Blue Coat®
Data Loss Prevention Appliance™
Administrator's Guide

Model DLP700/DLP1700/DLP2700

Release 9.0

BLUE COAT

Americas

Blue Coat Systems, Inc
420 N. Mary Ave.
Sunnyvale, CA 94085

Rest of the World

Blue Coat Systems International SARL
3a Route des Arsenaux
1700 Fribourg, Switzerland

BLUE COAT

Contents

DLP appliance Administrator's Guide

Chapter 3 Configure the DLP Manager

Chapter 4 Register Data for Detection

Chapter 10 Backing Up the DLP appliance

Chapter 11 Data-Usage Incident Management and Reporting

Chapter 12 Discovery Incident Management

BLUE COAT

1 Content Inspection and Security

DLP appliance Administrator's Guide

Blue Coat Systems' comprehensive content-security solution works to protect your company's confidential information and other intellectual property from accidental or malicious distribution. Real-time content inspection allows you to secure against the loss of data in all of its states:

- **Data In Motion**—Network traffic, including SMTP and Web protocols.
- **Data At Rest**—Client hard drives, network file shares, and data centers.
- **Data In Use**—File transfers at the endpoint and device-access control.

In addition, the solution scales so you can use a single appliance to protect the data on a single LAN, or tier multiple appliances and agents to protect LANs that are geographically distributed.

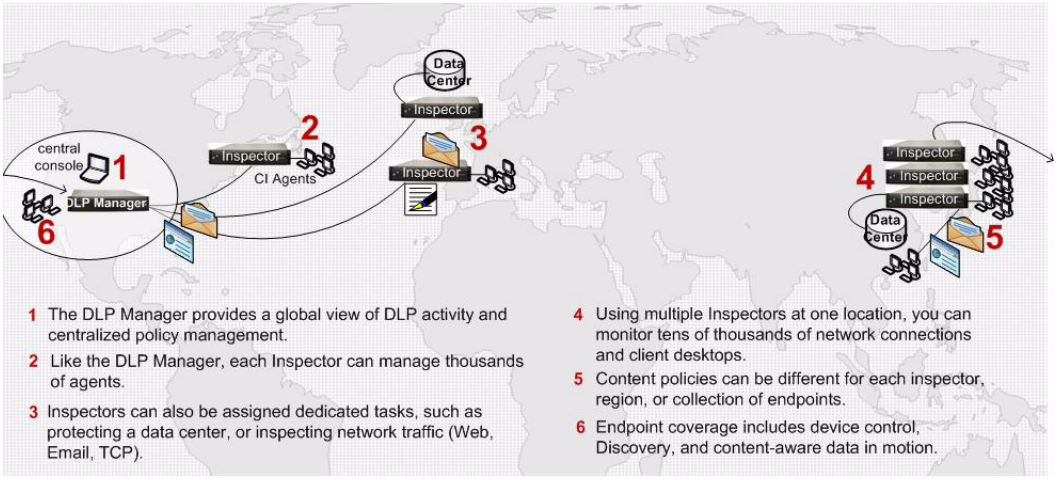


Figure 1.1: Using Inspectors with the DLP Manager and CI Agents allows you to secure data on tens thousands of clients and network connections.

A single DLP Manager can be deployed on the LAN to monitor out-bound email messages, Web uploads, data repositories, and client endpoints. For larger deployments, you need only add one or more Inspectors. CI Agents, deployed to the endpoint to provide real-time and/or scheduled monitoring, can report to the either the manager or a near-by Inspector. Roaming clients can automatically register with the nearest appliance whenever they log in to a branch of the network that is secured by the DLP appliance.

1.1 How It Works

In a nutshell, Content Inspection works by registering data that you want to secure. This data can be in almost any form, including a file share full of PDF and Microsoft Word documents, a database with millions of customer records, or intellectual property such as source code, CAD designs, or business plans. As it is registered, the data is either represented by a "fingerprint," or is recorded whole (if it is short and discrete).

Registered data is then incorporated into a policy. The policy can be associated with one or more inspection services (Data in Motion, Data at Rest, and Data in Use), and further focused to target selected users, groups, locations, etc. In the case of Data At Rest, when the inspection service is run, it will scan every eligible file looking for any that contain any bit of the registered data. For Data in Motion, it will scan the network traffic as it is transferred from one location to another. For Data In Use, agents installed on the endpoint will scan files as they are transferred to an external device, including USB devices such as iPhones and MP3 players, as well as bluetooth and WiFi devices.

Whenever protected content is detected, an incident is created at the DLP Manager and the file can be blocked, passed, retained with the incident, or another action taken. At the endpoints, users can self-remediate their incidents by providing an explanation, which is logged. Other types of incidents can be reviewed by staff.

1.1.1 Types of Inspection

The DLP appliance and CI Agent provide the following types of inspection, detection, and prevention:

Network Inspection - Data In Motion

- **Web traffic**—Inspect HTTP, HTTPS, and FTP traffic for protected data, including files and content typed into Web sites such as Webmail, blogs, Web forms, and some Web-based chat services.
- **Email traffic**—Inspect outbound email traffic, including the message header, body content, and attachments (including compressed files).

- **TCP traffic**—Perform packet-level content inspect of inbound and/or outbound TCP traffic.

File Detection - Data At Rest

- **Server Discovery (appliance based)**—Scan files in network file shares and repositories from either a DLP Manager or Inspector.
- **Endpoint Discovery (agent based)**—Scan files stored on end-user hard drives, attached and connected (Bluetooth and WiFi) devices, and mapped network drives (although appliance-based Discovery is usually recommended). Agent-based scans can be run from the DLP Manager or Inspectors.

Endpoint Protection - Data In Use

- **Content-based file transfers**—Block, allow, encrypt and allow, or justify and allow, file activity according to the file content as the file is being saved, copied, or moved to the protected device. Content is also checked when data is added to a file that already exists on the protected device and is subsequently saved.

  Monitoring can occur while the client is off-line, and the results are logged to the DLP appliance when the client reconnects.
- **Device-based access control**—Block, allow, or encrypt and allow file activity to attached devices according to device type, bus, or device driver (useful for singling out unknown or unique devices). Device policies can also be enforced while the client is off-line.

1.1.2 Components of the DLP Solution

The DLP appliance can be installed as single-tier solution to protect network traffic at a single location. The appliance also supports a variety of larger and/or more complex deployments. In a two-tier solution, the DLP Manager manages one or more Inspectors. Any of the appliances can perform Discovery scans, and any combination can inspect network traffic. The DLP Manager may also manage CI Agents.

In a three-tier solution, the DLP Manager manages one or more Inspectors, which in turn manage CI Agents running on remote endpoints. Inspectors can also be used to run Discovery scans, and/or inspect network traffic. Hundreds, perhaps thousands of agents can report to each appliance. The Inspectors all report back to the central DLP Manager, which can also manage agents and perform network inspection. Policies, reports, and incidents from all clients and inspectors are aggregated at the management console on the DLP Manager.

- **Management Console**— Provides single-point management of Inspectors and/or CI Agents; enables uniform policy construction and incident management, and report aggregation.
- **DLP Manager**—Provides appliance-based Discovery, real-time inspection of data-in-use (TCP, Web, FTP, and Email traffic) and can manage CI Agents and/or remote Inspectors (and their agents).

- **Inspectors**—(optional) Connect to the DLP Manager and can provide dedicated inspection of network traffic, local performance for remote sites, and endpoint management that includes intelligent roaming.
- **CI Agents**—(optional) Provide content-aware Discovery for client endpoints and support policy-based device-control. Activity logs and reports are centralized on the DLP Manager.

1.1.3 High Availability

The DLP Manager supports High Availability (HA) configuration with the addition of a second appliance configured as a redundant DLP Manager. The redundant appliance can be added to the network during the initial set up (recommended), or any time thereafter. HA is available as cold-standby fail-over for the DLP Manager. Configuration is done manually, and should be done in conjunction with Blue Coat Systems technical support.

Inspectors do not typically need HA, as they receive their configuration from the DLP Manager and can readily be replaced. If a Inspector that is managing CI Agents becomes unavailable, the agents reporting to it will automatically report to the DLP Manager, and continue operating in a limited-capacity mode.

In addition, both inspectors and the manager are designed with redundancies to allow immediate resolution in case of hardware failure.

- Dual, hot pluggable hard disks, with RAID 10
- Dual, hot swappable power supplies
- Dual, hot swappable, cooling fans

1.1.4 Endpoint and Appliance Discovery

The DLP appliance provides agent-based and appliance based Discovery. The same policies can be used in both types of Discovery. With agent-based Discovery, you can scan tens of thousands of client endpoints using the same policy, or create different policies for different users, locations, or groups. With the appliance-based Discovery, you can scan file-shares on the local network, and/or remote data centers. Network Discovery supports CIFS, SMB, NFS, WebDAV, and Documentum and can be used to scan terabytes of data.

As with all inspection services, Discovery can recognize data in more than 500 different file formats, scan multi-byte and non-English characters, and detect data contained in compressed archives. In addition, Discovery can support detecting data in hidden files, data that is "hidden," for example in a Microsoft Excel spreadsheet, and non-visible file metadata such as the owner, last modified date, and other associated descriptors.

1.1.5 Fingerprints and Data Detection

The DLP appliance uses a proprietary fingerprinting technology accurately detect data registered from a wide variety of structured and unstructured data sources, including database content, spreadsheets, .CSV files, source code, PDF file content, and Microsoft Office documents.

Data for registration can reside in databases, content management systems such as Stellent or Microsoft SharePoint server, and on network file shares. By default, registered data sources will be re-crawled (i.e., rechecked to include any updates) nightly to ensure that your policies always remain current; the data registered will not get stale.

Data Element Fingerprinting

Data Element Fingerprinting is a highly accurate technique that ensures minimal false positives. With it, you can fingerprint the exact data or personal information you want to protect, as opposed to relying on simple pattern matching or keyword techniques (as do other DLP vendors).

The DLP appliance supports registering up to 40 million data elements from database sources including, Microsoft SQL Server, MySQL, Oracle, Sybase, DB2, PostgreSQL, and CSV files. You can register individual data fields or columns of data that should be protected, and schedule frequent re-scans to ensure currency with the changing data source.

Deep Content Fingerprinting

The algorithms used to perform Deep Content Fingerprinting (DCF) result in fingerprint hashes that are tiny (as small as 1/300th the size of the original document) while at the same time retaining a recognition resolution that can be less than a sentence.

DCF protects unstructured data —content contained in virtually all file types, including Microsoft Office and other documents, across all languages, including multi-byte character sets. The technology consists of a series of sliding hashes that are mathematically reduced to uniquely represent a document and all of its constituent parts.

- Reliably and accurately detect derivatives and excerpts of confidential data independent of format and message protocol
- Supports fingerprinting all languages, including those with non-Roman scripts such as Japanese, Chinese, and Cyrillic.

You create Deep Content Fingerprints either automatically, by “scanning” data repositories, or manually, by uploading files from the Web or other location.

1.1.6 Data Registration

Scanning is a key feature of the DLP appliance, providing an efficient and scalable solution to rapidly register confidential data contained in file shares and repositories such as enterprise content management systems. The data scanning engine recursively traverses file system trees on a file share to identify and efficiently encode confidential data into a set of unique digital signatures. It does this by opening and inspecting files stored in data repositories and then generating unique signatures, similar to an individual's fingerprint. These fingerprints are then stored in a fingerprint database and later used to identify confidential data transmitted on the network, even if the data has been cut and pasted into another document, compressed, or modified.

Flexible Data Registration

- Databases: Microsoft SQL, MySQL, Oracle, Sybase, PostgreSQL, DB2, Informix, and CSV files
- Network Shares: CIFS, SMB, NFS
- Microsoft SharePoint
- Content Management Systems: WebDAV, Documentum, and Stellent

1.1.7 Incident Management

In the DLP domain, the term "Incident" is used to describe the detection of sensitive data that is stored or is being moved outside the LAN. It also includes the notion of intervening in the transaction, either by blocking it, and/or warning the user that the content is protected. Intervening creates a workflow, for example, a third-party review of the content to decide what to do with it. Incidents are automatically created for Data in Use, Data in Motion, and Data Discovery policy violations.

Incident details include a sample of the matching data and the context in which the violation occurred (source, destination, user, protocol, device, etc). In addition, you

can archive the file(s) involved, assign a priority, severity, and/or owner to support the remediation workflow in place for your organization.

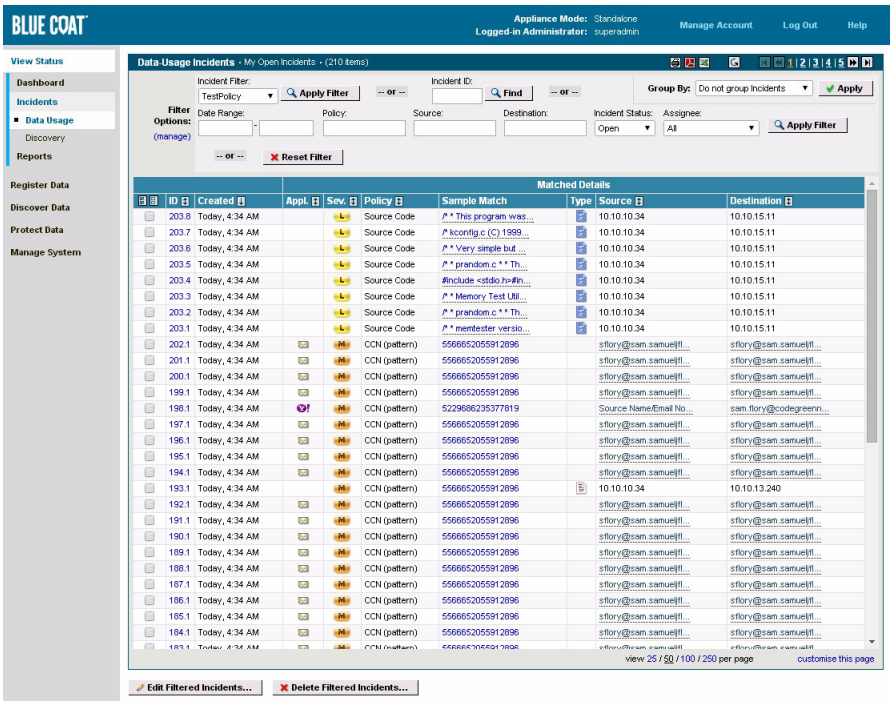


Figure 1.2: You can group incidents, as well as sort them by clicking a column header; clicking an ID will drill down in the Incident to display details.

Incident Notifications

The DLP appliance can automatically notify end-users, policy creators, the registered data owner, and other Incident Reviewers whenever an incident is detected. Configure these notification options in the individual policies. Detailed logging is provided for auditing and forensic investigations. For ICAP incidents, the DLP appliance can block the transaction and display HTML notification window. You can also configure who shall receive an email notifying them of the incident.

Self-Remediation for Endpoint Incidents

Violations at the endpoint can be blocked (that is, the copy or save action is not allowed), the file can be automatically encrypted, or, you can have the user provide a justification and then complete his or her file transfer. Called self remediation, the latter option is used in many organizations as a way of acknowledging the sense of immediacy that is associated with the use of devices used at the endpoint.

With self-remediation, the user's reason is logged with the incident. In addition, you can choose to archive the associated file(s), and/or receive notification of the event. You can also create a custom Action (including notifications and incident assignment) for use with Self Remediation, and in that Action, tailor the notification text you want your users to see.

Discovery Incidents

The DLP appliance supports both appliance-based and agent-based Discovery Discovery. As with Data-in-Motion inspections, when a match for registered data is detected during a Discovery scan, an Incident is created if a condition matching a policy is discovered. The remediation actions you can take for both appliance-based discovery scans and agent-based scans include the ability to copy, move, or delete the file that triggered the Incident.

1.1.8 False Positive Reduction

False positives are the correct detection of incorrect data, and there are two main reasons they can occur in data loss prevention:

To prevent false positives:

1. The data is legitimate for the context in which it was detected (i.e., it is not a mis-use).
2. The source data that was originally registered for detection contained bogus data (for example, in data entry "dummy data" such as 000-00-0000 or "none" is commonly entered in a field that cannot be left blank).

The DLP appliance can mitigate these causes of false positives, providing not only a high detection rate, but high levels of accuracy as well.

Methods of false positive reduction include the DLP appliance GreenList™, row correlation and proximity limits, policy techniques, built-in integrity checking for formulaic numbers (credit cards and social security numbers), and pattern verification.

Pattern Verification

The DLP appliance includes more than 100 pre-defined Regular Expressions that can be used to validate matches prior to creating an incident. In addition, you can create your own RegEx expression to validate your particular data (recommended).

Predefined patterns include credit card numbers, medical codes, US driver's licenses, social security numbers, and European VAT and identification numbers. For custom patterns, the DLP appliance supports standard PERL-compatible regular expressions.

Pattern verification uses the Data Tag feature in DLP appliance to process structured, registered after an initial match has been made. Matches are checked against the appropriate pattern, and only after validity has been determined, is an incident created. See Chapter 4, "Registering Data" on page 48 for details.

1.1.9 Detection Policies

Blue Coat Systems provides a range of customizable, predefined policy templates so you can quickly start detecting data. Policies are assembled from registered data, context constraints, and actions. Context constraints include file filters, source and destination addresses, and protocol constraints. The policy can also be designed to apply to inbound or outbound traffic or both. Exceptions from the GreenList™ can be included to eliminate false positives from commonly used text.

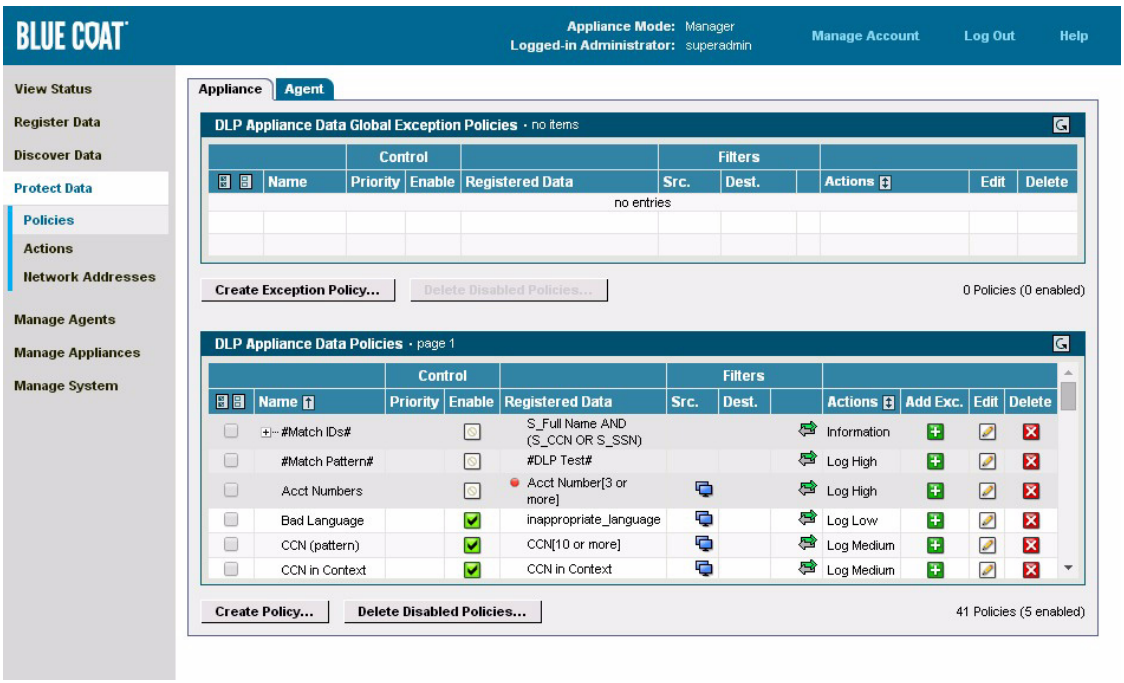


Figure 1.3: Predefined policy templates let you quickly start detecting registered data.

Policy actions determine how a policy will respond when its conditions are met. Network traffic is inspected in real time and compared to policies for matches. Whenever policy conditions are met and a detection occurs, an incident is created that can be assigned to specified reviewers or groups for workflow-driven management. DLP appliance The DLP appliance can also forward messages that match a policy to another MTA for whatever additional processing you need.

Flexible policies allow business rules for data security to be enforced by the DLP appliance. Policies may be based on data as well as contextual constraints including source, destination, protocol, device, or user. The DLP appliance solution comes with predefined policy templates for detecting regulatory compliance violations, personally identifiable information, and personal health information.

All data can be inspected whether occurring in network traffic, or found when scanning for registered data. Sensitive data can be detected in compressed archives, in OLE embedded-objects, and even if the file name and extension have been changed to

disguise the contents (for example, if a file was renamed from **creditcards.doc** to **ssl.dll**). Partial files are detected as well as with entire file matches.

When a violation is detected, policy-based actions allow automatic enforcement of business rules. Other actions include allow, block, quarantine, reroute, and retain a copy.

1.1.10 Exception Policies

You can create an exception policy (as shown in Figure 1.3) attached to a main policy to help target a given type of content occurrence. Exception policies are used to implement the logic, "perform the action in Policy X when a violation is found, except when Policy Y also applies, in which case perform the action in Policy Y." In other words, if all the conditions are met in both the main policy and the exception policy, the action in the exception policy will take precedence.

For example, you might create a policy to monitor all outgoing email except when it comes from the CEO. In this example, you would create a main policy with that monitors your entire email domain, and then attach an exception policy with a source constraint that contains the CEO's email address. The action in the main policy would be to create an incident and send a notification, whereas the action in the exception policy would be set to "Do Nothing."

Each policy can have up to 10 exception policies attached. Upon detecting a policy match, the DLP appliance will then quickly check the list of policy exceptions (if any). If an exception is found to apply, further evaluation will stop and any remaining exceptions on the list will be skipped. As such, you can order the list according to priority and the likelihood of a match.

Exception policies are parent-specific; they cannot be reused in other policies. You can, of course, always clone an exception and attach it to other policies.

2 Set Up the Appliance Hardware

The tasks in this chapter focus on connecting the DLP appliance to your network and configuring it to accept network traffic. You should have an environment suitable for the initial deployment of a network scanning device, i.e., one with access to "living" resources such as high-volume network traffic, an MTA, a populated LDAP, yet at the same time, one that will not put your network at risk in case of error during set up.

This chapter covers the following tasks:

2.1 Overview of the Network Setup

You will need to assign an IP address to each DLP appliance port you will run a cable to, including the management console and (optionally) the CI Agent communications port. Have those IP addresses ready, as well as a network switch with as many as six available ports.

If you will be using a tap (for packet monitoring) put the tap just inside the gateway or firewall, between segments, VLANs, or wherever it will encounter all TCP traffic. The tap ports, Ethernet port 0 and Ethernet port 1, do not need an IP address.

Note: Traffic scanned through eth3 (SMTP) and eth4 (Web) will also be detected through TCP packet monitoring at the tap ports (eth0 and eth1). Create exclusion policies to avoid redundant detection.

Begin by adding the appliance to the rack, then connect the power cables, keyboard, and monitor to the box. Connect Ethernet cables to the Appliance for the inspection services you will use, but wait before connecting them to the tap or mirror until you can confirm the connectivity of each assigned IP address and cable connection.

After you power on the box, the monitor will display the DLP appliance's command line interface. You will use it to assign an IP address to Ethernet port 2, the management console port. When finished, you can disconnect the monitor and keyboard and continue the remaining set up from the Web browser of a connected client.

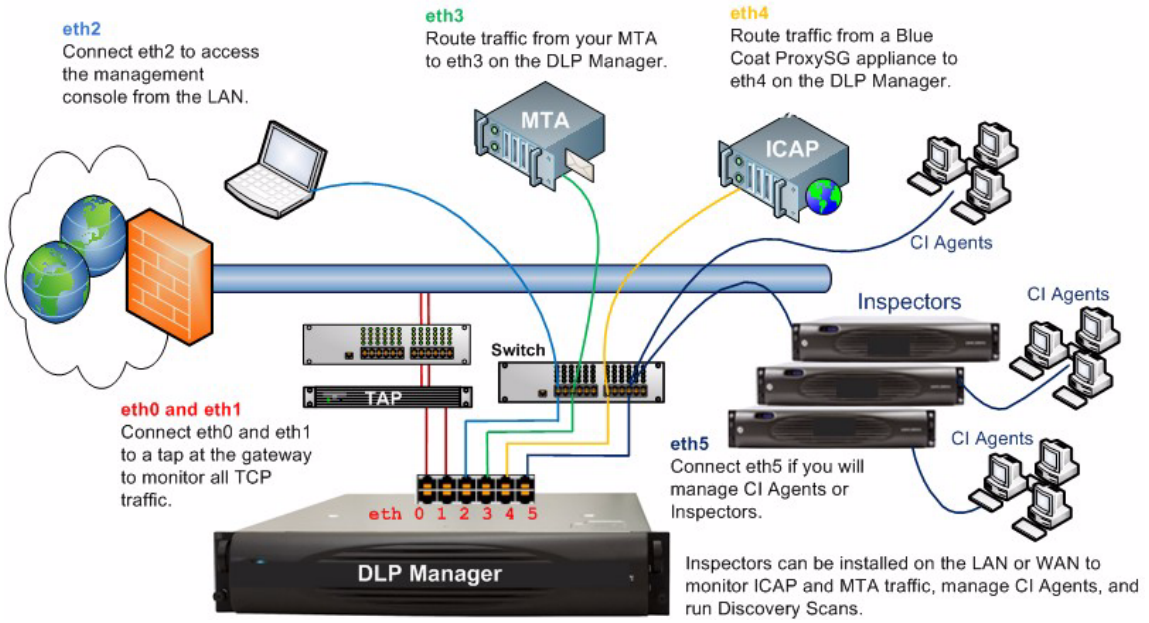


Figure 2.1: Ethernet ports eth0 and eth1 on the DLP appliance are connected to a tap (for TCP traffic auditing and policy testing) while eth2, eth3, eth4, and eth5 are connected to a switch.

In figure Figure 2.1, traffic from the MTA and ICAP proxy is routed through the DLP appliance, where the data is checked in real-time for the occurrence of content that has been registered for detection. Agent-based Discovery scans extend the protection to data repositories (i.e., client endpoints) while Appliance-based Discovery allows you to monitor the content of network file shares (CIFS, SMB, and others).

2.1.1 Ports and Layout

The DLP appliance includes six network ports, four for inspecting network traffic (TCP, SMTP, Web,) and two for management connections (Inspectors and/or CI Agents and the management console). The table below explains the function of each network port.

Table 2.1: DLP appliance ports and connections; ports are labeled on the DLP appliance.

Port	Function	Notes
eth0 eth1	TCP packet monitoring; audit only, optional	Typically connects to a network tap at the gateway, with Ethernet port 0 connected to the LAN and Ethernet port 1 to the WAN. You do not need to assign an IP address to either eth0 or eth1. **Note:** Packet monitoring is enabled by default in the management console. You can connect these ports to the network without affecting traffic whether or not you want to use Packet Monitoring.
eth2	Management console, required	Provides access to the browser-based management console. The IP address is pre-set to `192.168.127.127`.
eth3	MTA, optional	Receives SMTP traffic from a configured MTA; must be configured and enabled prior to use. Can be connected to the network and configured but not used. Traffic is controlled at the MTA. Can inspect inbound and outbound traffic with a duplex switch.
eth4	ICAP, optional	Typically configured to receive outbound Web traffic from an ICAP client. Must be configured in the management console prior to use. Can be connected to the network but not used. Traffic is controlled at the ICAP client. Can inspect inbound and outbound traffic with a duplex switch.
eth5	Central Management, optional	Used in Data Center Discovery for receiving files to scan. Receives incident logs from connected CI Agents. Handles data detection and device control policies for the endpoint. Also used to propagate policies to Inspectors in an two-tier topology. Must be enabled and configured prior to use. Can be connected and configured but not used.

Note: Refer to the back of the appliance for the Ethernet port labels.

2.2 Setting up the Appliance Hardware

The DLP appliance ships with the Versa Rail Slide Kit for mounting the DLP appliance into a rack. This kit includes two four-post rails that have round unthreaded holes and a mounting depth of 27-1/2 inches to 29 inches.

If you have a different rack configuration, contact Blue Coat Systems technical support.

Rack and Hardware:

- Suitable network environment for initial deployment and testing
- DLP appliance, including rack mounts and power cables
- Rack space, including power supply and switch ports
- Tap or mirror port, installed at the network gateway or other suitable location
- Up to six CAT5e or CAT6 copper Ethernet cables
- Up to six IP addresses, verified, that can be assigned to the DLP appliance
- USB keyboard
- Monitor with HD-15 VGA male connector
- Laptop or other workstation connected to the LAN on which the DLP appliance is being installed

DLP Appliance Parts and Hardware:

- Data Loss Prevention appliance
- Quick Start Guide
- AC power cords (2)
- Safety & Regulatory Compliances
- Rack-mounting kit
  - Rack-mounting instructions
  - Mounting rails
- Software License Agreement
- Accessing the Documentation

2.2.1 Mount the Appliance

Place the DLP appliance in a standard, 19-inch four-post rack, or on a free-standing device such as a sturdy desktop. Be sure to allow at least two inches clearance in all directions to ensure adequate ventilation and cooling.

2.2.2 Connect the Appliance to Power

The DLP appliance uses 120-volt, 60Hz alternating current.

1. Connect the power cables to each of the power connections on the back of the DLP appliance.
2. Plug one power cable into a power source, and the other into a backup power supply. Do not power on the appliance until after you have connected the network cables.

2.2.3 Power On the Appliance

1. Press the power button on the lower left of the front face of the DLP appliance. The power indicators will light up and the fans will turn on.
2. Attach the bezel to the front of the appliance.

2.2.4 Set the Management Port

Ethernet port 2 on the DLP appliance comes preset with the IP address, `192.168.127.127` that you can use to access the management console to change the Ethernet port 2 to one that is appropriate for your LAN.

If you are unable to open the management console by pointing a Web browser at `192.168.127.127`, you can connect a keyboard and monitor to the DLP appliance and then use the command console to assign an IP address to Ethernet port 2 and then access it using a Web browser to set the remaining configurations.

To configure the Ethernet 2 port (Command Line):

1. Connect a keyboard and monitor to the ports at the back of the DLP appliance.
2. If the power is not turned on, turn it on.
3. Log in to the appliance using the following credentials:

   Username: `dlpremote`

   Password: `Rem0teUs3r`
4. At the command prompt that appears, type the following: to assign an IP address to the management port:

   ```
   set_eth2 –a 10.10.1.5/22 –g 10.10.1.1
   ```

   where *10.10.1.5* is the IP address you will assign Ethernet port 2 and *10.10.1.1* is the corresponding gateway.
5. Log out when finished.

2.2.5 Connect the Remaining Cables

As a matter of convenience, you may want to attach cables to all the ports you will intend to use, and then configure the ports through the management console as you perform the larger task of setting up each given inspection service. If you decide to attach all the cables at once, be sure to confirm connectivity for each as it is connected.

To connect the remaining cables:

1. Ping the intended IP address to confirm it is not being used.
2. Connect one end of a Ethernet cable to a selected port on the appliance, and other to a switch (or tap, or mirror, or router) on the LAN.
3. Check the network lights at the back of the DLP appliance for port activity.
4. Open the management console and assign the remaining Ethernet ports, as explained next

2.2.6 Open the Management Console

To open the management console, relocate to a client with a Web browser that has access to the DLP appliance.

1. To open the management console:

   For initial configuration, type the IP address for Ethernet port 2 on the DLP appliance:

   `http://192.168.127.127`

2. Alternatively, type the IP address that you assigned Ethernet port 2 port, for example:

   `http://10.10.1.5`

3. In the management console that appears, log in using the following default credentials:

   - **Username**: superadmin
   - **Password**: password

4. Click **Log In**. The Dashboard appears.

2.2.7 Set the Remaining Ethernet Ports

Perform this task to assign an IP address and gateway to the Ethernet Ports on the DLP appliance.

To set a port:

1. In the management console, click **Manage System > Configuration > Network | Interfaces**.
2. Click the **Edit** icon for the Ethernet interface you want to set.
3. Click the **Settings** tab.
4. In the **IP Address/Mask** field, enter the IP address/mask and gateway you will assign to the ICAP port, for example,

   ```
   10.10.1.9/22
   10.10.1.1
   ```

5. In the **Speed/Duplex** field, accept the default value **Auto-negotiate** or choose one of the settings from the drop-down list to match your switch hardware.
6. If you want to change the name of the interface, click the **General** tab and enter the new name in the **Description** field.
7. Click **OK** to save the changes and close the window.

2.2.8 Confirm that the Appliance is Receiving Traffic

To confirm that the Appliance is receiving traffic:

1. In the management console, click **View Status > Dashboard.**
2. In the Health Monitor window pane, click the Inspection Services tab and/or Interfaces. The ICAP status icon should be green. If it is red (service is connected but not receiving traffic) or gray (service is disabled), check the associated message and begin troubleshooting.
3. If the icon is green, click **Manage System > Configuration > Inspection Services | ICAP | Statistics** for request and response statistics.
4. Alternatively, you can click **Manage System > Configuration > Network | Interfaces**.

5. In the window that appears, click the **Edit** icon for a port interface and then the Statistics tab.

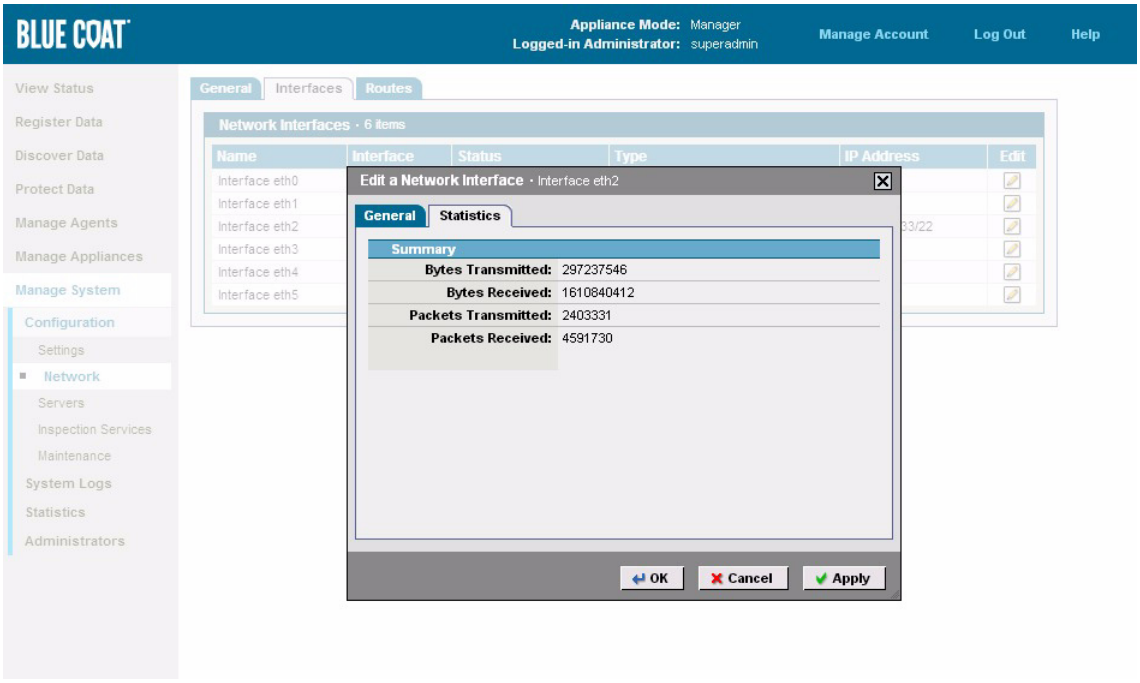


Figure 2.2: After assigning IP addresses the DLP appliance ports, check that they are receiving network traffic by viewing the Statistics tab (shown here).

3 Configure the DLP Manager

This chapter provides a logical procession of the configuration tasks that you need to put in place in support of data detection. It assumes you have made the hardware connections described in Chapter 3. Chapters 5, 6, and 7 build upon the tasks completed in this chapter to guide you through setting up network inspections, registering data, and creating detection policies.

This chapter includes the following tasks (those marked with an * are optional):

3.1 Open the Management Console

To open the management console, relocate to a client that has access to the DLP appliance. To use the management console, the client must have a supported Web browser: Internet Explorer version 7.0 and later or Firefox version 3.0 and later.

1. In the Web browser, type a URL using the IP address that you assigned to eth2 port. The default IP address is shown below:

   ```
   http://192.168.127.127/
   https://192.168.127.127/
   ```

2. Log in using the following default credentials:

   - **Username**—superadmin
   - **Password**—password

3.1.1 Opening the Management Console for Cloud-Based Discovery (Cloud Content Control)

When using a DLP appliance. to discover data on cloud-based file-sharing services ("clouds"), you need to log in to the Management Console using a secure HyperText Transfer Protocol (HTTPS) session and enter the fully qualified domain name (FQDN) of the appliance.

To open the Management Console and log into a cloud via the Cloud page (**Manage System> Configuration > Servers > Cloud):**

1. In the Web browser, enter https:// and type the fully qualified domain name (FQDN) for the DLP appliance, for example:

   ```
   https://dlpappliance.domain.com
   ```

3.2 Change the Management Console Password

The DLP appliance comes with two pre-defined user accounts, as shown in the table below. Blue Coat Systems recommends that you change the default passwords for both accounts to something more secure. In addition, you should create at least one addi-

tional Administrator account with superadmin rights. This backup account can be useful in case the superadmin account becomes inaccessible.

Table 3.1: Default accounts are shown below. User names and passwords are case sensitive.

User Name	Password	Description
superadmin	password	Complete view and edit rights for appliance management, incidents, and redacted content.
_____	_____	Backup superadmin-level account
incidentadmin	password	Limits access to only the Manage Appliances screens; administrators are unable to view incident data that has been redacted.

To change an account password:

1. Log in a "superadmin" and then, in the DLP Manager click **Manage System > Administrators**.
2. Click the **Edit** icon for the superadmin user.

In the screen that appears, type a new password for the superadmin user. Note that both the Username and Password are case sensitive.

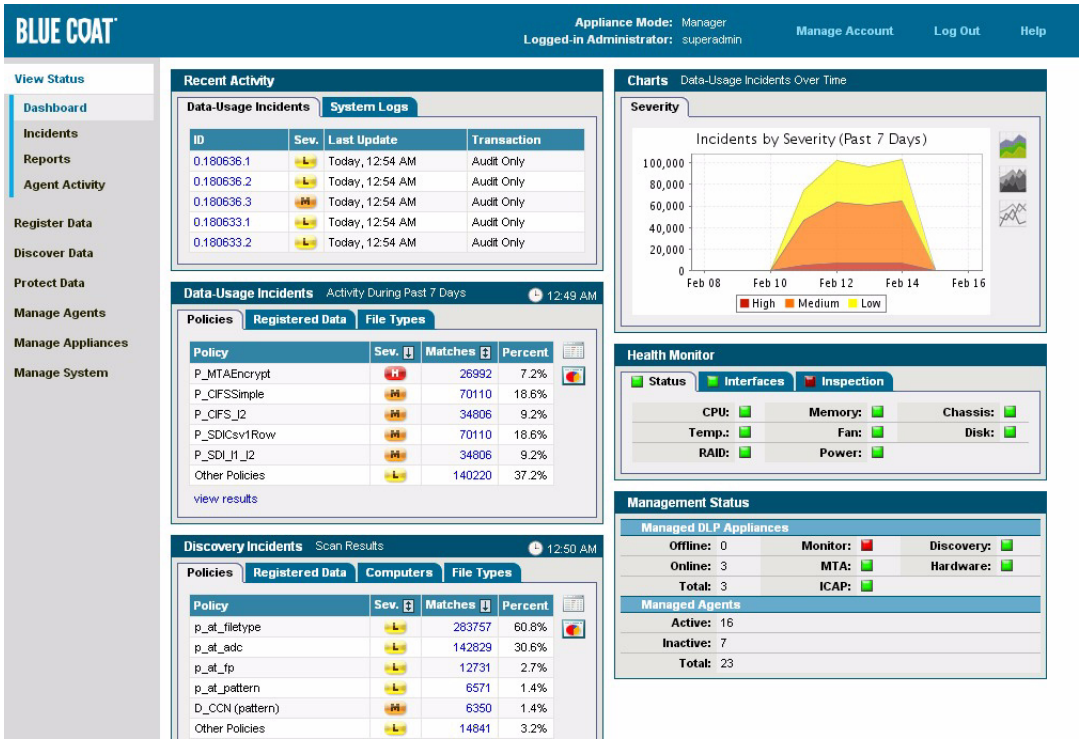


Figure 3.1: The DLP appliance Dashboard provides a snap shot of system data as well as navigational shortcuts.

3.3 Configure the Role of the Appliance

As noted in Chapter 1, any DLP appliance can designated as the Manager or an Inspector according to the deployment type. Choose **Stand-alone mode** if the DLP appliance will represent a single-tier solution, i.e. a single appliance will operate alone at one location to inspect network traffic. Multiple Managers can be deployed for independent operation within the same organization, of course, but in this case each must be individually maintained. To share policies and aggregate reports, etc. you would need a two-tier deployment.

Choose **Manager mode** if the DLP appliance will be part of s two- or three-tier solution. In a two-tier solution, the DLP Manager directly manages one or more Inspectors, and or CI Agents. Those devices report to the Manager. They can perform Discovery scans and/or inspect network traffic (as can the Manager). In a three-tier solution, the DLP Manager manages one or more Inspectors, which in turn manage CI Agents running on remote endpoints. Inspectors can also be used to run Discovery scans, and/or inspect network traffic. Hundreds, perhaps thousands of agents can report to each appliance. The Inspectors all report back to the central DLP Manager, which can also manage agents and perform network inspection. Policies, reports, and incidents from all clients and inspectors are aggregated at the management console on the DLP Manager.

Note: Provide a Host Name for a Manager or Inspector if it will manage CI Agents. This corresponds to the eth 5 interface on the appliance.

Choose **Inspector mode** if the DLP appliance will report to a Manager and/or manage CI Agents of it’s own. Inspectors receive their policy configurations from the Manager.

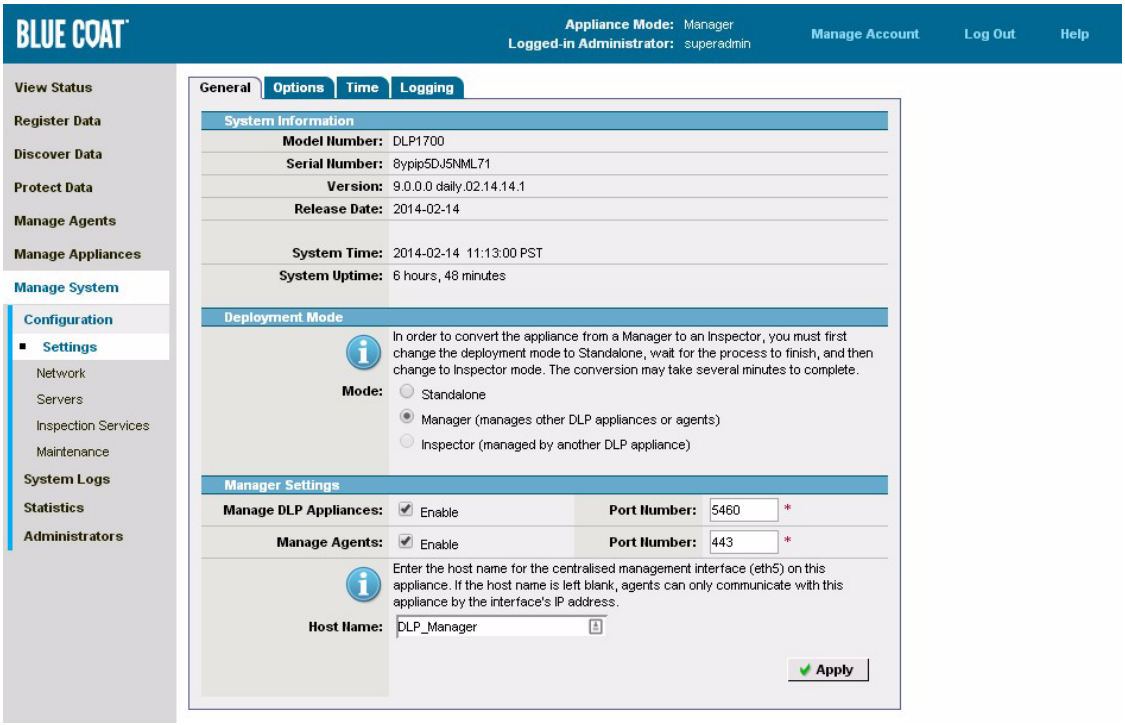


Figure 3.2: The DLP appliance can be deployed independently, in Stand-alone mode, it can manage other appliances and/or CI Agents in Manager mode, or it can serve as an Inspector to check data in motion and/or manage CI Agents.

In summary:

- **DLP Manager**—Provides appliance-based Discovery, real-time inspection of data-in-use (TCP, Web, FTP, and Email traffic) and can manage CI Agents and/or remote Inspectors (and their agents).
- **Inspectors**—(optional) Connect to the DLP Manager and can provide dedicated inspection of network traffic, local performance for remote sites, and endpoint management that includes intelligent roaming.
- **CI Agents**—(optional) Provide content-aware Discovery for client endpoints and support policy-based device-control. Activity logs and reports are centralized on the DLP Manager.

To configure the deployment mode:

1. In the management console, click **Manage System > Configuration > Settings | General.**
2. Under Deployment Mode, choose the role of the appliance: Stand-alone, Manager, or Inspector.
   - If the appliance is a Manager and manage Inspectors, configure the port they will use to connect. The default is 5460.

- If the appliance is a Manager or Inspector and will manage CI Agents, likewise, configure the port they will use to connect. The default is 443.

3. Click **Apply** to save your changes.

3.4 Use a Host Name and Local DNS

You can have the DLP appliance use a local domain name server to resolve IP addresses; this will allow you to use the host name rather than IP address for the DLP Manager URL. In addition, it will allow you to enter host names rather than IP addresses for such configurations in the management console. This can be advantageous, for example, in the event that the IP address for a server the DLP appliance connects changes. You will not need to update the DLP Manager or the Agent/Inspector security certificates to retain the connection.

1. In the management console, click **Manage System > Configuration > Network | General.**
2. Under Domain Name Server IP Addresses, enter the IP address of up to three DNS servers that are accessible to the DLP appliance (typically, the corporate DNS).

