132</td>
<td>Text Mail</td>
</tr>
<tr>
<td>133</td>
<td>Mac Word 97</td>
<td>134</td>
<td>Interleaf Japan</td>
</tr>
<tr>
<td>135</td>
<td>MIFF 3.0 Japan</td>
<td>136</td>
<td>MIFF 4.0 Japan</td>
</tr>
<tr>
<td>137</td>
<td>MIFF 5.0 Japan</td>
<td>138</td>
<td>MIFF 5.5</td>
</tr>
<tr>
<td>139</td>
<td>WordPerfect 8.0/10.0</td>
<td>140</td>
<td>Ichitaro 8.x/9.x/10.x/11.x/12.x/13.x/2004</td>
</tr>
<tr>
<td>141</td>
<td>vCard</td>
<td>142</td>
<td>HTML - Cascading Style Sheets</td>
</tr>
<tr>
<td>143</td>
<td>MS Outlook</td>
<td>144</td>
<td>Pocket Word</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------</td>
<td>-----</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>145</td>
<td>WordPro 97/Millennium</td>
<td>146</td>
<td>Microsoft Word 2000</td>
</tr>
<tr>
<td>147</td>
<td>Word 2000 HTML</td>
<td>148</td>
<td>Excel 2000 HTML</td>
</tr>
<tr>
<td>149</td>
<td>PowerPoint 2000 HTML</td>
<td>150</td>
<td>Extensible Markup Language (XML)</td>
</tr>
<tr>
<td>151</td>
<td>Wireless Markup Language (WML)</td>
<td>152</td>
<td>WMLB</td>
</tr>
<tr>
<td>153</td>
<td>HTML - Japanese (JIS)</td>
<td>154</td>
<td>WML - Chinese (Big5)</td>
</tr>
<tr>
<td>155</td>
<td>WML - Chinese (EUC)</td>
<td>156</td>
<td>WML - Chinese (GB)</td>
</tr>
<tr>
<td>157</td>
<td>WML - Cyrillic (ANSI 1251)</td>
<td>158</td>
<td>WML - Cyrillic (KOI8-R)</td>
</tr>
<tr>
<td>159</td>
<td>WML - Japanese (JIS)</td>
<td>160</td>
<td>WML - Japanese (ShiftJIS)</td>
</tr>
<tr>
<td>161</td>
<td>WML - Japanese (EUC)</td>
<td>162</td>
<td>WML - Korean (Hangul)</td>
</tr>
<tr>
<td>163</td>
<td>WML - Central European</td>
<td>164</td>
<td>WML – CSS</td>
</tr>
<tr>
<td>165</td>
<td>StarOffice 5.2 Writer</td>
<td>166</td>
<td>MIFF 6.0</td>
</tr>
<tr>
<td>167</td>
<td>MIFF 6.0 Japan</td>
<td>168</td>
<td>MIFF</td>
</tr>
<tr>
<td>169</td>
<td>Java Script</td>
<td>170</td>
<td>ASCII Text</td>
</tr>
<tr>
<td>171</td>
<td>Handheld Device Markup Language (HDML)</td>
<td>172</td>
<td>Compact HTML (CHTML)</td>
</tr>
<tr>
<td>173</td>
<td>XHTML Basic</td>
<td>174</td>
<td>AvantGo HTML</td>
</tr>
<tr>
<td>175</td>
<td>Web Clipping Application (WCA) HTML</td>
<td>176</td>
<td>SearchML</td>
</tr>
<tr>
<td>177</td>
<td>Pocket Word - Pocket PC</td>
<td>178</td>
<td>Wireless HTML</td>
</tr>
<tr>
<td>179</td>
<td>Hangul 97 Word Processor</td>
<td>180</td>
<td>Hangul 2002 - 2007 Word Processor</td>
</tr>
<tr>
<td>181</td>
<td>Internet HTML – Unicode</td>
<td>182</td>
<td>XML With Doctype HTML</td>
</tr>
<tr>
<td>184</td>
<td>EBCDIC encoded Text</td>
<td>185</td>
<td>Microsoft Word 2002</td>
</tr>
<tr>
<td>186</td>
<td>Microsoft Word 2003/2004</td>
<td>187</td>
<td>Internet Message</td>
</tr>
<tr>
<td>188</td>
<td>StarOffice 6 &amp; 7 Writer</td>
<td>189</td>
<td>Microsoft Outlook PST/OST 97/2000/XP</td>
</tr>
<tr>
<td>190</td>
<td>XHTML</td>
<td>191</td>
<td>Microsoft Works 2000</td>
</tr>
<tr>
<td>192</td>
<td>Internet Mail Message</td>
<td>193</td>
<td>Internet News Message</td>
</tr>
<tr>
<td>194</td>
<td>Outlook Express News Message</td>
<td>195</td>
<td>Outlook Express Mail Message</td>
</tr>
<tr>
<td>196</td>
<td>vCalendar</td>
<td>197</td>
<td>Transport-Neutral Encapsulation Format(TNEF)</td>
</tr>
<tr>
<td>198</td>
<td>MHTML (Web Archive)</td>
<td>199</td>
<td>Search HTML</td>
</tr>
<tr>
<td>200</td>
<td>Search Text</td>
<td>201</td>
<td>PST Fields File</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------</td>
<td>-----</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>202</td>
<td>Microsoft Outlook PST/OST 2003/2007</td>
<td>203</td>
<td>Microsoft Outlook PAB</td>
</tr>
<tr>
<td>204</td>
<td>SearchML 20</td>
<td>205</td>
<td>SearchML 30</td>
</tr>
<tr>
<td>206</td>
<td>Yahoo! Messenger Archive</td>
<td>207</td>
<td>Microsoft Word XML 2003</td>
</tr>
<tr>
<td>208</td>
<td>MS Office 12 Word format</td>
<td>209</td>
<td>StarOffice 8/Open Office 2.x Writer</td>
</tr>
<tr>
<td>210</td>
<td>SearchML 31</td>
<td>211</td>
<td>Outlook Form Template</td>
</tr>
<tr>
<td>212</td>
<td>Microsoft Word 2007</td>
<td>213</td>
<td>Password Protected Microsoft Word 2007</td>
</tr>
<tr>
<td>214</td>
<td>Microsoft Word 2007 Template</td>
<td>215</td>
<td>SearchML 32</td>
</tr>
<tr>
<td>216</td>
<td>DRM protected Unknown</td>
<td>217</td>
<td>DRM protected Microsoft Word</td>
</tr>
<tr>
<td>218</td>
<td>DRM protected Microsoft Word 2007</td>
<td>219</td>
<td>File sealed by Oracle IRM</td>
</tr>
<tr>
<td>220</td>
<td>Extensible Metadata Platform</td>
<td>221</td>
<td>SearchML 33</td>
</tr>
<tr>
<td>222</td>
<td>PHTML</td>
<td>223</td>
<td>Open Office Writer 6</td>
</tr>
<tr>
<td>224</td>
<td>Open Office Writer 8</td>
<td>225</td>
<td>IBM Lotus Symphony Document</td>
</tr>
<tr>
<td>230</td>
<td>Smart Database</td>
<td>231</td>
<td>DBase III</td>
</tr>
<tr>
<td>232</td>
<td>DBase IV or V</td>
<td>233</td>
<td>Framework III</td>
</tr>
<tr>
<td>234</td>
<td>Microsoft Works DB</td>
<td>235</td>
<td>DataEase 4.x</td>
</tr>
<tr>
<td>236</td>
<td>Paradox 2 or 3</td>
<td>237</td>
<td>Paradox 3.5</td>
</tr>
<tr>
<td>238</td>
<td>Q&amp;A Database</td>
<td>239</td>
<td>Reflex</td>
</tr>
<tr>
<td>240</td>
<td>R:Base System V</td>
<td>241</td>
<td>R:Base 5000</td>
</tr>
<tr>
<td>242</td>
<td>R:Base File 1</td>
<td>243</td>
<td>R:Base File 3</td>
</tr>
<tr>
<td>244</td>
<td>First Choice DB</td>
<td>245</td>
<td>Mac Works 2.0 DB</td>
</tr>
<tr>
<td>246</td>
<td>Windows Works DB</td>
<td>247</td>
<td>Paradox</td>
</tr>
<tr>
<td>248</td>
<td>Microsoft Access</td>
<td>249</td>
<td>CEO Decision Base</td>
</tr>
<tr>
<td>250</td>
<td>Windows Works 3.0 DB</td>
<td>251</td>
<td>Windows Works 4.0 DB</td>
</tr>
<tr>
<td>252</td>
<td>Microsoft Access 7</td>
<td>253</td>
<td>Microsoft Project 98</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------</td>
<td>-----</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>256</td>
<td>MS Project 2007</td>
<td>257</td>
<td>Lotus Notes database</td>
</tr>
<tr>
<td>258</td>
<td>Symphony</td>
<td>259</td>
<td>Lotus 1-2-3 1.0</td>
</tr>
<tr>
<td>260</td>
<td>Lotus 1-2-3 2.0</td>
<td>261</td>
<td>Lotus 1-2-3 3.x</td>
</tr>
<tr>
<td>262</td>
<td>Smart Spreadsheet</td>
<td>263</td>
<td>Microsoft Excel 2.x</td>
</tr>
<tr>
<td>264</td>
<td>Enable Spreadsheet</td>
<td>265</td>
<td>Microsoft Works SS</td>
</tr>
<tr>
<td>266</td>
<td>VP-Planner</td>
<td>267</td>
<td>Mosaic Twin</td>
</tr>
<tr>
<td>268</td>
<td>SuperCalc 5</td>
<td>269</td>
<td>Quattro Pro</td>
</tr>
<tr>
<td>270</td>
<td>Quattro</td>
<td>271</td>
<td>PFS: Plan</td>
</tr>
<tr>
<td>272</td>
<td>First Choice SS</td>
<td>273</td>
<td>Microsoft Excel 3.0</td>