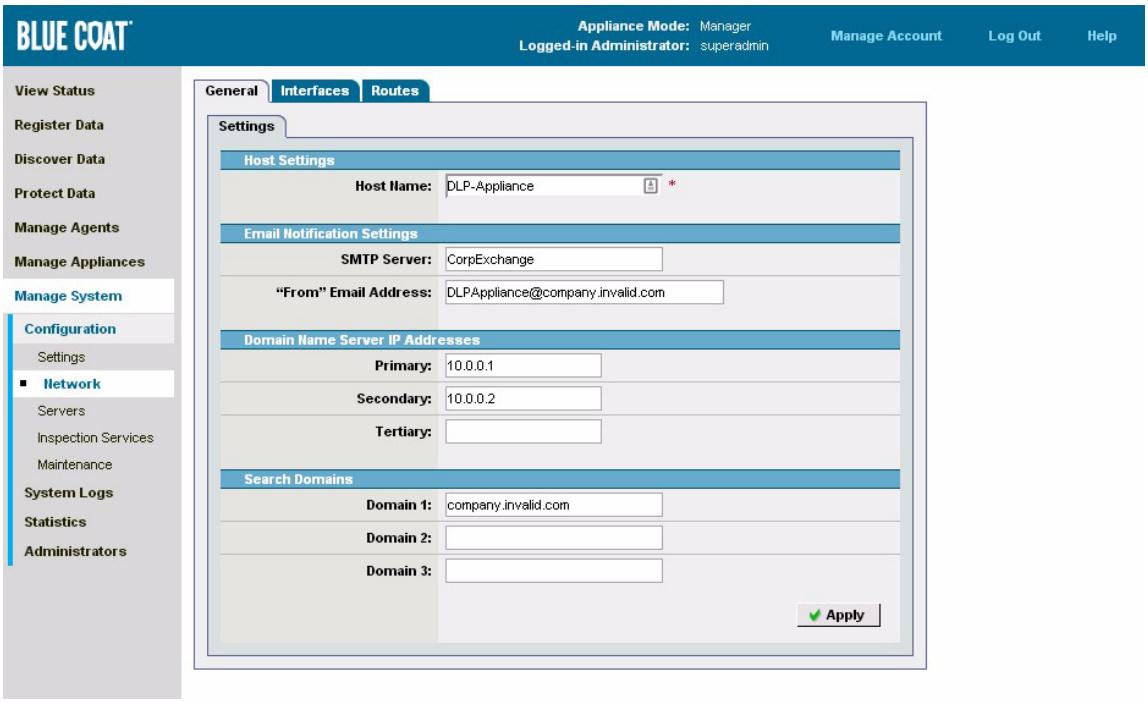


Figure 3.3: Give the DLP appliance a host name (for eth2) and provide a search domain and DNS to make configurations more robust.

3.5 Configure Email Notifications

You can have the DLP appliance automatically email you or designated others whenever it detects a policy match during network inspection (i.e., an incident occurs), when a scan for a share or a table is completed during Discovery, or when incident updates occur.

Notifications can be sent to Incident Reviewers, the person who created policy that triggered the match, and/or the person who registered the data that triggered the match. By creating different detection thresholds and Actions for different event severities, you can control when and how often a given notification will be triggered.

For email incidents, you have the option to send an email message to the Sender whenever a policy match occurs. You can also configure the DLP appliance to send notifications for system events, configuration changes, incident updates, and whenever someone logs in to the console.

When conducting a Discovery scan of a file share, there are implicit email notifications for the Scan Creator and the Scan Owner. The Scan Creator will be sent an email upon completion of the scan for each share defined in the CSV file for the scan. The Share Owner defined in the CSV file will receive an email if an email address is specified in the share_owner_email_address field in the CSV file for each share that has an email address defined for it. See "Creating a New Workflow Action" on page 169 for more information.

Start by setting up a SNMP server for notifications and then configure an email address to the administrator account, one or more Actions that include sending a notification, and a Policy that includes the Action with the embedded notification rule.

3.5.1 Set up a Notification Server

The SMTP server you designate for email notifications must be configured to allow message relays from the DLP appliance.

To designate a SMTP server for notifications:

1. In the management console, click **Manage System > Configuration> Network | General**.
2. In the **SMTP Server:** field, enter the host name or IP address of the server you will use to send notifications (see Figure 3.3).
3. Enter the email address you want to use as the message Sender; this address will appear in the From: field (and may receive Reply To responses from notified users).

3.5.2 Configure an Email Address

Email addresses can be attached to administrator accounts. Because user accounts can be included in Actions and Actions attached to Policies, email notifications can be sent to designated users whenever a policy match or a specified type of incident update occurs. The same holds true for log events.

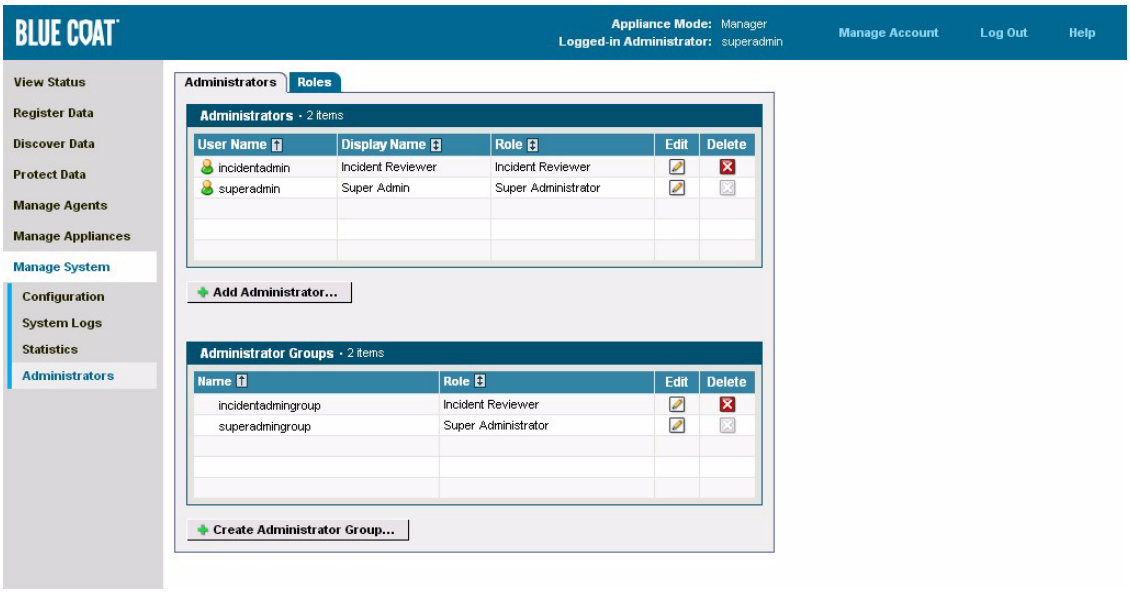


Figure 3.4: Assign an email address to one or more Administrator accounts so the account can receive email notifications.

Note that you should already have a notification server set up before assigning an email address for the user account.

To enable an administrator to receive email notifications:

1. In the management console, click **Manage System > Administrators**.
2. Click the **Edit** icon for the desired administrator user (or click the **Add Administrator...** button to create a new user to whom you want to send notifications).
3. Enter the email address to which you want notifications sent. Fill out the rest of the screen as desired, and click **OK**.

   Hint: If you want notifications to reach multiple recipients, or recipients who do not have an account on the DLP appliance, specify a Distribution List (supported on the SMTP relay) for the given account. For example, create a new administrator with the name "notification-list" and specify an email address that is a DL for the target recipients.

3.5.3 Add a Notification to an Action

You should already have a notification server configured and an email address assigned to the superadmin (or another) account before creating a notify Action. See the procedures above for instructions.

Note: These notifications are used for data-usage incidents only, not for Discovery incidents.

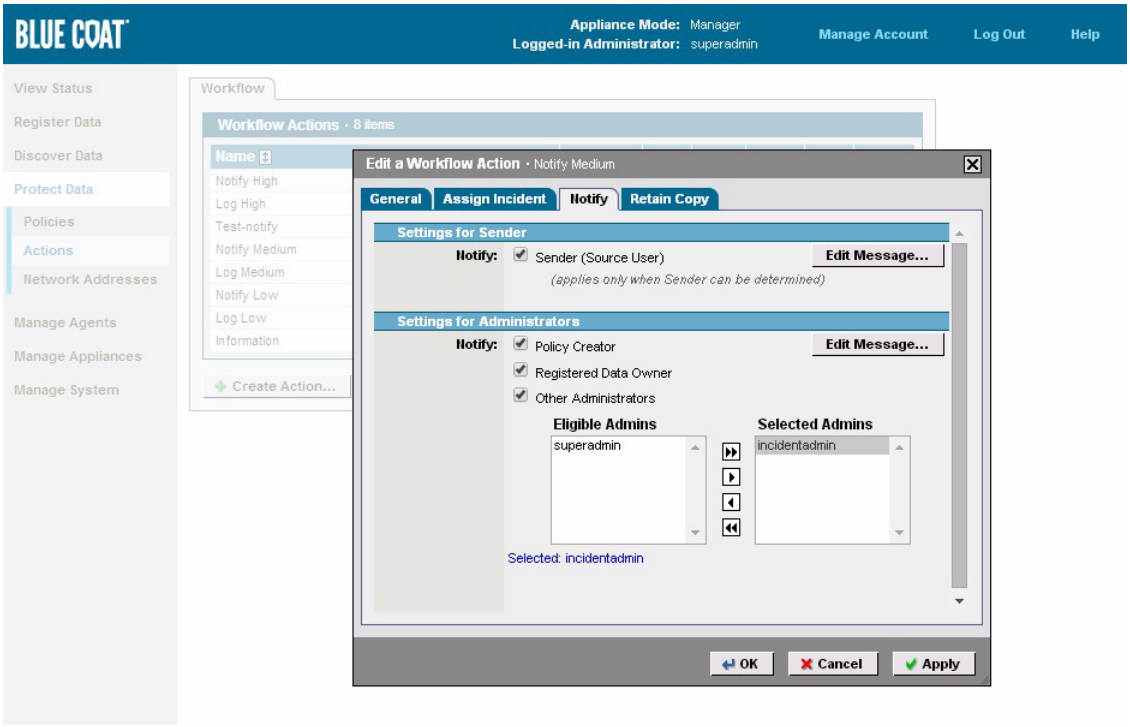


Figure 3.5: Create a new Action or modify an existing one to send a notification message whenever an incident occurs.

To add notifications to an existing Action:

1. In the management console, click **Protect Data > Actions** and then the **Edit icon** for the Action you will use in the first policy that you create (or, click the **Create Action...** button to create a custom action with a unique name).
2. Fill out the general options on the screen that appears. For this example, create a name that starts with the word "notify" to make this Action clear when it appears in a list of Actions.
3. Select **Enable** for the **Notify** option.
4. Next, configure the Incident options (explained below):
   - **Sender**—choose this option to automatically notify the email Sender whenever a message they originated is found to contain sensitive or restricted data. Note: In addition to notifying the sender, you can automatically block sensitive messages.

- **Policy Creator**—choose this option to notify the administrator who created the policy that triggered the match that a violation has been detected.
- **Registered Data Owner**—choose this option to notify the administrator who registered the data, or created the "fingerprint," that a data match has been detected.
- **Other Administrators**—choose this option to notify the selected accounts whenever a policy match occurs.
- **Edit Messages...**—choose this option and then either create a custom message or use the default. An example notification message is shown below (note that the To and From fields have been redacted, as configured on the **Manage System > Configuration > Settings | Options** page).

```
A recent transmission has automatically been logged due to
its content.

Transmission Details:
Incident ID             : 1327.22
Status                  : Audit Only
Time                    : 2011-06-03 10:46:22 PST
From                    : ########@############.###;
To                      : ########@############.###;
Subject                 : testing notifications
Matched Details:
Policy Name             : Competition
Action Taken            : email swenson
```

5. When finished, the Action will be available to embed in policies.

3.5.4 Add Enable Notifications in a Policy

You should already have a notification server configured and an email address assigned to the superadmin (or another) account, as well as one or more Actions configured to include Notifications before adding the Action to a policy. See the procedures above for instructions.

To enable notifications in a policy:

1. In the management console, click **Protect Data > Policies** and then either the **Create Policy...** button or the **Edit** icon to the right of an existing policy).
2. In the **General** tab that appears, select an Action that includes a "notify" option.

3. Configure the rest of the policy. When data is detected that contains registered data, and the conditions meet all of the criteria specified in the policy, a notification will be sent according to the settings in the Action.

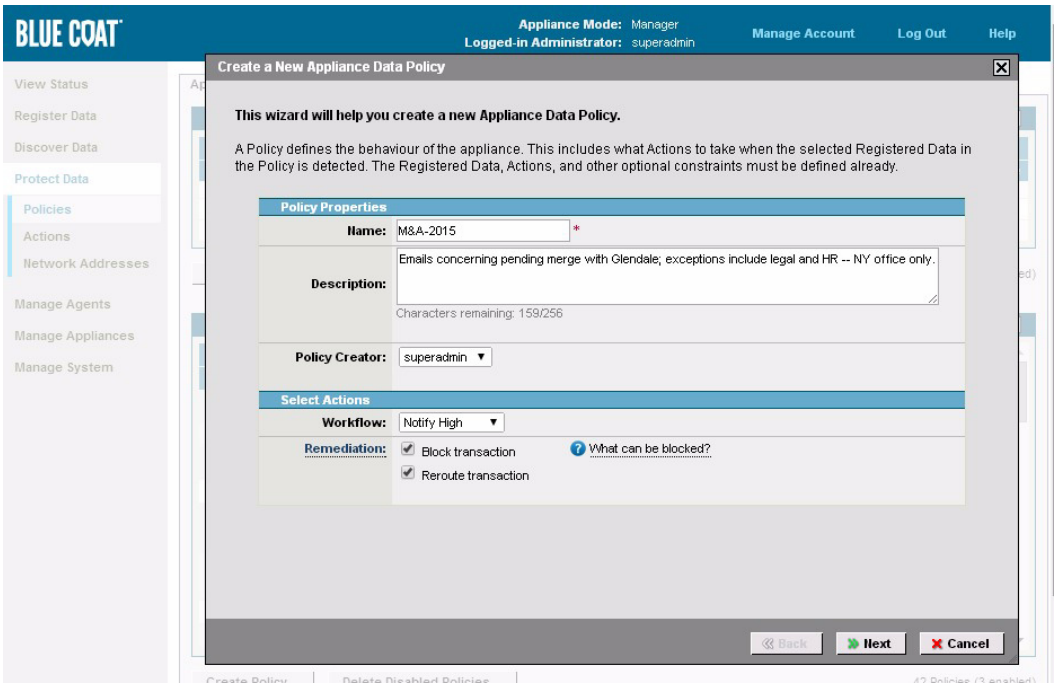


Figure 3.6: Receive incident notifications by specifying an Action with “notify” in the Policy.

3.5.5 Configure Incident Management Notifications

You should already have a notification server configured and an email address assigned to the superadmin (or another) account. See the procedures above for instructions.

You can configure email notifications to be sent to administrators when certain incident updates occur. These email notifications are designed to alert administrators when an incident that is assigned to them or to their assignee group is updated by another administrator. The table below describes the incident updates that can be selected to trigger an email notification to be sent.

Table 3.2: Incident Updates to Trigger Email Notifications.

Value	Description
I am added to this capacity (after incident creation)	Email notification is sent when the selected administrator is added as an incident assignee after the incident has been created.
The Resolution changes	Email notification is sent when the incident's Resolution category changes.
The Severity, Priority, or Incident Status changes	Email notification is sent when the incident's Severity, Priority, or Incident Status changes.
A comment is added	Email notification is sent when a comment is added to the incident.

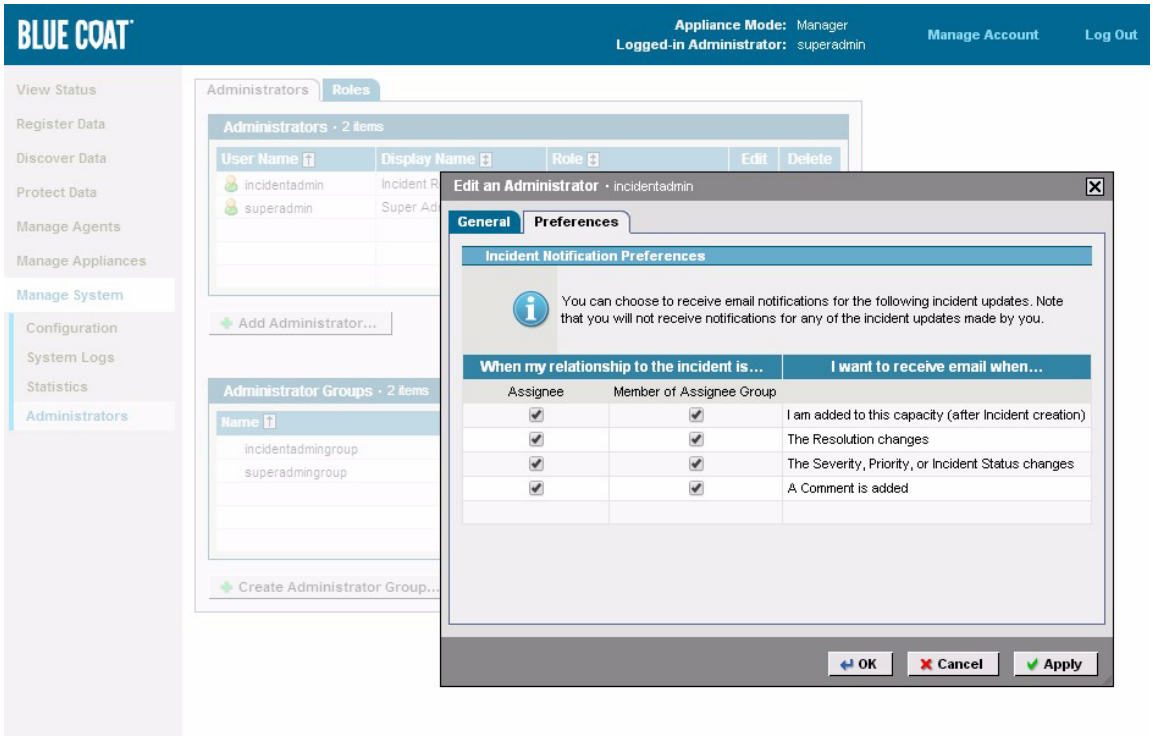


Figure 3.7: Configure email notifications for incident updates.

To configure email notifications to be sent when incident updates occur:

1. In the management console, click **Manage System > Administrators**. The Administrators screen is displayed.
2. Click the **Edit** icon beside the administrator for whom you want to configure email notifications. The Edit an Administrator dialog box is displayed.
3. Click the **Preferences** tab.
4. For each type of incident update for which you want the selected administrator to receive email notifications, check the **Assignee** and/or **Member of Assignee Group** box. Check **Assignee** to enable email notifications for updates made to incidents assigned to the selected administrator; check **Member of Assignee Group** for updates made to incidents assigned to the selected administrator's assignee group.
5. Click the **Apply** button and then the **OK** button.

3.6 Connect to an Active Directory Server

Connecting the DLP appliance to an LDAP server allows you target your Policies according to the users, groups, and/or computers in your directory. This can be especially useful when using CI Agents to monitor client endpoints because it allows you to view workstation names and user log in credentials. In addition, you can consolidate related email and ICAP incidents by user name. Without AD, you will need to create (and separately manage) users for named policy targets.

DLP appliance supports the following LDAP servers:

- Microsoft Active Directory 2000, 2003, 2008
- openLDAP
- Apple Directory Services

The configuration described below is for Microsoft Active Directory. See your LDAP server documentation to find the equivalent of any AD example shown below.

To connect to an Active Directory server:

1. In the console, click **Manage System > Configuration > Servers | Active Directory.**

2. Click **Enable** to use Active Directory, and fill out the rest of the page as appropriate for your environment (refer to the online help for questions on a particular field).

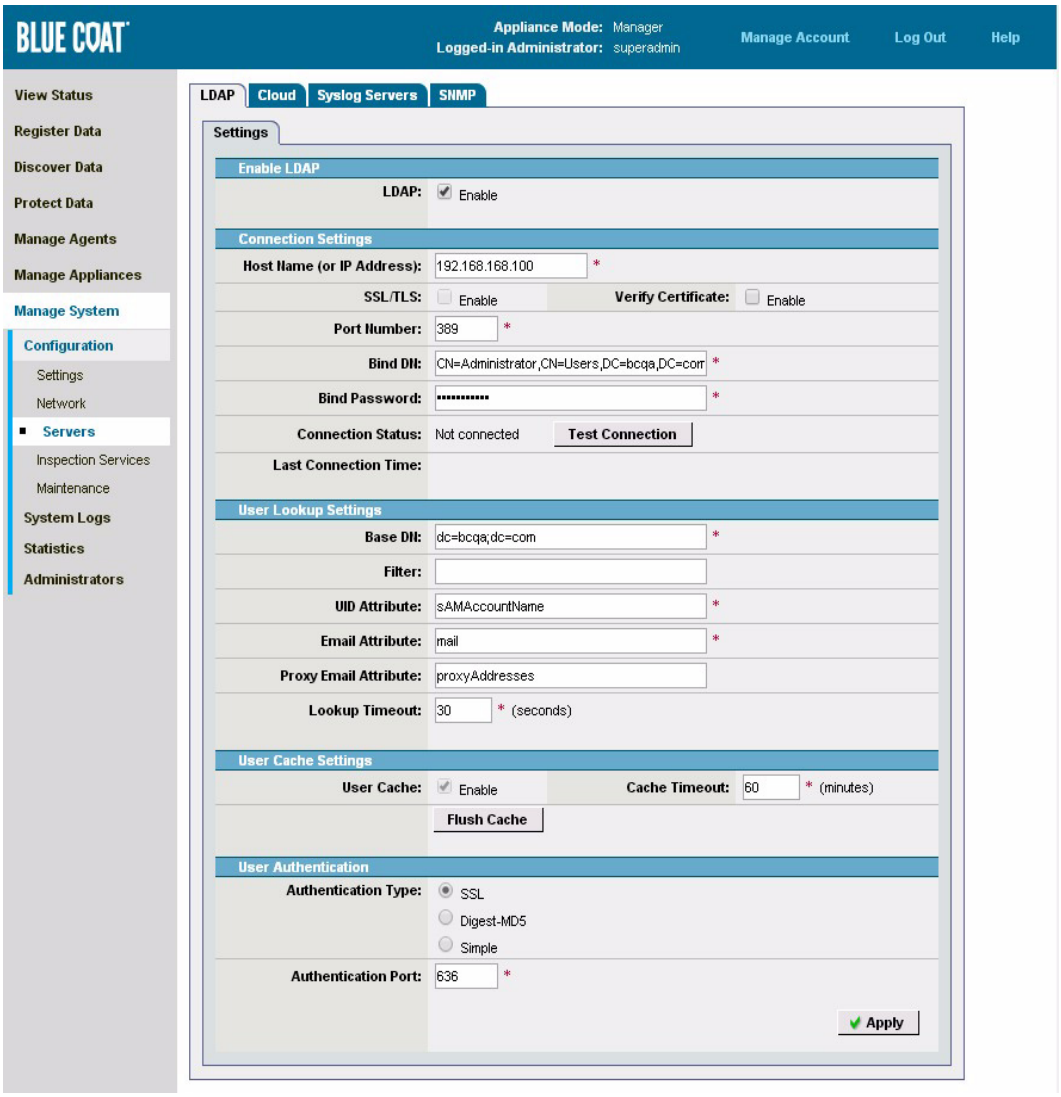


Figure 3.8: Setting up a connection to an LDAP server can extend the power of the DLP appliance.

3.7 Set the System Time

System time is used for logs and reports. You can set the time manually, connect to the pre-configured Internet time servers (0.us.pool.ntp.org or 0.asia.pool.ntp.org), or define your own time server and point to that.

Note: If multiple DLP appliances are connected across different time zones (for example, with Inspectors or CI Agents), the time displayed is that of the local

appliance. System times are recorded in UTC and "translated" to the local time; in this way, log and report times are also normalized.

To set the system time using an Internet time server:

1. In the management console, click **Manage System > Configuration > Settings | Time.**
2. Choose your time zone.
3. Check **Enable** in the NTP field to use the default NTP server.
   - Alternatively, you can use your own time server by clicking the **Add NTP Server...** button and then typing its host name or IP address next to the **Specify** option.
4. Click **Apply** to save the new settings.

3.8 Configure Logging Options

You can have the DLP appliance send system and other logs to as many as four existing syslog servers, where they can be aggregated with logs from other applications and managed through a third-party log management system. In addition, notifications based on log type and/or severity can be automatically emailed to designated users. The procedures are described below.

To view system logs:

- In the management console, click **Manage System > System Logs.**

To send logs to a syslog server:

1. In the management console, click **Manage System > Configuration > Servers | Syslog Servers.**
2. Click the **Edit** icon next to each server you want to enable.
3. In the window that appears, enter the server IP address and port (it is currently not recommended to use a host name for syslog servers).
4. Click **OK**.

To email event notifications:

1. In the management console, click **Manage System > Configuration > Settings | Logging.**
2. Click the **Edit** icon next to the log type you want to configure.

a. In the window that appears, choose the syslog server you want to route this type of log to, and specify the severity threshold.
b. Click the **Notify** tab, and then **Enable** the Notify option.
c. Choose the log level for which you want notifications sent.
d. Designate the user(s) who will receive the event notifications.

3.9 Register Data and Create a Detection Policy

The DLP appliance can detect whatever content you register, including specific "strings" such as a name or social security number, the content of entire documents (even if it has been excerpted, altered, and/or copied in to another document) and data patterns.

Because you need to configure the inspection services and register data before creating a policy and using it to detect sample data, it is recommended that you complete the tasks in this chapter, then register data pasted from the clipboard (Chapter 4, "Registering Clipboard Data or a Document" on page 56) to include in a policy configured for TCP inspection.

Registering Data is covered in Chapter 4 of this Administrator's Guide, and creating detection policies is covered in Chapter 5-7 (Email, TCP, and ICAP inspection) and Chapter 9 (Discovery).

That said, a quick summary of steps for creating a test policy is provided below.

To use a default policy for packet monitoring:

1. In the management console, click **Protect Data > Policies**.

2. In the list of policies that appears, locate the one named Email Addresses and then click the **Edit** icon next to it. The Edit a New Policy window appears.

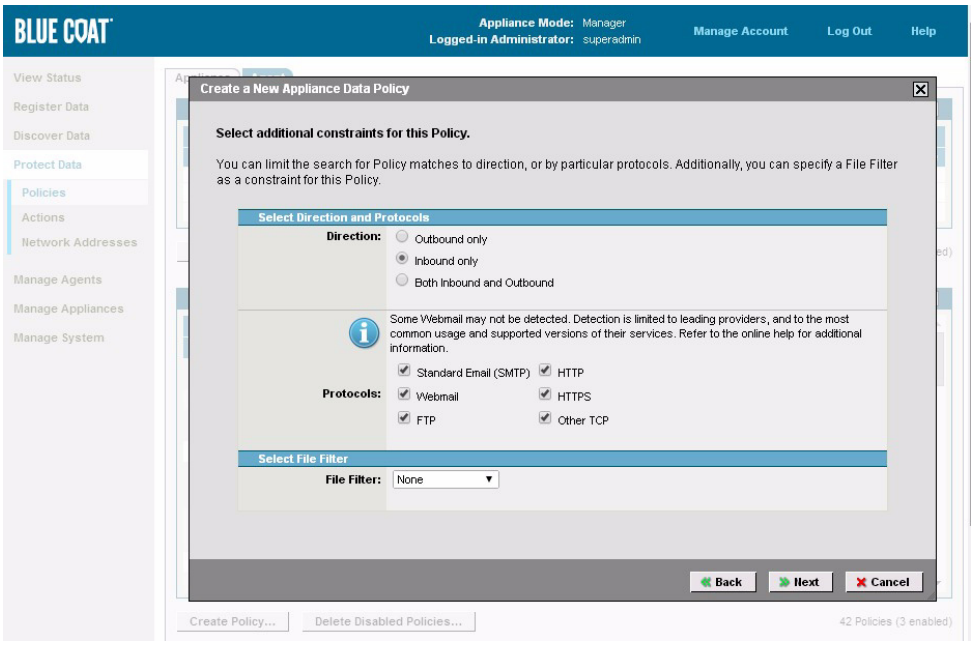


Figure 3.9: Inspect outbound TCP traffic (from a network tap on eth0 and eth1 of the appliance) using sample data to see how inspection works.

3. Review the Policy Properties if you'd like, and then click the **Constraints** tab. For an explanation of the different choices, see 5.2 "Detect Registered Content in Email Traffic" on page 74.
4. In the screen that appears, enable **Outbound Only** and click all the available protocols: SMTP, Webmail, FTP, HTTP, HTTPS, and other TCP.
5. If the DLP appliance is managing Inspectors, you can have all Inspectors enforce the policy, or you can assign it to one or more particular Inspectors. For example, say you have registered data that is in French. You can include that data in a policy and deploy the policy to only those regions where the lingua franca is French.
6. Click **OK** when finished.
7. In the **Summary** screen that appears, review you choices and then click **Finish** to return to the Policies page. The policy will be enabled and packet monitoring on the selected protocols will begin immediately.
   - Remove the **Enable** check mark to stop monitoring the registered data in this policy.
   - Click the **Edit** icon to change any of the scan parameters.

3.10 Enable SNMP Notifications

SNMP is useful for debugging and monitoring. The DLP appliance supports MIB-II (Linux), which allows the use of HP OpenView or any other MIB-II-compliant Linux tools.

To set SNMP notifications:

1. In the management console, click **Manage System > Configuration > Servers | SNMP.**
2. Select **Enable** in the SNMP field.
3. In the **System Location** field, accept the default value or enter a system location.
4. In the **System Contact** field, enter the contact name and host name of the system contact, for example root@localhost.
5. In the **Community String** field, accept the default value or enter a community string such as "public" (often reflects what has been configure on the trap host for other devices).
6. Click **Apply** to save the configuration.

3.11 Create a Network Address Group

Network Address groups are frequently used in detection policies to "aim" the policy at the collection of computers represented by the group. Different groups can be created from discrete IP addresses, a domain, or a range of IP addresses. The group can be re-used in any number of policies to define the users to include or exclude from inspection.

Network Address groups can also be used to accommodate the mobility of user endpoint that are running a CI Agent. In this case, Network Address Groups can be used to facilitate the automatic hand off, from one inspector to another, Agent assign-

ments to provide continued coverage whenever the Agent moves from on geographic location to another (such using the laptop at different branch offices when traveling).

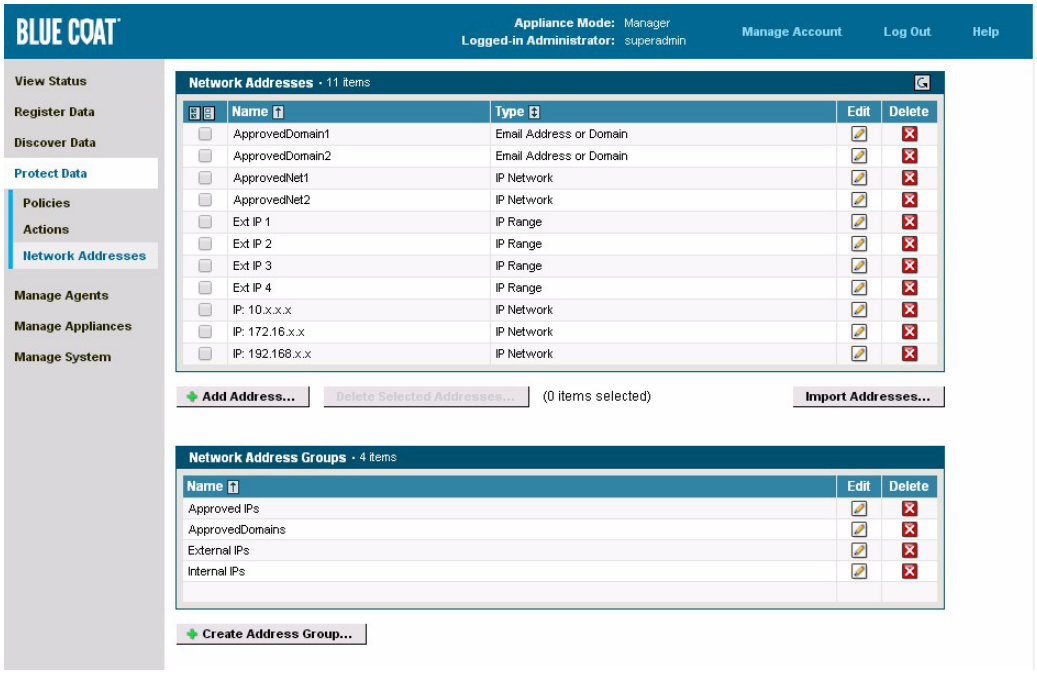


Figure 3.10: Use Network Address Groups to create inspection policy "targets" and also to allow CI Agents to "rove" amongst Inspectors depending according to LAN.

To create a network address:

1. In the management console, click **Protect Data > Network Addresses**.
2. Click the **Add Address...** button. The Add a New Address window appears.
3. Fill out the General properties as explained below, and then click **OK**.
   - **Name**—the name you type here will appear in the Network list
   - **Description**—the description appears when you mouse-over the name.
     - **IP Address**—include octet markers, like so: 127.0.0.1
     - **IP Range**—must be on same subnet
     - **IP Network**—include CIDR prefixes, like so: 192.168.127.127/24
     - **Email Domain**—yourcompany.com
4. Click **OK** when finished.

3.12 Get System Information

Use the information provided under System Information to find out if you are using the most current software version, need to get quick status check, or if you need to contact technical support about a software or hardware issue.

To view system information:

- From the management console, click **Manage System > Configuration > Settings | General**. You can find the following information about your DLP appliance:
  - **Model Number**: DLP2700, DLP1700, or DLP700
  - **Version**: *#.#.#.#—major.minor.build.increment*
  - **Serial Number**:*—14 alpha numerics; use when contacting Blue Coat Systems or the hardware vendor*
  - **Release Date**: 2011-05-01
  - **System Time**: 2012-07-04 14:03:42 PST
  - **System Uptime**: 326 days, 02:41 hours—*time since last restart*

3.13 About the Hardware Watchdog

The hardware watchdog will restart the DLP appliance if the system stops responding in a timely manner to ensure that it does not remain in an inoperable state. By default, the DLP appliance Hardware Watchdog is enabled and should only be disabled to troubleshoot a persistent issue.

In the event of a reboot, a cluster of events will be recorded in the system log starting with ”Hardware watchdog.” Note that you must have logging enabled in **Manage System > System Logs** for these logs to be collected. In addition, an event notification can be sent to the recipient(s) configured in **Manage System > Configuration > Settings | Logging**.

The hardware watchdog can be triggered by any of the following circumstances:

- Hardware failure.
- The operating system crashes or becomes unresponsive.
- Extremely high system loads prevent the watchdog beacon from being received within the time frame.

You can view the operational status of system hardware from the DLP Manager Dashboard: click **View Status > Dashboard** and then check the **Health Monitor** window. Click any of the indicator lights to open the System Log screen, where you can find additional details.

3.14 Set up an Inspector

Set up one or more Inspectors, for example if you need to distribute inspection tasks across multiple appliances to reduce the load on the central manager or in order to provide local inspection services and/or agent management for a geographically diverse network. For example, it might be necessary to install multiple inspectors and

dedicate each to a different task (such as email inspection, ICAP inspection, and agent management) if traffic on the LAN exceeds the capacity of a single machine.

Inspectors receive their policy configurations and other settings from the DLP Manager. For example, you cannot create a policy on an inspector, or register data. On the other hand, you must enable each inspection services locally, from the Inspector's management console, in order for that service to be available.

Note that you should only configure a DLP appliance as an Inspector after the DLP Manager has been set up. You will be prompted to provide connection details and to import security certificates from the manager to complete the Inspector setup.

Configure a central management port:

An inspector uses the central management port (Eth5) to connect to the DLP Manager and/or to accept connects from CI Agents.

Before assigning an IP address to the central management port, be sure the intended IP address is available, and that a route exists between the Inspector and DLP Manager, the Inspector and Agents, and/or between the Manager and Agents. Of course, the Inspector should be connected to the network.

1. From the management console on appliance that will become an Inspector, **Manage System > Configuration > Network | Interfaces**.
2. Click the **Edit** icon for the eth5 interface. Change the name of the interface by editing the **Description** field, or click the **Settings** tab.
3. In the **IP Address/Mask** field, enter the IP address/mask and gateway you will assign to the port, for example,

   ```
   10.10.1.9/22
   10.10.1.1
   ```

4. In the **Speed/Duplex** field, accept the default value **Auto-negotiate** or choose one of the settings from the drop-down list to match your network hardware.
5. Click **OK** to save the changes and close the window.
6. Confirm the Interface connection by returning to the main menu and clicking **View Status > Dashboard.** Under **Health Monitor**, click the **Interfaces** tab. The eth5 status icon should be green.

   Note: If the icon is red (service is connected but not receiving traffic) or gray (service is disabled), click the icon to open the **Manage System > Configuration > Network | Interfaces** page, then click the Edit icon and open the Statistics tab to see if the port is sending/receiving traffic.

Set the appliance to Inspector mode:

1. From the management console of the machine you want to place in Inspector mode, click **Manage System > Configuration > Settings | General.**
2. Under Deployment Mode in the screen that appears, choose Inspector. Note that if the appliance was previously configured as a manager, you will need to change first to Standalone mode and then to Inspector.

3. The **Manager Connection Settings** option appear when the appliance is Inspector mode. Configure the following:
   - **Manager Host Name**—Type the host name that is associated with IP address assigned to Eth5 on the DLP Manager (not this inspector). The inspector will use this and the port specified to connect to the manager. Note that this host name should exist in the DNS. Blue Coat Systems recommends using a host name rather than an IP address so that if the IP address schema ever changes on the network, you will not have to re-register each Inspector with the DLP Manager to reflect the change.
   - **Upload Certificates**—Because the Manager-Inspector communications are encrypted, you must upload security certificates from the Manager to the Inspector. Typically, this occurs via a third location that is accessible to both systems. Click the **Browse** button to locate and import the security certificates on the Inspector.

Enable the Inspector for Agent management:

1. If you will deploy CI Agents to the endpoints and want this Inspector to manage them, enable the **Manage CI Agents** option.
2. Specify the port on which this Inspector will listen for inbound agent connections.
3. Next, specify the **Host Name** that is associated with IP address assigned to Eth5 on this Inspector. The agents will use this and the port specified to connect to the inspector. Note that this host name should exist in the DNS. Blue Coat Systems recommends using a host name rather than an IP address so that if the IP address schema ever changes on the network, you will not have to re-register each CI Agent (from the endpoint) with the Inspector to reflect the change.

3.15 Creating a Policy Action

As introduced in 3.5.3 "Add a Notification to an Action" on page 27, you can have the DLP appliance execute a complex of actions whenever it finds data that it was configured to detect. Blue Coat Systems recommends that prior to launching an "aggressive" custom action, you first assign an Information action and audit the policy's detection results for several days. Using the Incident Management screen (**View Status > Incidents > Management**) you can query for incidents with **Severity = Info** and then drill down into the incidents to see the data and/or file that triggered the match.

To create an action for inclusion in a policy:

1. In the management console, click **Protect Data > Action.**
2. Click the **Create Action...** button. The Create an Action window appears.
3. Fill out the General and Logging properties as explained below, and then click **Next**.
   - **Name**—the name you type here will appear in the Action list
   - **Description**—the description appears when you mouse-over the Action name

- **Notify**—enable; you will be able to designate who you want to receive notifications and either use the default notification text or create your own message
- **Retain Copy**—enable; stores a copy of the matching data
- **Logging Options**—choose a syslog server if you have configured this option in **Manage System > Configuration > Servers | Syslog Servers**.

4. Fill out the Default Settings as explained below, and then click **Next**. See Figure 1.3 for an example of how Status, Severity, Priority and Assignee are used.

   - **Incident Status**—default status for incidents until they have been remediated and closed.
   - **Severity**—use this to indicate the degree of urgency; useful for the person responsible for incident remediation.
   - **Priority**—use this by itself or in combination with Severity to indicate the degree of urgency
   - **Assignee**—choose who you want the incident assigned to.
     - **Group**—assign incident ownership any DLP appliance Group
     - **Individual**—assign incident ownership any DLP appliance user
     - **Policy Creator**—assign incident ownership to the administrator who authored the policy
     - **Registered Data Owner**—assign incident ownership to the user who registered the data that was detected in the match

5. **Other Administrators**—assign incident ownership any DLP appliance user.

6. Fill out the settings for sender and Incident Reviewer as explained below, and then click **Next**.

   - **Notify Sender (or source user), when possible**—for MTA inspection, you can notify the sender of an email if his/her message contained data that violates policy; for Web traffic, you can pop up a Web notification to inform the source users.
   - **Notify Policy Creator**—notify the person who created the policy that triggered the detection
   - **Registered Data Owner**—notify the person who registered the data that was detected
   - **Other Administrators—**notify selected others by adding them to the Selected Admins window

7. Choose whether to keep a copy of the file or data that triggered the incident on the DLP appliance, and then click **Next**.

8. Click **Finish** in the review screen that appears. The action you created appears in the Action List and is available to be used in any policy.

4 Register Data for Detection

DLP appliance Administrator's Guide

After installing the hardware and setting up the DLP appliance for your environment, the next task is typically to locate and register the data in your organization that you want to monitor and protect.

This chapter begins with a few short explanations of fundamentally important concepts and then takes you through the process of registering different kinds of data.

4.1 How Data Registration Works

You register data so the DLP appliance knows what to detect. During data registration, the appliance uses clever algorithms to summarize the content down to a tiny fraction of the original size, while at the same time retaining a very high recognition resolution (a couple sentences copied from Document A can be detected in a 200-page Document B, even if it has been compressed and is being sent as an email attachment).

4.1.1 Data Types

The DLP appliance categorizes source data into two main types: structured and unstructured. This is the data that you will register in order to prevent it from leaving the network via Web uploads, email, or by being copied onto unauthorized client machines. It is also the data you would want to know about if it is being stored on public file shares, or contained in documents available on your Website or intranet.

- **Structured data** is content that which comes from a database. Supported types include, Microsoft SQL, MySQL, PostgreSQL, Oracle, DB2, and Sybase. Structured data also includes any data that has been saved in CSV (comma separated values) format, for example, any spreadsheet contents and query results that have been saved as CSV. This data is tabular, and each column reliably contains the same type of information, for example social security or credit card numbers, or mailing addresses. A structured database scan will use an SQL query to scan an SQL or Oracle database and register data fields that you specify.

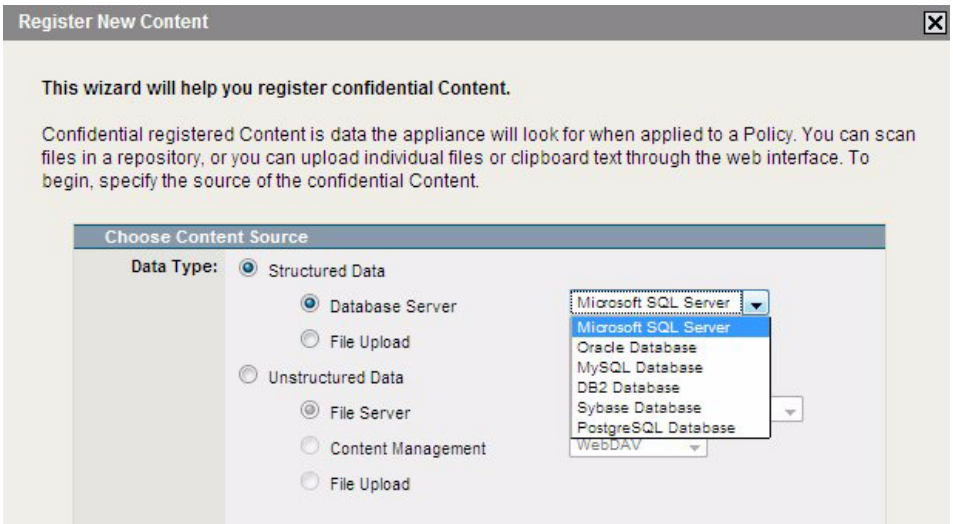


Figure 4.1: You can register data that is stored in a structured source such as s database, or unstructured, such as a fileshare, spreadsheet, or even text from pasted the clipboard.

- **Unstructured data** consists of any content that comes from a document, including email, presentations, design documents such as CAD, Web pages, or word processor documents. This data can include the document as a whole, or

any excerpt or bits therein that you deem confidential and therefore want to monitor. Register unstructured data by adding it to the DLP appliance RedList™.

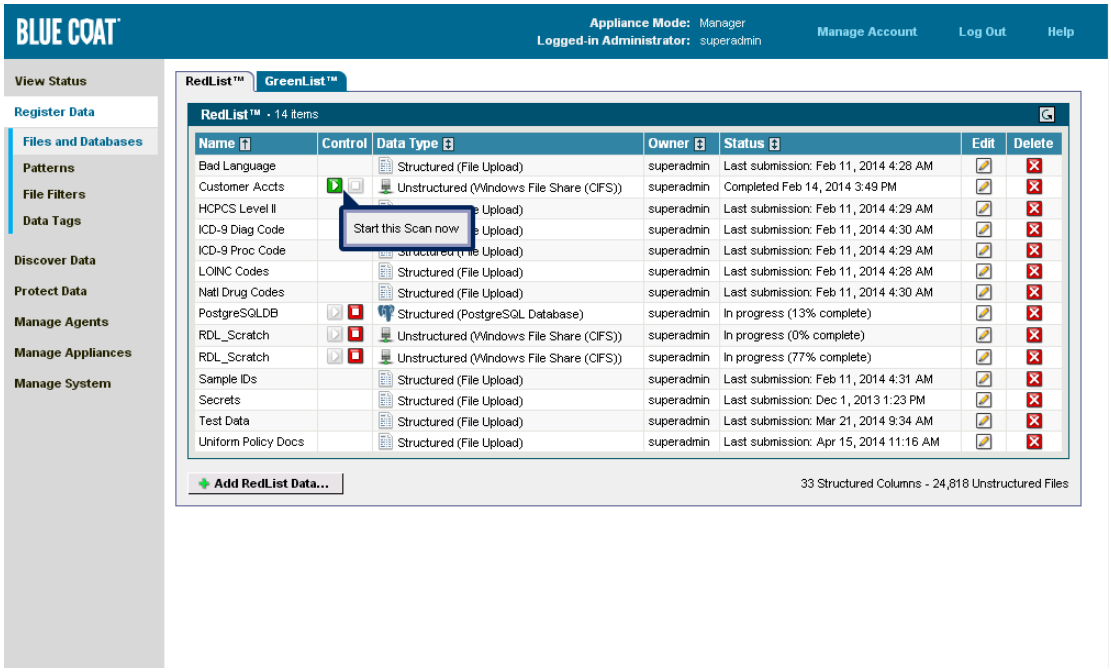
4.1.2 Fingerprints

As introduced in Chapter 1, the DLP appliance uses "fingerprinting" to register structured and unstructured data.

- **Data Element Fingerprinting** registers the exact *structured* data you want to secure. It is not simple RegEx pattern or keyword matching. Instead, it is the most efficient and accurate means of conducting DLP while at the same time keeping false positives to a minimum. You can register as many as 40 million structured elements at a granularity which will allow you to detect tiny bits of registered data anywhere on the data store.
- **Deep Content Fingerprinting** is Blue Coat Systems' proprietary technology that allows you to register data from virtually all file types, and supports content from any language, including multi-byte character sets such as Japanese and Cyrillic. Deep content fingerprinting is also fast and efficient. The fingerprint hashes are encrypted, can be a tiny fraction the size of the original source, and are representative enough of the data to detect snippets and derivatives of the registered document.

4.1.3 The RedList™ and GreenList™

You can register almost any content and/or data and create a detection policy around it. Simply add the data you want to detect to the RedList™. Add what you want to exempt from detection to the GreenList™. There is almost no limit to what you can register and examine. The RedList™ also comes with a variety of pre-registered data to support the common requirements of different industries, for example, the medical codes used in health care.