</tr>
<tr>
<td>274</td>
<td>Generic WKS</td>
<td>275</td>
<td>Mac Works 2.0 SS</td>
</tr>
<tr>
<td>276</td>
<td>Windows Works SS</td>
<td>277</td>
<td>Microsoft Excel 4.0</td>
</tr>
<tr>
<td>278</td>
<td>Quattro Pro for Windows</td>
<td>279</td>
<td>Lotus 1-2-3 4.x / 5.x</td>
</tr>
<tr>
<td>280</td>
<td>Quattro Pro Windows Japan</td>
<td>281</td>
<td>CEO Spreadsheet</td>
</tr>
<tr>
<td>282</td>
<td>Microsoft Excel 5.0/7.0</td>
<td>283</td>
<td>Multiplan 4.0</td>
</tr>
<tr>
<td>284</td>
<td>Windows Works 3.0 SS</td>
<td>285</td>
<td>Quattro Pro 4.0</td>
</tr>
<tr>
<td>286</td>
<td>Quattro Pro 5.0</td>
<td>287</td>
<td>Quattro Pro Win 6.0</td>
</tr>
<tr>
<td>288</td>
<td>Lotus 123 Release 2 for OS/2</td>
<td>289</td>
<td>Lotus 123 for OS/2 Chart</td>
</tr>
<tr>
<td>290</td>
<td>Windows Works 4.0 SS</td>
<td>291</td>
<td>Quattro Pro Win 7.0/8.0</td>
</tr>
<tr>
<td>292</td>
<td>Quattro Pro Win 7.0/8.0 Graph</td>
<td>293</td>
<td>Lotus 1-2-3 97 Edition</td>
</tr>
<tr>
<td>294</td>
<td>Microsoft Mac Excel 4.0</td>
<td>295</td>
<td>Microsoft Mac Excel 5.0</td>
</tr>
<tr>
<td>296</td>
<td>Microsoft Excel 97/98/2004</td>
<td>297</td>
<td>MS Excel 3.0 Workbook</td>
</tr>
<tr>
<td>298</td>
<td>MS Excel 4.0 Workbook</td>
<td>299</td>
<td>MS Excel Mac 4.0 Workbook</td>
</tr>
<tr>
<td>300</td>
<td>MS Excel Mac 4.0 Workbook</td>
<td>301</td>
<td>Lotus 1-2-3 98/Millennium Edition</td>
</tr>
<tr>
<td>302</td>
<td>Quattro Pro 8.0</td>
<td>303</td>
<td>Quattro Pro Win 9.0 / X3</td>
</tr>
<tr>
<td>304</td>
<td>Microsoft Excel 2000</td>
<td>305</td>
<td>Quattro Pro Win 10.0</td>
</tr>
<tr>
<td>306</td>
<td>Microsoft Excel 2002</td>
<td>307</td>
<td>StarOffice 5.2 Calc</td>
</tr>
<tr>
<td>308</td>
<td>Quattro Pro Win 11.0</td>
<td>309</td>
<td>Microsoft Excel 2003</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------------</td>
<td>------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>310</td>
<td>StarOffice 6 &amp; 7 Calc</td>
<td>311</td>
<td>Quattro Pro Win 12.0</td>
</tr>
<tr>
<td>312</td>
<td>StarOffice 8/Open Office 2.x Calc</td>
<td>313</td>
<td>Microsoft Excel 2007</td>
</tr>
<tr>
<td>314</td>
<td>Password Protected Microsoft Excel 2007</td>
<td>315</td>
<td>Microsoft Excel 2007 Binary</td>
</tr>
<tr>
<td>318</td>
<td>MS Works SS6</td>
<td>319</td>
<td>Open Office Calc 6</td>
</tr>
<tr>
<td>320</td>
<td>Open Office Calc 8</td>
<td>321</td>
<td>IBM Lotus Symphony Spreadsheet</td>
</tr>
<tr>
<td>322</td>
<td>Excel Template 2007</td>
<td>323</td>
<td>Excel Macro Enabled</td>
</tr>
<tr>
<td>324</td>
<td>Excel Template Macro Enabled 2007</td>
<td>325</td>
<td>Windows Bitmap</td>
</tr>
<tr>
<td>326</td>
<td>Tagged Image File Format</td>
<td>327</td>
<td>Paintbrush</td>
</tr>
<tr>
<td>328</td>
<td>Compuserve GIF</td>
<td>329</td>
<td>EPS (TIFF Header)</td>
</tr>
<tr>
<td>330</td>
<td>CCITT Group 3 Fax</td>
<td>331</td>
<td>Mac PICT2</td>
</tr>
<tr>
<td>332</td>
<td>WordPerfect Graphic</td>
<td>333</td>
<td>Windows Metafile</td>
</tr>
<tr>
<td>334</td>
<td>Lotus PIC</td>
<td>335</td>
<td>Mac PICT</td>
</tr>
<tr>
<td>336</td>
<td>Ami Draw</td>
<td>337</td>
<td>Targa</td>
</tr>
<tr>
<td>338</td>
<td>GEM Image</td>
<td>339</td>
<td>OS/2 Bitmap</td>
</tr>
<tr>
<td>340</td>
<td>Windows Icon</td>
<td>341</td>
<td>Windows Cursor</td>
</tr>
<tr>
<td>342</td>
<td>Micrografx product</td>
<td>343</td>
<td>MacPaint</td>
</tr>
<tr>
<td>344</td>
<td>Corel Draw 2.0</td>
<td>345</td>
<td>Corel Draw 3.0</td>
</tr>
<tr>
<td>346</td>
<td>HP Graphics Language</td>
<td>347</td>
<td>Harvard 3.0 Chart</td>
</tr>
<tr>
<td>348</td>
<td>Harvard 2.0 Chart</td>
<td>349</td>
<td>Harvard 3.0 Presentation</td>
</tr>
<tr>
<td>350</td>
<td>Freelance</td>
<td>351</td>
<td>WordPerfect Graphic 2</td>
</tr>
<tr>
<td>352</td>
<td>CGM Graphic Metafile</td>
<td>353</td>
<td>Excel 2.x Chart</td>
</tr>
<tr>
<td>354</td>
<td>Excel 3.0 Chart</td>
<td>355</td>
<td>Excel 4.0 Chart</td>
</tr>
<tr>
<td>356</td>
<td>Candy 4</td>
<td>357</td>
<td>Hanako 1.x</td>
</tr>
<tr>
<td>358</td>
<td>Hanako 2.x</td>
<td>359</td>
<td>JPEG File Interchange</td>
</tr>
<tr>
<td>360</td>
<td>Excel 5.0/7.0 Chart</td>
<td>361</td>
<td>Corel Draw 4.0</td>
</tr>
<tr>
<td>362</td>
<td>PowerPoint 4.0</td>
<td>363</td>
<td>Multipage PCX</td>
</tr>
<tr>
<td>364</td>
<td>PowerPoint 3.0</td>
<td>365</td>
<td>Corel Draw 5.0</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------</td>
<td>-----</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>366</td>
<td>OS/2 Metafile</td>
<td>367</td>
<td>PowerPoint 7.0</td>
</tr>
<tr>
<td>368</td>
<td>AutoCAD DXF (ASCII)</td>
<td>369</td>
<td>AutoCAD DXF (Binary)</td>
</tr>
<tr>
<td>370</td>
<td>AutoCAD DXB</td>
<td>371</td>
<td>Freelance 96/97/Millennium Edition</td>
</tr>
<tr>
<td>372</td>
<td>Mac PowerPoint 3.0</td>
<td>373</td>
<td>Mac PowerPoint 4.0</td>
</tr>
<tr>
<td>374</td>
<td>WordPerfect Presentations</td>
<td>375</td>
<td>OS/2 Warp Bitmap</td>
</tr>
<tr>
<td>376</td>
<td>AutoCAD Drawing 12</td>
<td>377</td>
<td>AutoCAD Drawing 13</td>
</tr>
<tr>
<td>378</td>
<td>Adobe Illustrator</td>
<td>379</td>
<td>Corel Presentations 7.0 - 12.0 / X3</td>
</tr>
<tr>
<td>380</td>
<td>WordPerfect Graphic 7.0/8.0/9.0</td>
<td>381</td>
<td>Adobe Acrobat (PDF)</td>
</tr>
<tr>
<td>382</td>
<td>Framemaker</td>
<td>383</td>
<td>RAS - Sun Raster</td>
</tr>
<tr>
<td>384</td>
<td>AutoShade Rendering</td>
<td>385</td>
<td>Kodak Photo CD</td>
</tr>
<tr>
<td>386</td>
<td>PowerPoint 4.0 (extracted from docfile)</td>
<td>387</td>
<td>Mac PowerPoint 4.0 (extracted from docfile)</td>
</tr>
<tr>
<td>388</td>
<td>Enhanced Windows Metafile</td>
<td>389</td>
<td>GEM</td>
</tr>
<tr>
<td>390</td>
<td>Mac PowerPoint 3.0</td>
<td>391</td>
<td>Mac PowerPoint 4.0</td>
</tr>
<tr>
<td>392</td>
<td>Harvard Graphics for Windows</td>
<td>393</td>
<td>IGES Drawing File Format</td>
</tr>
<tr>
<td>394</td>
<td>IBM Picture Interchange Format</td>
<td>395</td>
<td>X-Windows Bitmap</td>
</tr>
<tr>
<td>396</td>
<td>X-Windows Pixmap</td>
<td>397</td>
<td>CALS Raster File Format</td>
</tr>
<tr>
<td>398</td>
<td>Portable Network Graphics Format</td>
<td>399</td>
<td>X-Windows Dump</td>
</tr>
<tr>
<td>400</td>
<td>CorelDraw ClipArt</td>
<td>401</td>
<td>HP Gallery</td>
</tr>
<tr>
<td>402</td>
<td>Graphics Data Format</td>
<td>403</td>
<td>Micrografx Designer</td>
</tr>
<tr>
<td>404</td>
<td>Post Script</td>
<td>405</td>
<td>Microsoft PowerPoint 97-2004</td>
</tr>
<tr>
<td>406</td>
<td>Corel Draw 6.0</td>
<td>407</td>
<td>Corel Draw 7.0</td>
</tr>
<tr>
<td>408</td>
<td>PDF MacBinary Header</td>
<td>409</td>
<td>AutoCAD Drawing - Unknown Version</td>