Name	Control	Data Type	Owner	Status	Edit	Delete
Bad Language		Structured (File Upload)	superadmin	Last submission: Feb 11, 2014 4:28 AM		
Customer Accts		Unstructured (Windows File Share (CIFS))	superadmin	Completed Feb 14, 2014 3:49 PM		
HCPCS Level II		Upload)	superadmin	Last submission: Feb 11, 2014 4:29 AM		
ICD-9 Diag Code		Upload)	superadmin	Last submission: Feb 11, 2014 4:30 AM		
ICD-9 Proc Code		Upload)	superadmin	Last submission: Feb 11, 2014 4:29 AM		
LOINC Codes		Structured (File Upload)	superadmin	Last submission: Feb 11, 2014 4:28 AM		
Natl Drug Codes		Structured (File Upload)	superadmin	Last submission: Feb 11, 2014 4:30 AM		
PostgreSQLDB		Structured (PostgreSQL Database)	superadmin	In progress (13% complete)		
RDL_Scratch		Unstructured (Windows File Share (CIFS))	superadmin	In progress (0% complete)		
RDL_Scratch		Unstructured (Windows File Share (CIFS))	superadmin	In progress (77% complete)		
Sample IDs		Structured (File Upload)	superadmin	Last submission: Feb 11, 2014 4:31 AM		
Secrets		Structured (File Upload)	superadmin	Last submission: Dec 1, 2013 1:23 PM		
Test Data		Structured (File Upload)	superadmin	Last submission: Mar 21, 2014 9:34 AM		
Uniform Policy Docs		Structured (File Upload)	superadmin	Last submission: Apr 15, 2014 11:16 AM		

Figure 4.2: The RedList™ contains policies with the data you want to detect. The GreenList™ contains data, that, when detected in conjunction with a RedList™ item, will create an exception. An incident will not occur.

- **The RedList™ contains fingerprints for all the data you want to secure.** Any data that has been registered from a structured source is added to the RedList™ and will be detected. Data from unstructured sources, on the other hand, often contains of mixture sensitivity levels. You can register the entire contents of an unstructured document, or, more typically, portions such as sensitive tables, pages, and passages by copying them from the document for fingerprinting and adding them to the RedList™.
- **Items added to the GreenList™** come from unstructured data. They are the data you explicitly want to exclude from detection, typically to address an issue with false positives. The GreenList™ typically ends up containing recurring data such as certain URLs, legal boilerplate, company contact information, etc. that may end up in the RedList™ (for example if you register the entire document rather than specific sensitive passages), but that you don't want to trigger a policy match. Whenever registered data from the RedList™ is detected, the DLP appliance does a quick cross-check of content in the GreenList™ to see if the RedList™ match should be exempted.

4.1.4 Data Tags

Data Tags make it easy to group similar data, and they allow you to begin to use pre-existing policies as soon as you have registered the data you want to secure.

Three things make Data Tags especially useful:

1. Structured Data Tags can also be used to validate the integrity of scan detections. Use them in conjunction with one of the provided Regular Expression to weed out "bogus" data that may have been registered in with the source data (for example, common place holders such as 000-00-0000 for unknown Social Security numbers). You can also create your own RegEx, as indicated below.
2. Data Tags can be used like buckets, for sorting and storing similar objects (or, in this case, data types) that come from any number of different sources or locations. For example, say you want to protect against the loss of client social security numbers (SSNs). Over time, different collections of these numbers have accumulated in various databases and locations. You can register the numbers from each source, and by tagging them with the same Data Tag, include all the SSNs your company is responsible for in the same policy. (Automatic re-rescanning ensures that all the registered data is kept up to date.)
3. Data Tags make it easy to start using one of the dozens of the DLP appliance's default policies. Simply register your particular data and add it to an existing Data Tag, and then you can immediately start using the content in Network, Discovery, or Endpoint policies.

Notes:

- You can create Data Tags for both RedList™ and GreenList™ items. Use them in a GreenList™, for example, as a catch-all for odds and ends such as the company address, common URLs, recurring phone numbers, boilerplate text, and repeating headers/footers.
- All data represented by the same tag must be of the same kind—all structured or all unstructured. And, all data represented by the same tag should be of the same type— all credit card numbers, or all names, rather than a mixture of different types of data.
- Attach the Data Tag when selecting Registered Data in your policy. The Registered Data included in a Data Tag can also be used in a policy on its own.

4.2 Constraints

Data registration in the DLP appliance is very powerful. As previously noted, you can register data from a huge number of locations (including various file shares, databases, and data management systems), and create remarkably accurate fingerprints for detection. At the same time, it is often desirable to limit the scope of what you register. In a file share of 10,000 legal documents, only a small number may actually contain data that needs to be monitored and/or restricted. The same idea holds true for database data—you may only want to register certain types, or patterns of data, instead of all the data available.

Occurrence Threshold

When creating a detection policy, you can set an occurrence threshold to restrict the conditions under which the policy triggers an incident. For example, if you set the

threshold to 10 occurrences, an incident will only be created if 10 or more matches are detected in a single email or document.

4.2.1 Patterns

When you register data, you can use patterns to filter out non-conforming source documents. So, for example, if you point the registry crawl to a network share that has 10,000 files, you can use a file filter to limit the crawl to Microsoft Office documents and then use a pattern to register only those documents that meet the criteria of your regular expression. In other words, you can scan all the documents on the file store, but only register the contents of those few (hundred, thousand) that contain the type of content you are interested in securing.

When you create a policy, patterns can also be used to detect short strings of data of a fixed format that match a literal string or a regular expression, for example, to find all documents on the public file share that contain the company conference bridge number and password. Another example would be to check for legal documents, or confidential intellectual property that has been improperly stored on a public location (including the intranet or Web site).

The DLP appliance comes with many pre-defined patterns that represent common forms, for example, a variety of Personal identification numbers for the U.S. and EU and credit card numbers). It supports most PERL-compatible standard regular expressions. See the Online Help for a list of included patterns, their RegEx, and a reference for writing PERL RegEx.

4.2.2 File Filters

You can create File Filters so they will be available later, when you register data and create policies. File filter can include any combination of file attributes, including size, data, property, type and extension. They are a convenient way to define a set of characteristics once, and then have them available for re-use in various policies from that point on. The DLP appliance includes a number of default, common file filters that you can use, or you can create a library of whatever filters you need.

When file filters are used in RedList™ or GreenList™ repository scans, they limit the files that are registered to those that meet the criteria set in the filter. When file filters are used in policies, they limit the policy to find a match only when the transaction includes certain kinds of files. For file filters used in a policy, you could for example, create a policy to detect only AutoCAD documents that contain RedList™ data. In this case, the policy would include a RedList™ but would also include a file filter for the AutoCAD file type. You could also trigger policy violations for all transmissions of AutoCAD documents, regardless of data. In this case, you would create a policy that was not based on data but included a file filter to limit violations to documents of AutoCAD format.

4.3 Registering Data

You register data so the DLP appliance knows what to detect. During data registration, the appliance uses clever algorithms to summarize the content down to a tiny fraction of the original size, while at the same time retaining a very high recognition resolution (a couple sentences copied from Document A can be detected in a 200-page Document B, even if it has been compressed and is being sent as an email attachment). For registered data, the resolution is virtually perfect—a single SSN can be detected whether it is being copied to a USB drive, sent in an email, posted to the Web, or saved in a spreadsheet.

You can register data from a variety of sources:

- Individual documents
- All documents in a given directory
- All documents matching a given criteria (file and/or content type, etc.)
- Text from a snippet that you copy/paste from any source
- Data from a content management system:
  - Stellent
  - WebDAV
  - Documentum
- Content/data from a database:
  - Oracle
  - Microsoft SQL
  - MySQL
  - PostgreSQL
  - DB2
  - Sybase
  - Informix
- Tabular data saved as a comma separated values (.csv) file (database queries, spreadsheets, XML, etc.)
- Content on the following file servers:
  - CIFS (Windows File Share)
  - SMB (Windows File Share)
  - NFS (Network File System)

Registered data is stored on the DLP appliance and is secure; it is encoded as one-way hashes and cannot be used to reconstruct the original data.

4.3.1 Exact and Partial Matching

Crawling a large repository (i.e., millions of documents) of unstructured content on a file share or in a content management system can be resource intensive, both on the

DLP appliance and on the repository itself. When automatic daily scan is also enabled, the process is repeated in its entirety each day. However, if you know in advance whether the policy will be designed to detect documents as a whole or bits of content from within the documents, you can reduce potential overhead by specifying whether to crawl the repository for the purpose of exact matches and/or partial matches.

- **Register for Exact and Partial Matches**—Documents will be fingerprinted for exact matches, and the contents of the documents will be processed using algorithms that enable the detection engine to recognize small segments of content from the document in different contexts. For example, a sentence or two taken from a 100 page PDF file that has been pasted into a Word document, compressed and attached to an email can be detected in a partial match. The trade-off for this resilience is that fewer documents can be stored for partial matches (hundreds of thousands versus millions).
- **Register for Exact Matches Only**—Exact match is frequently used with large repositories (millions of documents) because registering data for exact matches is faster and more records can be stored. An exact match will only be triggered if the file registered and the file detected are identical (except for metadata such as the file name and date).

You can change from Exact to Partial matches or vise-versa after the data has been registered by editing the crawl parameters in the RedList or GreenList. In addition, you can apply Exact match standards at the level of policy.

Note that Changing the scope from Exact to Partial matches will cause the repository be re-crawled in order to include partial matches in addition to the fingerprints.

4.3.2 Using Row Correlation to Reduce False Positives

Row correlation is a feature that can be applied to data registered from a structured source (e.g., a database) as a means of increasing the relevancy of matches. For example, say five columns of data are registered from a database with 1 million rows. With row correlation as a part of the inspection policy, the DLP appliance will only create an incident if it detects the occurrence of all five items— from the same row, from the same data source, and occurring in the same document. Documents that contain a variety of matching items from the database will not trigger a match unless the items all belong to the same row.

Historically, row correlation did not take into account the proximity of items. Continuing the example above, if all five items were found to occur anywhere in a 1,000 page document, that document would trigger an incident. Row correlation now includes a proximity threshold, however, which further decreases the likelihood of false positives. By default, this threshold is 1024 characters (including spaces) on either side of a matching item. As a point of reference, that is equivalent to about a half page of text on either side of the matching item.

Notes:

- Correlated data must all be from the same source.

- Columns added as constraints in the policy must be connected by the AND operand.
- The detection frequency for all items must be the same.
- Contact Blue Coat Systems if you need to adjust the default proximity threshold.

4.3.3 Registering Data From a Database

You can pull query data, register it, and then create a detection policy to find that data as it moves across the network in email or Web traffic. Registered data can also be used to locate protected data on unauthorized client endpoints, and to identify it amongst the data stored on network file shares, document repositories, and Internet/intranet sites.

The DLP appliance supports fingerprinting data from Microsoft SQL, MySQL, Oracle, Sybase, DB2, Informix, and PostgreSQL databases. To register data from these sources, you should know the database schema well enough to write a SQL query, or have the cooperation of someone who does. Blue Coat Systems also recommends that you create a dedicated, read-only account on the database for the DLP appliance to use.

To register data from a database:

1. In the management console, click **Register Data > Files and Databases| RedList**.
2. Click the **Add RedList Data..**. button. The Register New Content window appears.
3. Choose **Structured Data | Database server** and select the type of database you want the DLP appliance to access. Click **Next**.

4. Fill out the fields as appropriate for the data source. Note that for databases, Blue Coat Systems recommends that you use read-only login credentials.

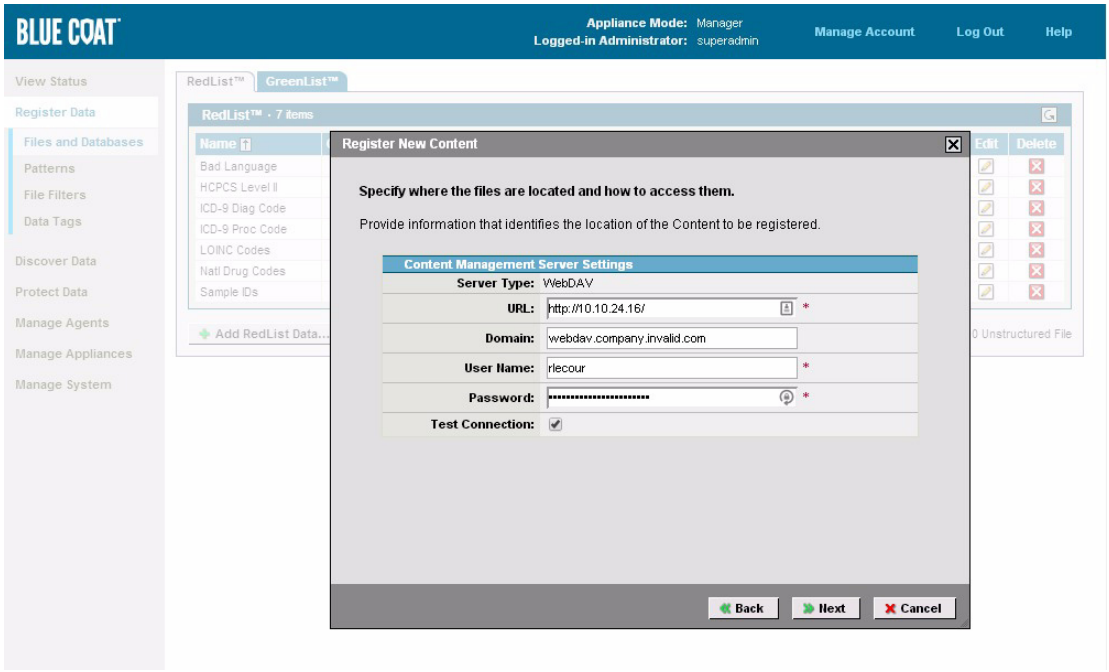


Figure 4.3: Tell the DLP appliance how to connect to the data source.

5. Click **Next** to test the location, connection and credentials you provided.
6. In the Query String window that appears, type or paste from the clipboard the query you want to use. There is a 1024 character limit for the query string, so instead of editing a complex query here to avoid invalid data, you can call a stored procedure on the database or use another of the techniques suggested in 4.5 "Tips for Avoiding False Positives" on page 63.

   ```
   SELECT * FROM [table_name];
   ```

7. Next, you are prompted to select from the database the individual columns you want to register. Check at least one column and then click **Next**. See "Data Tags" on page 45 for information about including the registered data in a larger group of like data from other sources.
8. Click **Next**, and then select **Initiate Scan Now** and **Automatic Daily Scan**.
9. Click **Finish** in the review screen that appears to start the scan. The name you entered in Step 1 will appear in the list of RedList™ names, and the DLP appliance automatically begins its crawl and will create a fingerprint for each eligible data cell from the table specified.
10. In the RedList™, click the **Edit** icon for the item you just added.
11. In the screen that appears, click the **Statistics** tab to view the scan progress. For a related example, See Figure 4.7.

4.3.4 Registering Data From Tabular Files

You can register data and/or data from any .csv file. You can register the contents of a single .csv, or register a number of different .csv files and keep them in the same RedList™. The .csv data can be numerical or text. For example, if you have a collection of prohibited vocabulary (be it a list of derogatory words or a lexicon of terms from a confidential project), that you want to detect in outbound email, you could upload that list and create a policy to detect their occurrence in outbound email (SMTP and webmail clients).

The DLP appliance supports UTF-8, Japanese Shift-JIS, and Big 5 Traditional Chinese character sets. The data in the file can be delimited with any of the following:

`Comma, Tab, Semicolon(;), Caret(^), Pipe(|), or Tilde(~)`

The .csv data can be data from a spreadsheet, database query, XML tables, or any number of sources. Note: that unlike data registered from a database, which can be automatically rechecked each day for changes, data from .csv file is static—updates will not be automatically re-registered. The first row of the file must be the header row.

To register data from a .csv file:

1. In the DLP Manager, click **Register Data > Files and Databases| RedList.**
2. Click the **Add RedList Data..**. button. The Register New Content window appears.
3. Choose **Structured Data | File Upload** and then click **Next**.
4. Type a name that identifies the data you will register. This name will appear in the RedList™, and is also what you will use to find this "fingerprint" when adding it to a detection Policy. The description will appear when you mouse over the name in the RedList™.
5. Click the **Browse button to locate and upload the .csv file with content you want to register.**
6. Select the character set and delimiter for the data in the file you uploaded. (If you receive an error such as column size is too long, check that, but also be sure you have specified the correct delimiter or character set.)

7. Next, you are prompted to select the individual columns you want to register. Check at least one and then click **Next**.

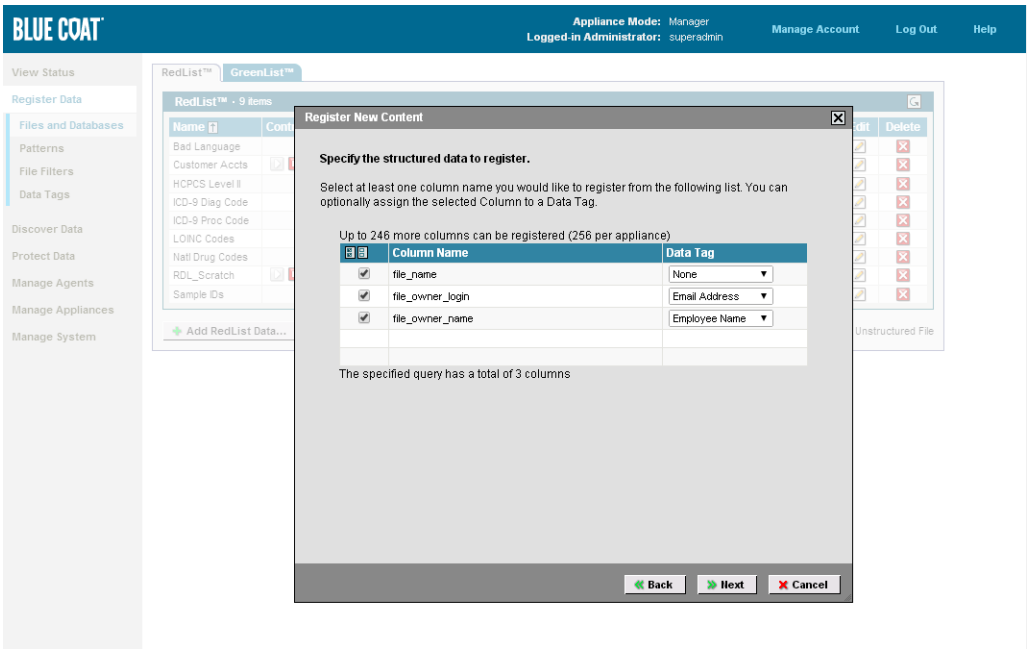


Figure 4.4: Select the columns you want to register from the .csv file. See "Data Tags" on page 45 for information on using data tags.

8. Click **Finish** in the review screen that appears to start the scan. The name you entered in Step 1 will appear in the list of RedList™ names, and the DLP appliance automatically begins its crawl and will create a fingerprint for each eligible data cell from the table specified.

To change the .csv source or add .csv files:

1. In the management console, click **Register Data > Files and Databases| RedList.**
2. Select the name of the .csv file you want to modify from the RedList™ and click its **Edit** icon.

3. Click the **Upload** tab in the window that appears, and then either the **Edit** icon or the **Add File...** button.

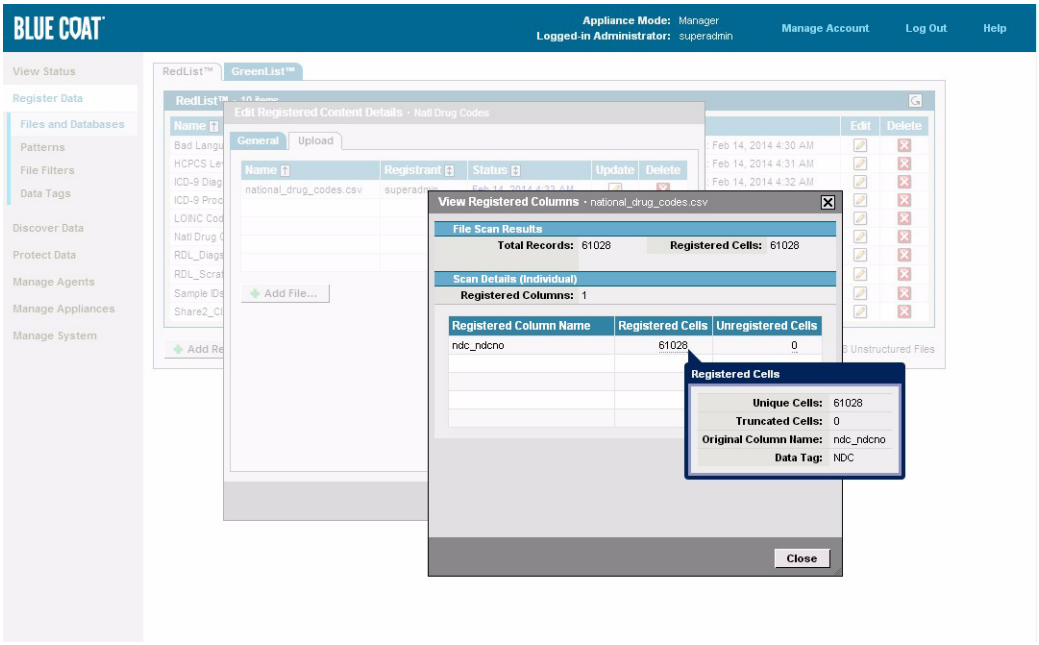


Figure 4.5: You can include multiple .csv files in a single RedList™, update or change the source .csv, and view pertinent statistics about the data that was registered.

4.3.5 Registering Data Stored on a File Share

Unstructured data can include things like resumes, legal documents, business data, forecasts, and analyses, embargoed press releases, blueprints, engineering drawings, project code names and other irregular, or non-tabular data.

In the procedure that follows, you will register all unstructured documents in a given location, thus creating a fingerprint for each, which can be used later when creating a detection policy. You will need access to a network share that contains a sample document that you can register. For this example, choose a location that contains only a few documents, and whose documents contain data that is common enough that it will be readily detected when you perform the scan.

To register data from documents (unstructured data):

1. In the management console, click **Register Data > Files and Databases| RedList.**

2. Click the **Add RedList Data...** button. The Register New Content window appears.

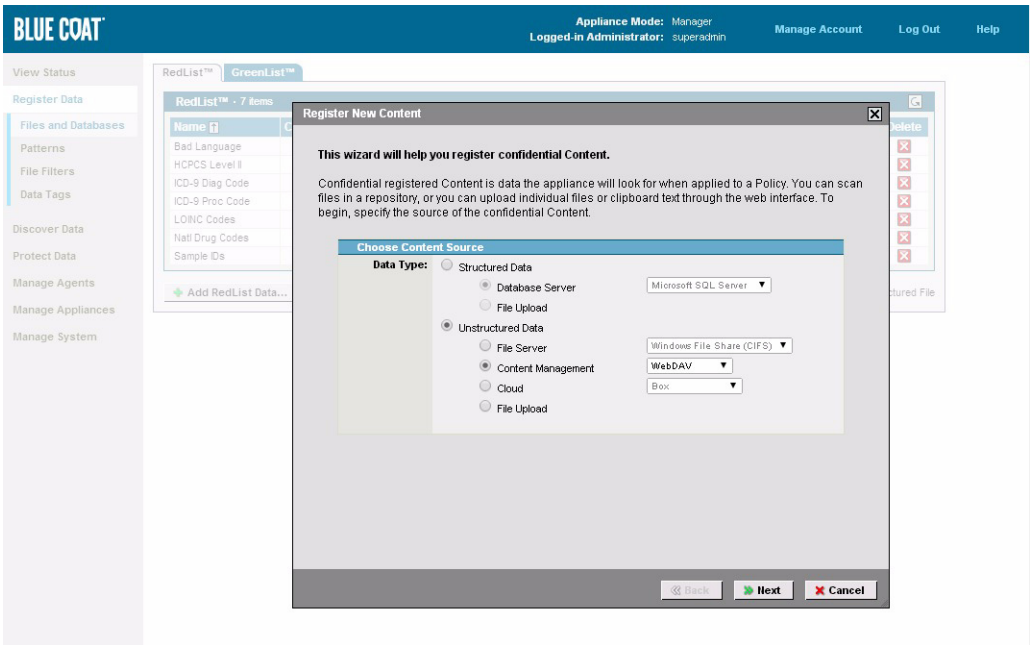


Figure 4.6: Select the network location of the documents you want to register.

3. Choose **Unstructured Data | File Server** and then select the type of network share your target data is on: CIFS, SMB, or NFS. In this example, a Windows share (CIFS) is used. Click **Next**.

   Note: To register the data of a single file on your local drive, choose **File Upload** and follow the instructions in Section 4.3.6 "Registering Clipboard Data or a Document" on page 56.

4. Type a name that identifies the data you will register, and a description. This name will appear in the RedList™, and is also what you will use to find this "fingerprint" when adding it to a detection Policy, and the description appears when you mouse-over the name in the RedList™.
5. For Data Tag, keep the default, "none" and then click **Next**.
6. Specify the location and login credentials for the file share that has the data you want to register.
7. Click **Test Connection** to confirm that you can access the location from the DLP appliance and then click **Next**.
8. For Patterns and File Filters, choose the defaults, **Any** and **Any**, and then click **Next**. (See 4.2.1 "Patterns" on page 47and 4.2.2 "File Filters" on page 47 for more information.)
9. Enable the **Initiate Scan Now** option, and disable **Automatic Daily Scan**, then click **Next**.
10. Click **Finish** in the review screen that appears to start the scan. The DLP appliance automatically begins its crawl and will create a fingerprint for each eligible document in the location specified.

11. In the RedList™, click the **Edit** icon for the item you just added.
12. In the screen that appears, click the **Statistics** tab to view the scan progress.

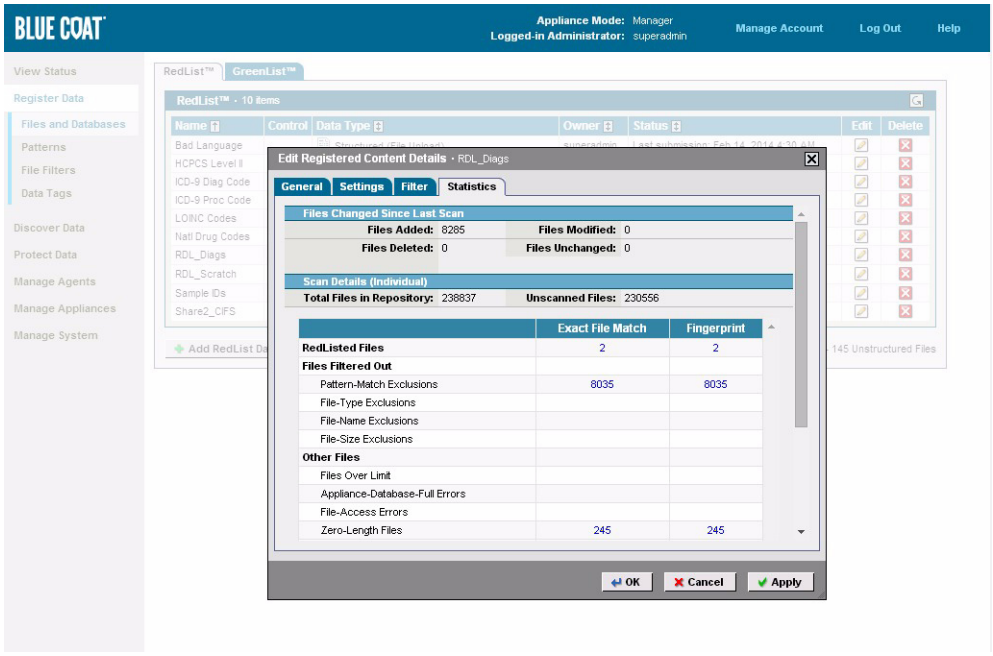


Figure 4.7: The Statistics tab is available after registration. Click the **Edit** icon to Start, Stop, and schedule scan reoccurrence.

4.3.6 Registering Clipboard Data or a Document

In the procedure below, you will register some data by copying it from the source and pasting it in the RedList™ item you are creating. See "To register data from documents (unstructured data):" on page 54 for screenshots and information on embedded choices.

Note: For this example, choose sample data that is common enough that it will be readily detected when you perform the scan.

To register data from the clipboard:

1. In the management console, click **Register Data > Files and Databases| RedList.**
2. Click the **Add RedList Data...** button. The Register New Content window appears.
3. Choose **Unstructured Data | File Upload** and then click **Next**.
4. Type a name that identifies the data you will register. This name appears in the RedList™, and is what you will use to find this "fingerprint" when adding it to a detection Policy. The description appears when you mouse over the name in the RedList™ (for example, you may want to include the original location of the data.)
5. For Data Tag, keep the default, "none" and then click **Next**.

6. In the **Upload File** option, choose **Clipboard**. Give it a name that will clearly identify the data of the snippet, and copy/paste the text you want to detect in to the **Registered Data** field (requires at least 100 characters in the clipboard to make a fingerprint).
7. Click **Finish** in the review screen. The name you entered in Step 4 will appear in the list of RedList™ names.

4.4 Reducing False Positives with Pattern Verification

You can improve the quality your detection results by having the DLP appliance verify the matches it makes against a Regular Expression. The DLP appliance includes more than 100 regular expressions that you can use, or you can create your own. A list of all patterns and their RegEx can be found in the On-line Help.

The DLP appliance pattern verification is possible for just about any kind of structured data (internal verification is already applied to Social Security and credit card numbers). Pattern verification works by creating a pattern, including it in a structured Data Tag, and then using that Data Tag to group registered data. You then attach the Data Tag to any inspection policy. Under the rules of such policies, the DLP appliance will check its matches against the RegEx and only trigger an incident if the match qualifies according to the expression.

4.4.1 Detecting False Positives

False positives may occur with any data, but valid, numerical data tends to be most common because these strings are so ubiquitous and occur in many forms. For example, take a date such as 11-07-2011. When these are fingerprinted, the non-numeric separators are stripped because there are many forms they can take (11/07/2011, 11.07.201, etc.). With the separators removed, the remaining eight-digit string, 11072011 is not so unique. It may be the same as a medical code, an ID, or an account number. So in these cases, the false positive is due to the correct detection of registered data, but in an incorrect context.

The following example uses a defunct, but real, Social Security Number to show how pattern validation can work to accept some number strings but not others. If the SSN is 078-05-1120, then

- 078-05-1120 , 078051120 , 078 05 1120 will match because it satisfies the Social Security number pattern on the DLP appliance.
- 07/8/05 1120 , 078,05,1120 will not match because they fail the verification used in that pattern.

You can use this principle to write your own RegEx for pattern verification and reduce false positives by exploiting one or more unique qualities in the data you register.

False positives can also occur when bogus data is contained in the source data that is being registered. For example, it is not uncommon for those who enter the data to type *000-00-0000, none, not provided*, or *name@domain* to fill in a required field. These commonly occurring, bogus entries will be fingerprinted and subsequently detected in innocuous documents during inspection, however, unless you can weed them out.

Overview of Tasks

The main pattern verification tasks are listed below. The step-by-step procedure for each can be found in the sections that follow.

1. Identify the data you want to verify.
2. Create a Pattern.
3. Create a Data Tag.
   - Add the pattern you created to the Data Tag.
4. Create a structured RedList™.
   - Assign the Data Tag to the registered column you want to validate.
5. Create a Policy (Discovery, Network, or Agent).
   - Specify the Data Tag you created, or the registered column.

4.4.2 Identify the Data You Want to Verify

Every organization will have its own special data that it wants to verify, and you can write your own RegEx to accomplish that. For the tasks below, however, we will use the existing pattern for Social Security Numbers (SSNs). In addition, we will create a special Data Tag (to distinguish it from the default SSN Tag), and register data from a database that includes SSNs.

Task prerequisites:

- A data source, preferably a database that you know the structure of, and that contains SSNs.
- Alternatively, you can add the following two numbers to a .csv file and then use it as the source file for registration (See 4.3.4 "Registering Data From Tabular Files" on page 52 for information on registering data from a .csv file):
  - 078-88-1772
  - 146-77-1267

  One number will pass the pattern verification, the other will fail.
- Query access rights to the database that contains the data
- Ability to create network traffic that will cross the network gateway (or at least pass through the DLP appliance where it is tapped) and that will contain some of the same data as was registered from the database.

4.4.3 Create a Pattern

Create a Pattern so it will be available when you create your Data Tag.

1. In the management console, click **Register Data > Pattern**.
2. Click the **Create Pattern...** button. The Create a New Pattern window opens.
3. Provide a **Name** and **Description**, and click **Next**. The Create Pattern window opens.
4. For **Pattern Type**: choose *US Social Security Number* and click **Next**.
5. Click **Finish** to add your pattern to the pattern list.

4.4.4 Create a Data Tag

Create a Data Tag so it will be available when you register the target data and create an inspection policy.

1. In the management console, click **Register Data > Data Tags**.
2. Click the **Create Data Tag...** button. The Create a New Data Tag window opens.
3. Provide a **Name** and **Description**, and then choose **Structured Data** for the Data Type. The **Inspection Pattern** field appears, as shown in Figure 4.8.

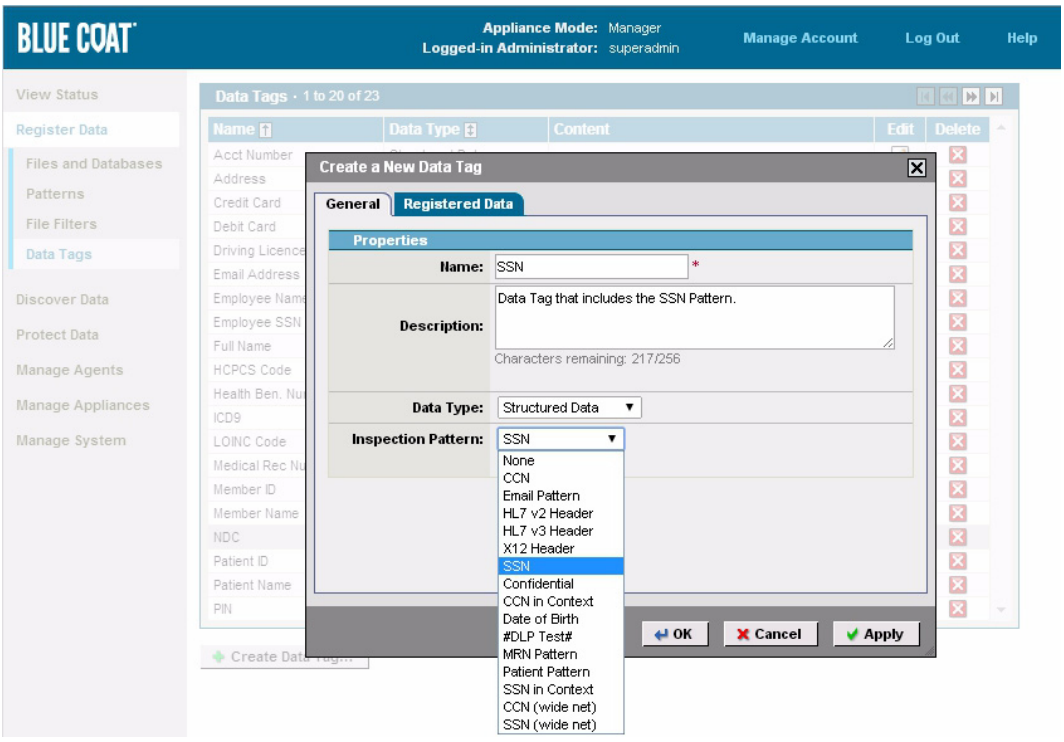


Figure 4.8: Select **Structured Data** when creating a new Data Tag to display the **Inspection Pattern** field, and then add a pattern to use this Data Tag for incident verification.

4. Choose the Pattern you just created from the drop-down list, and click **OK** to add this Data Tag to the Data Tag list.

4.4.5 Create a RedList™ Item

Register target data and add it to the RedList™ so your inspection policy will have something to detect. In this case, we will register SSNs from a database. Step 8, in which you assign the Data Tag you included the Pattern in, is the crucial step for match verification.

1. In the management console, click **Register Data > Files and Databases| RedList**.
2. Click the **Add RedList Data...** button. The Register New Content window appears.
3. Choose **Structured Data | Database server** and select the type of database you want the DLP appliance to access. Click **Next**.
4. Fill out the fields as shown in Figure 4.9. Blue Coat Systems recommends that you use read-only login credentials for the database.

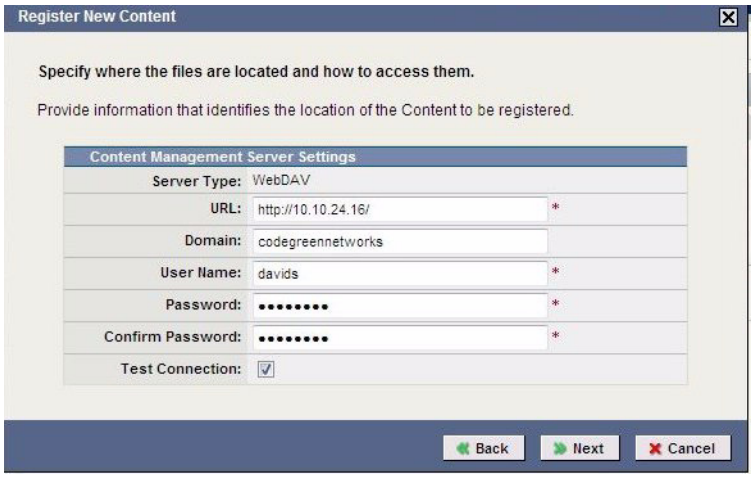


Figure 4.9: Tell the DLP appliance how to connect to the database.

5. Click **Next** to test the location, connection and credentials you provided.
6. In the Query String window that appears, type or paste from the clipboard the query you want to use, for example:

```
SELECT * FROM table_name;
```

7. Select the columns you want to register, making sure to include the column that contains Social Security numbers (or whatever data you have access to and can support with a RegEx) and then click **Next**.

8. In the same window, assign the *Social Security numbers* Data Tag you just created to the SSN column in the database, as shown in Figure 4.10.

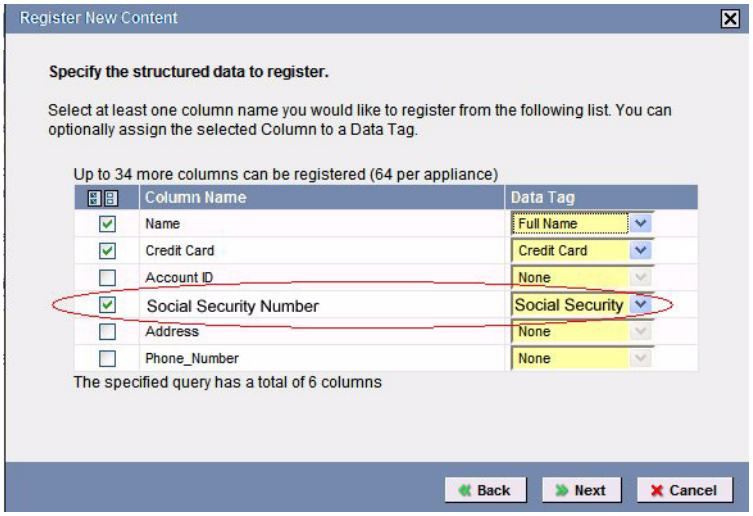


Figure 4.10: Assigning the Data Tag that has your pattern to the data you will register is the key to leveraging pattern verification.

9. Click **Next** if prompted to review registered column names.
10. Select **Initiate Scan Now** and then **Next** and **Finish**. The DLP appliance will crawl the data source and register the data, creating a fingerprint for each eligible data cell in the table.
11. To check the progress for the registered data scan, click the **Edit** icon for the RedList™ data you just added. In the screen that appears, click the **Statistics** tab

4.4.6 Create an Inspection Policy

Create a policy to govern what and where you will scan. In this case, we will use TCP auditing to check network traffic that contains some of the actual SSNs from a database content we registered (or .csv, if you created one to register the sample data). Step 5, in which you choose the Registered Data to include in the policy, is the crucial step here. You need to be sure and select the Data Tag you created.

1. In the management console, click **Protect Data > Policies.**
2. Click the **Create Policy...** button. The Create a New Policy window appears.
3. Fill out the Policy Properties as you wish and click **Next**.
4. In the window that opens, choose **Specify Registered Data that will be used as a content constraint in this policy.**

5. Choose *Data Tag* from the drop-down and the select the Data Tag you created using the Pattern, as shown in Figure 4.11, and then click **Next**.

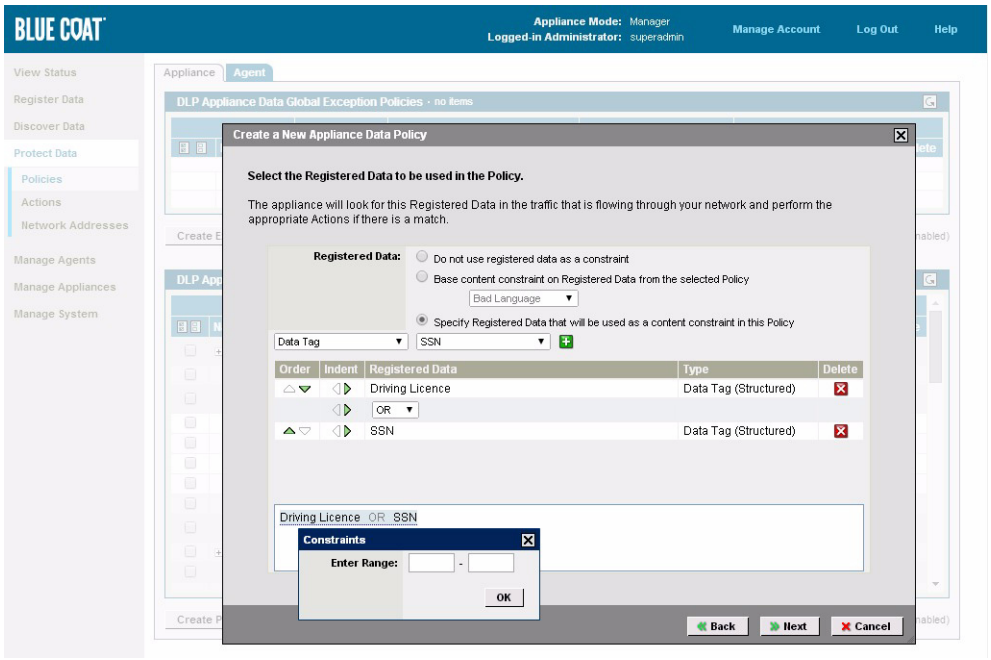


Figure 4.11: Choose Data Tag for the Registered Data. In the above example, you would not specify a range in the Constraints dialog box because it may prevent the sample data from reaching the detection threshold.

6. Accept the default source and destination and click **Next.** The Additional Constraints window opens.
7. Accept the defaults to monitor outbound network traffic, all protocols. Note that network traffic within the LAN will not be checked—to verify these procedures you will need to generate outbound network traffic that will pass through the DLP appliance.
8. Click **Next** without selecting a File Filter and then **Finish** in the Summary window that opens.

4.4.7 Test Your Configuration

Copy some files that contain the registered data to an external location to see how pattern verification on structured data works.

- Enable the Packet Monitor by clicking **Manage System > Configuration > Servers > Inspection Services** | **Packet Monitor** and then **Enable**.
- Check that you are passing TCP traffic through the DLP appliance by clicking **Manage System > Configuration > Network | Interfaces**. Click the **Edit** icon for Eth0 and/or Eth1 and then the Statistics tab. Check the bytes transmitted/received and confirm that the numbers increase by send monitored network traffic.

- Copy to an external location a file that contains valid SSNs.
- Copy to an external location a file that contains a sample that contains an invalid SSN.
- Check for Incidents by clicking **View Status > Incidents** (take off any filters that may restrict your view). Click an incident ID to drill down into the details, including an archive of the offending file, as shown below.

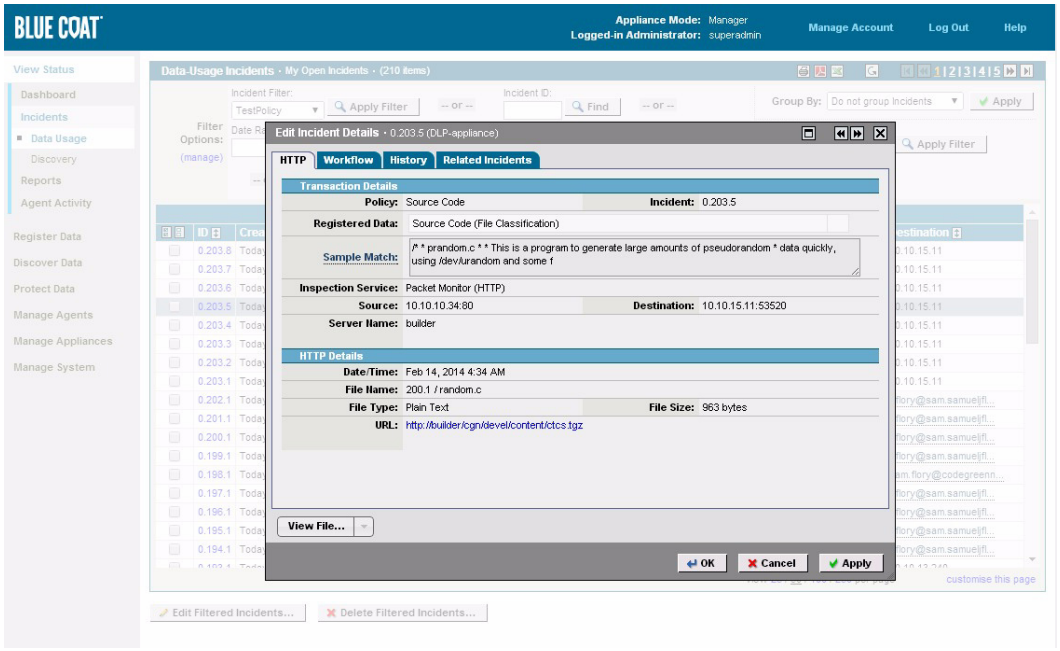


Figure 4.12: Click an incident to drill down and see details, such as the match data.

4.5 Tips for Avoiding False Positives

False positives are the correct detection of incorrect data, and there are two main reasons they can occur in data loss prevention:

1. The data is legitimate for the context in which it was detected (i.e., it is not a mis-use).
2. The source data that was originally registered for detection contained bogus data (for example, in data entry, "dummy data" such as 000-00-0000 or "none" is commonly entered in a field that cannot be left blank).

Three methods for reducing false positives are provided below.

4.5.1 Reducing False Positives in Structured Data

Perhaps the biggest contributor to false positives, or the correct detection of incorrect data, it that the data is "dirty." Quite often, a structured field such as social security numbers will contain a startling amount of entries like 000-00-0000, 111111111,

none, ###-##-####, 999-99-9999, etc. because data entry operators need to fill a required field without having the actual number. Fingerprinting this type of data is going to cause many false detections.

There are several things you can do to "pre-qualify" the data you register:

- Write a query that will return only unique, valid data from the table. There is a 1024 char limit on query strings. A simple example to eliminate repetitive and "junk" data from the SSN field follows:

```
SELECT DISTINCT FROM customer WHERE
(SSN <> "000-00-0000") OR
(SSN <> "000000000") OR
(SSN <> "999-99-9999") OR
(SSN <> "none") OR
(SSN <> "na")
```

- Better yet, use the query field to call a **stored procedure** on the database. A stored procedure, often written by the DBA, can be written to validate data quality and/or prevent dirty data in the query results. A stored procedure is likely to be much more efficient than the example query above.
- Common addresses, phone numbers, names, etc. should not be registered
- Normalize unknown/missing data as "Null" rather than zeros, "Blank", 010101, or "Needed"
- Run a simple query to select all data from a given table and column, and then save the results to a .csv file. Open the file in a spreadsheet and sort it. Look at the top and bottom to identify groups of non-standard data. Copy that data out and register it to a GreenList™.
- Create a policy that looks for the occurrence of one kind of data only in the context of another. For example, you can create a policy that will trigger an incident only if three or more social security numbers are detected in a single document, or only if a social security number is detected along with a name or another piece of personally identifying data.
- Monitor incident results by drilling down to see what triggered the detection, and if it was a false-positive, how frequently it occurred so you can either add it to a GreenList™ (as unstructured data) or refine the query you use to rip and register the data.

In all these cases, a certain amount of trial-and-error experimentation can be expected before finding the method that works best for your data and organization.

Limits and considerations

- Data registered from a database is restricted to the first 32 characters of any given cell. For "wordy" data, consider registering it as unstructured data or creating a regular expression (**Register Data > Patterns**).
- No more than 64 columns of data from all tables (and .csv data) can be registered. In other words, you could register two columns of data (name and SSN) per table from as many as 32 different tables, or eight columns of tables from eight different tables using any number of queries.

- Registered data column names must be unique. The DLP appliance will automatically rename duplicate column names.

4.5.2 Use Row Correlation

Row correlation can be applied to data registered from a structured source (e.g., a database) as a means of increasing the relevancy of matches. For example, say five columns of data are registered from a database with 1 million rows. With row correlation as a part of the inspection policy (as shown in Figure 4.13), the DLP appliance will only create an incident if it detects the occurrence of all five items— from the same row, from the same data source, and occurring in the same document. Documents that contain a variety of matching items from the database will not trigger a match unless the items all belong to the same row.

Historically, row correlation did not take into account the proximity of items. Continuing the example above, if all five items were found to occur anywhere in a 1,000 page document, that document would trigger an incident. Row correlation now includes a proximity threshold, however, which further decreases the likelihood of false positives. By default, this threshold is 1024 characters (including spaces) on either side of a matching item. As a point of reference, that is equivalent to about a half page of text on either side of the matching item.

Notes:

- Correlated data must all be from the same source.
- Columns added as constraints in the policy must be connected by the AND operand.

- The detection frequency for all items must be the same.

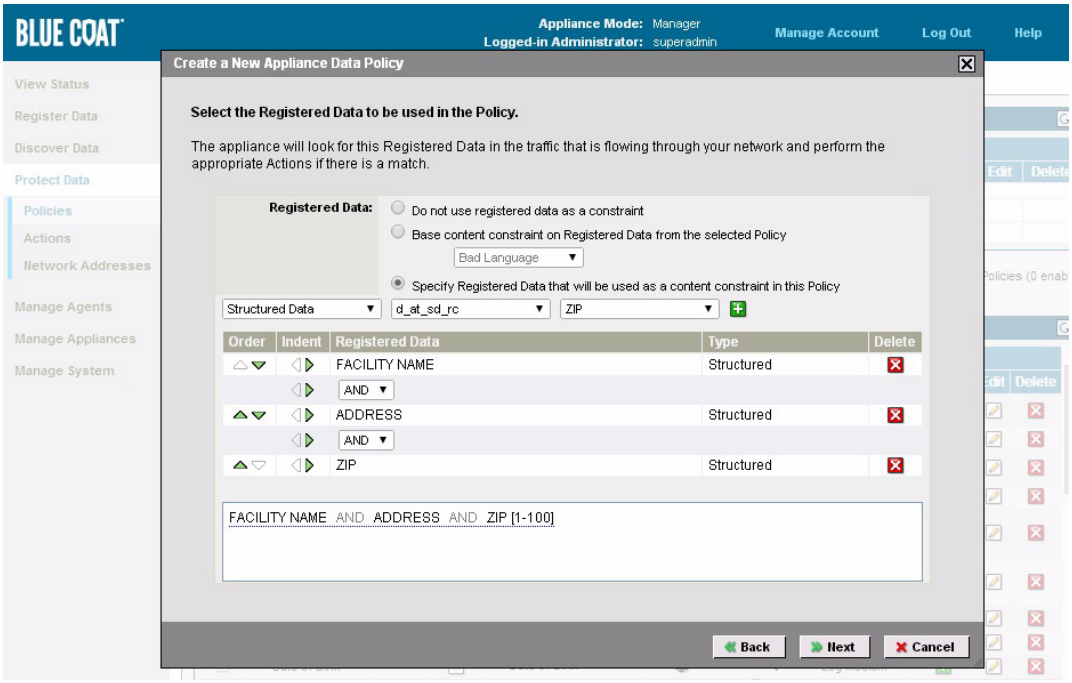


Figure 4.13: This inspection policy includes row correlation; each constraint comes from the same registered data source (i.e., RedList™), the columns are connected with the AND operand, and the detection frequency for each is the same. In the above example, MRN Pattern and Inappropriate_language provide row correlation.

4.5.3 Reducing False Positives in Unstructured Data

One of the biggest contributor to false positives in unstructured data it that the some or all of a registered document is not uniquely confidential. The most prevalent example occurs when boilerplate, the company masthead, contact information, or URLs are inadvertently registered along with sensitive data.

Files in a folder marked "Confidential" are usually not all confidential. For example, blindly registering the data of a Windows "Documents and Settings" folder will likely contain archived post office folders (.pst) which will include amongst the emails, recurring signatures, employee names, and a host of other non-sensitive data.

- Files should be confidential in their entirety, otherwise consider registering only the confidential portions as shown in "Registering Clipboard Data or a Document" on page 56.
- The number of files registered should be strictly limited (tens or hundreds, not millions)
- Files should be of recent origin (the secret marketing plans from years ago are now public knowledge)

- Monitor incident results by drilling down to see what triggered the detection, and if it was a false-positive, how frequently it occurred so you can add it to a Green-List™ (as unstructured data).

In all these cases, a certain amount of trial-and-error experimentation can be expected before finding the method that works best for your data and organization.

Limits and considerations

- Using a GreenList™ is a good way to exempt certain data from detection. However, if that same data has already been registered and added to a RedList™, adding it to the GreenList™ it will not remove the fingerprints. As such, it is far better to register unstructured data carefully by reviewing folder and document contents.
- There is no way to exclude a given subdirectory when registering data in the parent directory. Likewise, you cannot exclude a particular file type from an unstructured crawl. For this reason, it is best to create a directory and then add the documents you want to register.
- When setting up and/or testing the detection rate of newly registered data, set the Action to "Information" to avoid triggering actionable incidents or notification messages.

4.5.4 Using a GreenList™ to Reduce False Positives

You can prevent false positives from triggering an incident by adding unstructured data (that is, not database content) to the GreenList™. In some cases, you can predict what will trigger a false positives (such as common URLs and dummy data) and in others you can drill down in the Incident Details list to find out what triggered a given match.

Note: GreenList™ items override RedList™ items and are applied to all scans by default. As an extreme example, if you were to GreenList™ the word, "the", it is likely that all your data detections would be over-ridden by the exemption. Be careful not to make your GreenList™ data too general or broad (and test it before a wide deployment).

Before beginning the procedure below, re-query the data you registered earlier and save the column of data as a .csv file. Open the .csv in Microsoft Excel, sort it, and then review the data to assess its integrity. Typically, invalid entries float to the top or sink to the bottom when sorted. Copy and paste the obviously invalid data to a text file.

To add data to the GreenList™ (unstructured data only):

1. In the management console, click **Register Data > Files and Databases| GreenList™.**
2. Click the **Add GreenList™ Data...** button. The Register New Content window appears.
3. Choose **File Upload** for this example and then click **Next**.
4. Type a name that identifies the data you will register. This name will appear in the RedList™, and is also what you will use to find this "fingerprint" when adding

it to a detection Policy. The description will appear when you mouse over the name in the RedList™.

5. For Data Tag, keep the default, "none" and then click **Next**.
6. In the **Upload File** option, choose **Clipboard**. Give it a name that will clearly identify the data of the snippet, and copy/paste the text you want to detect to the **Registered Data** field.
7. Click **Finish** in the review screen. The name you entered in step 1 will appear in the list of RedList™ names.

4.6 About the RegEx Used in the DLP Manager

The DLP appliance uses the Perl-compatible ICU library for Regular Expression matching. This RegEx is used both for matching Pattern Objects from policy content rules, and for Inspection Patterns used in Structured Data tags.

For comprehensive usage guidelines, see the ICU project website:

`http://userguide.icu-project.org/strings/regexp`

4.6.1 Selected RegEx Expressions Used in Patterns

For a complete list of the RegEx used to create the DLP patterns available in the DLP appliance, open the online help and type "RegEx" in the Search field. The table below provides some examples for your reference.

Table 4.1: Sample RegEx used in DLP patterns

Pattern	RegEx
Generals credit cards, including: American Express, Discover, JCB, Master Card, Visa	`\b((\d{15}\d?)|(\d{4}[ -\.]((\d{4}[ -\.]\d{4}[ -\.]\d{4})|(\d{6}[ -\.]\d{5}))))\b` Note that card-specific RegEx is also provided in the online help.
CDA Medical Claim	`levelone(\s+)xmlns(\:cda|\:hl7)?(\s*)=(\s*).?urn\:*hl7-org\:v(\d)([\p{Nd}\.]*)/cda.?`
Email Address	`\b[A-Z0-9\._%+\-]+@[A-Z0-9\.\-]+\.([A-Z]{2,3}|(aero|arpa|asia|coop|info|jobs|mobi|museum|name|travel))\b`
US Social Security Number	`(?<!mso-font-signature)(?:[\t\(\[\{ :,=]|^)\d{3}[-]?\d{2}[- ]?\d{4}(?:[\t\)\]\} ,.]|$)`
Test pattern	#DLP Test#

5 Inspect Email Traffic

The DLP appliance can detect whatever content you register, including specific "strings" such as a name or social security number, the content of entire documents (even if it has been excerpted, altered, and/or copied in to another document) and data patterns. Email inspection checks the message subject, body, and any attachments.

This chapter provides information on how to install and configure the DLP appliance MTA inspection service. It begins by summarizing a few fundamental concepts and then takes you through the process of creating several different kinds of email inspection policies. At the end of the chapter are some examples to illustrate the range and versatility of inspection.

5.1 Configuring Email Inspection

You can route traffic from an MTA to the DLP appliance for data inspection, and then to another MTA for delivery. Inspection includes the email body and any attachments, including compressed files. Encrypted files are not inspected, but a policy can be created for special handling of these files. Incidents are kept,

and key identifying information redacted so it will visible only to the Super Administrator user ("superadmin").

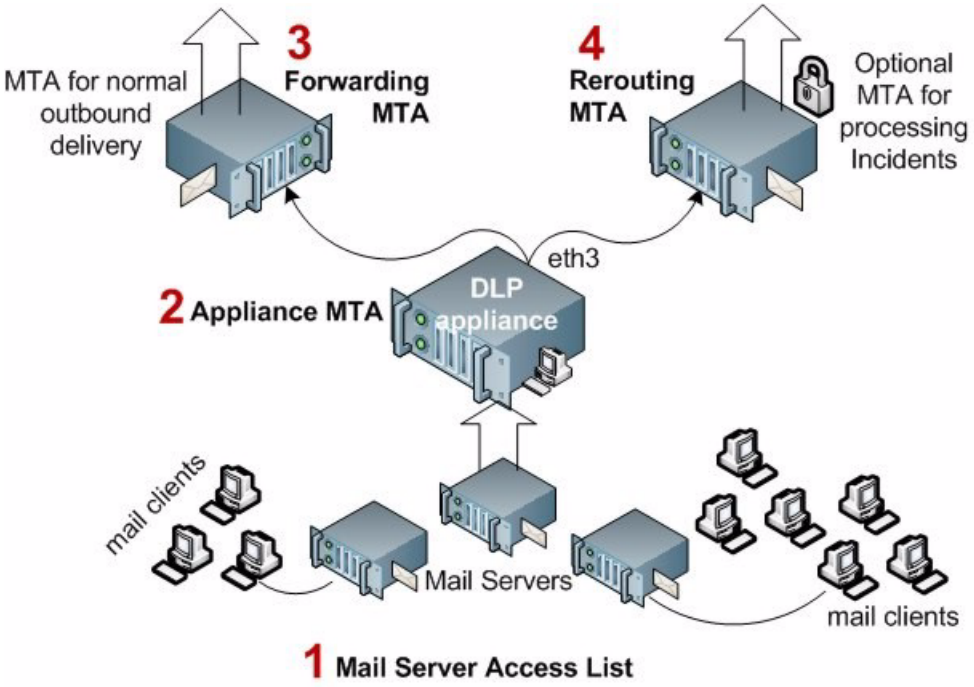


Figure 5.1: Client emails sent to their MTA (1) which forwards them to the DLP appliance (2) for inspection. After inspection, the appliance forwards messages to a default MTA (3) for delivery as usual, or, optionally, to a rerouting server (4) for special handling.

5.1.1 Configure the MTA Port

Perform this task to assign an IP address and gateway to the MTA port (eth3) on the the DLP appliance. The MTA port should already be connected to a network that allows access to one or more mail servers from which the DLP appliance will receive mail, a mail forwarding server, and, optionally, a rerouting server.

Note: The content of outbound messages encrypted at the client cannot be inspected.

To configure the MTA port:

1. In the DLP Manager, click **Manage System > Configuration > Network | Interfaces**.
2. Click the **Edit** icon for the MTA interface.
3. If you want to change the name of the interface, enter the new name in the **Description** field.
4. Click the **Settings** tab.

5. In the **IP Address/Mask** field, enter the IP address/mask and gateway you will assign to the MTA port, for example,

   ```
   10.10.1.6/22
   10.10.1.1
   ```

6. In the **Speed/Duplex** field, accept the default value **Auto-negotiate** or choose one of the settings from the drop-down list to match your switch hardware.
7. Click **OK** to save the changes and close the window.

5.1.2 Configure the MTA Inspection Service

Perform this task to enable the MTA inspection service on the DLP appliance. You will need to configure at least one MTA to forward traffic to the DLP appliance for inspection, and another MTA to deliver inspected traffic to the recipient. You can also configure a third MTA and have the DLP appliance route sensitive or restricted traffic to it for additional processing prior to delivery.

To route email traffic to and from the DLP appliance:

1. In the DLP Manager, click **Manage System > Configuration > Inspection Services | MTA**. Click **Enable** to inspect the content of outbound email, and then set the following:

   Appliance MTA Settings—optional. Use this host name, or the IP address assigned to eth3, to configure the remote MTA(s). This setting will also appear in message headers.

   a. Enter the DLP appliance host name, if any, that has been assigned to eth3, or the IP address of eth3 (click **Manage System > Configuration > Network | MTA** to see the IP address for eth3).

   b. Accept the default, 16, for maximum concurrent connections unless the Forwarding MTA frequently has to re-send messages to the DLP appliance.

   Forwarding MTA Settings—required. This is the MTA that will deliver outbound messages that have been inspected by the DLP appliance. To avoid looping, do not use one of the MTAs specified in the Remote Access List unless you have configured that MTA not to forward messages received from the appliance back to the appliance.

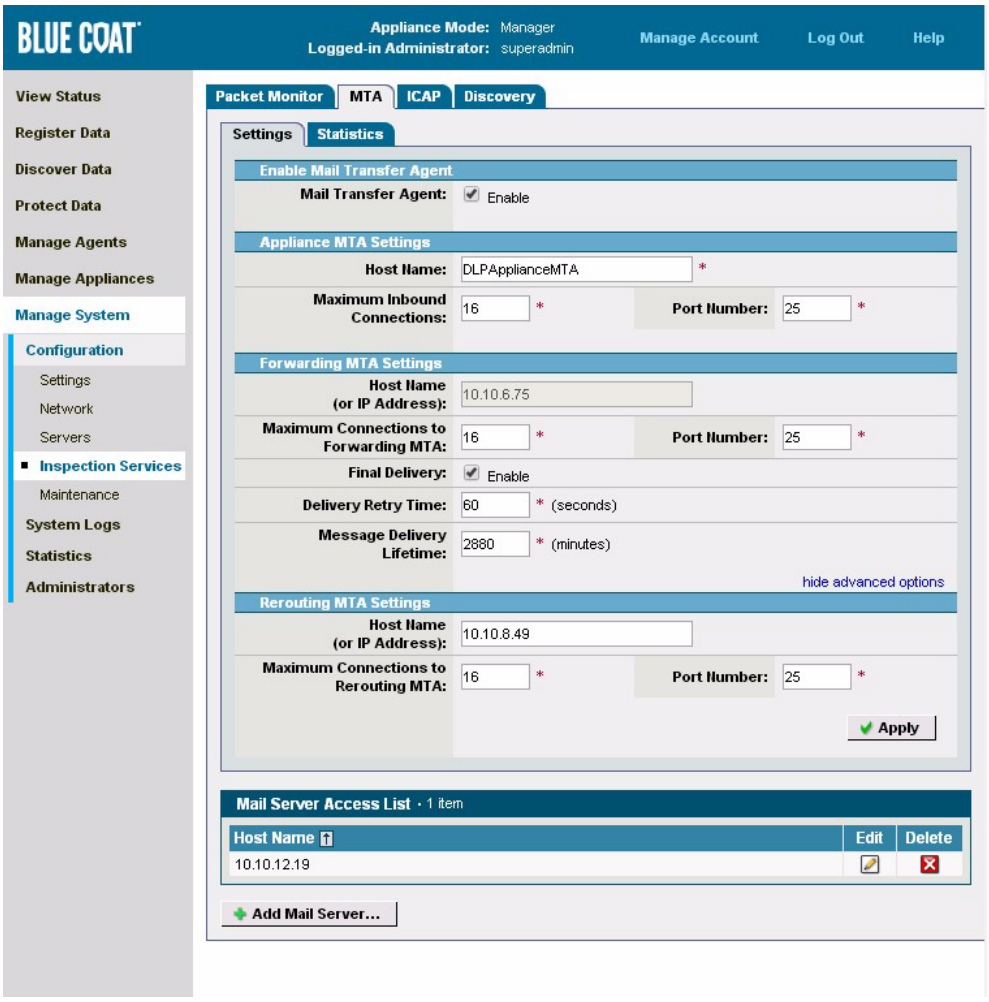


Figure 5.2: Configure the DLP appliance to receive outbound emails and then forward inspected messages to another MTA for delivery.

a. Enter the host name or IP address of the MTA that will deliver inspected traffic to the recipient.

b. Accept the default, 16, for maximum concurrent connections.

Notes:

- You can check the performance of mail forwarded from the DLP appliance to the delivery MTA (i.e., send errors, retries, delivery queue) by clicking the **Statistics** tab.

- To prevent Non-Delivery Report (NDR) for undeliverable mail from being sent to the outbound MTA rather than back to the inbound MTA, be sure both MTAs have the same delivery settings.

Rerouting MTA Settings—optional. This is MTA is an alternative to the Forwarding MTA and can be used to perform any special handling (all other messages would be routed, as usual, to the Forwarding MTA).

See Figure 5.1 for an illustration showing how the MTAs configured in Figure 5.2 are used.

a. Enter the host name or IP address of the MTA that will perform post-inspection processing.

b. Accept the default, 16, for maximum concurrent connections.

Note: Click the **Apply** button to save your settings before configuring the Mail Server List.

Mail Server Access List—required. The DLP appliance will only accept email forwarded to it from MTAs that are listed here. You must indicate at least one MTA for email inspection to occur.

a. **Click the Add Mail Server** button.

b. Enter the IP address or Host Name of each MTA that will forward email traffic to the DLP appliance for inspection.

c. Click **OK** to save your changes

2. Click the **Apply** button again to save your settings.

5.1.3 Configure MTA(s) to Forward Email Traffic

In addition to telling the DLP appliance which MTAs to accept email traffic from, you need to configure those MTAs to send traffic to the DLP appliance for inspection. The same may be true for the Forwarding MTA that will receive inspected mail from the DLP appliance, and, optionally, the Rerouting MTA. Use the documentation provided with your mail server to make the appropriate routing changes.

Note: The host name and port used by the DLP appliance to accept traffic from expected MTAs can be found at **Manage System > Configuration > Inspection Services | MTA | Settings**.

Blue Coat Systems recommends that you start by forwarding traffic from only one MTA to the DLP appliance for testing and policy tuning before pointing all your email traffic to it.

5.2 Detect Registered Content in Email Traffic

If you have connected eth3, the DLP appliance MTA port, to your network and are routing SMTP traffic to it you can create a policy that monitors inbound and/or outbound email messages for whatever registered data you want.

Note: Before beginning the procedure below, check the status of the MTA in the **View Status** dashboard by looking at the Health Monitor. Both the **Inspection Services** and **Interface** tabs should show a green light for MTA. If the light is gray, the service has not been enabled. If it is red, there is a connectivity issue. Click either light to open the MTA configuration page.

Notes about MTA scanning:

Depending on deployment topology, when email is routed through the DLP appliance MTA, email leaving the network may pass through both the DLP appliance MTA port and the data port for the interface that inspects all traffic leaving the network. This means that two incidents will be created, with the following properties.

- The incidents will appear under two separate transaction numbers, even though the incident refers to the same policy match in the same email.
- The incident created by the network monitor will always show Audit Only as the value for Transaction Status, regardless of how the policy action is configured.
- The incident created for the MTA transaction will show a Transaction Status value of Blocked or Audit Only, as determined by the policy action.
- If the Packet Monitor and the MTA inspection service are enabled at the same time, it is a good idea to filter the data and reports to avoid duplicates.

Depending on how email clients are configured, they may include the text of the email in more than one format (HTML, text, RTF). This can cause one match to be counted more than once, which can affect the policy action if an occurrences threshold is set. In addition, the over-count will appear in the incident's Matched Details. The Number of Unique Matches can be a more accurate count.

To turn off MTA inspection:

1. In the management console, click **Manage System > Configuration > Inspection Services | MTA | Settings**.
2. Add or remove the check from **Mail Transfer Agent**: option.
3. Confirm you changes by clicking **View Status**. The MTA status light should be gray.

5.2.1 Inspect SMTP Traffic

In the procedure below, you will create a policy to inspect email traffic for any occurrences of the data registered in Chapter 4.

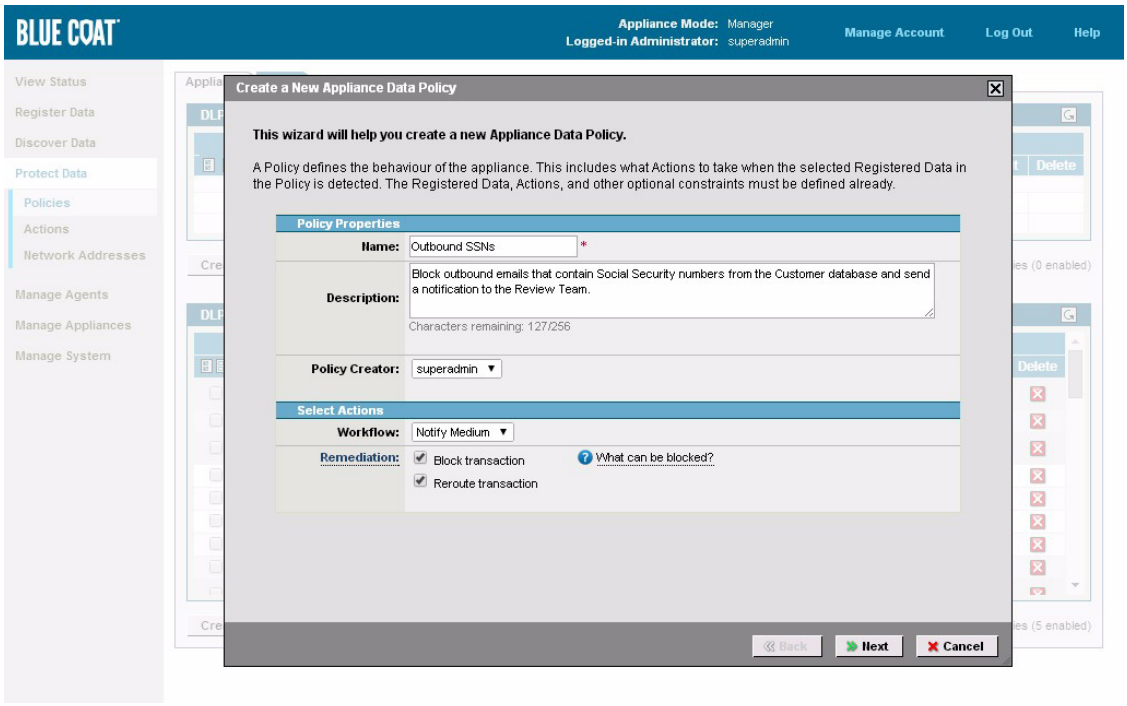


Figure 5.3: You can have the DLP appliance automatically block email found to contain registered data.

To scan MTA traffic:

1. In the management console, click **Protect Data > Policies.**
2. Click the **Create Policy...** button. The Create a New Policy window appears.
3. Fill out the Policy Properties as shown below, and then click **Next**.
   - **Name**—type name will identify the policy in the Policy List.
   - **Description**— type a description; it will appear when you mouse over the policy name and typically includes a summary of the policy, for example, who requested it and what it checks
   - **Policy Creator**—this option is recorded with any incidents and can be used to direct notifications.
   - **Action**—both pre-defined and custom actions appear in the list. For this example, choose the Action you created in "Create a Network Address Group" on page 36.

   Transaction Options

   - **Block**—blocked messages will not be delivered, and the sender will not be notified. Blocked messages are held with the Incident for review.
   - **Reroute**—choose this option to have messages that match a given policy routed to a second MTA instead of the default forwarding MTA. Note that a

Rerouting MTA must be configured on the DLP appliance (**Manage System > Inspection Services | MTA | Settings**) and that the target MTA must be configured to accept mail relays from the appliance.

4. Choose which data you want the policy to use for detection, and then click **Next**.

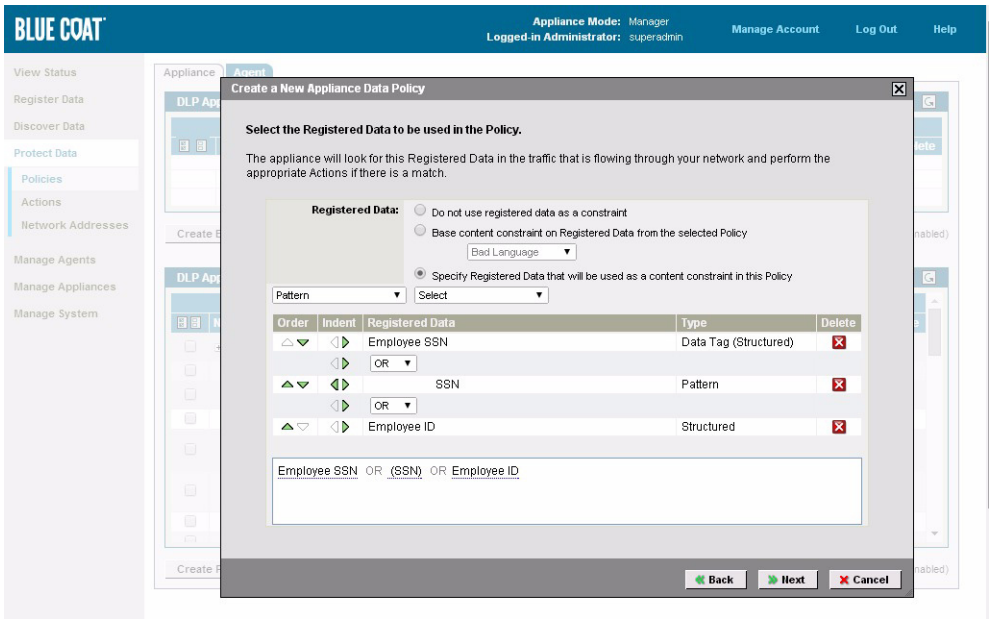


Figure 5.4: Choose the data you registered in "Registering Data" on page 48. You can combine registered data from different sources, including patterns.

- **Do not use registered data as a constraint**—Choose this option if you want to identify files based on one or more properties instead of data (seldom used).
- **Base content constraint on Registered Data from the selected Policy**—Choose this option if you want to inherit the Registered Data portion of an existing policy. This is especially useful, for example, if you have created a Discovery Policy that you want to re-use for Data In Motion. Click the drop-down list to show all available (i.e. existing) constraints, and select the one or ones you want to use. You can use the inherited constraint "as is" or modify it by adding or removing elements from Registered Data.
- **Specify Registered Data that will be used as a content constraint in this Policy**—Choose this option for the current example. It allows you to select the data you registered previously. You can choose additional constraints and/or combine them (combining restraints can reduce false positives by creating more conditions). Mouse-over the Registered Data column in the Policy List to view a summary of the applied constraints.

5. Select the source and/or destinations you want the policy to apply to and then click **Next**. All traffic is monitored, but only those transmissions meeting the criteria selected below are analyzed against the policy.

   Source/Destination

   - **Apply this Policy to all Users**—choose this option for the current example. It will apply the policy to all email transactions.

- **Apply this Policy only to specific Users or Groups**—choose this option to apply the policy to only those users you select from the DLP appliance user list or, if you have it connected, your LDAP directory
- **Network Address Filter**—choose this option to apply the policy to the sender/recipient according to network address, domain, or network group you created in Chapter 3, "Create a Network Address Group" on page 36.

6. Select any additional constraint, explained below, and click **Next**.

   Direction: (messages between users within the LAN are not checked)

   - **Inbound only**—apply the policy to email received from the Internet
   - **Outbound only**—apply the policy to email sent out of the LAN
   - **Both Inbound and Outbound**—choose this option for the current example

   Protocols

   - **Standard Email (SMTP)**—Choose this option for the current example. Note that the DLP appliance should already configured for email inspection, connected to an MTA, and that the MTA must be configured to forward traffic to DLP appliance.
   - **HTTP**—requires ICAP proxy
   - **Webmail**—includes Google Mail, AOL Mail, Yahoo! Mail, Hotmail, and MSN Live Mail (Full and Light). Webmail that cannot be identified is classified as an HTTP transaction.
   - **HTTPS**—requires ICAP proxy
   - **FTP**—requires ICAP proxy
   - **Other TCP**—must have packet monitoring enabled

7. You can further narrow eligible data by selecting a **File Filter**. The policy will always be applied the message body (or form post). If there's an attachment and if it is the right type, the attachment will be scanned. File type determination is made according to the file metadata. Click **Next**.

8. In the Summary screen that appears, then click **Finish** to return to the Policies page. The policy will be enabled and MTA traffic monitoring will begin immediately.

   - Remove the **Enable** check mark to stop monitoring SMTP traffic for the registered data in this policy.
   - Click the **Edit** icon to change any of the scan parameters

9. Click the **Add Exception** icon to create and attach an second policy to reduce false positives caused by dirty data. In this example policy, use the **GreenList™** you created previously. This list contains the invalid data of the type you are detecting in this policy, for example, all the records with 000-00-0000 and "none" for a social security number.

More about exception policies

- Exception policies are used in the case when you want to implement the logic, "perform the action in Policy X when a violation is found, except when Policy Y also applies, in which case perform the action in Policy Y"
- Exception policies are single-use; exceptions can only be attached to one policy
- You can attach multiple exceptions to any given policy

- The order in which exception policies appear on the list is significant; the first exception is evaluated first, etc. and as soon as a match is found any remaining exception are skipped

5.3 Example Policies

The examples below describe common security goals and how they can be implemented with DLP appliance policies.

5.3.1 Monitor Outbound Traffic to Analyze Usage

Suppose you want to analyze outbound traffic and then generate reports to get a sense of what kind of information is leaving the network, which protocols are being used, who is sending it, and who is getting it. For example, you might want to know where SMTP mail is going when it leaves the corporate network, or how often Webmail is used and what it contains. The goal can be restated in more detail as "Log an incident for all network traffic and retain copies of the transactions when possible."

To meet this goal, a single policy could be created with the following components:

- **Registered data**—None (all traffic will trigger a violation regardless of data)
- **Action**—Use the predefined Notify Medium Risk (**Protect Data > Actions**), which will create incidents, retain copies of the transaction when possible, and assign the incidents to the policy creator.
- **Constraints**—None

When you create reports to summarize the incident data, you can constrain the data set in various ways and group on various categories, such as protocol, source or destination of the transaction, or file types transmitted.

5.3.2 Take Conditional Action

This is an example of a policy with constraints. For example, when sensitive data is detected, you might want to create an incident only when it is coming from particular sources, or going to particular destinations. This goal can be stated as "When sensitive data is detected, create an incident only when certain conditions are met." For example, you might want to take action only when the destination of an email is the domain of certain competitors.

Create a policy with the following components:

- **Registered data**—RedList™
- **Action**—A predefined or custom an action to create an incident, plus any other response (notification, incident assignment, sending to a logging server)

- **Constraints**—A source or destination constraint

5.3.3 Take Conditional Action (example 2)

This logic can be rephrased in the following statement: "Create an incident when Data A is detected, except under certain conditions, in which case no action should be taken." For example, you might want to take action on the transmission of nonpublic personal information except when the destination of the email is a third-party benefits administrator. A main policy would be created with an exception policy attached. This is an example of a main policy with a more restrictive action than the exception policy.

Create a main policy with the following components:

- **Registered data**—RedList™ or file class
- **Action**—Use a predefined action to Block the transaction, create an incident, and also perform any other response you want (notification, incident assignment, sending to a logging server)
- **Constraints**—None

Create an exception policy with the following components:

- **Registered data**—Same RedList™ as main policy
- **Action**—Use a predefined action to Allow the transaction and create an incident.
- **Constraints**—Desired conditions (for example, if the condition were "except when sent to trusted partner Z," then partner Z would be named as a destination constraint)

5.3.4 Respond With Action Depending on Condition

This logic can be rephrased in the following statement: "Create an incident of low severity when Data A is detected, except under certain conditions, in which case create an incident of high severity and take other actions." For example, in the less extreme case you might want to allow the transaction to pass through but merely create an incident, but in the more severe case you might want to block the transaction and send notifications.

A main policy would be created with an exception policy attached. This is an example of a main policy with a less restrictive action than the exception policy.

Create a main policy with the following components:

- **Registered data**—RedList™ or file class
- **Action**—Use a predefined action, such as Medium Risk (log an incident, assign to policy creator, retain a copy), Low Risk (log an incident, assign to policy creator) or Information (log an incident only)
- **Constraints**—None

Create an exception policy with the following components:

- **Registered data**—Same RedList™ as main policy
- **Constraints**—Desired conditions (for example, if the condition were "except when sent from suspect employee Z," then employee Z's email address would be named as a source constraint)

5.3.5 Detect Registered Data

Unstructured documents often contain a mix of sensitive information and boilerplate text. An example of boilerplate text is the standard information about a company that always appears in press releases or financial statements. Boilerplate text tends to appear in a number of different documents.

Boilerplate text is best handled in either of two ways:

- Create a GreenList™ and use the file upload method to paste in the boilerplate.
- Create one or more files containing the boilerplate text in a special directory, then create a repository scan GreenList™ to register all the data in that directory.

This means that if documents in a scanned directory contain boilerplate text, the boilerplate text portion of the document will be registered in both the RedList™ and a GreenList™. Since GreenList™s apply to all policies, you only need to set up a policy for the RedList™.

Create a main policy with the following components:

- **Registered data**—RedList™ or file class
- **Action**—Any action, which will create an incident for a data violation unless a GreenList™ also applies)
- **Constraints**—None

5.3.6 Block Sensitive SMTP or Webmail

Blocking is accomplished as part of a policy action. SMTP mail blocking requires configuration of the DLP appliance MTA inspection service, and Webmail blocking requires configuration of the ICAP inspection service with a supported proxy server.

When SMTP mail blocking is enabled, the blocked transaction can be reviewed as part of incident management, and, if approved, will be forwarded on to its destination. When HTTP Webmail blocking is enabled, the blocking action is permanent.

Suppose you have both the MTA and ICAP inspection services enabled and you want to set up a policy to block email and HTTP data.

Create a main policy with the following components:

- **Registered data**—RedList™
- **Action**—An action that will create an incident of high severity, assign a reviewer or review group, retain a copy, send a notification, and block the transaction

- **Constraints**—Protocol = SMTP or HTTP

Since blocking is a severe measure, in most cases, you would want to fine-tune the sensitivity of the policy by setting up constraints in the main policy or by attaching an exception policy, as described in previous examples.

Note: The Packet Monitor inspection service, if enabled, will create incidents for the same policy violations as the MTA and ICAP inspection services, since it will monitor the same traffic. Therefore, it is a good idea to create filters or query constraints to limit the data to particular inspection services when viewing incidents and creating report templates.

5.3.7 Use Webmail as a Policy Constraint

Webmail as a policy constraint allows a policy to be triggered based on Webmail traffic, distinct from other HTTP/HTTPS traffic.

Create a main policy with the following components:

- **Registered data**—Do not use Registered Data as a policy constraint
- **Action**—An action that will create an incident but allow the traffic to pass
- **Constraints**—Protocol = Webmail; Direction = outbound traffic

6 Inspect TCP Traffic

The tasks in this chapter focus on configuring the DLP appliance receive and inspect network traffic. You should have an environment suitable for the initial deployment of a network-scanning device, i.e., one with access to high-volume network traffic, an LDAP, and an proxy server.

Once you have registered some data, the next thing to do is create a scan policy and start inspecting network traffic for the existence of that data. The policy tells the DLP appliance where to look for the data you want to detect, and, depending on the kind of scan, what to do: block, reroute, or let it pass.

- **Packet Monitoring** (TCP traffic inspection) allows you to create an audit record of data matches detected in TCP traffic without taking any action or requiring a special workflow.
- **ICAP Inspection** is explained in Chapter 7. It checks Web traffic routed to the appliance from a proxy server for restricted content. Traffic can be inbound or outbound, and includes Webmail, HTTP, HTTPS, and FTP.

This chapter includes the following:

6.1 Packet Monitoring

Packet Monitoring is especially useful for testing intended policies. You can register data, configure a policy, and then audit that policy to understand

whether it is detecting the kind and amount of incidents you intended. You can audit traffic for 24 hours, or even a week, to establish an incident baseline for intended policies. Packet monitoring is also a good way to verify the quality of your registered data or regular expressions (i.e. RegEx, or Patterns) to see if anything is going to trigger an unacceptable number of false positives. If you find that false positives are coming from your registered data, you can add these items to the GreenList™ to exempt them. Likewise, you can refine any RegEx pattern that is not detecting the data you have in mind.

Once you have had the policy in place long enough to be confident of the detection quality, you can re-target the policy to actively scan (and create incident for) detections by the ICAP inspection services. Keeping all inspection services enabled at the same time can result in duplicate incidents (one as passes through eth0/eth1, and one as it passes the ICAP port).

Note: Depending on how and where you have installed the network tap for packet monitoring, email or other network traffic that has been routed through a DLP appliance inspection service may also be detected by the Packet Monitor and two incidents created. To address this, you can either install the tap in such as way as to avoid double-scanning, or use the Logs and Reports filter to remove the duplicates from view.

By default, Packet Monitoring (all TCP traffic) is enabled on the DLP appliance and will occur as soon as eth ports 0 and 1 are connected to the network, via tap or mirror. The Packet Monitor ports do not require an IP address or Gateway assignment, and the default settings do not typically need to be changed. The policy-specific options to Block and/or Reroute traffic do not apply to packet monitoring.

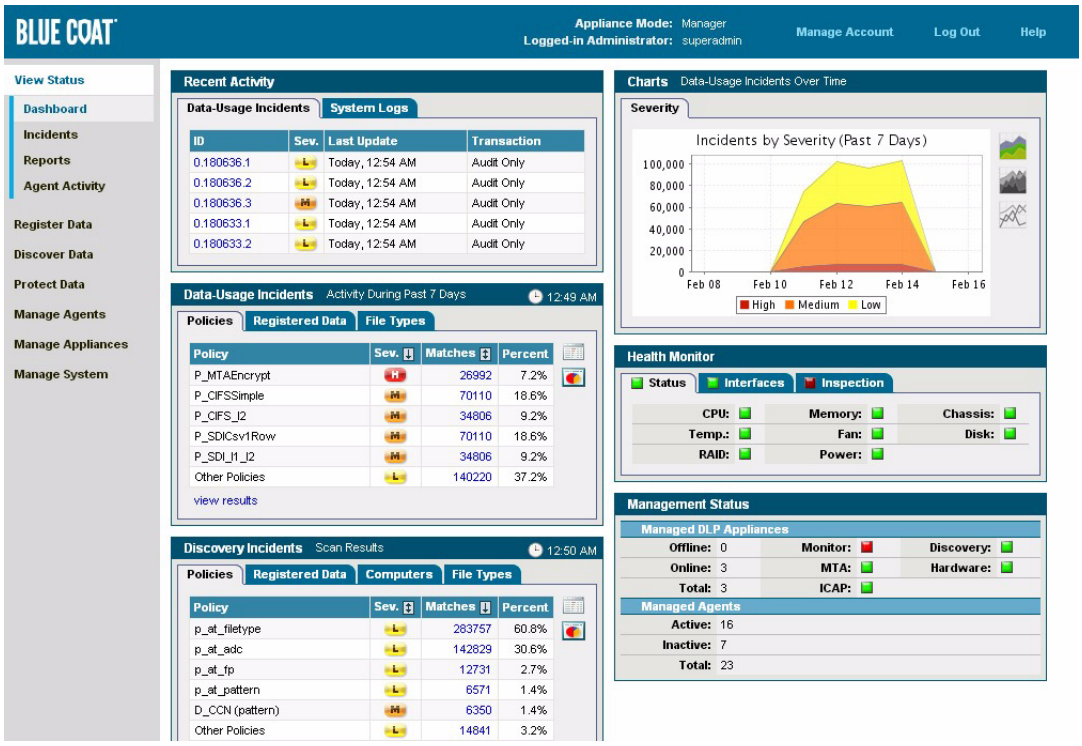


Figure 6.1: In the Health Monitor, you can click a given status to open the configuration page for that inspection service.

Because the Packet Monitor is passive, providing audit data only, in most cases there is no reason to disable it. However, if you will dedicate a particular DLP appliance to ICAP or MTA traffic inspection, you may want to disable Packet Monitoring on that appliance.

6.2 Set up Packet Monitoring

By default, Packet Monitoring (all TCP traffic) is enabled in the management console and will occur as soon as eth ports 0 and 1 are connected to a network tap. The Packet Monitor ports do not require an IP address or Gateway assignment, and the default settings do not typically need to be changed. If, however, you want to dedicate a particular DLP appliance to inspect ICAP traffic or check outbound email from an MTA you may want to disable Packet Monitoring on that appliance.

Additional Notes

- The Block, and Reroute policy options do not apply to packet monitoring.
- If the Packet Monitor and the MTA and/or ICAP inspection services are enabled at the same time, data detections may be recorded twice (depending on how you have the services deployed on the network).

To verify the Packet Monitor:

1. In the management console, click **View Status > Dashboard.**
2. In the **Health Monitor** window pane, click the **Inspection Services** tab and/or Interfaces as shown in Figure 6.1.
   - If the icon is green, the packet monitor is connected to the network and auditing traffic. To confirm this,
     - Click **Manage System > Configuration > Network | Interfaces**.
     - Click the **Edit** icon for Interface eth0 and then for Interface eth1.

- Open the **Statistics** tab in the window that appears. The number of bytes and packets will be greater than zero if the port is getting traffic.

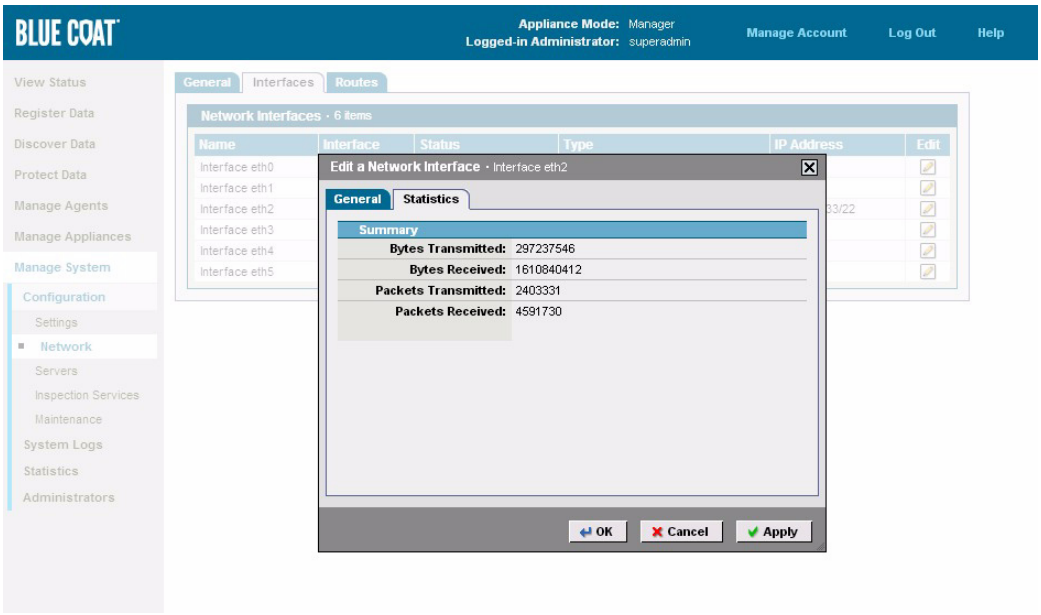


Figure 6.2: Check Statistics to see whether the port is receiving network traffic.

- If the status icon is red or gray, either Packet Monitoring is disabled or there is a problem with connectivity.
  - Click the icon as a shortcut to opening the **Manage System > Configuration > Inspection Services | Packet Monitor** screen and confirm that Packet Monitoring is enabled, and that the Topology matches your hardware (tap or mirror).
  - Click **Manage System > Configuration > Network | Interfaces** to check the status of Interface eth0 and eth1. You may also need to test the physical ports to confirm that TCP traffic is being received.
  - Once again, click **Manage System > Configuration > Network | Interfaces**, and then the **Edit** icon for eth0 or eth1 and open the **Statistics** tab.

6.2.1 Disable Packet Monitoring

Blue Coat Systems generally suggests having the Packet Monitor inspection service run on the DLP appliance. One exception is if you are setting up a second instance of the DLP appliance and want to dedicate it to MTA and/or ICAP inspection.

To disable Packet Monitoring:

1. In the DLP Manager, click **Manage System > Configuration > Inspection Services.**
2. In the **Packet Monitor** field, select **Enable**.

3. Select **Tap Mode** or **Mirror Mode** to reflect whether the appliance is connected to the network through a tap or a mirror port.
4. Click **Apply** to save the settings.

6.2.2 Modify the Default Settings (seldom used)

By default, the Packet Monitoring ports are set for Auto-negotiate, 100Mb, and half duplex. They will automatically synchronize to the appropriate settings for your tap or mirror.

To modify the Packet Monitoring configuration:

1. In the DLP Manager, click **Manage System > Configuration > Network | Interfaces**.
2. Click the icon in the Edit column for either of the Packet Monitor interfaces (eth0 or eth1).
3. Click the **Settings** tab.
4. In the **Speed/Duplex** field, accept the default value **Auto-negotiate** or choose one of the settings from the drop-down list.
5. (Optional) To change the name of the interface, click the **General** tab and enter the new name in the **Description** field.
6. Click **OK** to save the changes and close the window.

6.3 Creating Network Inspection Policies

In conjunction with a supported ICAP proxy server, the DLP appliance can monitor and detect secure data in HTTP, HTTPS and FTP traffic in real-time. Typical applications of this inspection service are to monitor outbound traffic, including Web uploads, FTP file transfers, content as it is posted to a blog, content that is entered into Web forms, and posts to an Internet Web server.

In addition, the ICAP inspection service supports all the most frequently used Webmail clients, including Yahoo, GMail, Hotmail, MSN, and others. ICAP inspection can detect restricted data that is included in the body of an email, as well as in any attachments. If it detects a policy violation, the DLP appliance will create an incident (retaining the mail body and any attachments), and either block the transmission or allow it to pass. If you choose to notify users and an incident is blocked, they will see a Web page with a default or customized explanation of what happened.

6.3.1 Create a Policy and Detect Registered Data

Note: Before beginning the procedure below, check the status of the ICAP proxy in the **View Status** dashboard by looking at the Health Monitor. Both the **Inspection Services** and **Interface** tabs should show a green light for ICAP. If the light is gray, the service has not been enabled. If it is red, there is a connectivity issue. Click either light to open the configuration page.