</tr>
<tr>
<td>410</td>
<td>Visio 4.x</td>
<td>411</td>
<td>AutoCAD Drawing 14</td>
</tr>
<tr>
<td>412</td>
<td>PBM (Portable Bitmap)</td>
<td>413</td>
<td>PGM (Portable Graymap)</td>
</tr>
<tr>
<td>414</td>
<td>PPM (Portable Pixmap)</td>
<td>415</td>
<td>Adobe Photoshop</td>
</tr>
<tr>
<td>416</td>
<td>Microsoft PowerPoint Dual 95/97</td>
<td>417</td>
<td>Paint Shop Pro</td>
</tr>
<tr>
<td>418</td>
<td>Kodak FlashPix</td>
<td>419</td>
<td>Visio 5.x</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>---------------------------------</td>
<td>-----</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>420</td>
<td>Corel Draw 8.0</td>
<td>421</td>
<td>Visio 6.x</td>
</tr>
<tr>
<td>422</td>
<td>Corel Draw 9.0</td>
<td>423</td>
<td>Progressive JPEG</td>
</tr>
<tr>
<td>424</td>
<td>Microsoft PowerPoint 2000/2002</td>
<td>425</td>
<td>Bentley Microstation DGN</td>
</tr>
<tr>
<td>426</td>
<td>Windows 98/2000 Bitmap</td>
<td>427</td>
<td>Wireless Bitmap</td>
</tr>
<tr>
<td>428</td>
<td>MIFF Graphic</td>
<td>429</td>
<td>Microsoft PowerPoint 2</td>
</tr>
<tr>
<td>430</td>
<td>WordPerfect Graphic 10.0</td>
<td>431</td>
<td>Visio 3.x</td>
</tr>
<tr>
<td>432</td>
<td>Micrografx Designer</td>
<td>433</td>
<td>PDF Image</td>
</tr>
<tr>
<td>434</td>
<td>StarOffice 5.2 Impress</td>
<td>435</td>
<td>Adobe Illustrator 9</td>
</tr>
<tr>
<td>436</td>
<td>AutoCAD 2000/2002 Drawing</td>
<td>437</td>
<td>AutoCAD 2.5 Drawing</td>
</tr>
<tr>
<td>438</td>
<td>AutoCAD 2.6 Drawing</td>
<td>439</td>
<td>AutoCAD 9 Drawing</td>
</tr>
<tr>
<td>440</td>
<td>AutoCAD 10 Drawing</td>
<td>441</td>
<td>QuarkXPress 3.0 For Macintosh</td>
</tr>
<tr>
<td>442</td>
<td>QuarkXPress 3.1 For Macintosh</td>
<td>443</td>
<td>QuarkXPress 3.2 For Macintosh</td>
</tr>
<tr>
<td>444</td>
<td>QuarkXPress 3.3 For Macintosh</td>
<td>445</td>
<td>QuarkXPress 4.0 For Macintosh</td>
</tr>
<tr>
<td>446</td>
<td>QuarkXPress 3.3 For Windows</td>
<td>447</td>
<td>QuarkXPress 4.0 For Windows</td>
</tr>
<tr>
<td>448</td>
<td>QuarkXPress 5.0 For Windows</td>
<td>449</td>
<td>Export Image</td>
</tr>
<tr>
<td>450</td>
<td>StarOffice 6 &amp; 7 Draw</td>
<td>451</td>
<td>StarOffice 6 &amp; 7 Impress</td>
</tr>
<tr>
<td>452</td>
<td>JBIG2 Bitmap</td>
<td>453</td>
<td>Corel Draw 10.0</td>
</tr>
<tr>
<td>454</td>
<td>Corel Draw 11.0</td>
<td>455</td>
<td>Microsoft Visio 2003</td>
</tr>
<tr>
<td>456</td>
<td>StarOffice 8 Draw</td>
<td>457</td>
<td>StarOffice 8/Open Office 2.x Impress</td>
</tr>
<tr>
<td>460</td>
<td>Microsoft XML Paper Specification</td>
<td>461</td>
<td>Password Protected Microsoft Powerpoint 2007</td>
</tr>
<tr>
<td>462</td>
<td>AutoCAD 2007 Drawing</td>
<td>463</td>
<td>OS/2 v.2 Bitmap</td>
</tr>
<tr>
<td>464</td>
<td>StarView Metafile</td>
<td>465</td>
<td>eFax Document</td>
</tr>
<tr>
<td>475</td>
<td>DRM protected Microsoft Powerpoint</td>
<td>476</td>
<td>DRM protected Microsoft Powerpoint 2007</td>
</tr>
<tr>
<td>477</td>
<td>AutoDesk DWF</td>
<td>478</td>
<td>Corel Draw 12.0</td>
</tr>
<tr>
<td>479</td>
<td>JPEG 2000</td>
<td>480</td>
<td>Adobe InDesign</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------</td>
<td>-----</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>481</td>
<td>JPEG 2000 jpf Extension</td>
<td>482</td>
<td>JPEG 2000 mj2 Extension</td>
</tr>
<tr>
<td>483</td>
<td>WordPerfect Inform 1.0</td>
<td>484</td>
<td>Lotus Screen SnapShot</td>
</tr>
<tr>
<td>485</td>
<td>Lotus Screen Snapshot</td>
<td>486</td>
<td>Interchange Format</td>
</tr>
<tr>
<td>487</td>
<td>Microsoft Escher Graphics</td>
<td>488</td>
<td>Windows Sound</td>
</tr>
<tr>
<td>489</td>
<td>Windows Video</td>
<td>490</td>
<td>MIDI File</td>
</tr>
<tr>
<td>491</td>
<td>Macromedia Director</td>
<td>492</td>
<td>Macromedia Flash</td>
</tr>
<tr>
<td>493</td>
<td>Macromedia Flash</td>
<td>494</td>
<td>Quicktime Movie</td>
</tr>
<tr>
<td>495</td>
<td>MPEG Layer3 ID3 Ver 1.x</td>
<td>496</td>
<td>MPEG Layer3 ID3 Ver 2.x</td>
</tr>
<tr>
<td>497</td>
<td>ID3 Ver 1.x</td>
<td>498</td>
<td>ID3 Ver 2.x</td>
</tr>
<tr>
<td>499</td>
<td>MPEG-1 audio - Layer 3</td>
<td>500</td>
<td>MPEG-1 audio - Layer 1</td>
</tr>
<tr>
<td>501</td>
<td>MPEG-1 audio - Layer 2</td>
<td>502</td>
<td>MPEG-2 audio - Layer 1</td>
</tr>
<tr>
<td>503</td>
<td>MPEG-2 audio - Layer 2</td>
<td>504</td>
<td>MPEG-2 audio - Layer 3</td>
</tr>
<tr>
<td>505</td>
<td>Advanced Systems Format</td>
<td>506</td>
<td>Windows Media Video (ASF subtype)</td>
</tr>
<tr>
<td>507</td>
<td>Windows Media Audio (ASF subtype)</td>
<td>508</td>
<td>Microsoft Digital Video Recording (ASF subtype)</td>
</tr>
<tr>
<td>509</td>
<td>Real Media (both Real Audio and Real Video)</td>
<td>510</td>
<td>MPEG-1 video</td>
</tr>
<tr>
<td>511</td>
<td>MPEG-2 video</td>
<td>512</td>
<td>ISO Base Media File Format</td>
</tr>
<tr>
<td>513</td>
<td>MPEG-4 file</td>
<td>514</td>
<td>MPEG-7 file</td>
</tr>
<tr>
<td>515</td>
<td>EXE / DLL File</td>
<td>516</td>
<td>.COM File</td>
</tr>
<tr>
<td>517</td>
<td>.ZIP File</td>
<td>518</td>
<td>Self UnZIPping .EXE</td>
</tr>
<tr>
<td>519</td>
<td>.ARC File</td>
<td>520</td>
<td>MS Office Binder</td>
</tr>
<tr>
<td>521</td>
<td>UNIX Compress</td>
<td>522</td>
<td>UNIX Tar</td>
</tr>
<tr>
<td>523</td>
<td>Envoy</td>
<td>524</td>
<td>QuickFinder</td>
</tr>
<tr>
<td>525</td>
<td>Windows Clipboard File</td>
<td>526</td>
<td>Envoy 7</td>
</tr>
<tr>
<td>527</td>
<td>StuffIt</td>
<td>528</td>
<td>LZH Compress</td>
</tr>
<tr>
<td>529</td>
<td>Self-Extracting LZH</td>
<td>530</td>
<td>UNIX GZip</td>
</tr>
<tr>
<td>531</td>
<td>Java Class File</td>
<td>532</td>
<td>mbox(RFC-822 mailbox)</td>
</tr>
<tr>
<td>533</td>
<td>Lotus Notes Database R6.x</td>
<td>534</td>
<td>Generic Password Protected Microsoft Office 2007 Document</td>
</tr>
<tr>
<td>535</td>
<td>Microsoft Cabinet File</td>
<td>536</td>
<td>.RAR File</td>
</tr>
<tr>
<td>537</td>
<td>Self extracting RAR File</td>
<td>538</td>
<td>Microsoft InfoPath</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------------------</td>
<td>-----</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>549</td>
<td>Flexiondoc 1 (original) schema</td>
<td>550</td>
<td>Flexiondoc 2 schema</td>
</tr>
<tr>
<td>551</td>
<td>Flexiondoc 3 schema</td>
<td>552</td>
<td>Flexiondoc 4 schema</td>
</tr>
<tr>
<td>553</td>
<td>Flexiondoc 5 schema</td>
<td>554</td>
<td>Flexiondoc 5.1 schema</td>
</tr>
<tr>
<td>555</td>
<td>OASIS OpenDocument v1.0</td>
<td>556</td>
<td>Flexiondoc 5.2 schema</td>
</tr>
<tr>
<td>557</td>
<td>Domino XML schema</td>
<td>558</td>
<td>Adobe InDesign Interchange</td>
</tr>
<tr>
<td>559</td>
<td>XML Visio</td>
<td>560</td>
<td>Mail archive DXL</td>
</tr>
<tr>
<td>561</td>
<td>Mail message DXL</td>
<td>562</td>
<td>Generic DXL</td>
</tr>
<tr>
<td>564</td>
<td>AutoCAD DWG 2008</td>
<td>565</td>
<td>Publisher 2003</td>
</tr>
<tr>
<td>566</td>
<td>Publisher 2007</td>
<td>567</td>
<td>Open Office Impress 6</td>
</tr>
<tr>
<td>568</td>
<td>Open Office Impress 8</td>
<td>569</td>
<td>IBM Lotus Symphony Presentations</td>
</tr>
<tr>
<td>570</td>
<td>Open Office Draw 6</td>
<td>571</td>
<td>Open Office Draw 8</td>
</tr>
<tr>
<td>572</td>
<td>PowerPoint 2007 Template</td>
<td>573</td>
<td>PowerPoint 2007 Macro Enabled</td>
</tr>
<tr>
<td>574</td>
<td>PowerPoint 2007 Template Macro Enabled</td>
<td>575</td>
<td>PowerPoint 2007 Slideshow file</td>
</tr>
<tr>
<td>576</td>
<td>PowerPoint 2007 Template Macro Enabled</td>
<td>577</td>
<td>Oracle Multimedia internal raster format</td>
</tr>
<tr>
<td>578</td>
<td>TK thesaurus</td>
<td>579</td>
<td>TK abbrev</td>
</tr>
<tr>
<td>580</td>
<td>TK dictionary</td>
<td>581</td>
<td>TK quote</td>
</tr>
<tr>
<td>582</td>
<td>TK written word</td>
<td>583</td>
<td>TK culturelit</td>
</tr>
<tr>
<td>584</td>
<td>TK grammar</td>
<td>585</td>
<td>TK thessyn</td>
</tr>
<tr>
<td>586</td>
<td>Text - (ASCII)</td>
<td>587</td>
<td>Text - (Hex)</td>
</tr>
<tr>
<td>588</td>
<td>Text - (ANSI)</td>
<td>589</td>
<td>Text - (Unicode)</td>
</tr>
<tr>
<td>590</td>
<td>Text - (ASCII)</td>
<td>591</td>
<td>Text - (ANSI 8)</td>
</tr>
<tr>
<td>592</td>
<td>Text - Unknown format</td>
<td>593</td>
<td>Text - MAC - 7bit</td>
</tr>
<tr>
<td>594</td>
<td>Text - MAC - 8bit</td>
<td>595</td>
<td>Text - Japanese (ShiftJIS)</td>
</tr>
<tr>
<td>596</td>
<td>Text - Chinese (GB)</td>
<td>597</td>
<td>Text - Korean (Hangul)</td>
</tr>
<tr>
<td>598</td>
<td>Text - Chinese (Big 5)</td>
<td>599</td>
<td>Code page 852 - MS DOS Slavic</td>
</tr>
<tr>
<td>600</td>
<td>Text - Japanese (EUC)</td>
<td>601</td>
<td>Text - Hebrew (7-bit)</td>
</tr>
<tr>
<td>602</td>
<td>Text - Hebrew (IBM PC8)</td>
<td>603</td>
<td>Text - Hebrew (VAX E0)</td>
</tr>
<tr>
<td>604</td>
<td>Text - Hebrew (Windows ANSI 1255)</td>
<td>605</td>
<td>Text – Arabic 710</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>----</td>
<td>-----------</td>
<td>----</td>
<td>-----------</td>
</tr>
<tr>
<td>606</td>
<td>Text – Arabic 720</td>
<td>607</td>
<td>Text - Arabic (Windows ANSI 1256)</td>
</tr>
<tr>
<td>609</td>
<td>Text - Japanese (JIS)</td>
<td>610</td>
<td>Text - Central European</td>
</tr>
<tr>
<td>611</td>
<td>UTF-8 encoded Text</td>
<td>612</td>
<td>Text - U.S. English/Portuguese (EBCDIC 37)</td>
</tr>
<tr>
<td>613</td>
<td>Text - Austrian/German (EBCDIC 273)</td>
<td>614</td>
<td>Text - Danish/Norwegian (EBCDIC 277)</td>
</tr>
<tr>
<td>615</td>
<td>Text - Finnish/Swedish (EBCDIC 278)</td>
<td>616</td>
<td>Text - Italian (EBCDIC 280)</td>
</tr>
<tr>
<td>617</td>
<td>Text - Spanish (EBCDIC 284)</td>
<td>618</td>
<td>Text - U.K. English (EBCDIC 285)</td>
</tr>
<tr>
<td>619</td>
<td>Text - French (EBCDIC 297)</td>
<td>620</td>
<td>Text - Belgian/International (EBCDIC 500)</td>
</tr>
<tr>
<td>621</td>
<td>Text - Eastern European (EBCDIC 870)</td>
<td>622</td>
<td>Text - Icelandic (EBCDIC 871)</td>
</tr>
<tr>
<td>623</td>
<td>Text - Turkish (EBCDIC 1026)</td>
<td>624</td>
<td>HTML - U.S. English/Portuguese (EBCDIC 37)</td>
</tr>
<tr>
<td>625</td>
<td>HTML - Austrian/German (EBCDIC 273)</td>
<td>626</td>
<td>HTML - Danish/Norwegian (EBCDIC 277)</td>
</tr>
<tr>
<td>627</td>
<td>HTML - Finnish/Swedish (EBCDIC 278)</td>
<td>628</td>
<td>HTML - Italian (EBCDIC 280)</td>
</tr>
<tr>
<td>629</td>
<td>HTML - Spanish (EBCDIC 284)</td>
<td>630</td>
<td>HTML - U.K. English (EBCDIC 285)</td>
</tr>
<tr>
<td>631</td>
<td>HTML - French (EBCDIC 297)</td>
<td>632</td>
<td>HTML - Belgian/International (EBCDIC 500)</td>
</tr>
<tr>
<td>633</td>
<td>HTML - Eastern European (EBCDIC 870)</td>
<td>634</td>
<td>HTML - Icelandic (EBCDIC 871)</td>
</tr>
<tr>
<td>635</td>
<td>HTML - Turkish (EBCDIC 1026)</td>
<td>636</td>
<td>UUE Encoded Text</td>
</tr>
<tr>
<td>637</td>
<td>UUE Encoded Continued Part</td>
<td>638</td>
<td>XXE Encoded Text</td>
</tr>
<tr>
<td>639</td>
<td>XXE Encoded Continued Part</td>
<td>640</td>
<td>YEnc Encoded Text</td>
</tr>
<tr>
<td>641</td>
<td>YEnc Encoded Continued Part</td>
<td>642</td>
<td>BinHex Encoded Text</td>
</tr>
<tr>
<td>643</td>
<td>BinHex Encoded Continued Part</td>
<td>644</td>
<td>Text - Arabic (ASMO-708)</td>
</tr>
<tr>
<td>645</td>
<td>Text - Arabic (DOS OEM 720 TRANSPARENT ASMO)</td>
<td>646</td>
<td>Text - Arabic (ISO 8859-6)</td>
</tr>
<tr>
<td>647</td>
<td>Text - Arabic (Mac)</td>
<td>648</td>
<td>Text - Baltic (ISO 8859-4)</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>-----------------------------------</td>
<td>-----</td>
<td>---------------------------------------------------------</td>
</tr>
<tr>
<td>649</td>
<td>Text - Baltic (Windows ANSI 1257)</td>
<td>650</td>
<td>Text - Central European (DOS OEM 852 Latin II)</td>
</tr>
<tr>
<td>651</td>
<td>Text - Central European (ISO 8859-2)</td>
<td>652</td>
<td>Text - Central European (Mac)</td>
</tr>
<tr>
<td>653</td>
<td>Text - Central European (Windows ANSI 1250)</td>
<td>654</td>
<td>Text - Chinese Simplified (Windows ANSI 936 [GB2312])</td>
</tr>
<tr>
<td>655</td>
<td>Text - Chinese Traditional (Windows ANSI 950 [BIG5])</td>
<td>656</td>
<td>Text - Cyrillic (DOS OEM 855)</td>
</tr>
<tr>
<td>657</td>
<td>Text - Cyrillic (ISO 8859-5)</td>
<td>658</td>
<td>Text - Cyrillic (KOI8-R)</td>
</tr>
<tr>
<td>659</td>
<td>Text - Cyrillic (Mac)</td>
<td>660</td>
<td>Text - Cyrillic (Windows ANSI 1251)</td>
</tr>
<tr>
<td>661</td>
<td>Text - Greek (ISO 8859-7)</td>
<td>662</td>
<td>Text - Greek (Mac)</td>
</tr>
<tr>
<td>663</td>
<td>Text - Greek (Windows ANSI 1253)</td>
<td>664</td>
<td>Text - Hebrew (DOS OEM 862)</td>
</tr>
<tr>
<td>665</td>
<td>Text - Hebrew (ISO 8859-8)</td>
<td>666</td>
<td>Text - Japanese (Mac)</td>
</tr>
<tr>
<td>667</td>
<td>Text - Korean (Windows ANSI 1361 [Johab])</td>
<td>668</td>
<td>Text - Korean (Windows ANSI 949)</td>
</tr>
<tr>
<td>669</td>
<td>Text - Russian (DOS OEM 866)</td>
<td>670</td>
<td>Text - Thai (Windows ANSI 874)</td>
</tr>
<tr>
<td>671</td>
<td>Text - Turkish (DOS OEM 857)</td>
<td>672</td>
<td>Text - Turkish (ISO 8859-9)</td>
</tr>
<tr>
<td>673</td>
<td>Text - Turkish (Mac)</td>
<td>674</td>
<td>Text - Turkish (Windows ANSI 1254)</td>
</tr>
<tr>
<td>675</td>
<td>Text - Vietnamese (Windows ANSI 1258)</td>
<td>676</td>
<td>Text - Western European (ISO 8859-1)</td>
</tr>
<tr>
<td>677</td>
<td>Text - Western European (Mac)</td>