In the procedure below, you will create a policy to detect the data you registered previously in Web traffic. Choose registered data that contains unambiguous data and a file share with documents you know have data that will be detected when you perform the scan.

You must have connected eth4, the DLP appliance ICAP port, to your network and be routing Web traffic through it before you create a policy to monitor outbound Web data.

Additional Notes

- If the Packet Monitor and the ICAP inspection service are enabled at the same time, it is a good idea to filter the data and reports to avoid duplicates.
- The Reroute policy options do not apply to Webmail—they are for MTA traffic only.
- Because of the variety of Webmail and FTP clients and frequency of change, not all data blocking actions occur in the same way. In most cases, users can receive separate notifications if an email attachment upload violates policy or if the message data does. In some cases, however, no notification will occur and the user will receive no feedback that his/her message was blocked. In either case, the violating text and/or attachments can be retained in the incident report.

  Note: The notification option requires that you have an LDAP server configured for user identification.

To inspect Web traffic:

1. In the management console, click **Protect Data > Policies.**

2. Click the **Create Policy...** button. The Create a New Policy window appears.

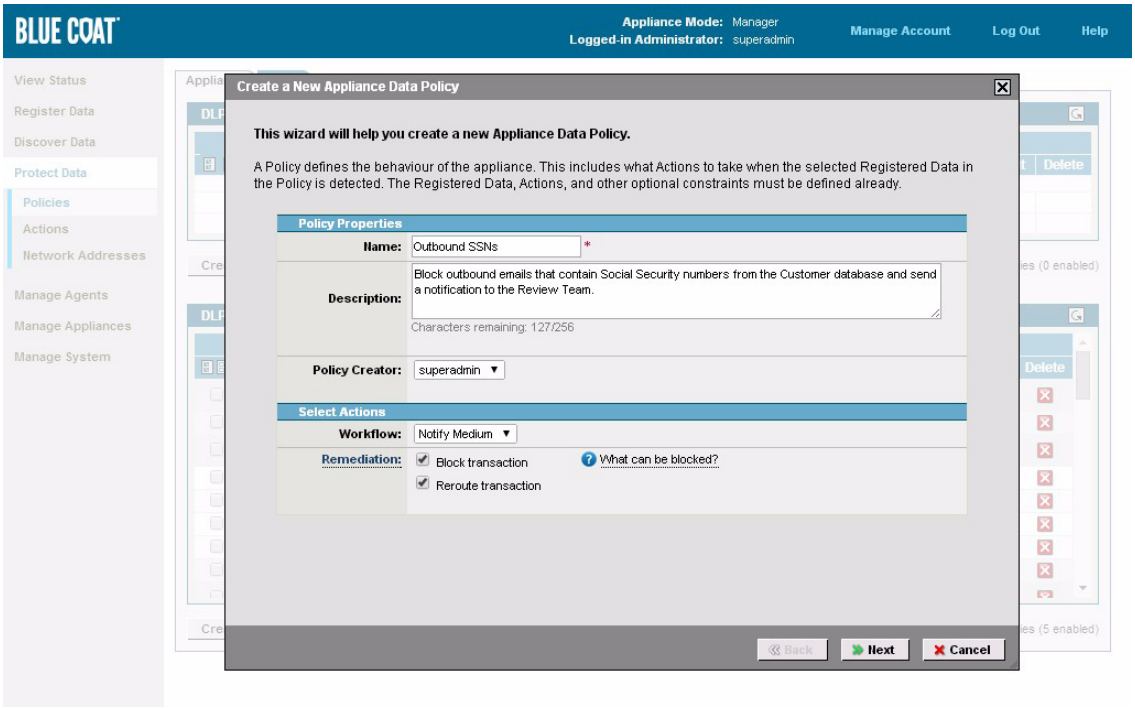


Figure 6.3: Create a TCP policy to detect registered data in outbound traffic.

3. Fill out the Policy Properties as shown below, and then click **Next**.

- **Name**—type name will identify the policy in the Policy List.
- **Description**— type a description; it will appear when you mouse over the policy name and typically includes a summary of the policy, for example, who requested it and what it checks
- **Policy Creator**—this option is recorded with incidents and can also be used to direct notifications.
- **Action**—both pre-defined and custom actions appear in the list. For this example, choose the Action you created in "Configure Email Notifications" on page 25.
- **Allow/Block**—In most cases, users can be notified via HTTP page.
- **Reroute**—does not apply to ICAP Inspection.

4. Choose which data you want the policy to use for detection, and then click **Next**.

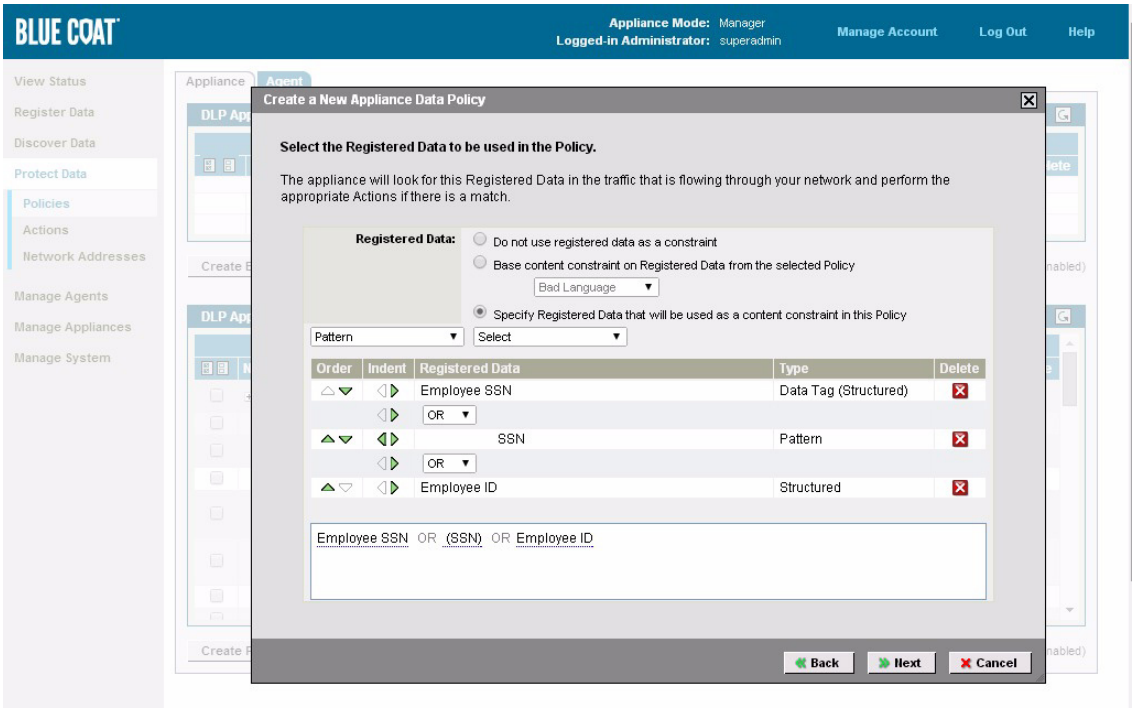


Figure 6.4: Choose the data you registered in "Registering Data" on page 48. You can combine registered data from different sources, including patterns.

- **Do not use registered data as a constraint**—Choose this option if you want to identify files based on one or more properties instead of data (seldom used).
- **Base content constraint on Registered Data from the selected Policy**—Choose this option if you want to inherit the Registered Data portion of an existing policy, and then select from the drop-down list the constraint you want. You can use the policy's constraint as is or modify it by choosing one or more additional elements from Registered Data.
- ***Specify Registered Data that will be used as a content constraint in this Policy**—Choose this option to select the data you registered in the previous chapter.

Note: It is a good idea to include more than one column of Structured Data in a policy and connect them in the policy using the AND operand. Using multiple columns provides context validation through Row Correlation and can greatly increase your incident validity. Only if an identical match is found for data from each column will an incident occur. (The data can be anywhere in the document and in any order—they do not need to be side by side.)

5. Select the source and/or destinations you want the policy to apply to and then click **Next**. All traffic is monitored, but only those transmissions meeting the criteria selected below are analyzed against the policy.

Source/Destination

- **Apply this Policy to all Users**—choose this option to apply the policy to all email transactions; use for the current example.

- **Apply this Policy only to specific Users or Groups**—choose this option to apply the policy to only those users you select from the DLP appliance user list or, if you have it connected, your LDAP directory
- **Network Address Filter**—choose this option to apply the policy to the sender/recipient according to network address, domain, or network group you created in 3.11 "Create a Network Address Group" on page 36.
- Select any additional constraints, explained below, and click **Next**.

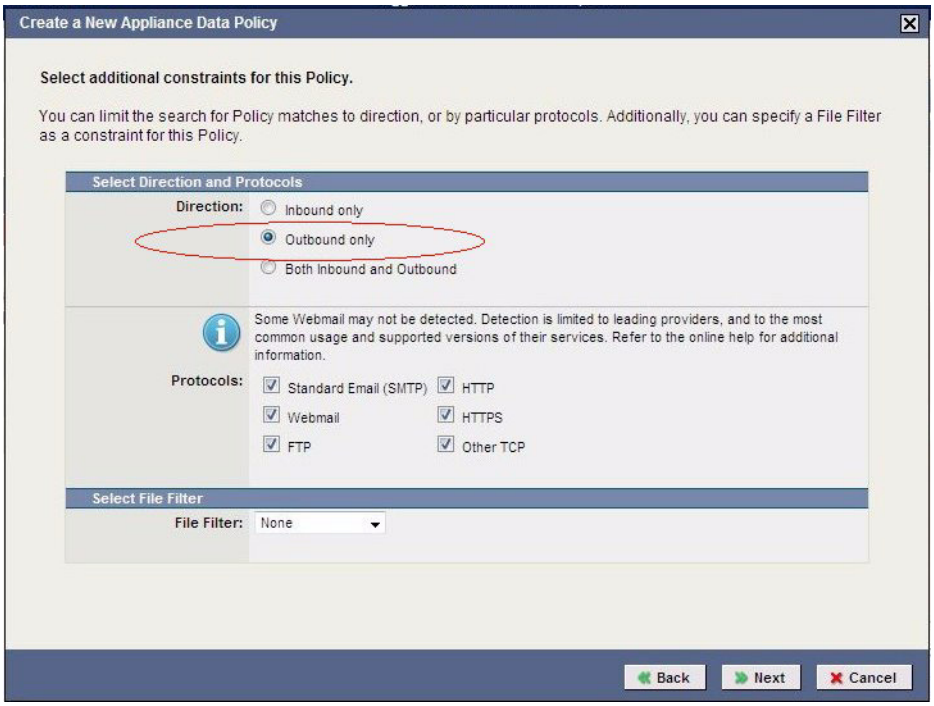


Figure 6.5: Choose the direction of the traffic you want to inspect, as well as the protocol.

Direction: (messages between users within the LAN are not checked)

- **Inbound only**—typically used only for email inspection
- **Outbound only**—apply policy to Web uploads from the LAN (Reverse proxy) or downloads to the Internet (Forward proxy); use for the current example
- **Both Inbound and Outbound**—(not recommended for Web inspection

Protocols:

- **Standard Email (SMTP)**—Email Inspection (do not enable for this policy)
- **HTTP**—ICAP Inspection
- **HTTPS**—ICAP Inspection
- **Webmail**—ICAP Inspection. Includes Google Mail, AOL Mail, Yahoo! Mail, Hotmail, and MSN Live Mail (Full and Light). Webmail that cannot be identified is classified as an HTTP transaction.
- **FTP**—ICAP Inspection
- **Other TCP**—Packet Monitoring

6. You can further narrow eligible data by selecting a **File Filter**. File type determination and is made according to the file metadata. Click **Next**.

7. In the Summary screen that appears, review you choices and then click **Finish** to return to the Policies page. The policy will be enabled and Web traffic monitoring will begin immediately.
   - Remove the **Enable** check mark to stop monitoring Web traffic for the registered data in this policy.
   - Click the **Edit** icon to change any of the scan parameters
8. Click the **Add Exception** icon to create and attach a second policy to reduce false positives caused by dirty data.

More about exception policies:

- Exception policies are used in the case when you want to implement the logic, "perform the action in Policy X when a violation is found, except when Policy Y also applies, in which case perform the action in Policy Y"
- Exception policies are single-use; exceptions can only be attached to one policy
- You can attach multiple exceptions to any given policy
- The order in which exception policies appear on the list is significant; the first exception is evaluated first, etc. and as soon as a match is found any remaining exception are skipped

7 Inspect ICAP Traffic

ICAP Inspection checks Web traffic routed to the appliance from a proxy server and checks it for restricted content. Traffic can be inbound or outbound, and includes Webmail, HTTP, HTTPS, and FTP.

The tasks in this chapter focus on configuring a Blue Coat® ProxySG appliance to route specified network traffic to the DLP appliance for inspection. You should have an environment suitable for the initial deployment of a network-scanning device, i.e., one with access to high-volume network traffic, an LDAP, and an proxy server.

Note: Refer to the Blue Coat documentation such as the *Blue Coat Systems SGOS Administration Guide*. The instructions provided here assume that you have a proxy already deployed on the network, configured, and that it is working properly. In addition, you should have the proxy connected to a directory server and set up to proxy SSL traffic.

This chapter covers the following:

7.1 About ICAP Inspection

ICAP works as a request and response pair, like HTTP. Each ICAP request can carry either an HTTP request or HTTP response. When the DLP appliance and a Blue Coat® ProxySG® appliance are configured to work together, the ProxySG appliance acts as an ICAP client. It can accept both outgoing HTTP requests and incoming HTTP responses and sends one or both to the DLP appliance in the form of ICAP requests. The DLP appliance acts as an ICAP server, accepting the ICAP requests and returning ICAP responses to the ProxySG appliance.

When the HTTP proxy is working as a normal (forward) HTTP proxy, HTTP requests (REQMOD) are always outbound and HTTP responses (RESPMOD) are always inbound.

The Blue Coat ProxySG appliance can also handle HTTPS and FTP, and these protocols are sent in ICAP requests as HTTP requests and responses, so HTTPS and FTP can undergo ICAP blocking as well. If the HTTP proxy is working as a reverse proxy, with the proxy server sitting outside the firewall, then the direction of HTTP Request and HTTP Response is opposite. The DLP appliance has a configuration setting for forward and reverse proxy so it will know whether HTTP Requests and Responses are incoming or outgoing.

ICAP requests that carry HTTP requests are called REQMOD requests; ICAP requests that carry HTTP responses are called RESPMOD requests.

REQMOD Traffic Flow

1. The client PC sends an HTTP Request.
2. The HTTP traffic is intercepted by the HTTP proxy, in this case the Blue Coat ProxySG appliance. The appliance sends an ICAP request for this HTTP request (REQMOD) to the DLP appliance's ICAP port.

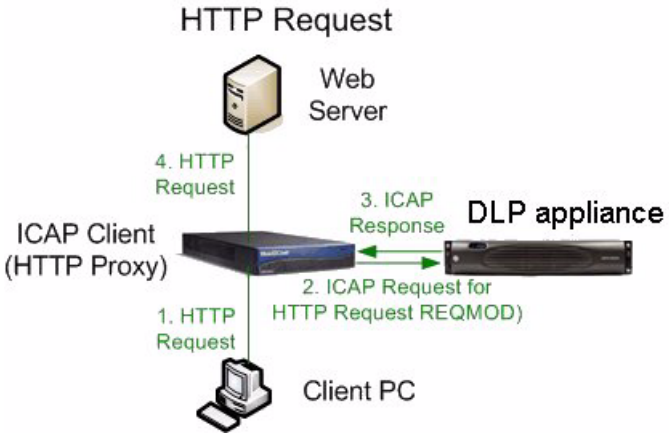


Figure 7.1: The HTTP Request shown here demonstrates an ICAP REQMOD request.

3. The DLP appliance inspects the contents of the HTTP traffic, then sends an ICAP Response to the HTTP proxy to either block or allow the traffic.
4. If the HTTP traffic is allowed, it is sent on to its destination.

RESPMOD Traffic Flow

1. The Web server sends an HTTP Response.
2. The HTTP traffic is intercepted by the ProxySG appliance. The appliance sends an ICAP request (RESPMOD) to the ICAP server (here, the DLP appliance).

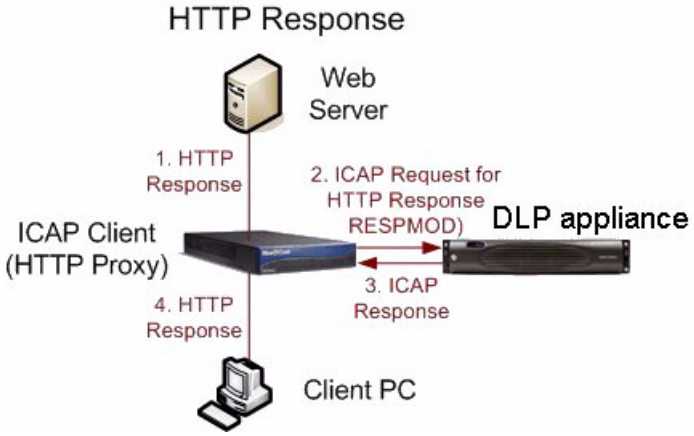


Figure 7.2: The HTTP Response process shown here demonstrates an ICAP RESPMOD command.

3. The DLP appliance inspects the content of the HTTP traffic, then sends an ICAP Response to the ProxySG appliance to either block or allow the traffic.
4. If the HTTP traffic is allowed, the HTTP traffic is forwarded to the client PC.

7.2 Network Inspection Planning

You can route traffic from a Blue Coat ProxySG appliance to the DLP appliance to inspect inbound and/or outbound Web traffic. The two main uses involve outbound Web traffic:

1. **Forward Proxy—**To inspect Web uploads from clients on the LAN to the Internet. This configuration allows you to monitor or block FTP and Web uploads including Webmail clients and posts to Web forms such as are commonly used in social networking sites.
2. **Reverse Proxy—**(not covered in this document) To inspect Web downloads from your Web site to Internet users. This configuration allows you to monitor or prevent sensitive content that may be inadvertently available on the site from being downloaded by unintended users. Content-level inspections on a download-by-download basis is the best way to prevent sensitive content from leaking out of the network regardless of the file in which it is contained or it's location on the site (e.g., customer forums, a knowledge base, or quasi-public FTP server).

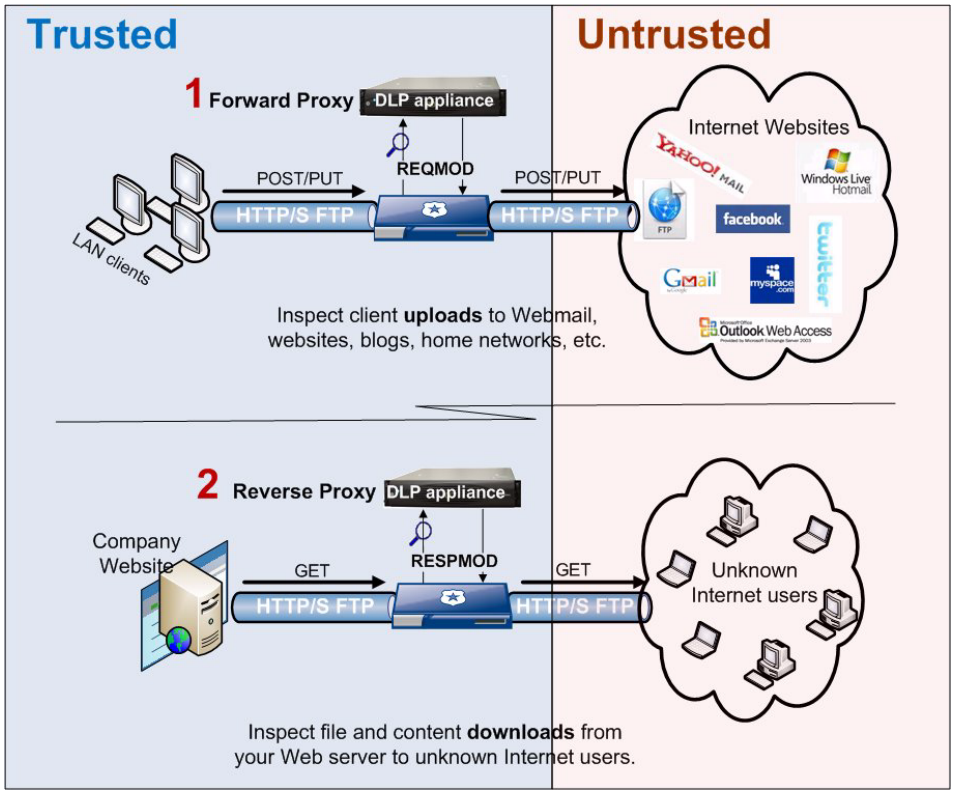


Figure 7.3: The DLP appliance supports scanning both inbound and outbound traffic. Contrary to malware protection, however, inspection typically occurs for outbound traffic (from your clients or Web site) rather than inbound traffic.

Inspecting *inbound* Web traffic for proprietary or other restricted content makes sense if you want to use a content policy to prevent users from accessing certain content that

is available on an intranet server. In this case, DLP appliance policies can be used as a filter to protect against content that has been mistakenly posted to a non-secure site.

7.2.1 Prerequisites

Before configuring either the DLP appliance or the Blue Coat ProxySG appliance, you should be aware of the following:

1. **Forward or Reverse Proxy**

   Will the proxy sit upstream or downstream from the target? In other words, will you inspect inbound (seldom used) or outbound traffic, and if outbound, will that traffic be from your LAN users to the Internet, or will it be from your Web server to Internet users?

2. **Connectivity**

   Ethernet port 4 on the DLP appliance should be connected to the network and have an IP address assigned. In addition, the appliance should be able to access the Blue Coat ProxySG appliance. Confirm the routing before you begin.

3. **Directory Server** (LDAP, Active Directory, or Others)

   Blue Coat Systems recommends that you have both the Blue Coat ProxySG appliance and the DLP appliance configured to access a directory server.

   On the Blue Coat ProxySG appliance, the directory server can provide Authenticated user data as well as the client and server IP addresses that can be used by the DLP appliance. On the DLP appliance, LDAP provides user detail in Incidents, logs, and reports and combines with the Authenticated user data from the Blue Coat ProxySG appliance to provide additional level of granularity in network policies (via Source and Destination user constraints).

4. **ProxySG Management Console Access**

   You will need Administrator credentials to log in to the ProxySG appliance management console and add the DLP appliance as an ICAP server.

5. **ProxySG Policy Configuration**

   If you will inspect HTTPS traffic, you must have an SSL Access Layer on the Blue Coat ProxySG appliance. See the *SGOS Administrator's Guide* for instructions on how to configure SSL Access Layer.

6. **Client Connectivity**

   Confirm that you can connect to the Internet from a client through the Blue Coat ProxySG appliance. This includes checking that the proxy is processing connections, and that the client is configured to use the Blue Coat ProxySG appliance and can access external sites.

7. **Instant Messaging and Steaming Protocols**

   When connected to a Blue Coat ProxySG appliance for outbound Web scanning, the ICAP inspection service scan does not support content detection in IM and streaming protocols. These include CIFS, MAPI, and TCP tunnels.

7.3 Configuring the DLP appliance

Configure the DLP Manager (and any Inspectors) as described below before you modify the ProxySG policy configuration to route traffic to the DLP appliance for inspection.

If the ICAP interface on the DLP appliance is already enabled, you can skip the instructions below.

To check the ICAP status:

- On the DLP Manager Dashboard (**Health Monitor | Interfaces** tab), the status light will be green for eth4 if the port is already configured. If it is red, click the icon to open the Interfaces page.

7.3.1 Assign an IP Address to the DLP Manager ICAP Port

Before you assign an IP address to ICAP port, the DLP appliance should be connected to the network and accessible from the ProxySG appliance.

To configure the ICAP port:

1. In the DLP Manager, click **Manage System > Configuration > Network | Interfaces**.
2. In the list that appears, click the **Edit** icon for "Interface eth4", the ICAP port.
3. Click the **Settings** tab.
4. In the **IP Address/Mask** field, enter the IP address/mask and gateway you will assign to the ICAP port, for example,

   ```
   10.10.13.244/24
   10.10.12.2
   ```

5. In the **Speed/Duplex** field, accept the default value **Auto-negotiate** or choose one of the settings from the drop-down list to match your switch hardware.
6. Click **OK** to save the changes and close the window.

7.3.2 Configure the DLP appliance to Inspect ICAP Traffic

Perform this task to enable the ICAP inspection service on the DLP appliance, according to the traffic direction you want to inspect; the DLP appliance supports both Forward Proxy Server, (REQMOD), and Reverse Proxy Server (RESPMOD). Configure the DLP appliance before making changes on the Blue Coat ProxySG appliance.

To configure ICAP scanning:

1. In the DLP Manager, click **Manage System > Configuration > Inspection Services |ICAP**.

2. Enable **ICAP Server** if it is not already checked.
3. Review the ICAP Settings, and accept the defaults unless your ProxySG appliance uses a different port, or if after some testing you want to fine-tune performance.
4. In the **ICAP Client Topology** field, choose the direction of the traffic you will receive from the ProxySG appliance, as shown in Figure 7.3.
   - Choose **Forward Proxy Server** and set the ProxySG appliance for REQMOD. This option allows you to inspect outbound traffic such as that which is being uploaded from the LAN to the Web.
   - Although it is not documented here, you can choose **Reverse Proxy Server** and set the Blue Coat ProxySG appliance for RESPMOD in order to inspect data as it is downloaded from a given Web or FTP server, for example to protect downloads from the corporate Web to unknown Internet users.
5. Click **Apply** when finished to save your changes.

7.4 Inspecting Web Uploads (Forward Proxy/REQMOD)

In this section you will find instructions for making the basic configuration changes necessary for a Blue Coat ProxySG appliance to route traffic to the DLP appliance for inspection. For complete information, including troubleshooting and advanced configuration changes, refer to the *Blue Coat Systems SGOS Administration Guide*.

To configure the ProxySG appliance to route traffic (and user information) to the DLP appliance, you need to create an ICAP service for the DLP appliance on the ProxySG appliance. Next, you will add that service to the appropriate ProxySG policy and then check that the proxy is forwarding traffic to the appliance. Instructions for each are provided below.

Use Directory Server

Connecting the ProxySG appliance to a directory server and the DLP appliance to an LDAP server is recommended. By default, the proxy will pass to the appliance the IP addresses of the requesting client(s) and target server. If the proxy is connected to an LDAP server, it will additionally pass Authenticated user data associate with the account. The appliance uses this data in Policy Constraints, and will also do a look up to retrieve additional details for inclusion in Incident Details and Reports.

7.4.1 Create a REQMOD Service

The ProxySG appliance configuration (REQMOD/RESPMOD) determines which traffic (inbound and/or outbound) will be routed from the proxy to the DLP appliance.

Configure a new REQMOD service from the ProxySG management console if you are going to inspect Web uploads from the LAN to the Internet and the proxy is a Forward proxy (i.e., downstream from the LAN clients). There is no need to configure a

RESPMOD service on the ProxySG appliance if you will only be inspecting outbound client traffic.

Note: Setting up a *RESPMOD* service on a *Forward* proxy tells the ProxySG appliance to forward all inbound traffic (i.e., traffic from the Internet to the LAN) through the DLP appliance. Even if you configure the DLP appliance to only *inspect* outbound traffic (as shown in Figure 7.4, below), the appliance will still, unnecessarily, *receive* all Web traffic.

Blue Coat Systems recommends that you only pass to the DLP appliance that traffic which you want to inspect. For REQMOD, this is typically Web uploads from LAN clients to the Internet.

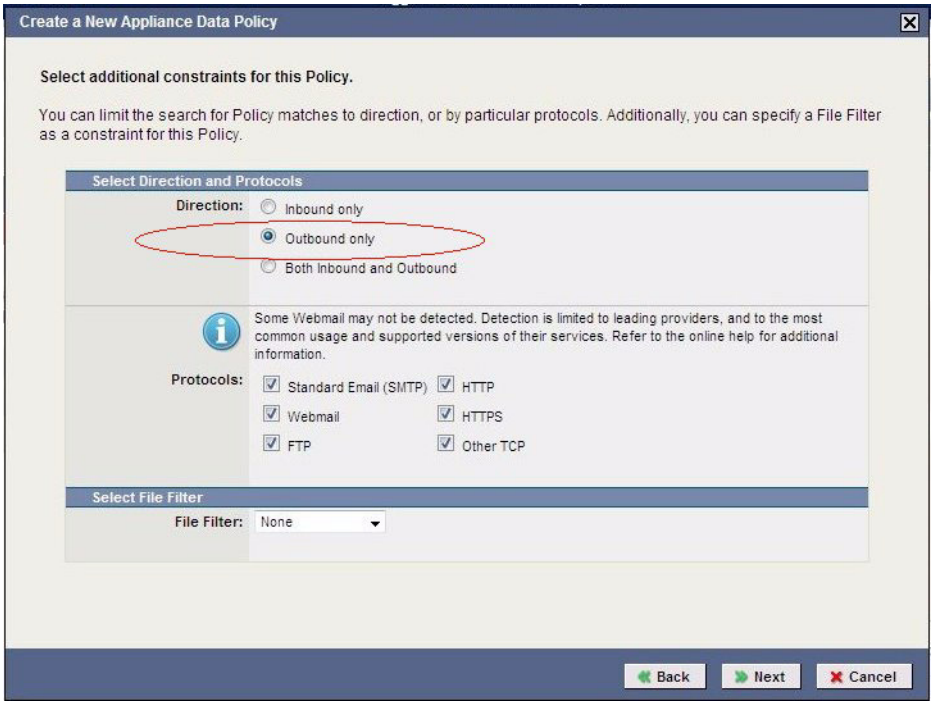


Figure 7.4: When creating an ICAP inspection policy on the DLP appliance, the Direction setting, as shown above, will determine whether the appliance inspects inbound and/or outbound traffic.

To create an ICAP service for the DLP appliance:

1. Open the ProxySG appliance management console, and then in the menu that appears, click **External Services > ICAP**. The ICAP Services screen appears, as shown below.

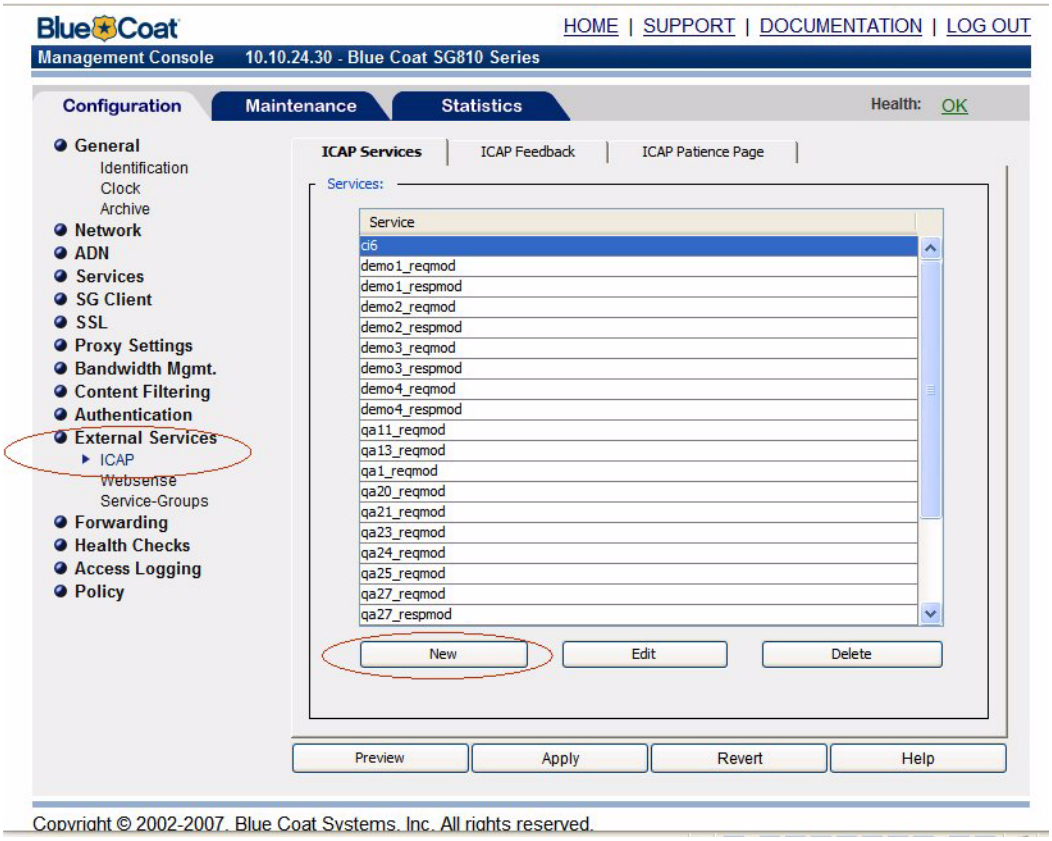


Figure 7.5: Create a service for the DLP appliance ICAP server.

2. Click the **New** button and then type a name for the service, for example, `DLP_REQMOD`
3. Click **OK** and then select the name you just created from the list.

4. Click **Edit**. The Edit ICAP Service window opens, as shown below.

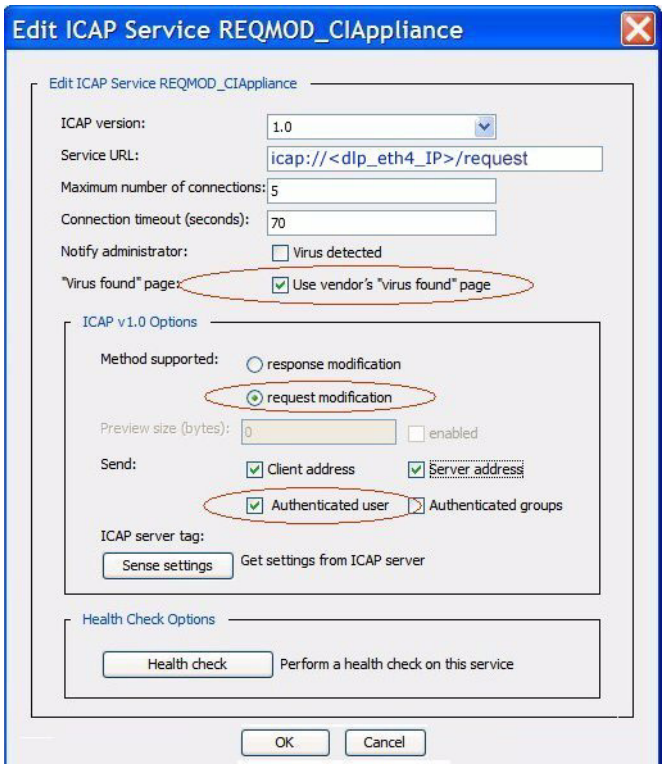


Figure 7.6: Create a REQMOD service for the DLP appliance to inspect Web uploads from clients to the Internet.

5. Accept the defaults, except for the following modifications:
   - For **Service URL**, type the IP address that is assigned to eth4 on the DLP appliance. Use the icap prefix and specify request:

     `icap://<dlp_eth4_IP>/request`

   - Enable **Use Vendor's "virus found" page** to display notification from the DLP appliance whenever registered data is detected in users' Web traffic.
6. Choose **request modification, enable Client address**, **Server address**, and **Authenticated user**.
7. Next, click the **Sense Settings** button to prompt the ProxySG appliance to contact the DLP Manager for an ICAP service tag. You can also click the **Health Check** button to confirm the ProxySG-DLP appliance connectivity (the window will close after each operation is complete).
8. Back on the ICAP Service tab, click the **Apply** button to save any changes to complete the procedure.

7.4.2 Add the REQMOD Service to a ProxySG Policy

The service you just created must be added to a new or existing ProxySG policy. The procedure below explains how to do this using Blue Coat Visual Policy Manager, although it is also possible to accomplish the same thing by editing the policy files. Note that saving changes created using either method can overwrite any changes made using the other. Refer to the *Blue Coat Systems ProxySG Appliance Visual Policy Manager Reference Guide* if you need anything more than a reminder (such as provided below) to understand these configuration changes.

The procedure below applies to inspecting Web uploads, i.e., traffic from the LAN to the Internet. It explains how to add a rule with the ICAP service you just created to the Web Access Layer of a ProxySG policy. The rule itself will identify which clients and protocol(s) you want to inspect, as well as the DLP appliances) the ProxySG will direct traffic to.

To add the REQMOD service:

1. In the ProxySG management console, click **Policy > Visual Policy Manager** and then click the **Launch** button. The window opens as shown Figure 7.7.
2. In the Visual Policy Manager menu, click **Policy > Add Web Access Layer...** and give the new layer a name when prompted. Alternatively, you can click the **Add Rule** button to add a rule to an existing layer.

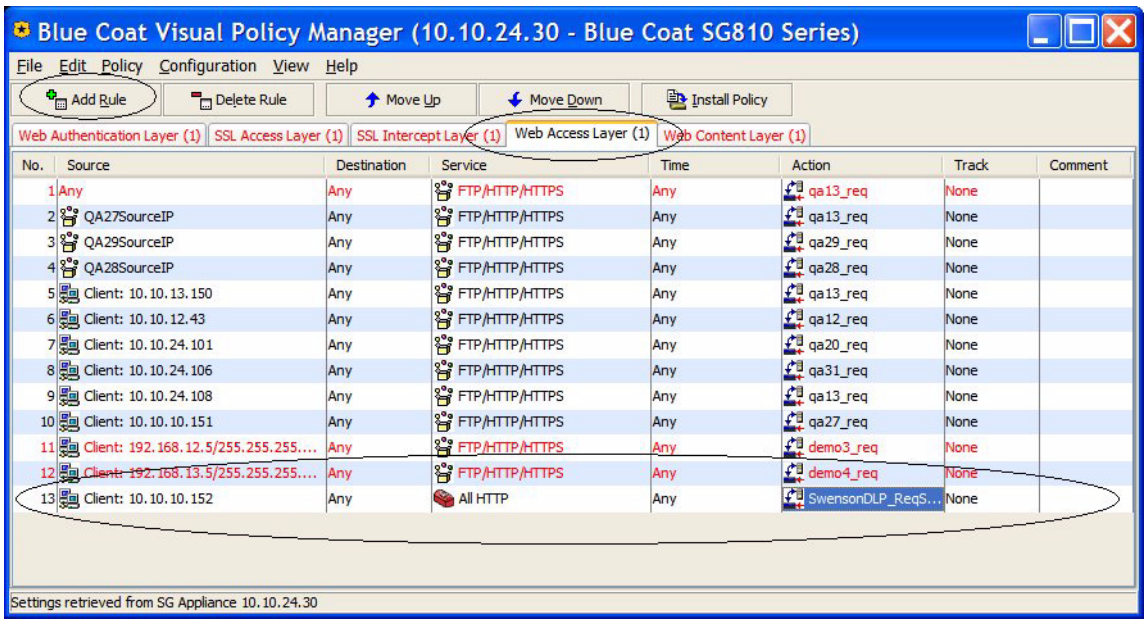


Figure 7.7: Add a rule for ICAP inspection to the Visual Policy Manager.

3. In the **Source** column, right click the rule you want to modify and then in the pop-up menu that appears, click **Set...**.

4. Select the **Source Objects** that you want the policy to apply to. Typically, for an initial set up, that will be the Client IP Address of the desktop on which you will run the initial verification. Of course, you can later change the Source to **Any** or whatever other Object group you want inspection to apply to.

5. In the **Services** column, right-click the rule you are modifying and then in the pop-up menu that appears, click **Set...** and then select the service object you want include in this rule.

   If no HTTP services are already defined,

   a. In the pop-up menu, click **Set...** and then the **New...** button as shown in Figure 7.9.

   b. Choose **Protocol Methods...** from the list that appears.

   c. Give the Object a name, such as HTTP/HTTPS or All HTTP.

   d. For the **Protocol** drop-down, choose HTTP/HTTPS.

   e. Select **Common Methods**, and then the following request methods:

      - PUT, POST

   f. Click **OK**, and then **OK** again to add the service to the Visual Policy Manager.

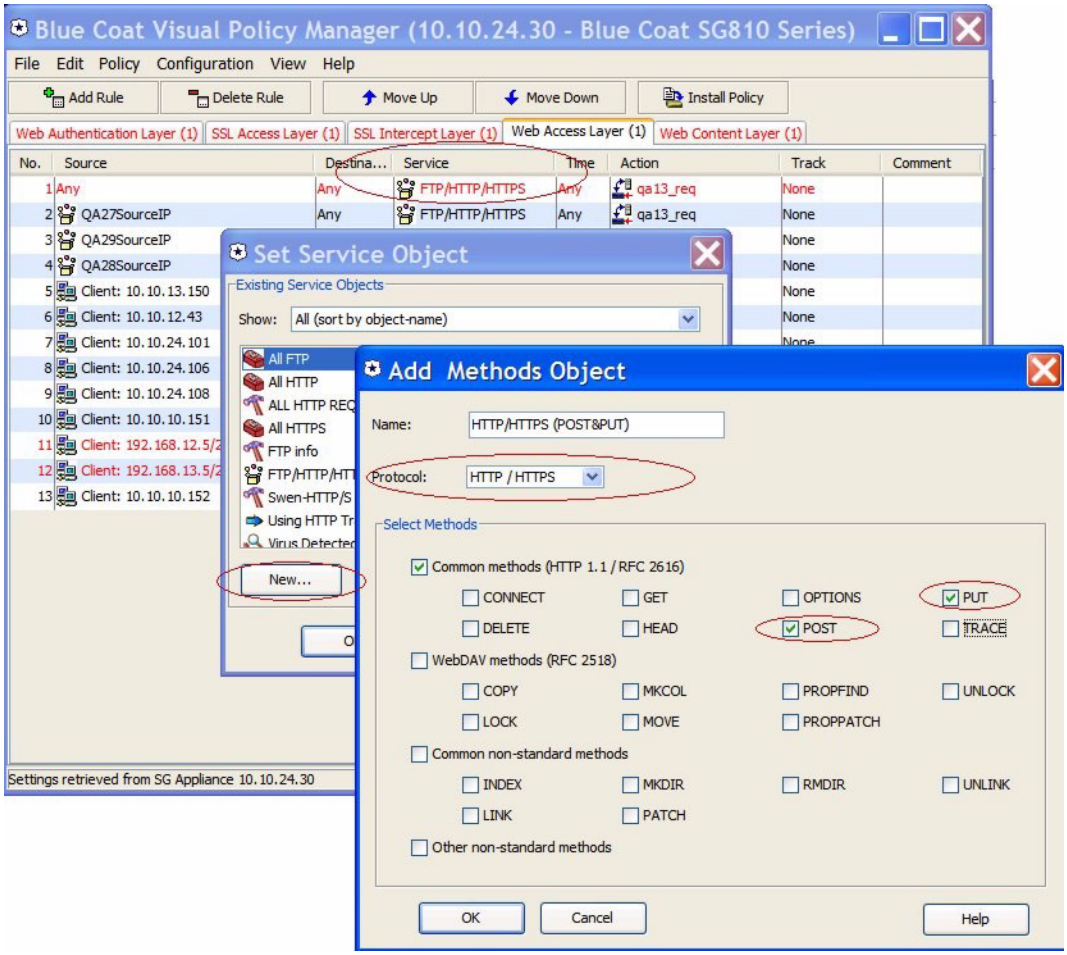


Figure 7.8: Identify the request methods you want to inspect. For outbound inspection, only PUT and POST are likely to contain restricted data.

- To inspect FTP uploads, repeat step 6, this time creating a Method Object for FTP traffic. Create one rule (Figure 7.7) for HTTP and another for FTP, or create a Combined Service Object (repeat step 6a once the each object has been defined) to represent both protocols in a single rule.

6. In the Time column, keep the default, **Any**.
7. In the **Action** column, right-click the rule you are modifying and then in the pop-up menu that appears, click **Set...**.
8. In the Set Action Object window that appears, click the **New...** button and then **Set ICAP Request Service** from the pop-up menu as shown in Figure 7.9.

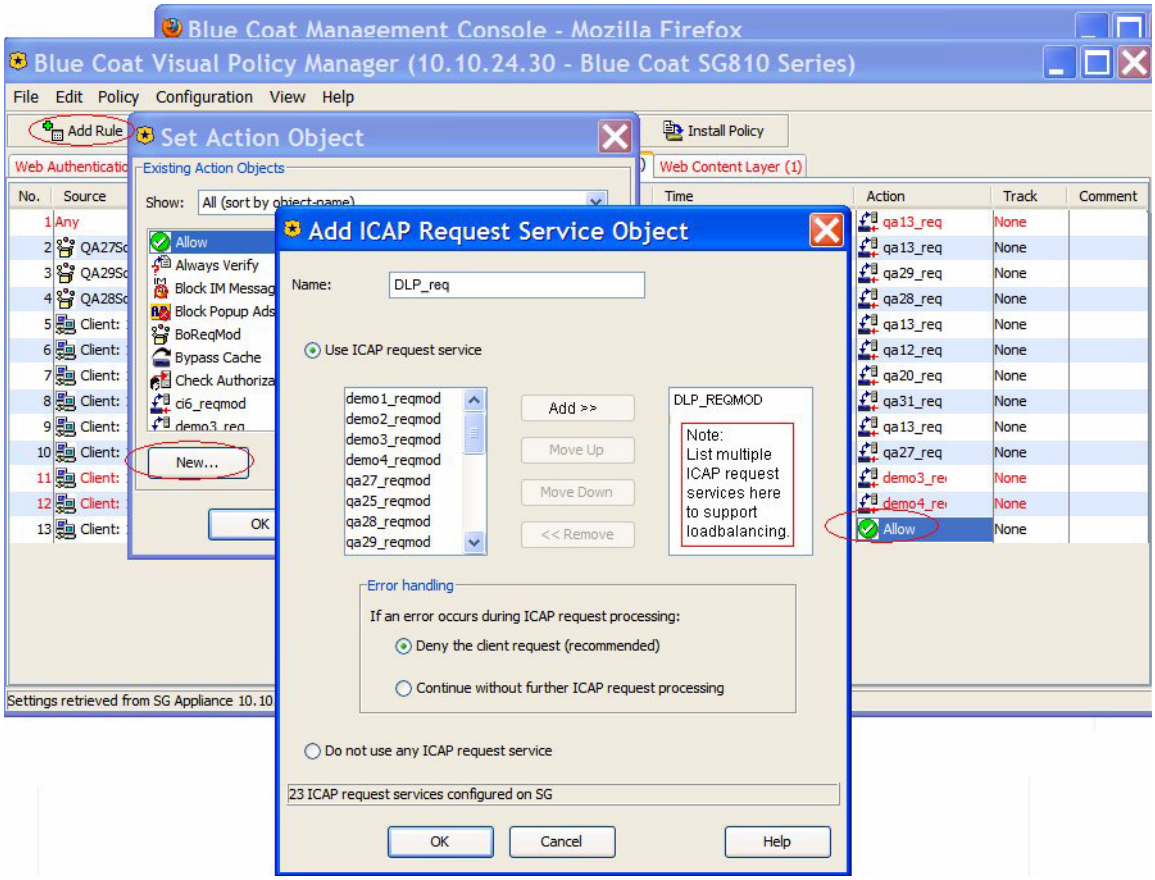


Figure 7.9: Add one Request Service Object for each DLP appliance that you want the rule in your Web content policy to apply to.

9. Give the object a name that will identify it in the Action column, and then choose from the list of available ICAP request services the one you just created in "Create a REQMOD Service" on page 98.

   Note: Add one request service for each DLP appliance that you want the proxy to route traffic to for inspection. For example, if you have deployed multiple appliances to accommodate high traffic volumes, redundancy, or load balancing, add the ICAP service for each appliance here.

10. Click **OK** when finished to close the window(s).
11. Compile and review the policy by clicking **View > Generated CLI...**, otherwise click the **Install Policy** button to enable it on the ProxySG.