<td>678</td>
<td>Text - Western European (Windows ANSI 1252)</td>
</tr>
<tr>
<td>679</td>
<td>HTML - Arabic (ASMO-708)</td>
<td>680</td>
<td>HTML - Arabic (DOS OEM 720 TRANSPARENT ASMO)</td>
</tr>
<tr>
<td>681</td>
<td>HTML - Arabic (ISO 8859-6)</td>
<td>682</td>
<td>HTML - Arabic (Mac)</td>
</tr>
<tr>
<td>683</td>
<td>HTML - Arabic (Windows ANSI 1256)</td>
<td>684</td>
<td>HTML - Baltic (ISO 8859-4)</td>
</tr>
<tr>
<td>685</td>
<td>HTML - Baltic (Windows ANSI 1257)</td>
<td>686</td>
<td>HTML - Central European (DOS OEM 852 Latin II)</td>
</tr>
<tr>
<td>687</td>
<td>HTML - Central European (ISO 8859-2)</td>
<td>688</td>
<td>HTML - Central European (Mac)</td>
</tr>
<tr>
<td>689</td>
<td>HTML - Central European (Windows ANSI 1250)</td>
<td>690</td>
<td>HTML - Chinese Simplified (EUC)</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>------</td>
<td>-----------------------------------------------</td>
<td>------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>691</td>
<td>HTML - Chinese Simplified (Windows ANSI 936 [GB2312])</td>
<td>692</td>
<td>HTML - Chinese Traditional (Windows ANSI 950 [BIG5])</td>
</tr>
<tr>
<td>693</td>
<td>HTML - Cyrillic (DOS OEM 855)</td>
<td>694</td>
<td>HTML - Cyrillic (ISO 8859-5)</td>
</tr>
<tr>
<td>695</td>
<td>HTML - Cyrillic (KOI8-R)</td>
<td>696</td>
<td>HTML - Cyrillic (Mac)</td>
</tr>
<tr>
<td>697</td>
<td>HTML - Cyrillic (Windows ANSI 1251)</td>
<td>698</td>
<td>HTML - Greek (ISO 8859-7)</td>
</tr>
<tr>
<td>699</td>
<td>HTML - Greek (Mac)</td>
<td>700</td>
<td>HTML - Greek (Windows ANSI 1253)</td>
</tr>
<tr>
<td>701</td>
<td>HTML - Hebrew (DOS OEM 862)</td>
<td>702</td>
<td>HTML - Hebrew (ISO 8859-8)</td>
</tr>
<tr>
<td>703</td>
<td>HTML - Hebrew (Windows ANSI 1255)</td>
<td>704</td>
<td>HTML - Japanese (Mac)</td>
</tr>
<tr>
<td>705</td>
<td>HTML - Japanese (Windows Shift-JIS ANSI 932)</td>
<td>706</td>
<td>HTML - Korean (Windows ANSI 1361 [Johab])</td>
</tr>
<tr>
<td>707</td>
<td>HTML - Korean (Windows ANSI 949)</td>
<td>708</td>
<td>HTML - Russian (DOS OEM 866)</td>
</tr>
<tr>
<td>709</td>
<td>HTML - Thai (Windows ANSI 874)</td>
<td>710</td>
<td>HTML - Turkish (DOS OEM 857)</td>
</tr>
<tr>
<td>711</td>
<td>HTML - Turkish (ISO 8859-9)</td>
<td>712</td>
<td>HTML - Turkish (Mac)</td>
</tr>
<tr>
<td>713</td>
<td>HTML - Turkish (Windows ANSI 1254)</td>
<td>714</td>
<td>HTML - Vietnamese (Windows ANSI 1258)</td>
</tr>
<tr>
<td>715</td>
<td>HTML - Western European (ISO 8859-1)</td>
<td>716</td>
<td>HTML - Western European (Mac)</td>
</tr>
<tr>
<td>717</td>
<td>HTML - Western European (Windows ANSI 1252)</td>
<td>718</td>
<td>Plugin</td>
</tr>
<tr>
<td>719</td>
<td>Text - Japanese (ShiftJIS)</td>
<td>720</td>
<td>Windows Metafile [5000]</td>
</tr>
<tr>
<td>721</td>
<td>WordPerfect Graphic [B]</td>
<td>722</td>
<td>Ami (internal bitmap)</td>
</tr>
<tr>
<td>723</td>
<td>Word (internal bitmap)</td>
<td>724</td>
<td>Mac PICT2 Binary</td>
</tr>
<tr>
<td>725</td>
<td>Windows Metafile [5005]</td>
<td>726</td>
<td>Windows Metafile [5006]</td>
</tr>
<tr>
<td>727</td>
<td>PerfectWorks Picture</td>
<td>728</td>
<td>WPG2 (internal bitmap)</td>
</tr>
<tr>
<td>729</td>
<td>Windows DIB</td>
<td>730</td>
<td>WPG1 (internal bitmap)</td>
</tr>
<tr>
<td>731</td>
<td>Embedded Bitmap</td>
<td>732</td>
<td>Embedded Bitmap</td>
</tr>
<tr>
<td>733</td>
<td>IAF (internal bitmap)</td>
<td>734</td>
<td>IAF (internal bitmap)</td>
</tr>
<tr>
<td>735</td>
<td>PICT (internal bitmap)</td>
<td>736</td>
<td>Export OCR data as Text, no formatting</td>
</tr>
<tr>
<td>ID</td>
<td>File Type</td>
<td>ID</td>
<td>File Type</td>
</tr>
<tr>
<td>-----</td>
<td>----------------------------------------------------</td>
<td>-----</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>737</td>
<td>Export OCR data as RTF, yes formatting</td>
<td>738</td>
<td>Export OCR data as HTML</td>
</tr>
<tr>
<td>739</td>
<td>EDRM export</td>
<td>753</td>
<td>Open Office 3.x Writer (ODF 1.2)</td>
</tr>
<tr>
<td>754</td>
<td>StarOffice 9 Writer (ODF 1.2)</td>
<td>755</td>
<td>Oracle Open Office 3.x Writer (ODF 1.2)</td>
</tr>
<tr>
<td>756</td>
<td>Samsung Jungum File</td>
<td>757</td>
<td>Kingsoft Office Writer File</td>
</tr>
<tr>
<td>758</td>
<td>Microsoft Word 2010</td>
<td>759</td>
<td>Microsoft Word 2010 Template</td>
</tr>
<tr>
<td>760</td>
<td>Microsoft Word 2010 Macro Enabled Document</td>
<td>761</td>
<td>Microsoft Word 2010 Macro Enabled Template</td>
</tr>
<tr>
<td>764</td>
<td>Microsoft Project 2010</td>
<td>765</td>
<td>Microsoft Excel XML 2003</td>
</tr>
<tr>
<td>766</td>
<td>Open Office 3.x Calc (ODF 1.2)</td>
<td>769</td>
<td>Microsoft Excel 2007 Excel Add-in Macro File</td>
</tr>
<tr>
<td>770</td>
<td>Lotus Data Interchange Format</td>
<td>771</td>
<td>StarOffice 9 Calc (ODF 1.2)</td>
</tr>
<tr>
<td>772</td>
<td>Oracle Open Office 3.x Calc (ODF 1.2)</td>
<td>773</td>
<td>Kingsoft Office Spreadsheet File</td>
</tr>
<tr>
<td>774</td>
<td>Corel Presentations X4</td>
<td>775</td>
<td>Microsoft Excel 2010 Macro Enabled Workbook</td>
</tr>
<tr>
<td>776</td>
<td>Microsoft Excel 2010 Template</td>
<td>777</td>
<td>Microsoft Excel 2010 Macro Enabled Template</td>
</tr>
<tr>
<td>778</td>
<td>Microsoft Excel 2010 Excel Add-in Macro File</td>
<td>779</td>
<td>Microsoft Excel 2010 Binary</td>
</tr>
<tr>
<td>782</td>
<td>Resource Interchange File Format</td>
<td>783</td>
<td>Microsoft OneNote 2007</td>
</tr>
<tr>
<td>784</td>
<td>Windows Media Player Playlist</td>
<td>786</td>
<td>Flexiondoc v5.4 (XML)</td>
</tr>
<tr>
<td>790</td>
<td>Open Office 3.x Impress (ODF 1.2)</td>
<td>791</td>
<td>Open Office 3.x Draw (ODF 1.2)</td>
</tr>
<tr>
<td>794</td>
<td>StarOffice 9 Impress (ODF 1.2)</td>
<td>795</td>
<td>StarOffice 9 Draw (ODF 1.2)</td>
</tr>
<tr>
<td>796</td>
<td>Oracle Open Office 3.x Impress (ODF 1.2)</td>
<td>797</td>
<td>Oracle Open Office 3.x Draw (ODF 1.2)</td>
</tr>
<tr>
<td>798</td>
<td>Microsoft PowerPoint 2010</td>
<td>799</td>
<td>Microsoft PowerPoint 2010 Template</td>
</tr>
<tr>
<td>800</td>
<td>Microsoft PowerPoint 2010 Macro Enabled Template</td>
<td>801</td>
<td>Microsoft PowerPoint 2010 Slideshow</td>
</tr>
<tr>
<td>802</td>
<td>Microsoft PowerPoint 2010 Macro Enabled Presentation</td>
<td>803</td>
<td>Microsoft PowerPoint 2010 Macro Enabled Slideshow</td>
</tr>
</tbody>
</table>
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 it can be a chained certificate that with a certification path to a trusted root 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 machine, 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. You see this message:
   