12. Close the Visual Policy Manager and log out of the ProxySG management console.

7.5 Testing Upload Inspection

The first thing to do after setting both the DLP appliance and ProxySG appliance is to make sure that the ProxySG is passing traffic correctly, and that the appliance is receiving it correctly.

To confirm that the DLP appliance is receiving ICAP traffic:

1. In the DLP Manager, click **View Status > Dashboard.**
2. In the **Health Monitor** windowpane, click the **Inspection Services** tab and/or Interfaces. The ICAP status icon should be green. If it is red (service is connected but not receiving traffic) or gray (service is disabled), check the associated message and begin troubleshooting.
3. If the icon is green, click **Manage System > Configuration > Inspection Services | ICAP | Statistics** to view the Request and Response statistics.
   - Additionally, you can click **Manage System > Configuration > Network | Interfaces**.
4. In the window that appears, click the **Edit** icon for the ICAP port interface (Interface eth4) and then the **Statistics** tab.

7.5.1 Point Client Web Browsers to the ProxySG Appliance

If your ProxySG appliance is not deployed for transparency, (i.e., clients must specify the proxy location in their Web browser to connect to the Internet) you may need to update that setting in all clients before inspection will occur. A reminder is shown in Figure 7.10.

Note that for testing, you will need to point the computer(s) you specified in the initial ProxySG policy (shown in Figure 7.7) to the proxy. Note too, that the localhost is not routed through the proxy (bypassed).

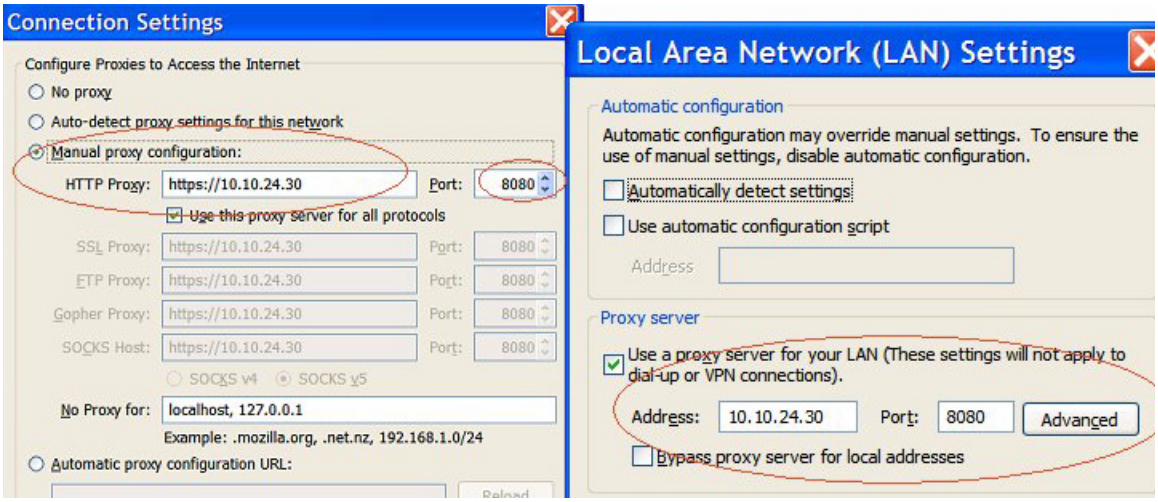


Figure 7.10: Example browser settings for connecting to the Internet. Depending on the topology, your clients may need to point to the ProxySG appliance to access the Internet and engage Web Inspection.

7.5.2 Upload Registered Content to the Web

You can confirm your ICAP inspection setup by using a Web browser to upload registered content to an Internet site. Run this quick test after you have set up both the DLP appliance and ProxySG appliance. For the sake of expediency, the procedure below uses existing registered data and very general policy settings. See Chapter 6, "Creating Network Inspection Policies" on page 86 for information on creating a more realistic policy.

To test uploads from the LAN to the Internet:

Note that the DLP appliance will only inspect traffic that the ProxySG appliance sends it (as is configured on the proxy).

1. In the DLP Manager, click **Protect Data > Policies**. The DLP appliance Data Policies window opens.
2. Click the **Create Policy...** button. The Create a New Policy... window opens.
   - For **Name:** type something like *Inspect Uploads*
   - For **Action:** Choose **Notify High**
   - Enable **Block transaction**
3. Click **Next**, and in the window that opens, click **Specify Registered Data that will be used as a content constraint in this Policy**. Make the choices shown below and then click the green + icon to include this registered data in the policy.
   - Choose **Structure Data** and then **HCPCS Level II** and then **hcpcs_code**.

4. Click **Next** and choose the following:

   Source Users (for a Forward proxy, as in this case, the source is your LAN clients).

   - Choose **Apply this Policy to all Source Users** to inspect all client uploads to the Internet. Otherwise, choose **Apply this Policy only to specific Users or Groups** to inspect the Web uploads of certain clients.

   Destination Users

   Note: If you only want to inspect uploads from LAN clients to a subset of Web sites, configure the ProxySG to select the traffic it passes to the DLP appliance. In this way, the DLP appliance will process all the ICAP traffic it receives, but it will only receive relevant traffic.

   - Choose **Apply this Policy to all Destination Users**, which in this case applies to all Internet clients.
   - **Network Address Filter**—Choose *None* to have the DLP appliance inspect all outbound traffic (Web uploads from LAN clients).

5. Click **Next** and in the window that opens (shown in Figure 7.4) choose the following:

   Direction

   - Outbound only

   Protocol

   - Webmail
   - HTTP
   - HTTPS

   File Filter

   - None

6. Click **Next** and then **Finish** when the Summary window opens.
7. Open a Web browser that points to the ProxySG appliance (as shown in Figure 7.10).
8. In the Web browser address bar, type or copy a URL for a Web site where you can paste content into a form. The URL for the Wikipedia public sandbox (which is intended for testing and frequently cleaned), is provided below. (Note that this URL is subject to change, so you may need to browse for the page.)

   ```
   http://en.wikipedia.org/wiki/Wikipedia:Sandbox
   ```

   Do not use a form such as the search field on the Google web site, since that content is not inspected. Nor should you use an intranet site since these connections may not go through the Blue Coat ProxySG appliance.

9. On the Wikipedia page, click the **Edit** tab and then copy and paste the following numbers:

   ```
   S2405001003 S2409001003 S2409002004 S2411001003 S2900001003
   S2900002004 S3000001003 S3005001003 S3600001003 S3601001003
   ```

10. On the Wikipedia page, click **Save Page**. If your ICAP setup on both the DLP appliance and the Proxy SG is correct, the Save action will be prevented. The

default DLP appliance blocking message will appear, as shown in Figure 7.11, below.

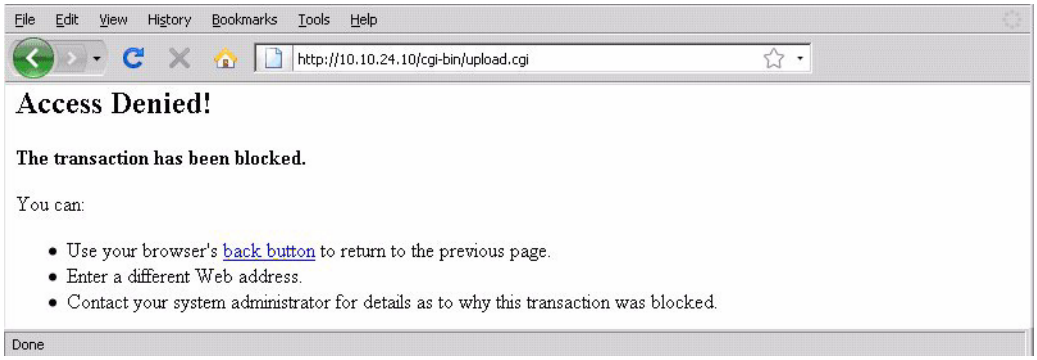


Figure 7.11: You can use the default, shown here, or create your own notification messages by creating or modifying **Actions**.

7.6 Inspecting Web Downloads (Reverse Proxy/RESPMOD)

As with setting up inspection for Web uploads, you will need to configure the Blue Coat ProxySG appliance to route traffic to the DLP appliance, and create an ICAP service for the DLP appliance on the Blue Coat ProxySG appliance. Next, you will add that service to the appropriate ProxySG policy and then check that the proxy is forwarding traffic to the appliance. Instructions for each are provided below.

7.6.1 Create a RESPMOD Service

The ProxySG policy configuration (REQMOD/RESPMOD) determines which traffic (inbound and/or outbound) will be routed from the proxy to the DLP appliance.

Configure a new RESPMOD service from the ProxySG Management Console if you are going to inspect Web download from a corporate Web server to the Internet and the proxy is a Reverse proxy (i.e., upstream from the Internet clients). There is no need to configure a RESPMOD service on the Blue Coat ProxySG appliance if you will only be inspecting LAN clients' outbound traffic.

Note: Setting up a *REQMOD* service on a *Reverse* proxy tells the proxy to forward all inbound traffic (i.e., requests from the Internet to the Web server) through the DLP appliance. Even if you configure the DLP appliance to *inspect* outbound traffic only (as shown in Figure 7.12, below), the appliance will still, unnecessarily, *receive* all requests.

Blue Coat Systems recommends that you only pass to the DLP appliance that traffic which you want to inspect. For RESPMOD and a Reverse proxy, this is typically Web downloads to the Internet from an internal Web server that you want to monitor.

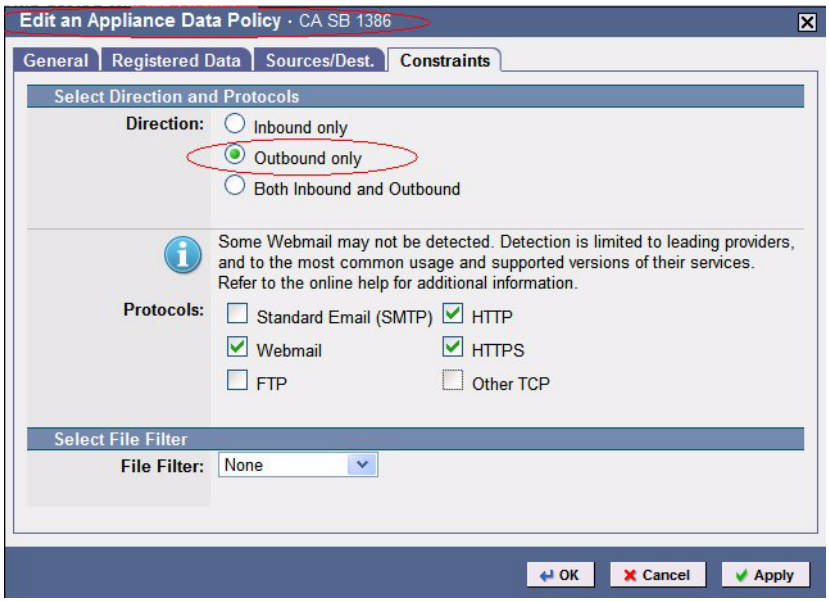


Figure 7.12: The ICAP policy configuration on the DLP appliance determines whether inbound and/or outbound traffic is inspected.

To create an ICAP service for the DLP appliance:

1. Open the ProxySG Management Console, and then in the menu that appears, click **External Services > ICAP**. The ICAP Services screen appears, as shown below.

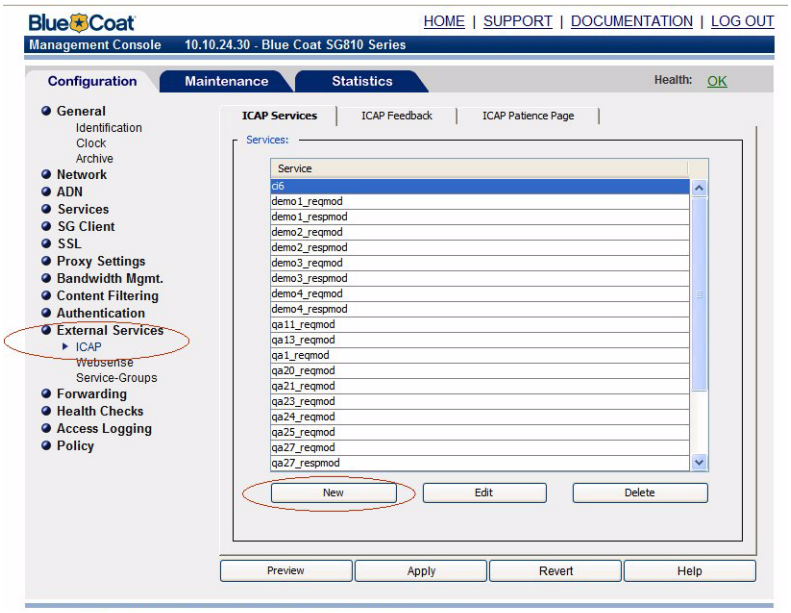


Figure 7.13: Create a service for the DLP appliance ICAP server.

2. Click the **New** button and then, type a name for the service, for example, `DLP_RESPMOD`
3. Click **OK** and then select the name you just created from the list.
4. Click **Edit**. The Edit ICAP Service window opens, as shown below.

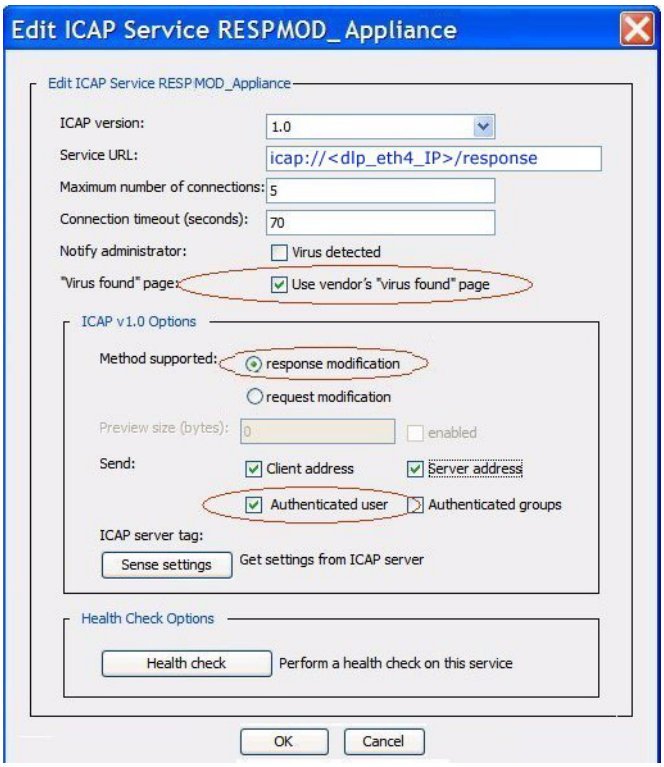


Figure 7.14: Create a RESPMOD service for the DLP appliance to inspect Web downloads from an internal Web server to the Internet.

5. Accept the defaults, except for the following modifications:
   - For **Service URL**, type the IP address that is assigned to eth4 on the DLP appliance. Use the icap prefix and either specify response:
     `icap://<dlp_eth4_IP>/response`
   - Enable **Use Vendor's "virus found" page** to display notification from the DLP appliance whenever registered data is detected in users' Web traffic.
6. Choose **response modification**, enable **Client address**, **Server address**, and **Authenticated user**.
7. Next, click the **Sense Settings** button to prompt the Blue Coat ProxySG appliance to contact the DLP Manager for an ICAP service tag. You can also click the **Health Check** button to confirm the proxy-appliance connectivity (the window will close after each operation is complete).
8. Back on the ICAP Service tab, click the **Apply** button to save any changes. to complete the procedure.

7.6.2 Add the RESPMOD Service to a ProxySG Policy

The service you just created must be added to a new or existing ProxySG policy. The procedure below explains how to do this using Blue Coat Visual Policy Manager, although it is also possible to accomplish the same thing by editing the policy files. Saving changes created using either method can overwrite any changes made using the other.

Note: To inspect SSL (HTTPS) traffic, an SSL Access Layer must already exist in the policy manager. Reference your Blue Coat documentation for information on setting up SSL.

The procedure below applies to inspecting ordinary Web downloads, i.e., non-encrypted traffic from an internal Web server to the Internet. In it, you will create a rule for the ICAP service you just created and add it to the Web Content Layer of the policy. The rule identifies the Web server(s) or sites that you want to monitor. It also identifies the DLP appliance(s) to which the Blue Coat ProxySG appliance will route relevant traffic.

To add the RESPMOD service:

1. In the ProxySG Management Console, click **Policy > Visual Policy Manager** and then click the **Launch** button. The window opens as shown Figure 7.15.
2. In the Visual Policy Manager menu, click **Policy > Add Web Content Layer...** and give the new layer a name when prompted. Alternatively, you can click the **Add Rule** button to add a rule to an existing layer.

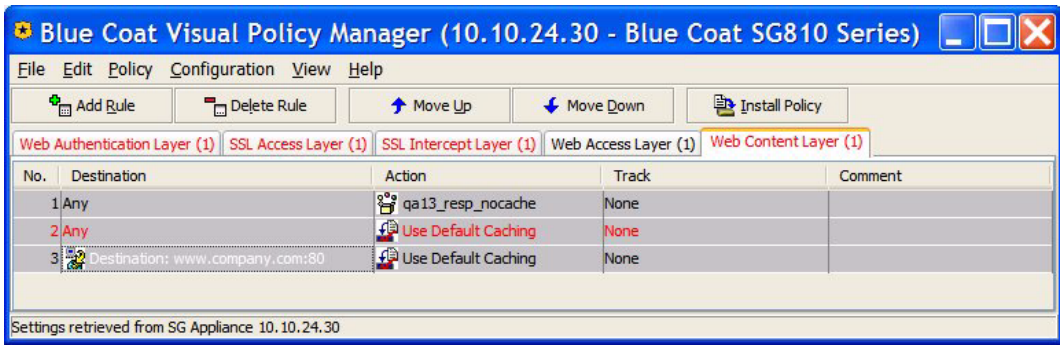


Figure 7.15: Add a rule for ICAP inspection to the Visual Policy Manager.

3. In the **Destination** column, right click the rule you want to modify and then in the pop-up menu that appears, click **Set...**.
4. Select the **Destination Objects** that you want the policy to apply to. For outbound Web downloads that will pass through a reverse proxy, the destination object is usually the IP Address or URL of the Web server that you want to secure. Whenever the proxy receives a request for this IP address or URL, it will pass the content retrieved from the URL to the DLP appliance for inspection; content that matches a policy can be blocked, encrypted, or the event recorded.

   If the Destination you want to protect is not already defined,

a. In the pop-up menu, click **Set...** and then the **New...** button. Choose either:
   - **Destination IP Address/Subnet...** to specify the IP address of the target Web server. The policy defined in this rule only applies to this address only or addresses within this subnet.
   - **Request URL...** to specify the URL of the target Web site.

b. Click **OK**, and then **OK** again to add the Destination to the Visual Policy Manager.

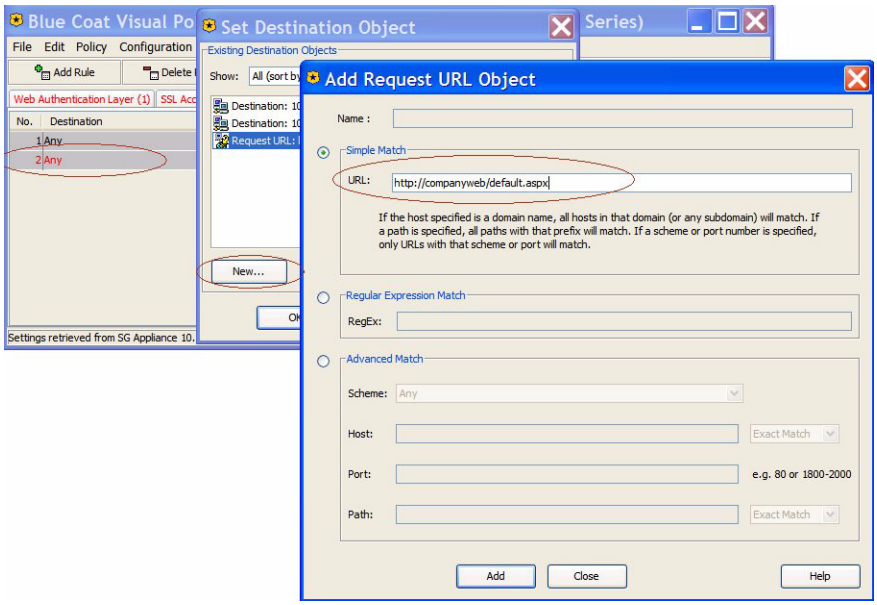


Figure 7.16: Create or choose a Destination object for the Web site/server you want to secure.

5. In the **Action** column, right-click the rule you are modifying and then in the pop-up menu that appears, click **Set...**.

6. In the Set Action Object window that appears, click the **New...** button and then **Set ICAP Response Service** from the pop-up menu.

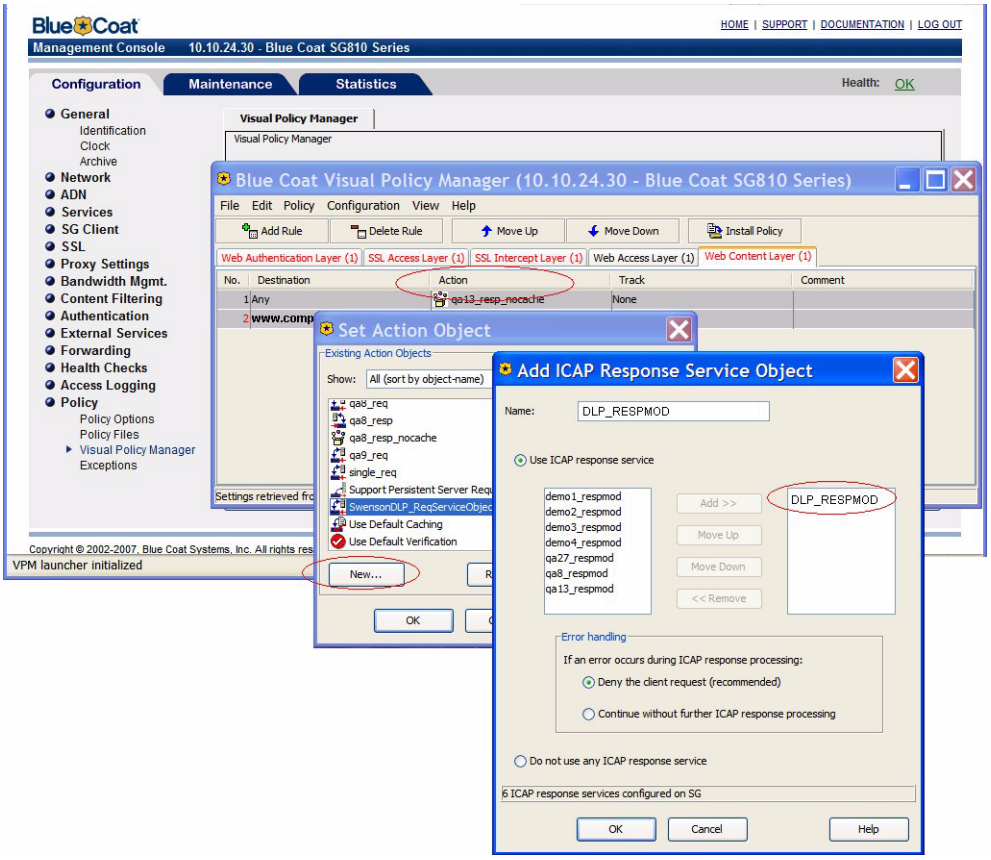


Figure 7.17: Add or Create an ICAP Response Service Object to identify the DLP appliance that will inspect outbound Web downloads.

7. Give the object a name that will identify it in the Action column, and then choose from the list of available ICAP request services the one you just created in "Create a RESPMOD Service" on page 108.
8. Click **OK** and **OK** to close the windows.
9. Compile and review the policy by clicking **View > Generated CLI...**, otherwise click the **Install Policy** button to enable it on the proxy.
10. Close the Visual Policy Manager and log out of the ProxySG Management Console.

7.7 Testing Download Inspection

If you have not already confirmed that the Blue Coat ProxySG appliance is passing traffic to the DLP appliance and it is being properly received, do so now.

To confirm that the DLP appliance is receiving ICAP traffic:

1. In the DLP Manager, click **View Status > Dashboard.**
2. In the **Health Monitor** windowpane, click the **Inspection Services** tab and/or Interfaces. The ICAP status icon should be green. If it is red (service is connected but not receiving traffic) or gray (service is disabled), check the associated message and begin troubleshooting.
3. If the icon is green, click **Manage Appliances > Configure System > Inspection Services | ICAP | Statistics** to view the Request and Response statistics.
   - Additionally, you can click **Manage Appliances > Configure System > Network | Interfaces**.
4. In the window that appears, click the **Edit** icon for the ICAP port interface (Interface eth4) and then the **Statistics** tab.

7.7.1 Point your Web Browser to the ProxySG Appliance

Because this policy is intended to inspect outbound traffic to the Internet, you may need to configure the browser you will use for testing to point to the proxy. Two such browsers screens are shown in Figure 7.18.

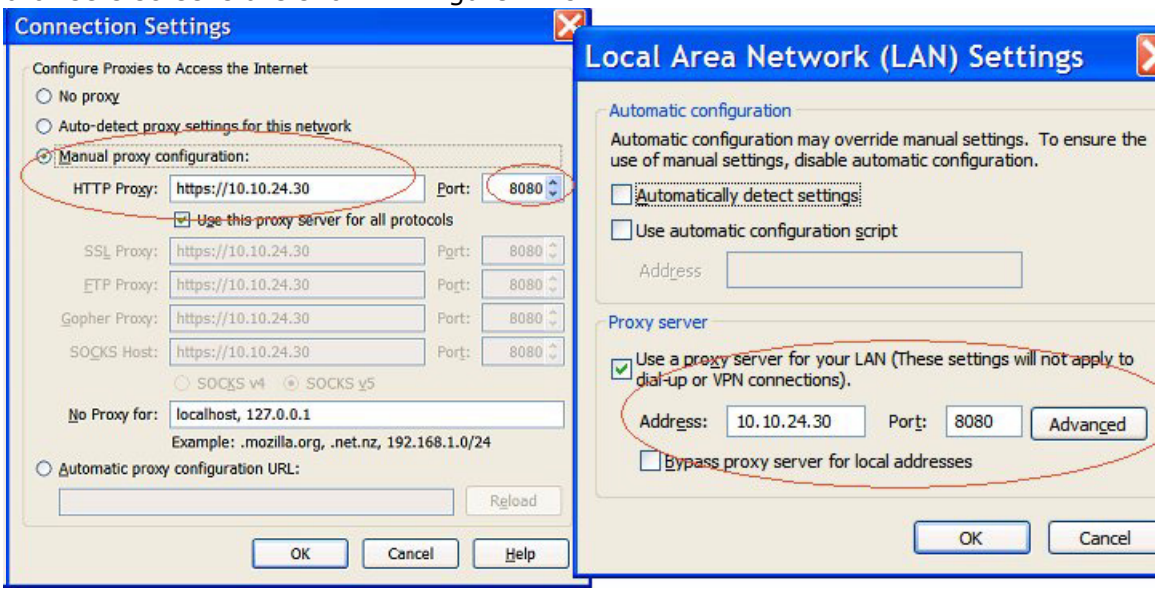


Figure 7.18: Example browser settings for connecting to the Internet.

7.7.2 Download Registered Content

You can confirm your ICAP inspection setup by downloading registered content from the protected Web server to a Web browser that is connected to the Blue Coat ProxySG appliance.

Run this quick test after you have set up both the DLP appliance and Blue Coat ProxySG appliance.

For the sake of expediency, the procedure below uses the default, pre-existing email pattern file and very general policy settings. As such, you will need to find content on the target Web site that does, in fact, contain one or more email addresses.

See Chapter 6, "Creating Network Inspection Policies" on page 86 for information on creating a more realistic policy.

To test downloads from a protected Web server:

For ICAP inspection the DLP appliance will only inspect traffic that the proxy sends it (as is configured on the proxy).

1. In the DLP Manager, click **Protect Data > Policies**. The DLP appliance Data Policies window opens.
2. Click the **Create Policy...** button. The Create a New Policy... window opens.
   - For **Name:** type something like *ICAP Test*
   - For **Action:** Choose **Notify High**
   - Enable **Block transaction**

   Note: The ICAP Inspection service must be enabled for this option to be available—click **View Status > Dashboard** and under **Health Monitor**, and then click the **Interfaces** tab to check that the ICAP status light is green. If it is not, click the green icon to configure the ICAP settings.
3. Click **Next**, and in the window that opens, click **Specify Registered Data that will be used as a content constraint in this Policy**. Make the choices shown below and then click the green + icon to include this pattern in the policy:
   - Pattern
   - Email Pattern
4. Click **Next** and choose the following:

   Source Users

   - Choose **Apply this Policy to all Source Users**. In addition,
   - Specify a **Network Address Filter** that identifies the Web server you want to secure.

   Destination Users

   Note: If you only want to inspect downloads to a certain Internet clients, use the ProxySG to select the traffic it passes to the DLP appliance. In this way, the DLP appliance will process all the ICAP traffic it receives, but it will only receive relevant traffic.

   - Choose **Apply this Policy to all Destination Users**, which in this case applies to all Internet clients.
   - **Network Address Filter**—Choose *None* to have the DLP appliance inspect all outbound traffic from the protected Web server.

5. Click **Next** and in the window that opens (as shown in Figure 7.4) choose the following:

   Direction

   - Outbound only

   Protocol

   - HTTP

   File Filter

   - None

6. Click **Next** and then **Finish** when the Summary window opens.
7. Open a Web browser that points to the ProxySG and enter the URL of the protected Web site.
8. Browse the Web site looking for a page that contains an email address, or a document that you know contains an email address. If your ICAP setup on both the DLP appliance and the ProxySG is correct, the Save action will be prevented. The default DLP appliance blocking message will appear, as shown below.

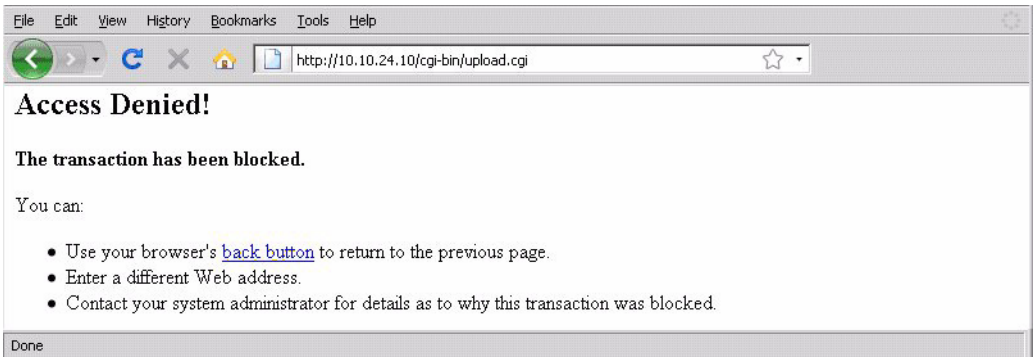


Figure 7.19: You can use the default, shown here, or create your own notification messages by creating or modifying **Actions**.

7.8 Summary of Related Configuration Settings

Inspect Uploads from the LAN

1. The Blue Coat ProxySG appliance is a forward proxy.
2. The proxy sends only REQMOD traffic to the DLP appliance.
   - Source is Any (LAN clients)
3. The DLP appliance is configured to inspect only Outbound traffic.
4. The DLP inspection policy specifies LAN clients for the Source User.

Inspect Downloads to the Web

1. The Blue Coat ProxySG appliance is a forward proxy.

2. The proxy sends only RESPMOD traffic to the DLP appliance.
    - Source is the protected Web server
3. The DLP appliance is configured to inspect only Outbound traffic.

The DLP inspection policy specifies All clients for the Source User.

8 Install and Manage CI Agents

CI Agents can report to both Managers and Inspectors. This three-tier management allows you to extend endpoint protection to an almost limitless number of clients, regardless of location. Clients can be in the same LAN, connected by a MAN, or separated by the WAN. Depending on the model DLP appliance you are using, tens of thousands of agents can report to a single Inspector, and dozens of Inspectors can report to the DLP Manager. Policy management is unified through a single DLP Manager, and reports are global to provide a comprehensive view of the DLP solution.

Using multiple Inspectors to manage agents also supports roaming clients. As a client moves from one location in a protected network to another, the CI Agent will automatically report to its local inspector rather than maintain a connection to the remote one.

Agents provide three types of endpoint protection:

- **CI Agent Device Policies** —Set up one or more policies to restrict access to all or only certain types of USB, bluetooth, and Wi-Fi devices for a given computer, computer group, or user or user group. For example, you can prevent data from being copied out of the network by creating a policy to deny write access to all USB-type storage devices.
- **CI Agent Data Policies**—Set up one or more policies to monitor device usage on the basis of data. For example, to learn whether any clients are copying sensitive data to personal devices, you would register data and attach it to a policy. Apply the policy to selected users and/or computers, and whenever a file that contains some or all of the registered data is detected, an Incident will be created. You can also block the file, intercept and encrypt, it warn the user, or require that the user explain his/her actions before completing the transaction.

- **Agent-based Discovery**—You can scan your endpoint hard drives for the existence of registered data. Scans can be scheduled to occur automatically, and you can specify which local paths to include or exclude in a scan.

  See Chapter 9, "Discover Data On Servers and Endpoints" on page 141 for information on running agent-based Discovery Scans.

Agent Visibility on the Endpoint

You can choose whether or not you want your protected clients to see the CI Agent icon on their Windows taskbar. If visible, user can right-click it and open the CI Agent Status window. Otherwise, the agent icon is hidden.

- In the management console, click **Manage Agents | Settings** and then check or uncheck the **Hide Agent Icon** option.

Agent Control from the Endpoint

End users who are not logged on to their client with Administrator privileges cannot stop the CI Agent process or remove the Agent software. If the end user has Administrator privileges and uses the Windows Task Manager to stop the CI Agent service, the service will automatically restart.

Note, however, that users with Administrator privileges can perform all the tasks associated with the credential: they can uninstall the CI Agent, stop the services, and override device-blocking policies using Windows' administrative tools.

Agents that have been uninstalled from an endpoint will appear in the Managed CI Agents list as *Deregistered*. In addition, if a client stops the CI Agent on his/her machine, it will no longer send status updates to the Inspector (or DLP Manager). Device policies that have been disabled at the client by an Administrator will not display any indicators in the management console.

8.1 Configuring an Appliance to Manage CI Agents

CI Agents can report to either the DLP Manager or any Inspector. Depending on the model, a DLP appliance may be able to manage from 250 agents (for the DLP700) to as many as 20,000 agents (for the DLP2700). Of course, many factors come into play in determining the actual limits. The numbers above should be considered a ballpark indication of capacity and are provided to illustrate the differences in model capacity.

Agents should be installed in the same proximity as the appliance to which they report for the best performance.

The number of Inspectors that can report to the same DLP Manager also varies by model, however Inspectors do not need to be in the same proximity as the DLP Manager.

Note: For the best deployment planning advice and recommendations, contact Blue Coat Systems technical support.

8.1.1 Set the Central Management Port

Every DLP appliance that will be used to manage CI Agents need to have an IP address and gateway to the Central Management Port (eth5).

To set the central management interface for Agents:

1. In the DLP Manager, click **Manage System > Configuration > Network | Interfaces**.
2. Click the Edit icon for the eth5 interface.
3. Click the Settings tab.
4. In the **IP Address/Mask** field, enter the IP address/mask and gateway you will assign to the Agent Management port, for example,

   ```
   10.10.1.9/22
   10.10.1.1
   ```

5. In the **Speed/Duplex** field, accept the default value **Auto-negotiate** or choose one of the settings from the drop-down list to match your switch hardware.
6. If you want to change the name of the interface, click the General tab and enter the new name in the **Description** field.
7. Click **OK** to save the changes and close the window.
8. To confirm the connection, click **View Status > Dashboard**, and then in the Health Monitor window pane, click the Interfaces tab.

   The eth5 status icon should be green. If the icon is red (service is connected but not receiving traffic) or gray (service is disabled), click the icon to open the **Manage System > Configuration > Network | Interfaces** page, then click the **Edit** icon and open the Statistics tab to check whether the port is sending/receiving traffic.

A Note About Security Certificates

Note: A new client certificate is created whenever the eth5 address is changed. This new certificate must be installed all clients and/or Inspectors that are currently being managed by the appliance.

To avoid re-installing the client certificates after an appliance reinstall or modifications, you can back up and restore the corresponding server certificate (**Manage System > Maintenance > Back Up | Certificates**).

8.1.2 Enable Agent Management and Discovery

By default, the DLP appliance is configured for Standalone Mode; it will not manage agents on client endpoints.

To enable Agent Management:

1. From the management console, click **Manage System > Configuration > Settings | General** and select **Manager** mode.
2. Enable **Manage CI Agents** and then choose a port on which both the Manager and Agents will communicate. Default is 443.

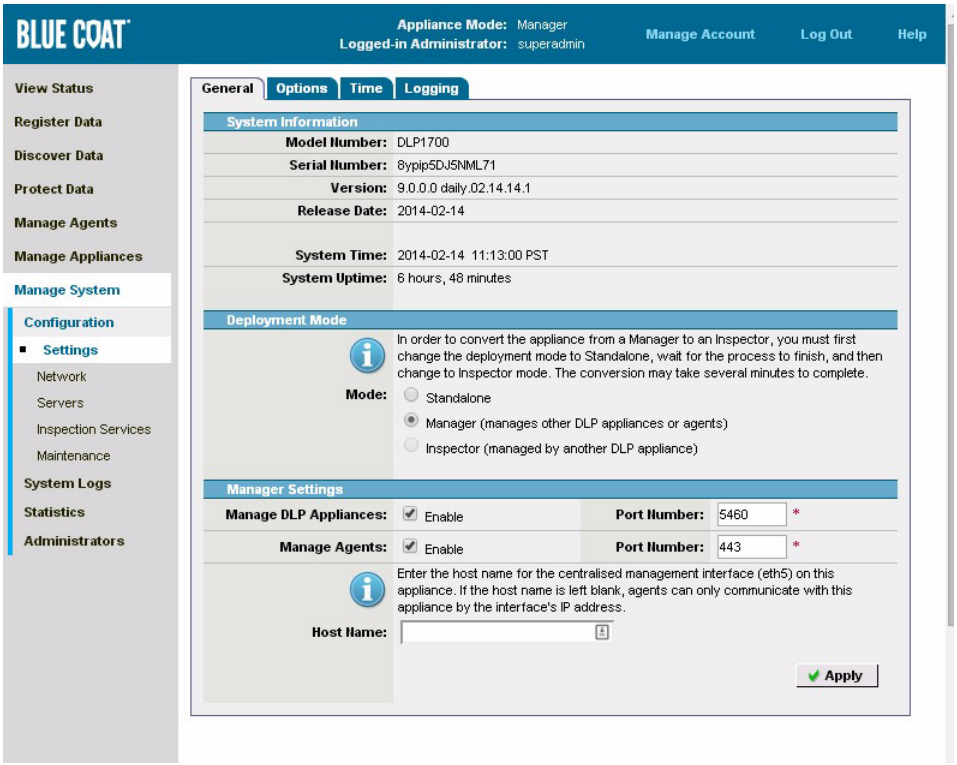


Figure 8.1: Certain menu options do not appear until you enable them.

3. Click **Apply**. The *Discover Data* and *Manage Agents* options will appear in the menu, as shown in the figure above.
4. In Discover Data that now appears in the menu, click **Manage Agents > Settings** to confirm that the various logging options have been enabled and to check the polling interval.

8.2 Managing CI Agents

You can configure the behavior of all registered CI Agents from the DLP Manager, including those that are reporting to an Inspector.

To configure Agents:

1. From the management console, click **Manage Agents > Settings | Settings** to open the global settings page for CI Agents.

   The following options are available:

- **Polling Interval**—Set the frequency at which changes to the DLP Manager are sent out to CI Agents. Increase the interval for example, if you have hundreds of CI Agents and you want to distribute an update across a longer time, or if you do not foresee frequent updates to the configuration (policies, registered data, etc.).

  If the DLP Manager has not received a contact from a CI Agent for a period of three times the polling interval, the agent will become grayed out in the Managed CI Agent list. Possible reasons include:

  • the endpoint is off line
  • the CI Agent service has stopped running on the endpoint
  • the IP address assigned to the Central Management Port has changed
  • the CI Agent has been uninstalled (in which case, you can deregister the agent)

- **Status Update Interval**—Set the frequency at which the CI Agent contacts the DLP Manager, for example to update the status of an on-going Discovery Scan. Results for each CI Agent can be seen in the **Last Status Update** column on the Managed CI Agent page (**Manage Agents > Agents**).
- **Idle-Time Scan Delay**—Use this option to pause scanning on the endpoint while the local mouse or keyboard are being used. If no activity has been detected on an endpoint for the period specified here, the scan will start or resume.
- **Hide Agent Icon in Taskbar**—Turn on or off CI Agent visibility for all protected clients. If this option is enabled, clients will not know there is an agent on their computer unless they are logged in with Administrator credentials and view their Services or running processes. If this option is not enabled, clients will see an agent icon and can right click it for more information.
- **Uninstall password**—Type a password to prevent the agent from being uninstalled by users who do not know the password. Without this option, users with Add/Remove Program rights on their computer may be able to remove the agent. Note that agents, if uninstalled, will appear as *Deregistered* in the Managed CI Agents list (**Manage Agents > Agents**).

  Note: If a password is set, the CI Agent can only be uninstalled when the password is provided (regardless of whether or not the endpoint is connected to the appliance). The password is not required to upgrade agents. Disable this setting before uninstalling multiple agents to avoid being prompted for the password for each agent. If the password is lost, contact Blue Coat Systems support for help in resetting it; endpoints will need to connect to the appliance to receive the new password before they can be uninstalled.

8.2.1 CI Agent Specifications

The CI Agents can be installed on the following Microsoft Windows clients:

- Windows 7 (64-bit and 32-bit)
- Windows XP with Service Pack 2 or 3

- Vista (64-bit and 32-bit)
- Windows 2003 and 2000 Server

Note: The CI Agent supports automatic file encryption for data transferred to client devices. This support is policy based and can be enabled according to device and/or bus type, user, or machine. If you plan to use this encryption, be sure your clients have 7-Zip (free, open source encryption and archiving software) installed to decrypt the files.

8.3 Installing CI Agents

Install CI Agent individually, or deploy them on all client endpoints in the LAN. CI Agents allow you to restrict or monitor content, and control access to connected devices. Policies can be enforced whether or not the client is connected to a DLP appliance.

To install CI Agents:

1. Download the agent install file from the Blue Coat Systems support portal.

   `Agent filename``: CIAgent-#.#.msi`

   Contact Blue Coat Systems support if you do not already have login credentials for the portal.

2. From the management console, click **Manage Agents > Agents** and then click the click **Export Certificate** button to download and save the file:

   `dlp_agent.zip`

3. Extract the contents of the file you just downloaded to a location that you can deploy the agents from. The folder that you install from must contain the agent install binary (.msi), and the two extracted files:

   ```
   dlp_agent_boot_config.xml
   dlp_agent_inspector.p12
   ```

4. To install a single instance of the agent, right click the .msi file and click **Install** from the menu that appears.

5. To deploy multiple agents across a network, use your preferred method for managing install and uninstalls.

6. Confirm the Agent installation in either of the following ways:

   - From the management console, click **Manage Agents > Agents**. Installed agents will appear in the list.
   - From the client where the agent is installed, right-click the CI Agent icon in the Windows taskbar and choose **View CI Agent status**. The icon will not appear on the client taskbar if you have **Hide Agent Icon** enabled at the appliance (**Manage Agents > Settings**).

Note about uninstalling password-protected agents:

If an uninstall password is set (**Manage Agents > Settings | Settings**), the CI Agent can only be uninstalled from a given endpoint after entering the uninstall password (at the endpoint), regardless of whether or not the endpoint is connected to the appliance.

The password is not required to upgrade agents. Disable this setting before uninstalling multiple agents to avoid being prompted for the password for each agent. If the password is lost, contact technical support for help in resetting it; endpoints will need to connect to the appliance to receive the new password before they can be uninstalled.

8.4 Assigning CI Agents to an Inspector

If you have Inspectors that will manage CI Agents, you need to assign those agents to the (closest) Inspector. More precisely, the action is not so much to "assign" an agent to an Inspector per se, as it is to define a range of IP addresses that the Inspector will cover. Clients whose IP address falls within the range specified for a given Inspector will automatically report to that Inspector.

A subtle benefit to this method of agent assignment is that supports roaming clients. Whenever a client moves from one location to another in the company, that client will automatically connect to the nearest Inspector when s/he logs on using the new IP address given for that access.

The DLP Manager will propagate the scan policy and assignments to all registered Inspectors, who will apply only those policies and manage only those agents that are relevant.

Notes:

1. Agents installed on the endpoints will contact the DLP Manager, which will then hand the agent off to the assigned Inspector.
2. Agents that are off-line, that is not connected to the corporate network, will be governed by any off-line behaviors as defined in the agent policy.
3. If the agent is unable to contact the assigned Inspector, it will default to the DLP Manager using a set of fall-back rules (Limited Service Mode) until contact with the Inspector is regained.

Limited Services Mode

When a CI Agent is disconnected from the Inspector to which it reports, the agent will automatically begin reporting to the DLP Manager in a “Limited Services Mode” (LSM).

In LSM, the CI Agent does the following:

- Sends system log messages to the DLP Manager
- Sends activity logs to the DLP Manager

- Queues rather than sends Data In Use requests (queuing will continue until the retention limit has been reached or the agent reconnects to the Inspector)
- Abstains from running Discovery scans or sending Discovery requests

To enable an Inspector for agent management:

Because different Inspectors may have different roles, you need to explicitly enable agent management on each Inspector that will assign agents to.

You can check this status on from the list of managed appliances. If the Agents column does not have a green check, you need to enable agent management on that appliance.

1. From the management console on the DLP Manager, click **Appliances** and then the Host Name of the Inspector that does not have agent management enabled.
2. Log in to the Inspector management console with it opens.
3. From the Inspector management console, click **Manage System > Configuration > Settings | General**.
4. At the bottom of the page that opens, under Agent Management Settings, **Enable** the Manage CI Agents option.
5. Confirm that the port is correct for the DLP Manager and add a Host Name if you want before clicking **Apply**.
6. Next, confirm that the Discovery Inspection Service is enabled:
   - Click **Manage System > Configuration > Inspection Services | Discovery**.
7. Log out of the Inspector and return to the console for the DLP Manager.

8.4.1 Assign Agents to an Inspector

Before you can assign agents to an Inspector, you need to create a Network Address group to define the range of IP addresses you want that Inspector to cover. Create at least one Network Address for each Inspector that will manage agents.

Alternatively, you can include all clients by choosing the "Any" option when making the appliance assignment. In this case, you do not need to create a network address.

To create a Network Address:

1. From the management console on the DLP Manager, **click Protect Data > Network Addresses** and then the **Create Address...** button.
2. Type a name and then select **IP Range**. (If you want to assign several disparate ranges or a collection of individual IPs to a given Inspector, create an Address Group to hold the assorted IP addresses.)

To make an appliance assignment:

Agent assignments can only be made for Inspectors (version 7.0 or later) that have registered with the DLP Manager. If you have just upgraded the DLP Manager and Inspector(s), be sure to upload the manager's new security certificate to the Inspector.

1. From the management console, click **Manage Agents > Settings | Assignment** and then the **Add Assignment** button.

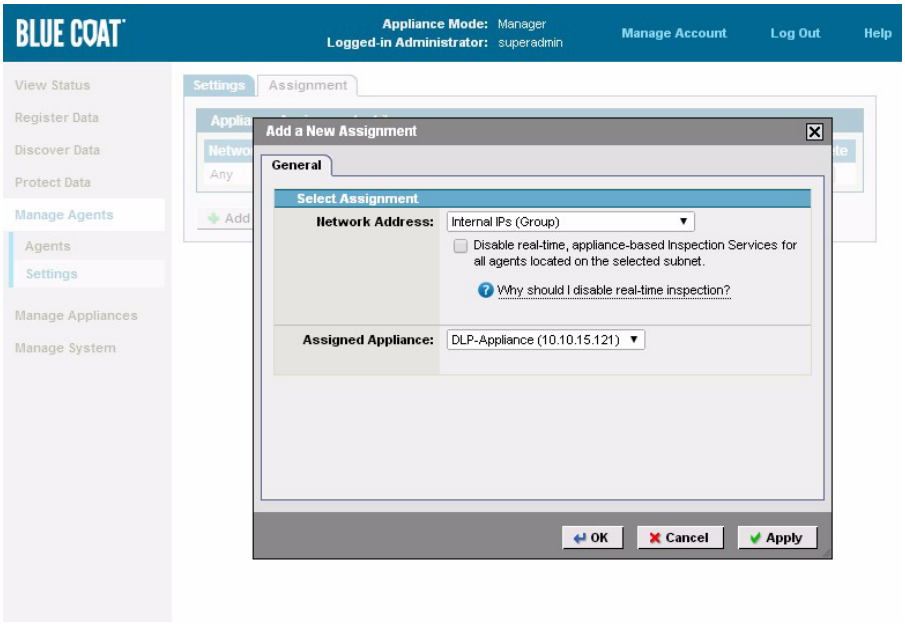


Figure 8.2: Connect a Network Address to an Inspector.

2. Select the Network Address or Group that you created, and then choose the DLP appliance that you want to manage clients who have an IP address in the range represented by the network address.
3. Click **OK** to save your assignment and close the window. The new assignment appears in the Appliance Assignment list.
4. Click the **Synchronize** button that appears in the lower left hand corner of the window to push the new settings to the Inspectors. Installing CI Agents

By default, the agent uses port 443 and contacts the DLP appliance using https. If you plan to use a different port, be sure that it is not blocked by a firewall, and that there is no client-side security program that may restrict outbound traffic on the port.

Agents can be installed individually on each target client by downloading the agent installation binary and then running the Installation. Alternatively, you can deploy the agents across multiple clients using a program such as Microsoft® System Management Server (SMS) 2003, or by using your own login script.

If you have upgraded the DLP appliance, you should also upgrade all of your agents by uninstalling the previous version and restarting the client before installing the new agent.

8.4.2 Create a Static Bypass on the Proxy Server

If you have a Blue Coat ProxySG appliance set up for transparent mode (i.e., it is in-line with the client network), and you have SSL interception enabled, the proxy may intercept all traffic between the CI Agent and DLP appliance. Agent communication will fail because the Blue Coat ProxySG appliance replaces the DLP appliance certificate with its own. To avoid this, you can set up a static bypass for the DLP appliance in the Blue Coat ProxySG appliance management console.

To set up a static bypass for the CI Agent:

1. Open the Blue Coat ProxySG appliance management console, and then in the **Configuration** menu that appears, click **Services > Proxy Services** and then the **Static Bypass List** tab.

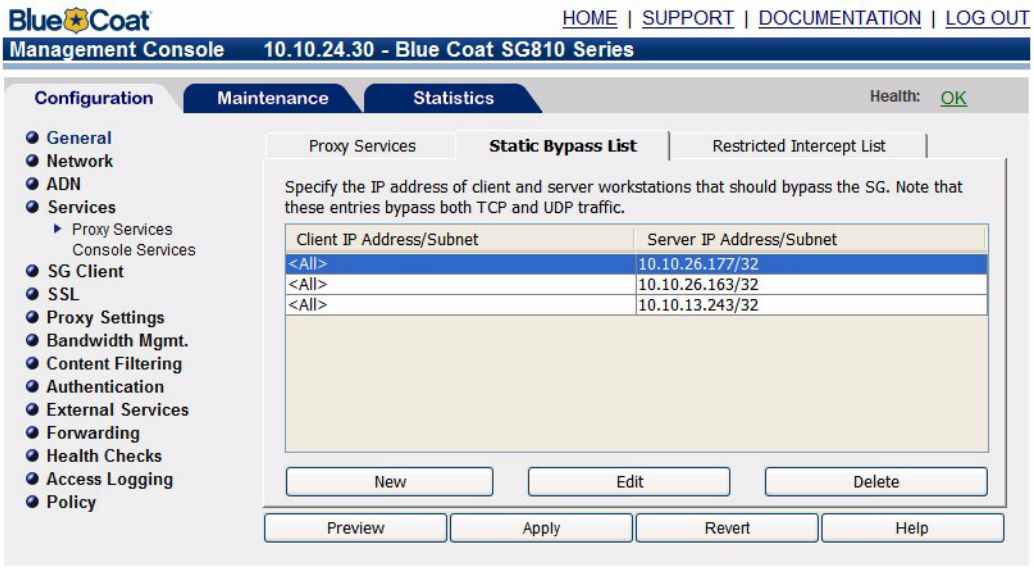


Figure 8.3: Set up a static bypass for the CI Agent on the ProxySG appliance.

2. Click the **New** button and then, choose **All Clients** for the **Client address**.
3. Under **Server address**, choose **Server host or subnet** and then enter the IP address and port used by the CI Agent.

   By default, the CI Agent connects to the DLP appliance using port 443 on the IP address you configured for eth5 (to check the IP address and subnet, in the management console, click **Manage System > Configuration > Network | Interfaces** tab).
4. Click **OK** and then **Apply** to create the static bypass.

8.5 Create a CI Agent Data Policy

You can set up agent data policies to check client file transfers for registered data. The principles are the same as for the other inspection services: register the sensitive data, attach it to a policy, and then specify which users, computers, and files to target. After you enable the policy, real-time content inspection at the endpoint will begin.

Whenever a user creates, moves, or copies a file with some or all of the registered data, an incident will be created. You can also configure the policy to block the transfer, encrypt the file and complete the action, and/or prompt the user for a justification for his/her actions in order for the transfer to be completed. This is called self-remediation.

Monitoring can occur while the client is off-line, and the results will be logged to the DLP appliance when the client reconnects.

8.5.1 About Implementation of CI Agent Data Policies

If a file write/copy operation is permitted based on the fact that there is no device policy blocking such action, or because there is an explicit device policy that allows such action, then the data being written to the external device will be inspected against the data policies defined for CI Agents. At that point, if a policy match occurs, the action for that policy will be executed (e.g. block the copy operation if there is sensitive data).

There is implicit policy prioritization for CI Agent policies (there are no explicit exception policies as there are with appliance-based policies). The more specific the policy, the higher its priority. For instance, a policy defined for a specific user takes precedence over a policy defined for a group to which the user belongs. It should be noted that policies that are to be applied to "all domain Users" are treated at an equal level to policies defined for specific User Groups if the logged-in user is a domain user and belongs to the specified group. Essentially, the "all domain Users" are treated as an equivalent to specified AD groups.

Data policies for client agents will be prioritized as follows:

a) Specific Computer and Specific User

b) Computer Group and Specific User

c) Specific Computer and User Group

d) Computer Group and User Group

e) Specific Computer and Any User

f) Computer Group and Any User

g) All Domain Computers and Specific User

h) All Domain Computers and User Group

i) All Domain Computers and Any User

8.5.2 About Self Remediation

The self-remediation option provides a number of practicalities:

1. It informs the user that the file he/she is transferring contains restricted data.
2. It passively but persistently creates an environment of awareness.
3. It reduces the number of incidents that require review and remediation from an Incident Reviewer.
4. It does not prevent users from completing their transfer as expected (unless they choose to).

The reason provided by the user can be logged at the DLP Manager as a part of the incident, along with a copy of the file in question. In addition, you can set up a notification email to be sent to designated users. You can also customize the notification message that end users will see and respond to.

For example, say that a user plugs in his/her USB memory stick and then proceeds to copy files from the network or local hard drive to the device (s/he could also save an open document to the USB -- the effect is the same). The CI Agent running on that endpoint will inspect the file as it is being copied. If a match is detected, the file will be suspended and a window will appear asking the user to provide a reason for the transaction.

Note: The CI Agent writes temporary content to a temporary file while the actual content is being inspected. If a user disconnects the target device during inspection or without providing a response to the acknowledgement window, the file will contain only the following: "Protected by Blue Coat Systems."

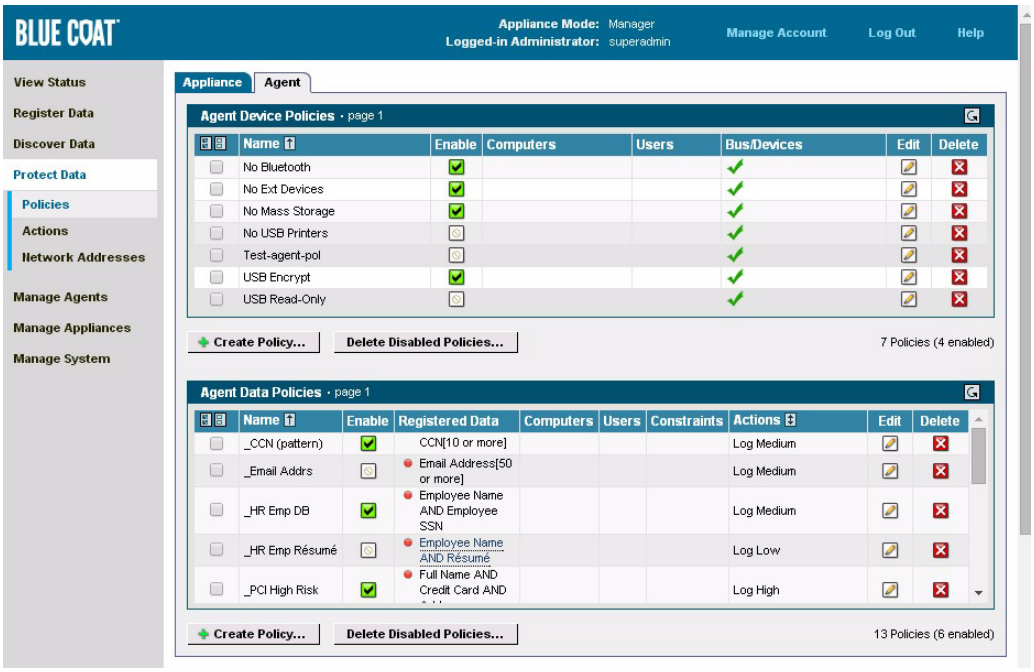
If the user subsequently reconnects the device and then makes the acknowledgment, the original content will be available. If the user disconnects the device, closes the acknowledgement window, and then reconnects the device, the file will contain only the temporary data.

8.5.3 Creating a CI Agent Data Policy

Perform the procedure below to create a CI Agent data policy.

To create a CI Agent Data Policy:

1. From the DLP appliance management console, click **Protect Data > Policies | Agent**.



2. In the middle of the screen that appears, click the **Create Policy...** button.
3. In the Agent Data Policy screen, provide the items below and then click **Next**.

- **Name**—The name typed here will appear in the Discovery Policies list.
- **Description**—The description will appear when you mouse-over the Name in the Discovery Policies list.
- **Policy Creator**—Your choice here can affect the incident workflow (including edit and review rights) notifications, and associated Actions.

Select Actions—

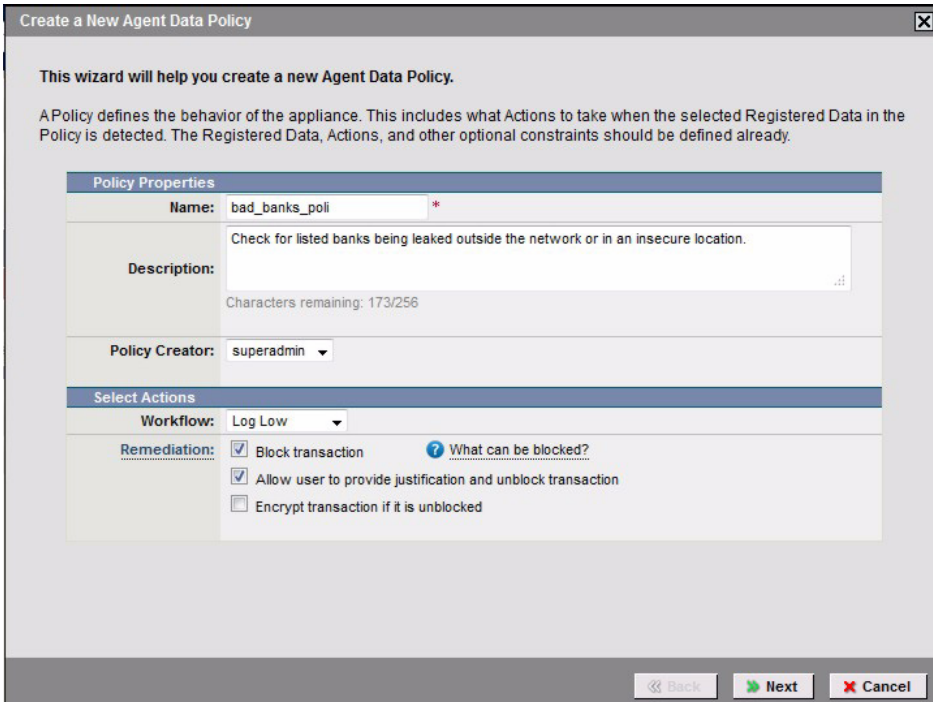
- **Action**—Available choices are taken from **Protect Data > Actions**, including any custom Actions you have created or changes made to the defaults. The actual response of a given Action selected from the drop-down will depend on what is configured for each Action and may include notification, archiving, logging, and automatic incident assignment.

Note: Choose "Do Nothing" if you do not want to notify the user of the violation or to retain a copy of the matching document. When this option is selected, Transaction Options will be disabled.

Transaction Options—

- **Block transaction**—Blocked transactions will not be written or saved to the protected device.
- **Ask user to justify their action**—Choose this option to prompt users to provide a reason for the transaction. This reason will be recorded with the other incident details.
  - To create a custom notification message, edit the Notify option on the Action you will use: Click **Protect Data > Actions** and then the **Edit** icon. Click the Notify tab and then enable Notifications for the Action.

- **Allow user to provide justification and unblock transaction**—Choose this option to let users unblock their file transaction after providing a reason.
- **Encrypt transaction**—Choose this option to encrypt any files found to contain data that matches the configured policy.



4. In the Create a New Agent Data Policy screen that appears, define data that you want this policy to scan for and click **Next** when finished:
   - **Do not use registered data as a constraint**—Choose this option if you do not want to consider registered data as a part of the policy.
   - **Base content constraint on Registered Data from the selected Policy**—Choose this option and then select from the available policies that appear. Use this to build-on, or to or re-use an existing policy. Changes made in this policy will not affect the policy you are basing them on.
   - **Specify Registered Data that will be used as a content constraint in this Policy**—Choose this option to select one or more elements of Registered Data. Combine multiple elements, connected with the AND operand, to initiate row correlation and reduce false positives.
5. Narrow the scan by selecting the computers you want the policy to apply to:
   - **Apply this policy to all domain computers**—All computers in the domain will be included.
   - **Apply this Policy only to specific Computers or Computer Groups**—You can select one or more mutually exclusive groups and/or users from your Active Directory listing. (When selecting multiple users or groups, be sure not to include the same computers in more than one group, or those computers may be scanned once for each group they belong to.)

6. Choose the computer users (based on domain login credentials) to whom you want the policy to apply:
   - **Apply this Policy to all Users**—Choose this option if you do not use Active Directory, or want the policy to apply without exception to all users in the network.
   - **Apply this Policy to all domain Users**—Eligible users include all endpoints running the CI Agent connected to any domain (computers configured for a Workgroup will not be included), and accessible from the DLP appliance.
   - **Apply this Policy only to specific Users or Groups**—Use this option with users and Groups to create exceptions, for example restricting access to all devices, except by users in a certain group (such as IT).
7. Choose a file filter to include only files of the selected type. Using file filters can significantly reduce the number of files to be scanned by filtering out those unlikely to contain editable data (such as .exe, .dll, etc.).
   - The list of available file filters includes the DLP appliance defaults, and any custom filters that you have created in **Register Data > File Filters**. File filters can be created to define a group according to file type, size, and/or extension. File type determination is made according to the file metadata rather than extension, which can be altered.
8. In the Summary screen that appears, review your choices and then click **Finish** to return to the CI Agent Discovery Policies page.
9. Click **Enable** to apply the policy to the targeted endpoints.

8.6 Create a CI Agent Device Policy

You can set up one or more agent device policies to restrict access to all or selected devices, according to device type, bus, or device driver. Unlike CI data policies, CI Agent device policies do not check for content violations. Devices can include USB, Bluetooth, and Wi-Fi, and you can target your different policies to different computers, computer groups, users, and user groups.

For example, you can prevent data from being copied out of the network by creating a policy to deny write access to all USB-type storage devices.

Only policies **Enabled** on the CI Agent Device list are active; once active, the policy will be enacted on protected clients at the next **Status Update** or after you click the **Synchronize Configuration** button.

8.6.1 About Implementation of CI Agent Device Policies

There is implicit policy prioritization for CI Agent policies (there are no explicit exception policies as there are with appliance-based policies). The more specific the policy,

the higher its priority. For instance, a policy defined for a specific user takes precedence over a policy defined for a group to which the user belongs.

Device policies for client agents will be prioritized as follows:

a) Specific Computer and Specific User

b) Computer Group and Specific User

c) Specific Computer and User Group

d) Computer Group and User Group

e) Specific Computer and Any User

f) Computer Group and Any User

g) All Domain Computers and Specific User

h) All Domain Computers and User Group

i) All Domain Computers and Any User

Similarly, there is implicit prioritization when defining device policies as far as the devices are concerned. Generally, a policy defined for a specific device will take precedence over a policy defined for a group of devices. For instance, if you define a policy to block all read/write operations from the USB bus, but then have a constraint that allows writes to a specific USB mass storage device (e.g. by using its serial number or device drive name), then the operation will be allowed for that particular device.

The prioritization follows the following model for USB mass storage devices:

1) USB Device Serial Number

2) USB Device Drive Name

3) USB Device

4) USB Bus

The above prioritization is for mass storage devices and does not apply to other devices, such as scanners. For instance, if you have a policy to disable the USB bus, but allow scanners, then the USB bus policy takes precedence. In order to support this case, you would need to define a policy to disable access to specific USB devices, such as USB mass storage devices, and allow access to scanners.

8.6.2 Restricting USB Use to Registered Devices Only

The DLP appliance provides an option via device policies that allows you to prevent users from using any USB device that has not been registered.

One restriction is based on the manufacture’s serial number for the USB device. Only devices whose serial number has been registered with the DLP appliance can be connected to endpoints, as specified by the device policy.

The serial numbers for devices can be manually entered, retrieved by pressing the button "Export Filtered Serial Numbers" on the Agent Activity logs page, or by going to the PC where the device was inserted and retrieving the usb_serial_numbers.csv file from the C:\Program Files\Code Green Networks\logs folder (the file will contain the device names and serial numbers for any devices plugged into this PC). When enabled, any of the specified computers/users will be able to use any device with a registered serial number. Conversely, devices without a registered serial number will not be able to connect.

Alternatively, another restriction can be based on the device drive name. In order for USB mass-storage devices to have their drive name appear in the list of drive names for a given device policy, insert the device into a PC and copy at least one file to it. After a few minutes, the drive name for that device will be added to the list of device drive names in the device policy as a valid constraint that can be selected.

8.6.3 Creating a CI Agent Device Policy

Perform the procedure below to create a CI Agent device policy.

To create a CI Agent Device Policy:

1. From the DLP appliance management console, click **Protect Data > Policies | Agent**.
2. Below CI Agent Device Policies in the screen that appears, click the **Create Policy...** button.
3. In the Agent Device Policy screen, provide the items below and then click **Next**:
   - **Name**—The name typed here will appear in the Discovery Policies list.
   - **Description**—The description will appear when you mouse-over the Name in the Discovery Policies list.
   - **Policy Creator**—Your choice here can affect the Incident workflow (including edit and review rights) notifications, and associated Actions.
4. Select the computers to which you want the policy to apply and click **Next** when you are done:
   - **Apply this policy to all domain computers**—All computers in the domain will be included.
   - **Apply this Policy only to specific Computers or Computer Groups**—You can select one or more mutually exclusive groups and/or users from your Active Directory listing. (When selecting multiple users or groups, be sure not to include the same computers in more than one group, or those computer may be scanned once for each group they belong to.)
5. Choose the computer users (based on domain login credentials) to whom you want the policy to apply and click **Next** when you are done:
   - **Apply this Policy to all Users**—Choose this option if you do not use Active Directory, or want the policy to apply without exception to all users in the network.

- **Apply this Policy to all domain Users**—Eligible users include all endpoints running the CI Agent connected to any domain (computers configured for a Workgroup will not be included), and accessible from the DLP appliance.
- **Apply this Policy only to specific Users or Groups**—Use this option with users and Groups to create exceptions, for example restricting access to all devices, except by users in a certain group (such as IT).

6. Choose which devices and or busses you want the policy to include by selecting from the options in the drop-down control. Click the green + icon to add that bus/device to the policy.

   Note: Adding a bus or device to the list automatically blocks read and write access, unless you explicitly enable that access for each device.

   The following options are available for each device included in the policy:

   - **Enabled**-unless checked, clients will receive an Access Denied message from the CI Agent whenever they connect a blocked device or try to access one that is already connected. The Windows operating system may also show its own message. If checked, clients will be able to browse folders, copy from the device, and open files. They will not be able to write to the device.
   - **Writable**-unless checked, clients will not be able to write to the device. See above.
   - **Encrypt**-Files copied to the device will automatically be encrypted using 7-Zip, the open source Windows utility for manipulating archives. This program is also required to decrypt the encrypted files. It can be downloaded from the 7-Zip web site at, http://www.7-zip.org

7. Click **Next** and then **Finish** to automatically enable the device policy and add it to the device policy list.

8.7 CI Agent Activity Logs

The following topics provide information about viewing the agent activity logs and configuring agent activity log settings (click **View Status > Agent Activity**).

The **CI Agent Activity Logs** summary page displays information about items in the activity log as described in Table 8.3, below.

You can sort any of these columns in ascending or descending order. You can also refresh the agent activity log.

Table 8.1: The CI Agent Activity Log summary page

Column	Description
Basic filter options and **Apply Filter** button	Allows you to filter the display of CI Agent Activity logs by changing the values set for date range, computer, user, activity, bus, and / or device. **NOTE:** The filtering of CI Agent Activity logs supports the wild card character (*).

Table 8.1: The CI Agent Activity Log summary page

Column	Description
Date/time	The time stamp of the activity log message.
Host	The name of the computer associated with the log.
User	The name of the person logged into the computer with the last status message.
Activity	Type of activity associated with the log (i.e., device removed, file copied from local drive to removable device, etc.)
Bus	The bus type used by the associated device.
Device	The device type.
File Type	The file type which caused the incident (i.e., .doc, .xls, etc.)
File Name	The name of the file.
Action	The action associated with the policy.
Policy	The name of the policy that matched the activity.
Delete Selected Agent Logs button	Permanently delete selected CI Agent Activity logs.
Export Filtered Agent Logs button	Export filtered CI Agent Activity Logs to a .CSV file.

8.7.1 Export Filtered CI Agent Activity Logs to a File

When you export the agent activity log, you see more information than when you are viewing the summary page. The following table describes the columns exported to a zipped file.

To export filtered CI Agent Activity Logs:

1. From the management console, click **View Status > Agent Activity**.
2. Click **Export Filtered Agent Logs**.
3. Click **OK** to confirm the export.

4. Select a destination on your local file system and optionally change the file name to finish the export. The default file name is *agentactivitylogs.zip*, which will contain a file called *agentactivitylogs.csv*.

Table 8.2: Sample contents from the agentactivitylogs.zip file.

Column	Description	Example
Display ID	The display ID generated on the management appliance at db insert time.	31
Host Name	The identification number of the managed device that created the incident.	2
Audit Log ID	ID number generated for the client.	1
Date/Time	The time stamp of the activity log message.	10/19/2008 2:12:00 PM
Agent Type	Indicates the agent type (i.e., file or device activity).	Device Activity
Managed Client ID	The unique ID for a managed client; issued to the client at registration time.	Online
Transaction	The transaction status for the file or device (i.e., Allowed / Blocked)	Allowed
Transmit Encrypt Status	Displays either Do Not Encrypt, Failed, or Succeeded.	Do Not Encrypt
Computer IP Address	A numerical identification (logical address) that is assigned to devices participating in a computer network utilizing the Internet Protocol for communication between its nodes.	192.168.127.127
Computer	The name of the computer associated with the incident.	CGNLAB3
Computer SID	Short for security identifier, a security feature of the Windows NT and 2000 operating systems. The GUID is a unique name (alphanumeric character string) that is used to identify an object, such as a user or a group of users in a network of NT/2000 systems.	862EF170C944D64EA9AC3C4DB0588E1F
User	The name of the person logged into the computer when the log is created.	Administrator
User ID	The series of characters a system or network uses to distinguish one user from another. Also called a user name.	0CB51BAD34E3894CABAF97EA5718F6BD

Table 8.2: Sample contents from the agentactivitylogs.zip file.

Column	Description	Example
Domain Name	A domain name provides symbolic representations, i.e., recognizable names, to mostly numerically addressed Internet resources.	SALES
Policy	The matching policy name, when a policy matches.	No Mass Storage
Policy Matched	Policy matched or not matched.	Matched
Application Name	The name of the application used that prompted an incident to be created.	explorer.exe - Windows Explorer
File Name	The name of the file.	foo.PNG
File Type	The file type which caused the incident (i.e., .doc, .xls, etc.)	Word, Excel, etc.
File Size	The size of the file.	13330 bytes
Operation Type	Operation type for the file activity.	File copied from Local Drive to Removable Device
Device Direction	The device direction involved in the incident.	To a device
Start File Operation Time	The start file operation time.	10/10/2008 5:16:00 PM
End File Operation Time	The end file operation time.	10/10/2008 5:16:00 PM
Source Device Drive Name	The name of the source device drive name.	Local drive - C:
Source Path	The path of the source drive.	C:Documents and Settingsadministrator.CGNSALESMy DocumentsMy Pictures oo.PNG

Table 8.2: Sample contents from the agentactivitylogs.zip file.

Column	Description	Example
Destination Device Drive Name	The name of the destination device drive.	Apple iPod USB Device
Destination Path	The path of the destination device.	E: oo.PNG
File Creation Time	The time when the file was created.	10/10/2008 5:15:00 PM
Last Access Time	The last file access time in GMT.	10/10/2008 5:15:00 PM
Last Write Time	The last file write time in GMT.	10/10/2008 5:15:00 PM
File Title	These fields are all sourced from the File Properties of Microsoft Office documents.	
File Subject	These fields are all sourced from the File Properties of Microsoft Office documents.	
File Category	These fields are all sourced from the File Properties of Microsoft Office documents.	
File Keywords	These fields are all sourced from the File Properties of Microsoft Office documents.	
File Comments	These fields are all sourced from the File Properties of Microsoft Office documents.	
File Source	These fields are all sourced from the File Properties of Microsoft Office documents.	
File Author	These fields are all sourced from the File Properties of Microsoft Office documents.	
File Revision Number	These fields are all sourced from the File Properties of Microsoft Office documents.	
Bus	The bus type used by the associated device.	USB
Device	The device type.	iPod
Device Name	The device name.	Apple iPod USB Device

Table 8.2: Sample contents from the agentactivitylogs.zip file.

Column	Description	Example
Device ID	The ID number of the device.	USBVid_05ac&Pid_1300&Rev_1001
Device Serial Number	The serial number of the device.	
Time Device Inserted	Time device inserted in GMT.	10/10/2008 5:15:00 PM
Time Device Removed	Time device removed in GMT.	10/10/2008 5:17:00 PM

8.7.2 Delete Selected CI Agent Activity Logs

1. From the management console, click **View Status > Agent Activity**.
2. Select the desired checkboxes next to the CI Agent Activity logs you want to delete. Select all the checkboxes to delete all of the CI Agent Activity logs.
3. Click **Delete Selected Agent Logs**.
4. Click **OK** to confirm the deletion. You can also delete all CI Agent Activity Logs from **Manage System > Maintenance | Data**.

BLUE COAT

9 Discover Data On Servers and Endpoints

9.1 Introduction

The DLP appliance supports both appliance-based Discovery and agent-based Discovery.

Appliance-based Discovery is ideal for scanning large file stores and databases, including Windows and Linux file servers, SharePoint, WebDAV, and other file repositories. You can also use appliance-based discovery to scan databases and cloud-based file-sharing services.

Agent-based Discovery allows you to find protected data on all your Windows clients and any supported drives, including removable media, such as flash drives.

As with Data-in-Motion inspection, when a policy-match for registered data occurs during a Discovery scan, an Incident is created. The remediation actions you can take for appliance- and agent-based Discovery scans include the ability to copy, move, or delete the file that triggered the Incident. Alternatively, you can choose the action to do nothing or to perform a custom action.

As with the other Blue Coat Systems inspection services, Discovery can recognize data in more than 800 file formats, scan multi-byte and non-English characters, and detect data contained in compressed archives. In addition, Discovery can detect data in hidden files, data that is "hidden," for example, in a Microsoft® Excel® spreadsheet, and file metadata, such as the owner or last modified date.

9.1.1 Support for Multiple Appliances/Inspectors for Discovery

Discovery with a single, stand-alone DLP appliance is supported. In addition, you can deploy multiple appliances with Managers, Inspectors, and possibly CI Agents and perform discovery. In general, every feature that is supported on a stand-alone appliance is supported by multiple appliances. Using multiple appliances to perform discovery may be appropriate when looking for sensitive data in different geographical locations, or to distribute the load when scanning very large repositories.

For Cloud Scans, you need to configure a specific appliance to scan the cloud. If your organization uses multiple cloud file-sharing services, you can assign a separate appliance to scan each cloud to balance the scanning load.

9.1.2 Understanding Discovery Policies and Scans

In general, policies are primarily intended to identify sensitive content you want to discover. Policies can be built with Registered Data, including fingerprinted information that is part of the RedList, patterns (e.g. credit card numbers), or other supported Registered Data. For example, you can use a credit card policy to discover credit card numbers in a data repository. After creating the desired policies, you then attach the policies to a scan. Discovery policies can be used in either appliance-based or agent-based scans.

Scans define the data repositories in which you want to search for the sensitive data. After you perform a scan, any content that matches a policy will be logged and can be viewed on the Discovery Incidents page (by choosing **View Status > Incidents > Discovery)**. You can view information about the policy that triggered the match, the file type, the Registered Data, and the number of matches that occurred, as well as a hit-highlighted copy of the file.

9.1.3 Enable the Discovery Inspection Service

In order to be able to perform appliance-based discovery, the Discovery Inspection Service must be enabled on each DLP appliance (Managers and Inspectors) that will perform Discovery.

To enable the Discovery Inspection Service:

1. From the management console of the target appliance, click **Manage System > Configuration > Inspection Services | Discovery**.
2. Check the **Enable** box and then click **Apply**.

9.1.4 Enable Agent Management

To perform agent-based Discovery, the DLP appliance must be in Manager or Inspector mode (the default is Standalone). Agent-based Discovery will not be available in the console until you change the deployment mode to Manager or Inspector and enable "Agent-Management." See 3.3 "Configure the Role of the Appliance" on page 22 for instructions on configuring the appliance mode.

9.1.5 Supported File Shares/Databases

For appliance-based scans, you can scan files on NFS, SMB, CIFS, WebDAV, and Documentum repositories. You can also scan cloud data stores, such as Box, Egnyte, and ShareFile. You can also scan Oracle, Microsoft SQL, MySQL, PostgresSQL, DB2, Informix, and Sybase databases. Note that appliance scans should be used for databases, file shares, and cloud data stores. Limits and/or special considerations for several formats are described below.

CIFS

All CIFS target files must be readable to the account used by Discovery to log on to the file share. For example, if you log Discovery on to the CIFS server as a guest, it will only have guest-level permissions, which might severely limit the number of files it is then able to evaluate. Not all shares may point to the same CIFS server.

Note: Appliance-based Discovery (CIFS servers only) cannot simultaneously mount the same server using two different sets of credentials. If two sets of credentials are provided in the scan definition file, the second mount will produce an error unless the first scan has been completed. See 9.3.2 "About the Scan Definition File" on page 155 for information.

NFS

Because the Discovery service does not run as root, all target files need to be readable from uid 499.

Appliance-based Discovery supports NFS version 2 and version 3; it does not support version 4. When connecting to Unix/Linux file shares, bear in mind that the system may also support CIFS, so you can connect via CIFS rather than NFS.

SMB

The DLP appliance provides SMB support for legacy SMB servers. Any current Windows servers will be using CIFS. Note that unlike CIFS, SMB does not support Unicode. Avoid including documents with non-English characters in the target scan. Alternatively, setting the code page may provide a work-around for documents with Unicode.

9.2 Configuration

Before creating policies, attaching policies to scans, performing scans (with or without remediation actions, such as copy, move, and delete), and then addressing incidents, you should do the following:

- Identify the data you want to protect. This could be credit card or Social Security numbers, source code, patient or medical data, and so on.
- Identify the locations where the data could be stored. This could be in network file shares, databases, Windows clients, cloud data stores, and other locations.

9.2.1 Creating a Discovery Policy

Use Discovery policies to identify the data that you are looking for and the actions to take when the data is found.

To create a Discovery policy:

1. From the DLP appliance management console, click **Discover Data > Policies**. The Discovery Policies page appears.
2. Click the **Create Policy...** button. The Create a New Discovery Policy wizard appears.
3. Give the policy a short name (<15 chars) and a description (<256 chars), for example, a summary of the scan parameters, or a note documenting the provenance of the policy.
4. Choose the desired workflow for the policy. See 9.6 "Configuring Actions" on page 169 for information on workflows.
5. Choose the desired remediation action for the policy. You can specify actions for appliance-based scans independently of the actions for agent-based scans. See 9.6.2 "Remediation Actions" on page 171 for more information. For copy and move actions, you need to first configure a destination vault. See 9.6.3 "Defining a Vault" on page 172 for information about vaults.
    - Copy: a file that matches the policy will be copied to the vault.
    - Move: a file that matches the policy will be removed from its current location to the vault. You can "undo" a move action.
    - Delete: a file that matches the policy will be deleted from its current location. You cannot "undo" a delete remediation action performed on a file.
    - Custom action: performs the remediation action specified in a script. See "Creating a New Remediation Action" on page 171 for information.
    - Do nothing: no action is taken when data matching the policy is discovered.

If you choose the move or delete action, you can check the **Leave text file with message** box to leave a text message in the location from which the file was moved or deleted to notify users of this action. The message will be left in a text file with the same name as the original file, with the ".txt" extension (e.g. sensitive.doc.txt).

If you choose a remediation action other than "Do nothing," you can select how the action will be performed.

- Select **Allow Remediation Action to run manually during incident review** to perform the specified action (for example, copy) manually during incident review. This setting is recommended. As an example, if you choose the copy action in a policy and this option is selected, when a file matching the policy is located, a Discovery incident will be created. When the incident is reviewed, the reviewer will be presented with a **Copy** button that can be used to copy the file to the vault.
- Select **Run Remediation Action automatically when incident is discovered** to perform the specified action automatically upon discovery.

Note: The above "automatic" remediation action implementation option is provided to allow for expedited workflow, but is generally not recommended. This is because you might execute actions on files, like delete, that you did not intend to delete.

Click **Next** to continue.

6. Select the data you want to scan for in this policy:

- **Do not use registered data as a constraint**—Choose this option if you want to identify files based on one or more properties (rather than data), for example to discover documents that are out of place, such as someone's email archive on a public file share or documents from the Legal Department on an unauthorized client. This option should not be used for database discovery.
- **Base content constraint on Registered Data from the selected Policy**—Choose this option if you want to inherit the Registered Data portion of an existing policy, and then select from the drop-down menu the constraint you want. You can use the inherited constraint "as is" or modify it by choosing one or more additional elements from Registered Data.

- **Specify Registered Data that will be used as a content constraint in this Policy**—Choose this option to select one or more elements from Registered Data. You can combine multiple elements to create a complex constraint.

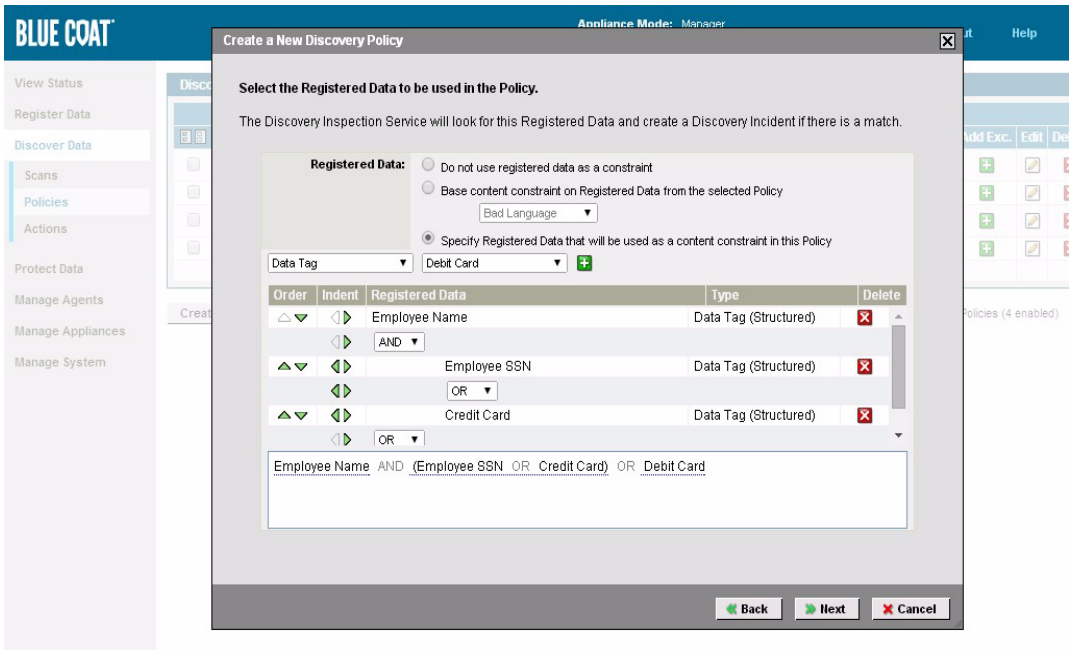


Figure 9.1: Discovery policies can be used for discovery scans hosted by the appliance and/or to detect restricted data on client endpoints.

Click **Next** to continue.

7. If you are creating a policy for an agent-based scan, you can narrow the scan by selecting which computers you want the policy to apply to:

   - **Apply this Policy to all scanned domain Computers**—eligible computers include all DLP-enabled clients connected to any domain (computers configured for a Workgroup will not be included), and accessible from the DLP appliance.
   - **Apply this Policy only to specific Computers or Computer Groups**—enter the name of the desired computer or Computer Group from your Active Directory (AD) listing. The system looks up the specified name and displays a match. Click the name and then click the plus sign (+) button to add the computer/Computer Group to the list. You can include any combination of groups and individual computers by choosing them from the AD list. Only DLP-enabled computers are eligible to be scanned.

   Click **Next** to continue.

8. Choose a File filter to include only files of the selected type.

   Click **Next** to continue.

9. In the Summary screen that appears, review your choices and then click **Finish** to return to the Discovery Policies page.

10. Check the **Enable** box to be able to use the policy in the Enabled Discovery Scans in the **Discover Data > Scans** table.

See 9.3 "Appliance-Based Discovery Scans" and 9.4 "Agent-Based Discovery Scans" on page 165 for information on attaching policies to scans.

9.3 Appliance-Based Discovery Scans

This section describes the procedure for creating an appliance-based scan and describes the scan definition file, which provides information about the data to be scanned.

9.3.1 Creating an Appliance-Based Discovery Scan

Appliance-based Discovery scans work by mounting one or more remote file shares, connecting to a cloud data store, or establishing a Java Database Connectivity-connection to a database, and then bringing the target files/data across the network to the hosting appliance for scanning. If the appliance is an Inspector, then the results of the scan are aggregated on the DLP Manager. The same Discovery policies can be used for both appliance-based and agent-based scans.

When dealing with network file shares, appliance-based Discovery scans are significantly faster than an agent-based scan (i.e., running an agent scan on a client PC that has the network file share mapped as a local drive). For example, say you have 45 different file shares that you want to scan (SMB, CIFS, and/or WebDAV). Each file share has its own directory structure, so there are several hundred different paths that will be targeted in the scans. You can choose to run all the scans from the DLP Manager, or if you have managed appliances, through any or all of the Inspectors. In either case, you would create a new Discovery scan, attach one or more policies, and then attach a scan definition file that identifies all 45 shares and, alternatively, the folders on each that you want to scan. For each share, you can also assign the DLP Manager or Inspector that you want to host the scan.

Connecting to Cloud Data Stores

When dealing with cloud data stores, you must first connect to the cloud you want to scan. To do this, connect to the appliance on which you want to run the scan against and then specify the credentials used to connect to the cloud respository. You only need to configure the cloud data store credentials once.

To connect to a cloud data store:

1. From the DLP appliance management console, click **Manage System > Servers | Cloud**. The Cloud Settings pane appears.

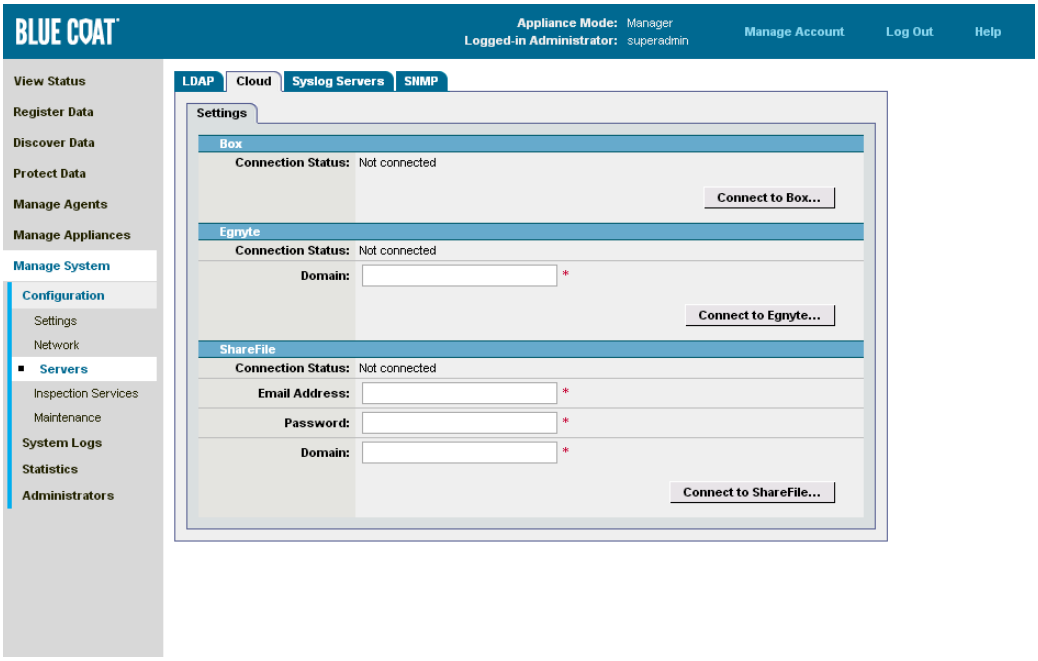


Figure 9.2: Cloud Settings Pane

Note: When connecting to Box, your role determines the files you have access to on Box. Scanning access will be restricted to the same access to files as the role used to configure the Box connection. Box allows one user the admin role. In general, the admin user has access to all the data users have added to Box. Users assigned to co-admin roles have more restricted access to data, and regular users have even more restricted access. To allow for maximum access to scan files on Box, it is recommend to connect to Box with the admin Box account credentials.

2. To connect to box:

   a. Click the **Connect to Box** button. A Web page appears in your Web browser.

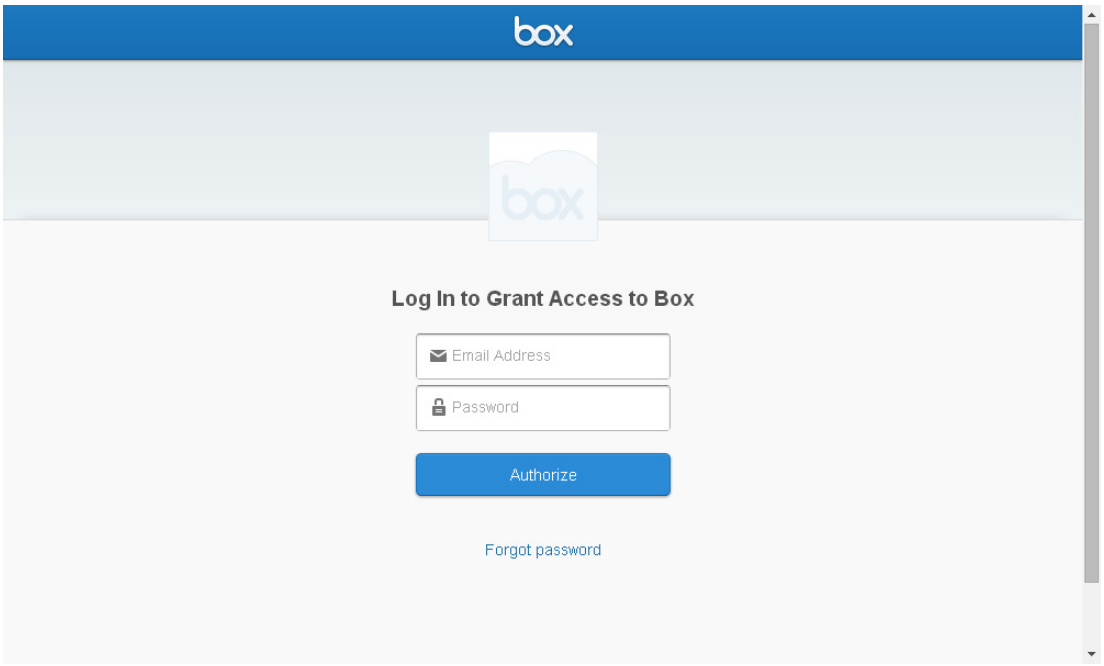


Figure 9.3: Box Log In Screen

   b. Enter your email address and Box password in the provided text boxes.

   a. Click on the **Authorize** button to authorize access. Another screen appears.

   b. Click the **Grant Access to Box** button. Your connection status, user name, and role are displayed in the management console.