   ```
   You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank. For some fields there will be a default value. If you enter '.', the field will be left blank.
   ```
   
   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:

   ```
copenssl pkcs12 -export -out <output file> -in <signed cert chain file> -inkey <private key file>
   ```

   For example:

   ```
copenssl pkcs12 -export -out server1.p12 -in server1.crt -inkey server1.key
   ```

   b) Enter the certificate password when prompted.

**Installing the Signed Certificate**

All portals on the same IP address use the same certificate. Define the IP address of the portal in the Portal Settings page for the blade/feature.

1. Import the new certificate to the gateway in SmartDashboard from a page that contains the Portal Settings for that blade/feature. For example:
   - Gateway Properties > Mobile Access > Portal Settings
   - Gateway Properties > SecurePlatform Settings
   - Gateway Properties > Data Loss Prevention
   - Gateway Properties > Identity Awareness > Captive Portal > Settings > Access Settings

   In the Certificate section, click Import or Replace.

2. Install the policy on the gateway.

   **Note** - The Repository of Certificates on the IPSec VPN page of the SmartDashboard 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 a Web browser:

The gateway uses the certificate when you connect with a browser to the portal. To see the certificate when you connect to the portal, click the lock icon that is next to the address bar in most browsers.

The certificate that users see depends on the actual IP address that they use to access the portal- not only the IP address configured for the portal in SmartDashboard.

To see the new certificate from SmartDashboard:

From the Gateway Properties > Data Loss Prevention page, click the View button in the Certificate section.
Appendix B

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\R75.20\PROGRAM\GuiDBedit.exe`
3. Go to Table > Other > dlp_data_tbl and select the data type that you want to change.

In This Appendix

<table>
<thead>
<tr>
<th>Case Sensitivity</th>
<th>134</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ordered Match for Names</td>
<td>134</td>
</tr>
<tr>
<td>Proximity of Matched Words</td>
<td>135</td>
</tr>
<tr>
<td>Match Multiple Occurrences</td>
<td>135</td>
</tr>
<tr>
<td>Match Whole Word Only</td>
<td>136</td>
</tr>
</tbody>
</table>

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.
# Appendix C

## Regular Expressions

**In This Appendix**

- Metacharacters 137
- Square Brackets 138
- Parentheses 138
- Hyphen 138
- Dot 138
- Vertical Bar 138
- Backslash 138
- Quantifiers 139

### Metacharacters

Some metacharacters are recognized anywhere in a pattern, except within square brackets; other metacharacters are recognized only in square brackets.

The Check Point set of regular expressions has been enhanced for R70 and above. The following table indicates if earlier versions do not support use of a given metacharacter.

<table>
<thead>
<tr>
<th>Metacharacter</th>
<th>Meaning</th>
<th>Earlier?</th>
<th>See</th>
</tr>
</thead>
<tbody>
<tr>
<td>\ (backslash)</td>
<td>escape character, and other meanings</td>
<td>partial</td>
<td>Backslash</td>
</tr>
<tr>
<td>[ ] (square brackets)</td>
<td>character class definition</td>
<td>yes</td>
<td>Square Brackets</td>
</tr>
<tr>
<td>( ) (parenthesis)</td>
<td>subpattern</td>
<td>yes</td>
<td>Parentheses</td>
</tr>
<tr>
<td>{ } (curly brackets)</td>
<td>min/max quantifier</td>
<td>no</td>
<td>Curly Brackets</td>
</tr>
<tr>
<td>. (dot)</td>
<td>match any character</td>
<td>yes</td>
<td>Dot</td>
</tr>
<tr>
<td>? (question mark)</td>
<td>zero or one quantifier</td>
<td>yes</td>
<td>Question Mark</td>
</tr>
<tr>
<td>* (asterisk)</td>
<td>zero or more quantifier</td>
<td>yes</td>
<td>Asterisk</td>
</tr>
<tr>
<td>+ (plus)</td>
<td>one or more quantifier</td>
<td>yes</td>
<td>Plus</td>
</tr>
<tr>
<td></td>
<td>(vertical bar)</td>
<td>start alternative branch</td>
<td>yes</td>
</tr>
<tr>
<td>^ (circumflex anchor)</td>
<td>anchor pattern to beginning of buffer</td>
<td>yes</td>
<td>Circumflex Anchor</td>
</tr>
<tr>
<td>$ (dollar anchor)</td>
<td>anchor pattern to end of buffer</td>
<td>yes</td>
<td>Dollar Anchor</td>
</tr>
</tbody>
</table>
Square Brackets

Square brackets ([ ]) designate a character class: matching a single character in the string.
Inside a character class, only these metacharacters have special meaning:
- backslash (\) - general escape character.
- hyphen (-) - character range.

Parentheses

Parentheses ( ) designate a subpattern. To match with either an open-parenthesis or closing-parenthesis, use the backslash to escape the symbol.

Hyphen

A hyphen (-) indicates a character range inside a character class. When used as a simple character in a character class, it must be escaped by using a backslash \

**For example:** [a-z] matches the lower-case alphabet.

Dot

Outside a character class, a dot (.) matches any one character in the string.

**For example:** .+ matches zero or more occurrences of any character
Inside a character class, it matches a dot (.)

Vertical Bar

A vertical bar (|) is used to separate alternative patterns.
If the right side is empty, this symbol indicates the NULL string: a| matches a or empty string

**For example:** a|b matches a or b

Backslash

The meaning of the backslash (\) character depends on the context. The following explanations are not all supported in earlier versions; see Earlier Versions for details.
In R70 and above, backslash escapes metacharacters inside and outside character classes.

Escaping Symbols

If the backslash is followed by a non-alphanumeric character, it takes away any special meaning that character may have. For example, \\* matches an asterisk, rather than any character. Also, you can escape the closing bracket with a backslash [\].
If the protection against the pattern is for earlier gateways as well as for newer ones, do not write one backslash inside square brackets. Instead, write two backslashes if you want to have a literal backslash inside square brackets.
You cannot use \ to escape a letter that is not a metacharacter. For example, because "g" is not a metacharacter, you cannot use \g.
Encoding Non-Printable Characters

To use non-printable characters (such as tab, return, and so on) in patterns, use the backslash before a character set reserved for non-printable characters.

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>\a</td>
<td>alarm; the BEL character (hex 07)</td>
</tr>
<tr>
<td>\cx</td>
<td>“control-x”, where x is any character</td>
</tr>
<tr>
<td>\e</td>
<td>escape (hex 1B)</td>
</tr>
<tr>
<td>\f</td>
<td>formfeed (hex 0C)</td>
</tr>
<tr>
<td>\n</td>
<td>newline (hex 0A)</td>
</tr>
<tr>
<td>\r</td>
<td>carriage return (hex 0D)</td>
</tr>
<tr>
<td>\t</td>
<td>tab (hex 09)</td>
</tr>
<tr>
<td>\ddd</td>
<td>character with octal code ddd</td>
</tr>
<tr>
<td>\xhh</td>
<td>character with hex code hh</td>
</tr>
</tbody>
</table>

Specifying Character Types

To specify certain types of characters (such as digits, whitespace, words) in patterns, use the backslash before a character set reserved for character types.

<table>
<thead>
<tr>
<th>Character</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>\d</td>
<td>any decimal digit</td>
</tr>
<tr>
<td>\D</td>
<td>any character that is not a decimal digit</td>
</tr>
<tr>
<td>\s</td>
<td>any whitespace character</td>
</tr>
<tr>
<td>\S</td>
<td>any character that is not whitespace</td>
</tr>
<tr>
<td>\w</td>
<td>any word character (underscore or alphanumeric character)</td>
</tr>
<tr>
<td>\W</td>
<td>any non-word character (not underscore or alphanumeric)</td>
</tr>
</tbody>
</table>

Quantifiers

Various metacharacters indicate how many instances of a character, character set or character class should be matched. A quantifier must not follow another quantifier, an opening parenthesis, or be the expression’s first character.

These quantifiers can follow any of the following items:
- a literal data character
- an escape such as \d that matches a single character
- a character class
- a sub-pattern in parentheses
Curly Brackets

Curly brackets (\{ \}) are used as general repetition quantifiers. They specify a minimum and maximum number of permitted matches.

For example:  \( a^{2,4} \) matches aa, aaa, or aaaa

If the second number is omitted, but the comma is present, there is no upper limit; if the second number and the comma are both omitted, the quantifier specifies an exact number of required matches.

For example:

- \([aeiou]{3,}\) matches at least 3 successive vowels, but may match many more
- \(\backslash d{8}\) matches exactly 8 digits

Note - A closing curly bracket } that is not preceded by an opening curly bracket { is treated as a simple character. However, it is good practice to use a backslash, \}, when using a closing curly bracket as a simple character.

Question Marks

Outside a character class, a question mark (?) matches zero or one character in the string. It is the same as using \{0,1\}.

For example:  \( c([ab]?r \) matches car, cbr, and cr

Inside a character class, it matches a question mark: \([?] \) matches ? (question mark).

Asterisk

Outside a character class, an asterisk (*) matches any number of characters in the string. It is the same as using \{0,\}.

For example:  \( c([ab])*r \) matches car, cbr, cr, cabr, and caaabbbr

Inside a character class, it matches an asterisk: \([*] \) matches * (asterisk).

Plus

Outside a character class, a plus (+) matches one or more characters in the string. It is the same as using \{1,\}.

For example:  \( c([ab]+)r \) matches character strings such as car, cbr, cabr, caaabbbr; but not cr

Inside a character class, it matches a plus: \([+] \) matches + (plus).
Appendix D

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 $DLPDIR/config/dlp.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.

In This Appendix

Character Set Aliases
# Character Set Aliases

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

<table>
<thead>
<tr>
<th>Name of Character Set</th>
<th>Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTF-8Encoded Unicode</td>
<td>UTF-8</td>
</tr>
<tr>
<td>UTF-7Encoded Unicode</td>
<td>UTF-7</td>
</tr>
<tr>
<td>ASCII (7-bit)</td>
<td>ASCII</td>
</tr>
<tr>
<td>Japanese (JIS)</td>
<td>JIS_X0201</td>
</tr>
<tr>
<td>Japanese (EUC)</td>
<td>EUC-JP</td>
</tr>
<tr>
<td>Korean Standard</td>
<td>KSC_5601</td>
</tr>
<tr>
<td>Simplified Chinese</td>
<td>GB2312</td>
</tr>
<tr>
<td>EBCDIC Code Page 37 (United States)</td>
<td>IBM037</td>
</tr>
<tr>
<td>EBCDIC Code Page 273 (Germany)</td>
<td>IBM273</td>
</tr>
<tr>
<td>EBCDIC Code Page 274 (Belgium)</td>
<td>IBM274</td>
</tr>
<tr>
<td>EBCDIC Code Page 277 (Denmark, Norway)</td>
<td>IBM277</td>
</tr>
<tr>
<td>EBCDIC Code Page 278 (Finland, Sweden)</td>
<td>IBM278</td>
</tr>
<tr>
<td>EBCDIC Code Page 280 (Italy)</td>
<td>IBM280</td>
</tr>
<tr>
<td>EBCDIC Code Page 284 (Latin America, Spain)</td>
<td>IBM284</td>
</tr>
<tr>
<td>EBCDIC Code Page 285 (Ireland, UK)</td>
<td>IBM285</td>
</tr>
<tr>
<td>EBCDIC Code Page 297 (France)</td>
<td>IBM297</td>
</tr>
<tr>
<td>EBCDIC Code Page 500 (International)</td>
<td>IBM500</td>
</tr>
<tr>
<td>EBCDIC Code Page 1026 (Turkey)</td>
<td>IBM1026</td>
</tr>
<tr>
<td>DOS Code Page 850 (Multilingual Latin I)</td>
<td>IBM850</td>
</tr>
<tr>
<td>DOS Code Page 852 (Latin II)</td>
<td>IBM852</td>
</tr>
<tr>
<td>DOS Code Page 855 (Cyrillic)</td>
<td>IBM855</td>
</tr>
<tr>
<td>DOS Code Page 857 (Turkish)</td>
<td>IBM857</td>
</tr>
<tr>
<td>DOS Code Page 860 (Portuguese)</td>
<td>IBM860</td>
</tr>
<tr>
<td>DOS Code Page 861 (Icelandic)</td>
<td>IBM861</td>
</tr>
<tr>
<td>DOS Code Page 863 (French)</td>
<td>IBM863</td>
</tr>
<tr>
<td>DOS Code Page 865 (Danish, Norwegian)</td>
<td>IBM865</td>
</tr>
<tr>
<td>DOS Code Page 869 (Greek)</td>
<td>IBM869</td>
</tr>
<tr>
<td>Name of Character Set</td>
<td>Alias</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Windows Code Page 932 (Japanese Shift-JIS)</td>
<td>Shift_JIS</td>
</tr>
<tr>
<td>Windows Code Page 874 (Thai)</td>
<td>ibm874</td>
</tr>
<tr>
<td>Windows Code Page 949 (Korean)</td>
<td>KS_C_5601-1987</td>
</tr>
<tr>
<td>Windows Code Page 950 (Traditional Chinese Big 5)</td>
<td>csBig5</td>
</tr>
<tr>
<td>Windows Code Page 1250 (Central Europe)</td>
<td>windows-1250</td>
</tr>
<tr>
<td>Windows Code Page 1251 (Cyrillic)</td>
<td>windows-1251</td>
</tr>
<tr>
<td>Windows Code Page 1252 (Latin I)</td>
<td>windows-1252</td>
</tr>
<tr>
<td>Windows Code Page 1253 (Greek)</td>
<td>windows-1253</td>
</tr>
<tr>
<td>Windows Code Page 1254 (Turkish)</td>
<td>windows-1254</td>
</tr>
<tr>
<td>Windows Code Page 1255 (Hebrew)</td>
<td>windows-1255</td>
</tr>
<tr>
<td>Windows Code Page 1256 (Arabic)</td>
<td>windows-1256</td>
</tr>
<tr>
<td>Windows Code Page 1257 (Baltic)</td>
<td>windows-1257</td>
</tr>
<tr>
<td>ISO-8859-1 (Latin 1)</td>
<td>ISO-8859-1</td>
</tr>
<tr>
<td>ISO-8859-2 (Latin 2)</td>
<td>ISO-8859-2</td>
</tr>
<tr>
<td>ISO-8859-3 (Latin 3)</td>
<td>ISO-8859-3</td>
</tr>
<tr>
<td>ISO-8859-4 (Baltic)</td>
<td>ISO-8859-4</td>
</tr>
<tr>
<td>ISO-8859-5 (Cyrillic)</td>
<td>ISO-8859-5</td>
</tr>
<tr>
<td>ISO-8859-6 (Arabic)</td>
<td>ISO-8859-6</td>
</tr>
<tr>
<td>ISO-8859-7 (Greek)</td>
<td>ISO-8859-7</td>
</tr>
<tr>
<td>ISO-8859-8 (Hebrew)</td>
<td>ISO-8859-8</td>
</tr>
<tr>
<td>ISO-8859-9 (Turkish)</td>
<td>ISO-8859-9</td>
</tr>
<tr>
<td>Mac OS Roman</td>
<td>csMacintosh</td>
</tr>
<tr>
<td>Russian KOI8-R</td>
<td>KOI8-R</td>
</tr>
</tbody>
</table>
Index

A
Action • 51
AD Based Configuration • 33
Adding a New Host Site • 51
Adding Data Types to Rules • 86
Adding Email Addresses and Domains to My Organization • 60
Adding Trusted CAs • 53
Advanced • 45
Advanced Configuration and Troubleshooting • 103
Advanced Expiration Handling • 106
Advanced FTP and HTTP Quotas • 107
Advanced Options for Data Types • 134
Advanced SMTP Quotas • 107
Advanced User Notifications • 108
Alternative Gateway Deployments • 12
Analytical Deployment • 79
Asterisk • 140
Auditing and Analysis • 68

B
Backslash • 138
Blade • 52
Blade Queries • 56
Bypassing HTTPS Inspection to Software Update Services • 52

C
Case Sensitivity • 134
Certificate Blacklisting • 55
Character Set Aliases • 142
Communicating with Data Owners • 72
Communicating with Users • 73
Completing the Wizard • 20
Configuring a Dedicated DLP gateway and Relay on DMZ • 26
Configuring a Dedicated DLP Gateway in Bridge Mode • 20
Configuring a DLP Gateway for a Web Proxy • 23
Configuring a DLP Gateway or Security Cluster • 17
Configuring a Locally Managed DLP-1 Security Cluster • 19
Configuring Active Directory and LDAP for DLP • 21
Configuring Bridge IP Address • 21
Configuring for a Web Proxy • 23
Configuring for an Internal Web Proxy • 24
Configuring HTTP Inspection on All Ports • 116
Configuring HTTPS Inspection • 47
Configuring Incident Log Handling • 40
Configuring More HTTP Ports • 102
Configuring Proxy Settings After Management Upgrade • 24
Configuring the Exchange Security Agent • 41
Configuring the Mail Relay • 25

D
Configuring User Access to an Integrated DLP Gateway • 103
Creating a CA Certificate • 47
Creating Different Rules for Different Departments • 99
Creating Exceptions • 83
Creating Exceptions for Destinations • 83
Creating Exceptions for Protocols • 84
Creating Exceptions for Users • 83
Creating Exceptions with Data Type Groups • 83
Creating New Rules • 79
Curly Brackets • 140
Customized Deployment • 85
Customizing DLP User-Related Notifications • 111
Customizing Notifications • 74
Customizing Notifications for Self-Handling • 75
Customizing Notifications to Data Owners • 75

Data Loss Prevention by Scenario • 79
Data Loss Prevention in SmartDashboard • 58
Data Loss Prevention Policies • 64
Data Loss Prevention Terminology • 10
Data Loss Prevention Wizard • 20
Data Owner and User Notifications • 71
Data Owners • 71
Dedicated Deployments • 18
Dedicated DLP gateway Deployment • 12
Default Deployment • 58
Defining Advanced Matching for Keyword Data Types • 95
Defining Compound Data Types • 89
Defining Data Type Groups • 95
Defining Data Types • 86
Defining Email Addresses • 97
Defining Internal Networks • 62
Defining Internal User Groups • 61
Defining Internal Users • 61
Defining Internal VPNs • 62
Defining My Organization • 60
Defining New File Types • 117
Defining Post Match CPcode for a Data Type • 96
Defining Protocols of DLP Rules • 101
Defining Strictest Security • 100
Deploying Certificates by Using Group Policy • 49
Destination • 50
DLP Actions • 68
DLP Administrator Permissions • 14
DLP and Privacy • 8
DLP Blade Wizard Options • 20
DLP General Columns • 69
DLP Portal • 76
DLP Restricted Columns • 69
DLP Rule Matching Order • 65
DLP Rule Matching with Exceptions • 65
DLP Rule Matching with Multiple Matches • 65
DLP Software Blade Trial License • 17
DLP Supported Platforms • 16
DLP-1 Security Cluster Wizard • 19
DNS Based Configuration • 35
Dot • 138
E
Editing Data Types • 92
Editing Exchange Security Agent Values • 115
Editing Extreme Condition Values • 114
Enabling HTTPS Inspection on a Gateway • 47
Encoding Non-Printable Characters • 139
Escaping Symbols • 138
Event Analysis in SmartEvent • 57
Exchange Security Agent - Configuration Summary • 43
Exchange Security Agent - General • 42
Exchange Security Agent - Inspection Scope • 42
Exchange Security Agent - Trusted Communication • 42
Exchange Server Configuration • 43
Excluding Networks from My Organization • 62
Excluding Users from My Organization • 61
Excluding VPNs from My Organization • 63
Exporting a Certificate from the Security Management Server • 48
Exporting and Deploying the Generated CA • 48
Exporting Data Types • 97
F
File Name Based Server Discovery • 32
Fine Tuning • 85
Fine Tuning for Protocol • 101
Fine Tuning Source and Destination • 98
Flagging Rules • 82
Focusing on Data • 86
G
Gateway Cleanup of All Captured Data • 110
Gateway Cleanup of Expired Data • 109
Gateways Pane • 52
Generating the Certificate Signing Request • 132
Generating the P12 File • 133
H
How it Operates • 46
How It Works • 10
HTTPS Inspection • 46
HTTPS Inspection in SmartEvent • 57
HTTPS Inspection in SmartView Tracker • 56
HTTPS Inspection Queries • 56
HTTPS Validation • 54
Hyphen • 138
I
Important Information • 3
Importing a CA Certificate • 47
Importing Data Types • 97
Initializing Trusted Communication • 43
Install On • 52
Installation and Configuration • 16
Installing the DLP gateway • 16
Installing the Signed Certificate • 133
Installing, Connecting, Verifying Clients • 38
Integrated Deployments • 17
Integrated DLP Security Gateway Deployment • 11
Internal DLP Policy Rules • 80
Internal Firewall Policy for a Dedicated DLP Gateway • 105
Introduction to Data Loss Prevention • 8
Isolating the DMZ • 100
L
Learning Mode • 77
Localizing DLP User-Related Notifications • 113
M
Mail Relay Required Configuration • 25
Managing Rules in Ask User • 77
Managing Rules in Detect • 66
Match Multiple Occurrences • 135
Match Whole Word Only • 136
Message Tracking • 44
Metacharacters • 137
More Options for Rules • 81
N
Name • 50
Notifying Data Owners • 73
Notifying Users • 74
Number (No.) • 50
O
Obtaining and Installing a Trusted Server Certificate • 132
Option Comparison • 32
Ordered Match for Names • 135
Out of the Box • 58
Overview of DLP Rules • 64
P
Parentheses • 138
Parts of the Rule • 50
Permissions for HTTPS Logs • 56
Plus • 140
Predefined Rule • 50
Predefining Rules • 82
Preparing Corporate Guidelines • 72
Prerequisites • 19
Protecting Data by CPcode • 91
Protecting Data By Keyword • 87
Protecting Data by Pattern • 89
Protecting Data by Weighted Keyword • 90
Protecting Documents by Template • 87
Protecting Files • 89
Providing Assistance • 40
Providing Keywords by Dictionary • 90
Proximity of Matched Words • 135
Q
Quantifiers • 139
Question Marks • 140
R
Recommendation - Testing Data Types • 96
Recommended Deployments of a DLP Gateway with a Mail Relay • 27
Regular Expressions • 137
Remote Registry • 36
Renaming the MSI • 37
Required Routing in Bridge Mode • 21
Required VLAN Trunk Interfaces • 21
Rerunning the Data Loss Prevention Wizard • 22
Role of DLP Administrator • 14
Rule Actions • 66
Rule Exceptions • 82
Rule Names and Protocols • 81

S
Saving a CA Certificate • 53
Selective Deployment - Gateways • 67
Selective Deployment - Protocols • 67
Server Certificates • 132
Server Discovery and Trust • 31
Server Discovery and Trust Options • 32
Server Validation • 54
Services • 50
Setting CPMSI_TOOL Parameters • 37
Setting Rule Severity • 82
Setting Rules to Ask User • 75
Setting Rules to Prevent • 86
Setting Up Rule Tracking • 66
Site Category • 50
SmartDashboard Configuration • 42
Source • 50
Specifying Character Types • 139
Square Brackets • 138
Starting the Exchange Security Agent • 44
Statistics • 44
Supported Character Sets • 141
Supporting LDAP Servers with UTF-8 Records • 113

T
The Check Point Solution for DLP • 9
The HTTPS Inspection Policy • 49
The Need for Data Loss Prevention • 8
TLS-Encrypted SMTP Connections • 29
Track • 52
Troubleshooting • 55
  Incidents Do Not Expire • 108
  Mail Server Full • 109
Troubleshooting - Displaying SRV Record Stored in the DNS Server • 36

U
Unhandled UserCheck Incidents • 77
Updating the Trusted CAs List • 53
Upgrading UserCheck Client • 39
UserCheck Client • 30
UserCheck Notifications • 77
Using SmartEvent • 70
Using SmartView Tracker • 68
Using UserCheck with Check Point Password Authentication • 39

V
Vertical Bar • 138
Viewing Information in SmartEvent • 57
Viewing the Certificate • 133

W
What Happens on Rule Match • 13
What Users See and Do • 76