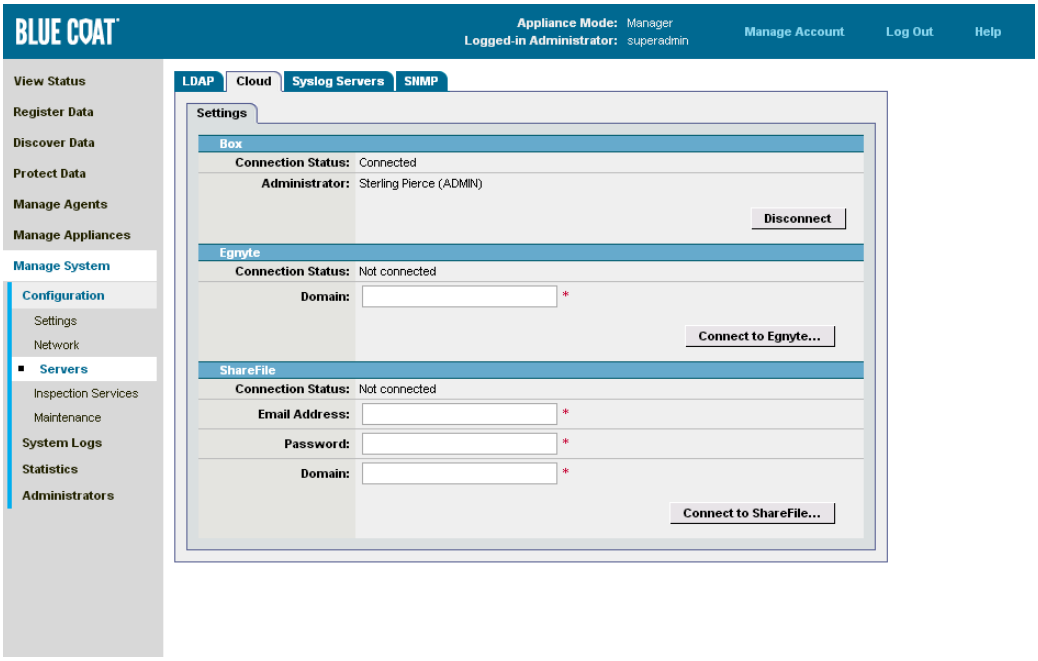


Figure 9.4: Cloud Pane After Logging Into Box

3. To connect to Egnyte:
   a. Enter the domain name assigned by Egnyte (for example, yourcompanyname.egnyte.com) in the Domain box.
   b. Click the **Connect to Egnyte** button. A Web page appears in your Web browser.

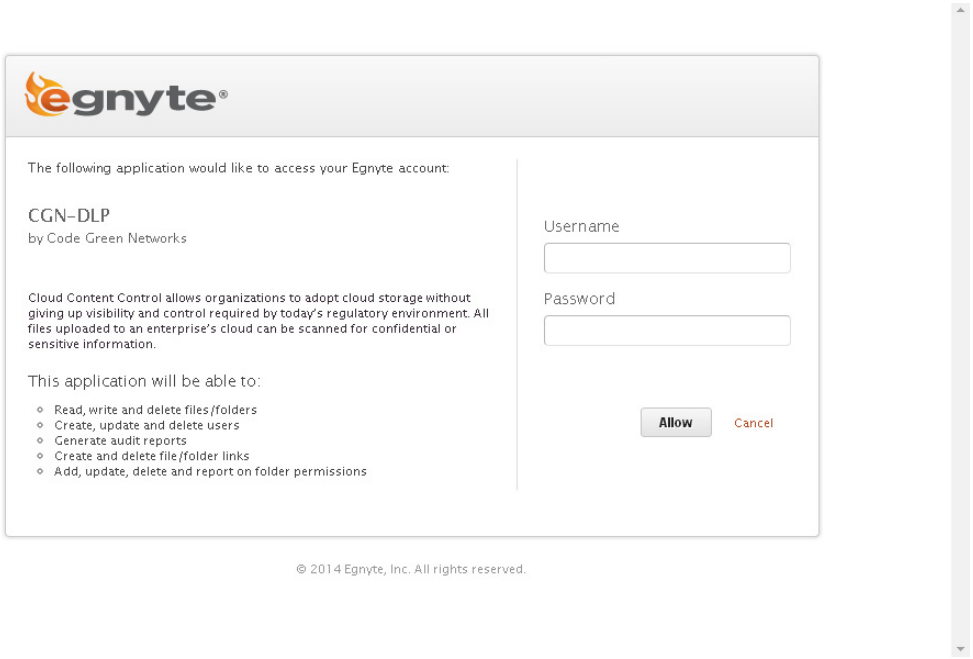


Figure 9.5: Egnyte Log In Screen

c. Enter your Egnyte user name in the Username text box; enter your Egnyte password in the Password text box.

Note: You need to enter your Egnyte user name and not your email address.

d. Click the **Allow** button.

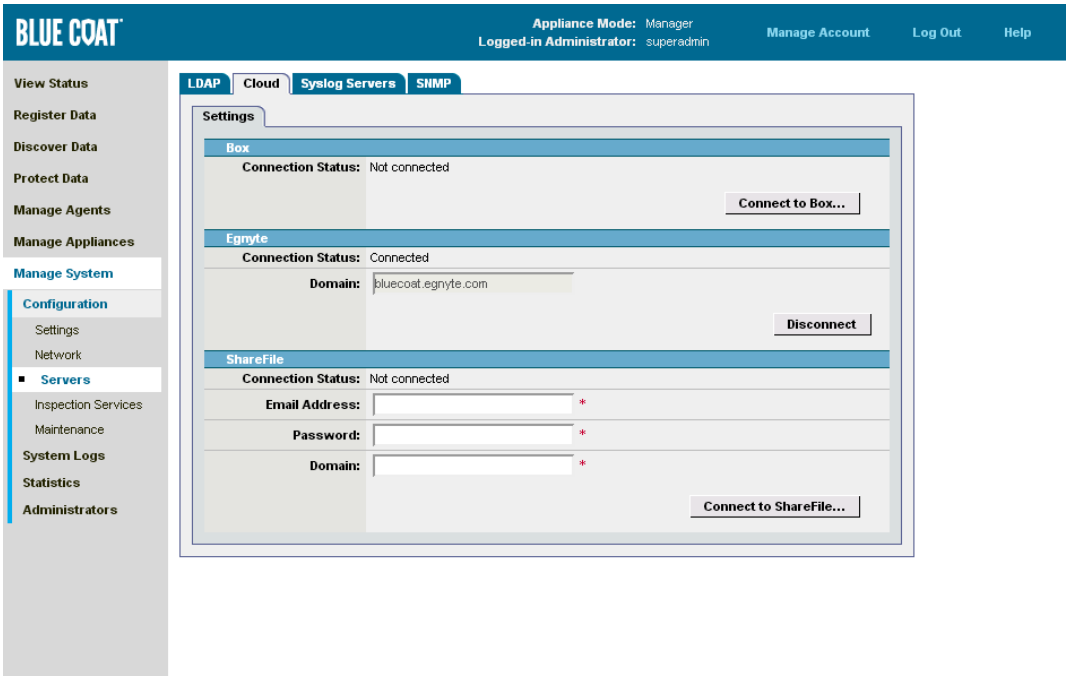


Figure 9.6: Cloud Pane After Logging Into Egnyte

4. To connect to ShareFile:
   a. Enter your email address (for example, name@domain.com) in the User Name text box.
   b. Enter your password in the Password text box.
   c. Enter the domain name assigned by ShareFile (for example, yourcompanyname.sharefile.com)in the Domain text box.
   d. Click the **Connect to ShareFile** button.

After connecting to the cloud data store, you return to the DLP appliance management console.

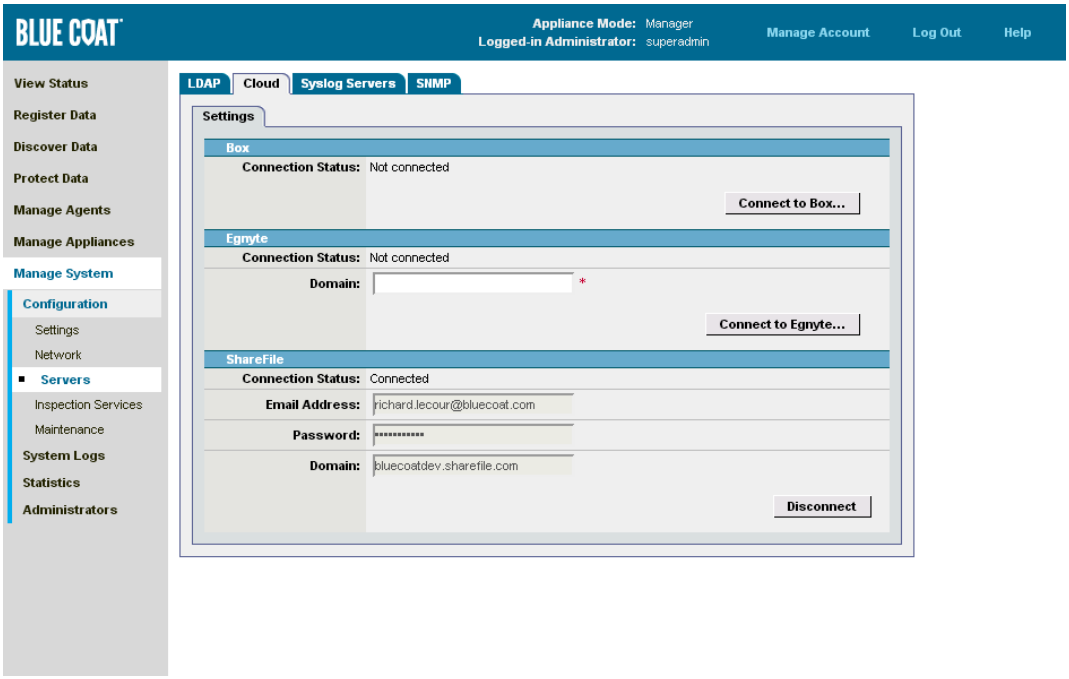


Figure 9.7: Cloud Pane After Logging Into ShareFile

To create an appliance-based scan:

Before creating a scan, be sure to have at least one scan policy that you would like to be used by the scan (see 9.2.1 "Creating a Discovery Policy" on page 144), and a scan definition file (see 9.3.2 "About the Scan Definition File" on page 155).

1. From the DLP appliance management console, click **Discover Data > Scans | Appliance** and then the **Create Scan...** button. The Create a New Discovery Scan wizard is displayed.
2. Give the scan a short name (<15 chars) and description (<256 chars), for example write a summary of the scan parameters, or a note documenting the provenance of the scan. Click **Next** to continue.
3. Choose which policies you want to include:
   - **Apply all enabled discovery policies to this scan**—Rather than specify policies by name, you can choose this option and then enable/disable certain policies to include them in the scan. Note that using this option in conjunction with scheduled scanning may produce inconsistent results depending one which policies are enabled when the scan is run.
   - **Apply specific policies to this scan**—Select one or more existing Discovery policies from the list. Click the plus sign (**+**) button to add the policy.

   Note: The selected policy must be enabled at the time the scan is run.

   Click **Next** to continue.
4. Upload the scan definition file you have created for this scan, as described below.

a. Click the **View the CSV template file** link to open a sample file in a text editor, where you can then add one or more lines to specify the shares/databases/cloud data store you want the DLP appliance-based Discovery to scan.

b. Save the file as a comma-separated text file.

c. Click **Choose File** to copy the file to the DLP Manager. A dialog box appears. Select the edited comma-separated (scan definition) file and then click the **Open** button. The name of the selected file appears in the wizard.

Because the scan definition file is saved as an ASCII file, the login credentials for each share/database will remain in clear text. If you want the credentials masked, leave the user name and password fields blank in the scan definition file and instead type the user name and password in the wizard/Shares screen. If you have multiple shares/databases with login credentials that you want masked, create a new Discovery scan for each different file share/database. Enter a user name and password for the share in the UI, and then create and attach a corresponding scan definition file for each file share/database. The only drawback to this method is that if you have multiple shares/databases with different login credentials that you want masked, you will need to create a Discovery scan and attach a scan definition file for each different file share/database so as to capture the login credentials.

Note: You need to enter the credentials for and connect to a cloud data store before running a scan against it. See "Connecting to Cloud Data Stores" on page 147 for information.

5. Click **Next** and then choose which files to include or exclude from the scan. File type determination is made according to the file properties rather than extensions, which can be faked.

- **No File Filter**—Scan includes all file types (including program files, such as .exe files, which do not contain data). Obviously, this option is inefficient when scanning entire drives. It is more typically used when scanning a particular location that contains a collection of various data files.
- **Included File Filter**—Scan excludes all file types except for those specified here. This option allows you to significantly reduce the number of files to be scanned by targeting only those files most likely to contain data. You can create whatever custom file filters you want using **Register Data > File Filters**, and they will be available in this file filter drop-down.
- **Excluded File Filter**—Scan includes all file types except for those specified here. Use this option to exclude non-data files, for example, or even as a quick way to include only certain files—excluding all files greater than 1MB means you are scanning all files smaller than 1MB. Paths in the Exclude File Filter take precedents over those identified for Include, so, for example, if the same folder is specified for both, the folder will be excluded.
- **Last Modified**—Dates used are from the file properties metadata.

Click **Next** to continue.

6. Enable and set the Schedule option to have the scan start automatically.

Note: Depending on the size of the scan target (and other factors), a Discovery scan may take longer than 24 hours to complete. If this occurs and a Daily Scan is scheduled, the scan will be interrupted and will not complete. Choices in this case include running the scan less frequently, or using a file filter to reduce the number of files scanned (you can also create two or more scans, each targeted at a different filter set).

7. Click **Next** to display the Summary page, and then click **Finish** to save your scan in the Discovery Scan list.
8. Check the **Enable** box for the scan and then click the **Start** icon to initiate the scan. Look at the scan's status indicator to check the scan's progress.

   Note: Click **View Status > Incidents > Discovery** to see any matches you have from the scan.

   Note: When conducting a scan of a file share, the scan creator will be sent an email upon completion of the scan for each share defined in the scan definition file for the scan (so if there are three shares defined in the scan definition file, the scan creator will get three emails, one for each share scanned). The share owner defined in the scan definition file for each share will receive an email if an email address is specified in the share_owner_email_address field in the scan definition file for that share. If you have three shares defined in the scan definition file and two of them have email addresses defined for them, two emails will be sent out upon completion of the scans.

9.3.2 About the Scan Definition File

To manage the versatility of Discovery scans, you need to create and upload a scan definition file that contains a list of the file shares/databases/cloud date stores you want to scan. A scan definition file template is included with the appliance to facilitate usage (see "Viewing the Scan Definition Template File" on page 156 for details). The scan definition file is especially useful for including a large number of file shares/databases under the umbrella of a single Discovery scan.

The scan definition file provides the login credentials for mounting the share/database/cloud data store type, defines the share format (CIFS, NFS, or SMB), CMS type (WebDAV or Documentum), or database (Oracle, Microsoft SQL, MySQL, PostgresSQL, DB2, Sybase, or Informix), and provides other information required to access the share/database. You can enter the username (in the user_name field) and password (in the password field) required to access the share/database to scan. If you don't enter these credentials, the credentials entered in the Shares pane (**Discover Data > Scans | Appliance | Edit** scan) will be used. For cloud-store scans, you need to enter the cloud-store credentials when connecting to the cloud (see "Connecting to Cloud Data Stores" on page 147 for information).

To scan Windows shares, configure scans for CIFS repositories; to scan Sharepoint servers, configure scans for WebDAV repositories. For more information on the supported share formats, see 9.1.5 "Supported File Shares/Databases" on page 143.

You can attach the same scan definition file to different Discovery scans, if associating different policies with different scans, or create a number of different scan definition files (i.e., a different collection of file shares and locations) to attach to different scans

in the Discovery Scan List. When you run the scan from the Discovery Scan List, it will apply the schedule, policies, and filters specified in the scan to the locations specified in the scan definition.

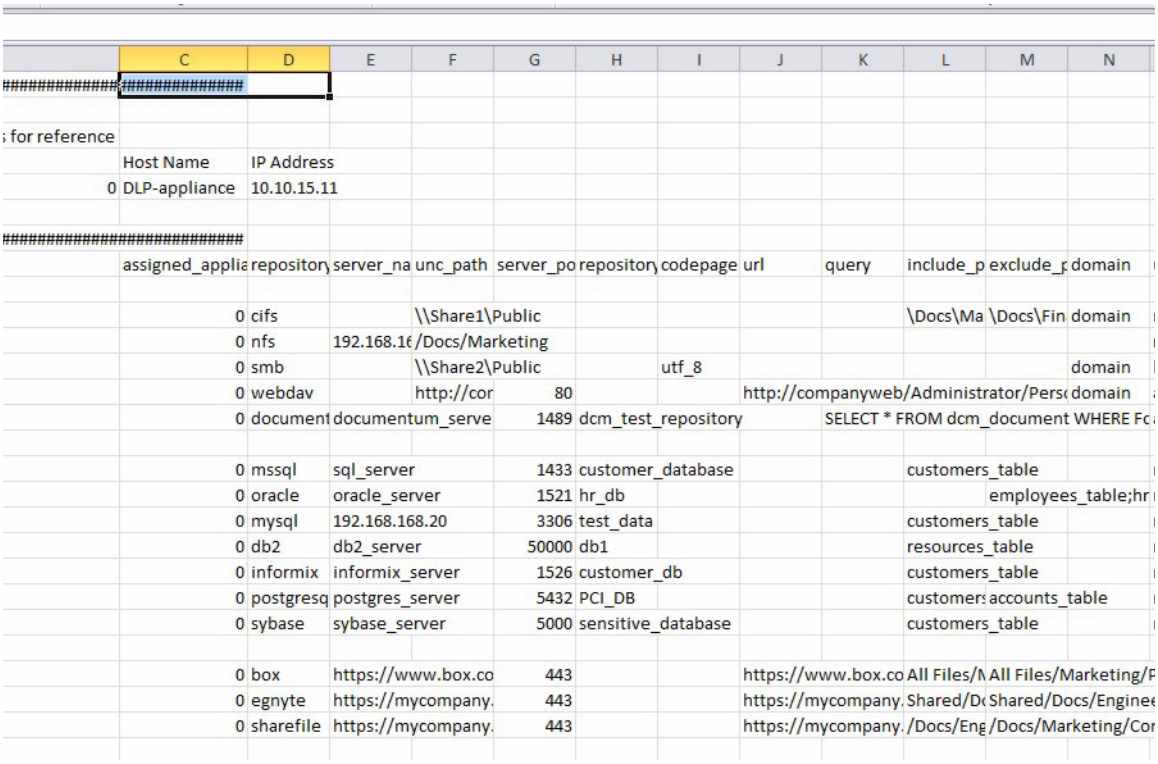
The scan definition file also allows you to throttle, or control, the network bandwidth consumed by the scan. For details on throttling network bandwidth, see "Controlling Discovery Scan Throughputs" on page 161.

Viewing the Scan Definition Template File

Perform the steps below to display the scan definition template file included with the appliance.

To view the scan definition template file:

1. From the management console, click **Discover Data > Scans > Appliance**.
   a. Create a new scan or edit an existing scan and then click the Shares tab. Click the **View CSV template file** link to open the sample file in a text editor. Include one line in the scan definition file for each file share/database/cloud data store you want to include in the Discovery scan.



	C	D	E	F	G	H	I	J	K	L	M	N
##########	##########											
; for reference												
	Host Name	IP Address										
0	DLP-appliance	10.10.15.11										
##########												
	assigned_applia	repository	server_na	unc_path	server_po	repository	codepage	url	query	include_p	exclude_p	domain
	0	cifs		\\Share1\Public						\Docs\Ma	\Docs\Fin	domain
	0	nfs	192.168.16	/Docs/Marketing								
	0	smb		\\Share2\Public			utf_8					domain
	0	webdav		http://cor	80			http://companyweb/Administrator/Pers				domain
	0	document	documentum_serve		1489	dcm_test_repository			SELECT * FROM dcm_document WHERE Fc			
	0	mssql	sql_server		1433	customer_database				customers_table		
	0	oracle	oracle_server		1521	hr_db					employees_table;hr	
	0	mysql	192.168.168.20		3306	test_data				customers_table		
	0	db2	db2_server		50000	db1				resources_table		
	0	informix	informix_server		1526	customer_db				customers_table		
	0	postgresq	postgres_server		5432	PCI_DB				customers	accounts_table	
	0	sybase	sybase_server		5000	sensitive_database				customers_table		
	0	box	https://www.box.co		443			https://www.box.co		All Files/M	All Files/Marketing/F	
	0	egnyte	https://mycompany.		443			https://mycompany.		Shared/Dc	Shared/Docs/Enginee	
	0	sharefile	https://mycompany.		443			https://mycompany.		/Docs/Eng	/Docs/Marketing/Cor	

Figure 9.8: Scan Definition (CSV) Template File

2. Save the file as a comma-separated text file. This is your scan definition file.

3. Click the **Browse** button to locate the scan definition file and upload it to the DLP appliance.

The table below describes each field and provides an example of the syntax.

Table 9.1: Scan Definition File Field Descriptions and Syntax Examples

Field Name -(applies to)	Parameter	Example	Notes
description -all	[text]	Scan CIFS share	Can be used as a summary of the purpose or files included in the scan.
enable_scan -all	enable disable	enable	Use when the same scan definition file is being used in different Discovery scans. In this way, you can direct one Discovery scan to scan one set of targets and disable scans on the rest.
assigned_appliance -all	[appliance_ID]	0 1 2 3	Use to assign a particular scan to a particular appliance, for example, if you want to distribute a scan across Inspectors or dedicate a single appliance for all Discovery scans. You can find the ID for each appliance by viewing the ID field in the scan definition (CSV) template file. CI Manager = 0 1st Inspector = 1 2nd Inspector = 2
repository_type -all	[text]	cifs nfs smb webdav documentum mssql oracle mysql db2 informix postgresql sybase box egnyte sharefile	Identify the protocol (or method) of the target file repository or database.

Table 9.1: Scan Definition File Field Descriptions and Syntax Examples

Field Name -(applies to)	Parameter	Example	Notes
server_name -NFS -Documentum -Microsoft SQL -Oracle -MySQL -DB2 -Informix -PostgreSQL -Sybase -Box -Egnyte -ShareFile	[ip address]	192.168.100.1 10.10.10.1 sql_server https://www.box.com	The IP address or name of the NFS, Documentum, or other server to connect to. For cloud data stores, the cloud data store's URL
unc_path -CIFS -SMB -NFS -WebDAV	[location]	\\share1\public \\share2\public /docs/marketing http://company.com	NOTE: Do not use a trailing \.
server_port -WebDAV -documentum -Microsoft SQL -Oracle -MySQL -DB2 -Informix -PostgreSQL -Sybase -Box -Egnyte -ShareFile	[port]	80 1489 1443 443	Specify the port number configured on your server for access.
repository_name -documentum -Microsoft SQL -Oracle -MySQL -DB2 -Informix -PostgreSQL -Sybase	[repository]	dcm_test_repository customer_database sensitive_database	Reflects the repository name.

Table 9.1: Scan Definition File Field Descriptions and Syntax Examples

Field Name -(applies to)	Parameter	Example	Notes
codepage -SMB	[code]	utf_8	valid codes: utf_8 iso_8859_1 iso_8859_2 iso_8859_3 iso_8859_4 737 Greek 850 Latin 1 852 Latin 2 932 Windows Japanese 936 Simplified Chinese 949 Korean 950 Big5 1251 Cyrillic
url -WebDAV -Box -Egnyte -Sharefile	http://[hostname]/	http:/company/ https://www.box.com https://mycompany.egnyte.com https://mycompany.sharefile.com	HTTP or HTTPS support may be limited as per application (SharePoint, exchange).
query -Documentum	[query string]	SELECT object_name, title FROM dcm_document WHERE FOLDER (ID('folder id')) AND title LIKE '%sr% select * from dcm_document where folder ('/Administrator/personal')	Uses Documentum Query Language (DQL) to identify the Docbase and documents to include in the scan. Note: validate the query prior to saving it in the scan definition file.
include_paths -CIFS -Microsoft SQL -MySQL -DB2 -Informix -PostgreSQL -Sybase -Box -Egnyte -ShareFile	[\path1];[\path2]	\Docs\legal;\Docs\public customers_table All Files/Marketing;All Files/Finance Shared/Docs;Private/Engineering/Docs/Engineering;/Docs/Marketing	Delimit paths with semicolons. Only the specified locations will be crawled. If blank, all paths will be crawled. Use with exclude_paths to prevent crawling of subdirectories. See "Including and Excluding Data from Scans" on page 162 for more information.
exclude_paths -CIFS -Oracle -PostgreSQL -Box -Egnyte -ShareFile	[\path1];[\path2]	\Docs\Marketing;\Docs\Engineering employees_table;hr_table accounts_table All Files/Marketing/PRD;All Files/Marketing/Contacts;	If include_paths is blank, then all paths will be scanned except those specified here. See above.
domain -CIFS -SMB -WebDAV	[text]	domain	

Table 9.1: Scan Definition File Field Descriptions and Syntax Examples

Field Name -(applies to)	Parameter	Example	Notes
user_name -CIFS -SMB -NFS -WebDAV -Documentum -Microsoft SQL -Oracle -MySQL -DB2 -Informix -PostgreSQL -Sybase	[text]	username ,, (empty field) login_with_guest_credential	If this field is empty, the user name and password specified in the GUI will be used. Note that "login_with_guest_credential" is a key term, used to log on to the target with a guest credential (as opposed to a specified user name, including guest).
password -CIFS -SMB -NFS -WebDAV -Documentum -Microsoft SQL -Oracle -MySQL -DB2 -Informix -PostgreSQL -Sybase	[text]	password ,, (empty field)	Note: Passwords are stored in clear text. Leave this field empty to use a user name and masked password specified in the GUI.
peak_max_mbps -all	[valid range for a limit is 0.001 to 8000]	5, 10 Specify "0" to suspend scanning; leave the field empty ,, or specify the keyword "unlimited" to impose no limit.	Mbps. Limits the rate at which data is sent over the network from the file share to the appliance for inspection during peak hours (as defined in the schedule page of the GUI). See "Controlling Discovery Scan Throughputs" on page 161 for more information.
peak_max_items_per_min -all	[valid range for a limit is 0.1 to 6000]	12, 50, 100 Leave the field empty ,, or specify the keyword "unlimited" to impose no limit.	Files/records. Limits the number of files/records per minute that are sent over the network from the file share to the appliance for inspection during peak hours (as defined in the schedule page of the GUI).
off_peak_max_mbps -all	[valid range for a limit is 0.001 to 8000]	10, 15, 100 Specify "0" to suspend scanning; leave the field empty ,, or specify the keyword "unlimited" to impose no limit.	Mbps. Limits the rate at which data is sent over the network from the file share to the appliance for inspection during non-peak hours (as defined in the schedule page of the GUI).

Table 9.1: Scan Definition File Field Descriptions and Syntax Examples

Field Name -(applies to)	Parameter	Example	Notes
off_peak_max_items_per_min -all	[valid range for a limit is 0.1 to 6000]	Leave the field empty ,, or specify the keyword "unlimited" to impose no limit.	Files/records. Limits the number of files/records per minute that are sent over the network from the file share to the appliance for inspection during non-peak hours (as defined in the schedule page of the GUI).
share_owner_email_address	[email address]	share_owner@example.com	If you specify an email address, a notification message will be sent to the email address when a Discovery scan has completed scanning the share. If left blank, no email will be sent for this share. By default, scan owners are always notified when a scan has completed.
optional_arguments			Use if directed to by Technical Support personnel.

Include one line for each file share you want to include in the Discovery scan. Note that different types of file shares/databases/clouds will require different supporting details; in most cases, some of the fields will be blank. Although they may be unused for a given share/database/cloud type, be sure to retain these empty fields by delimiting fields with commas, for example:

```
name,enable,0,,,,,next,more,,,done
```

Note: If you edit the scan definition (CSV) template file in a spreadsheet program, such as Excel, be sure to save it as CSV (ASCII only). You can also create the scan definition file using an ASCII editor. Copy the header line shown in the scan definition (CSV) template file to a text file saved with the .CSV extension and then provide the values relevant for the file share/database/cloud to be scanned.

Controlling Discovery Scan Throughputs

By default, there is no set limit on how much of a file server's resources or the network's bandwidth a Discovery scan will consume when reading and sending files from the file share/database/cloud data store to the DLP appliance for inspection. It will simply work as fast as the hardware and network allow to complete the task. On a high-capacity LAN or a high-end server that is not busy and where the defined file shares/databases/cloud data store do not include a huge file store, this may be fine.

On the other hand, you can control both the network bandwidth used and the disk access rate of the file share/database/cloud data store by setting a limit for one or both in the scan definition file that is attached to the Discovery scan. In addition, you can define "peak" and "off-peak" times so a scan can automatically run at its fastest when network traffic and/or server usage is light (referred to as "off-peak"). You can use

these features to help avoid overloading servers and networks with Discovery scans. These features can also be used to regulate the bandwidth consumed for scans conducted over a WAN link, for example to prevent traffic spikes or to keep Discovery scans within a set WAN allocation budget.

However, be aware that limiting Discovery scan throughput can significantly reduce Discovery scan performance and extend the time required to complete scans. When deciding to throttle scan throughput, consider whether data is scanned over a relatively low-bandwidth WAN link (for example, data stored on cloud data stores and remote servers) or a higher bandwidth (typically) LAN link (for example, data stored on local servers or stored on hybrid-clouds, where data is stored on local servers accessed via the cloud-data-store authentication service and Web interface). For data accessed over LAN connections, it might not be necessary or advisable to throttle scan throughput.

- Set throughput limits (**peak_max_mbps** and **off-peak_max_mbps** in the scan definition file) to control the amount of bandwidth used. This limit is expressed as megabits per second (Mbps).
- Set an items limit (**peak_max_items_per_min** and **off-peak_max_items_per_min** in the scan definition file) to govern how many files per minute the server will access, or the number of database records are read. This limit will prevent the server from serving the scan requests to such an extent that other access requests are slowed or prevented.
- Define peak and non-peak time on a per-scan basis in the Discovery scan to which the scan definition will be attached. In addition to reflecting office hours, you can create non-contiguous peaks, for example to accommodate periodic routines, such as backups or other sorts of network scans.

Including and Excluding Data from Scans

You can specify paths you want to include or exclude in scans. (For databases, you specify the tables to include or exclude.) Specify the paths to include in scans in the include_paths field; specify the paths to exclude in the exclude_paths field (in the row associated with the desired share/database/cloud). Use the format shown in the sample scan definition file. For file and content-management systems and clouds, delimit the paths with semi-colons (;).

Below is information about how to specify paths based on the directory structure that appears on several cloud data stores. This information reflects the default directory structure on the cloud data stores and might not reflect any custom configurations.

Box

1. To include or exclude a directory named Marketing that appears on Box as: All Files>Marketing.

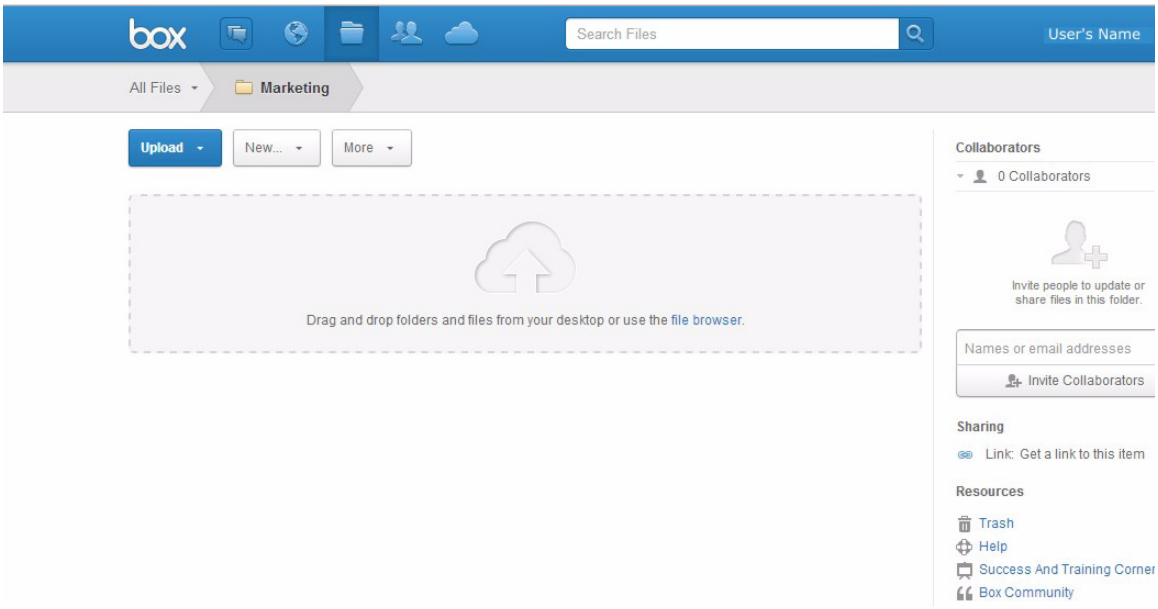


Figure 9.9: Box Directory Representation

enter:

```
All Files/Marketing
```

Egnyte

1. To include or exclude a directory named "Docs" that appears on Egnyte as: Shared / Docs

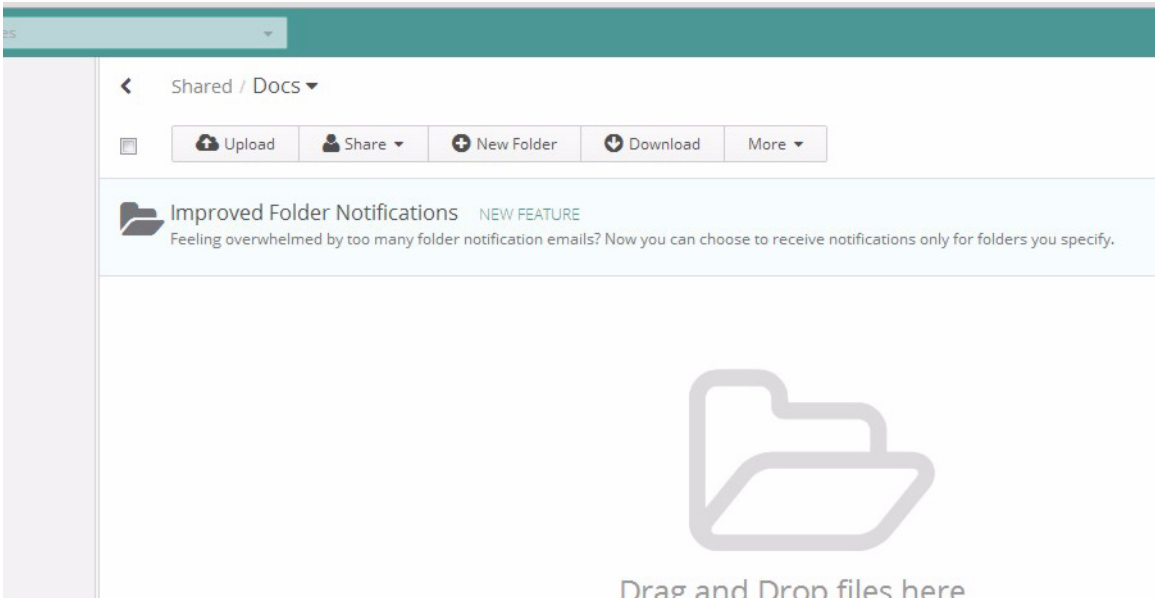


Figure 9.10: Egnyte Directory Representation

enter:

```
Shared/Docs
```

ShareFile

1. To include or exclude a directory named "Marketing" that appears on ShareFile as:
   Docs -> Marketing

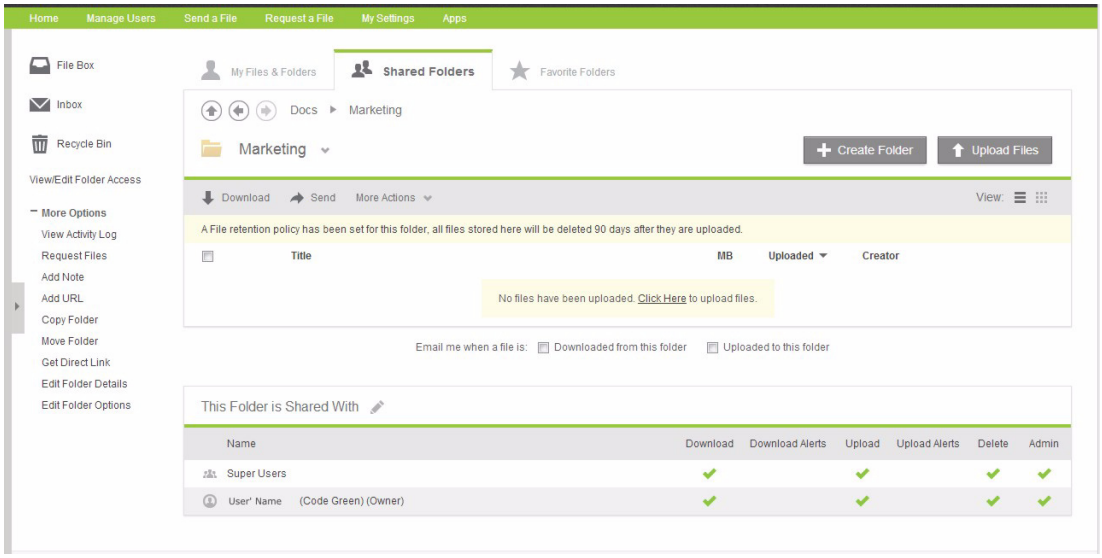


Figure 9.11: ShareFile Directory Representation

enter:

```
/Docs/Marketing
```

9.4 Agent-Based Discovery Scans

Agent-based Discovery scans occur on the targeted endpoint, where the installed agent uses the endpoint's resources to perform the scan. Agents can be managed by the DLP Manager and/or Inspectors.

9.4.1 Creating an Agent-Based Scan

As with appliance-based Discovery scans, you can configure different scans to target different groups of computers, users, file locations, and file types. In addition, you can attach one or more policies to each scan. The same Discovery policies can be used for both appliance-based and agent-based scans.

Note: Agent-based scans and policies both allow you to define which computers to include, and both support Active Directory groups. A policy can identify computer groups and the scan can define computer groups. The intersection of these computer groups defines which computers are included in the scan.

When you run a scan targeting multiple endpoints, the scan starts on all the endpoints at the same time. Results are aggregated at the DLP Manager. To stagger agent Discovery scans, you can create multiple scans, each of which targets a different group, and schedule them to run at different times.

To create an agent-based scan:

1. From the DLP appliance management console, click **Discover Data > Scans | Agent**. The default Discovery scan appears in the table.
2. Click the **Create Scan...** button. The Create a New Discovery Scan wizard appears.
3. Give the scan a short name (<15 chars) and description (<256 chars), for example, a summary of the scan parameters, or a note documenting the provenance of the scan. Click **Next** to continue.
4. Choose which Discovery policies you want to attach to the scan by choosing **Apply all enabled discovery policies to this scan**, or choose **Apply specific policies to this scan** and then select the specific policy or policies from the list. Note that in either case, the policy will only be enacted in the scan if it is enabled at the time the scan is run (manually, and for scheduled scans). Click **Next** to continue.
5. Choose the computers and folders to scan (specify locations either by inclusion, i.e., specifying only those you want to scan, or by exclusion, i.e., every location except those specified will be included in the scan). Note that as with the other scan settings, these settings are global—they will apply to all policies that are attached to the scan.

   - **Discover data across all domain computers—**eligible computers include all DLP-enabled clients connected to any domain (computers configured for a Workgroup will not be included), and accessible from the DLP appliance.
   - **Discover data only on specific computers—**select computers/Computer Groups from your Active Directory listing. You can include any combination of groups and individual computers by choosing them from the Active Directory list (it will appear a second after entering the first letter in the field). Only DLP-enabled computers are eligible to be scanned.

   Paths to Include—

   - **Include all paths on the selected drives**—Default; starts at the root and includes all files on each of the drives (local, network, or all) specified below. Obviously, this option takes the most time, much of which is spent on non-data files, such as those used by programs and the operating system. Consider using this option in combination with a filter, such as Exclude paths, File Types, and/or Last Modified date.
   - **Specify which paths to include**—Specify one or more folders to scan, typically those used for data storage, such as My Documents. Supports the * wildcard, for example, `C:\Users\*` to include all users on the computer.

   Paths to Exclude—

   - **Do not exclude any paths**—Default; the entire drive will be scanned.

- **Specify which paths to exclude**—specify folders to skip, for example, `c:\Windows`. All sub-folders from the path specified down will be excluded from the scan. This option is also useful for scanning all locations *except* those specified here. Supports the * wildcard.

Drives—

- **Local drives only**—Includes all physically connected devices, including hard drives, CD/DVD, and USB-connected mass-storage devices. This option is especially useful when scanning a series of clients that do not all share the same configuration. Each client configuration is assessed and the scan is run accordingly.
- **Network drives only**—Includes only network drives that have been mounted, i.e., mapped, to the client. Exactly what is included in the scan will vary according to the particular configuration of any given client.

Note: To avoid duplicate scanning of the network share, only choose **Network drives** or **All drives** if you are using a client to host a remote scan, for example, of a Windows fileshare. If you select this option for a scan that includes multiple clients, and each client has the same network file share mapped, that share would be scanned repeatedly -- one time for every client.

Note: Discovery remediation actions are not supported for agents that discover files on a mapped drive. The appliance will not generate an action request and the discovery incident management UI will not show remediation action options for these incidents even if these actions were specified in the policy configuration.

- **All drives**—Includes all drives; will vary according to the particulars of each client.

6. Click **Next** and then choose which files to include or exclude from the scan. File type determination is made according to the file properties rather than extensions, which can be faked.

- **No File Filter**—Scan includes all file types (including program files, such as .exe files, which do not contain data). Obviously, this option is inefficient when scanning entire drives. It is more typically used when scanning a particular location that contains a collection of various data files.
- **Included File Filter**—Scan excludes all file types except for those specified here. This option allows you to significantly reduce the number of files to be scanned by targeting only those files most likely to contain data. You can create whatever custom file filters you want using **Register Data > File Filters**, and they will be available in this file filter drop-down.
- **Excluded File Filter**—Scan includes all file types except for those specified here. Use it to exclude non-data files, for example, or even as a quick way to include only certain files—excluding all files greater than 1MB means you are scanning all files smaller than 1MB. Paths in the Exclude File Filter take precedents over those identified for Include, so, for example, if the same folder is specified for both, the folder will be excluded.
- **Excluded File Attributes**—Scan skips all files with the selected attribute(s). For example, you may want to skip System files, which are unlikely to contain data. Alternatively, this option can be used to scan only files with a given attribute—in this case, you would exclude all files with an attribute other than your target, for example, to focus a scan on Hidden files only, you could exclude Archive, System, and read-only files.

• **Last Modified Range**—Dates used are from the file properties metadata.

Click **Next** to continue.

7. You can set the scan to recur at specified intervals. To set up a recurring scan, check the Enable box and then specify a start time and frequency. For example, you can configure scans that recur weekly on a certain day of the week, monthly, and so on. Click **Next** to continue. The Summary screen is displayed.
8. Click **Finish** to save your scan in the Discovery Scan list.
9. Check the **Enable** box for the scan and then click the **Start** icon to initiate the scan. The scan will launch at the next Agent polling interval, or you can also trigger the agent update by clicking **Manage Agents** > **Settings**.

   Note: Click **View Status > Incidents > Discovery** to see any matches.

9.5 Scan Status

The status of each scan in the Discovery Scan List is shown in the Progress column. Click **Discover Data > Scans** to display the list.

- **Pending**—Indicates that the scan has been started at the DLP appliance but has not yet been enacted at the scan target or the Inspector.

  Note: Pending may indicate that the Discovery service has not been enabled on the DLP Manager and/or Inspectors (click **Manage System > Inspection Services | Discovery** to enable the service).

- **In progress**—Indicates that at least one scan in a group of targets is on-going.
- **Paused**—Indicates that the scan has been manually paused using the **Pause** control, and that no scans are in progress or have been stopped.
- **Completed**—Scan has finished running on all targeted file shares/databases/cloud data store or endpoints.
- **Will be run at next scheduled time**—Indicates that the scan has not been manually started (applies only if the Recurrence option has been enabled on the **Schedule** tab of the scan instance).
- **Stopping**—Indicates that the scan has been manually stopped using the **Stop** control, and that no scans are in progress.
- **Scan has been disabled**—Indicates that the **Enable** check box is not active. Enable that option and then manually start the scan.
- **Disabled**—Indicates that at least one target computer or DLP appliance is reporting a disabled state.
- **Scan has not been started**—Indicates that the scan configuration has changed, but that the scan has not been manually started (applies only to scans that have not been scheduled).
- **Not Applicable**—Indicates the number, if any, of endpoints/Inspectors that were not relevant to the scan. For example, if you have a population of 100 computers, but used an Active Directory group to target the scan at 80 computers, the status for the remaining 20 would be Not Applicable. The same is true for Inspectors,

they all received the same scan definition file, but only some of them were directed to conduct a scan.

- **Errors**—Number of errors, if any, encountered during the scan. You can refer to the **Status** field and the scan statistics to debug a scan (for instance, in the case where the number of files scanned does not match the expected number of files). You can also use the provided information to get more specific and detailed information and statistics about a scan. To view scan status and statistical information:
  - Hover the pointer over the **Status** field for the desired scan to display error information about the scan (appliance- or agent-based), or click the **Stats** icon and download a file containing statistics about the scan.
  - Click **Manage Appliances** and then the **Stats** icon to find out about errors in an appliance scan.
  - Click **Manage Agents** and then the **Stats** icon to find out about errors in an agent scan.

9.6 Configuring Actions

This section describes the workflow and remediation actions that can be implemented automatically or as part of the incident-review process.

9.6.1 Workflow Actions

A workflow action is attached to a policy to define the workflow, notifications, logging, and copy retention that occur whenever the policy detects a match. The DLP appliance provides seven ready-made workflow actions. You can also create your own actions.

Note: Workflow actions created for Discovery policies are shared with Data-Usage policies, and vice versa, therefore some settings may apply only to one policy type or the other.

Creating a New Workflow Action

You may modify an existing action or click the **Discover Data > Actions | Create Action...** button to create a new action. The procedure below describes how to create a new workflow action. To edit an existing workflow action, click on the **Edit** button for the desired action. The Edit a Workflow Action window is displayed. See the procedure below for more information.

To create a new workflow action:

1. From the DLP appliance management console, click **Discover Data > Actions**. The default workflow actions appear in the table.
2. Click on the **Create Action...** button. The Create a New Workflow Action wizard is displayed.

3. Give the action a short name (<15 chars) (each action must have a different name) and a description (<256 chars).

The notification feature controlled by the Enable Notify check box is not used for Discovery. However, it is used by Data-Usage policies and notification does occur when Data-Usage policies detect Incidents. Because the workflow actions are shared by Data-Usage and Discovery, do not change the settings for the Enable Notify check box when configuring for Discovery only. If you change this setting, your change may impact and adversely affect Data-Usage policies that use this feature.

Note: When conducting a Discovery scan of a file share, there are implicit email notifications for the scan creator and the scan owner. The scan creator will be sent an email upon completion of the scan for each share defined in the scan definition file for the scan (so if there are three shares defined in the scan definition file, the scan creator will get three emails, one for each share scanned). The share owner defined in the scan definition file will receive an email if an email address is specified in the share_owner_email_address field in the scan definition file for each share that has an email address defined for it. If you have three shares defined in the scan definition file and two of them have email addresses defined for them, two emails will be sent out upon completion of the scans.

4. Check the Retain Copy Enable box to indicate whether the action is set to save a copy of the inspected file or a subset of any matching database records on the DLP appliance.
5. Check one or more of the Syslog Server boxes to indicate whether the action will send a log to the syslog server. Note that one or more log servers must be configured for this to occur. Click **Next** to continue.
6. Specify the default settings for all incidents that are created by a policy with this workflow action.
    a. Select **New** to set the status for a new incident to New; select **Closed** to set the status for a new incident to closed.
    b. Choose the desired default severity for new incidents from the **Severity** drop-down menu.
    c. Choose the desired priority level for new incidents from the **Priority** drop-down menu.
    d. Specify the default assignee for new incidents. You can assign new incidents to groups and/or individuals. To assign new incidents to a group, check the **Group** box and choose the desired group from the drop-down menu. To assign new incidents to an individual, check the Individual box and select the desired individual from the list. To assign new incidents to other administrators, select **Other Administrators** and choose the desired administrator from the drop-down menu. Click **Next** to continue.
7. If you selected the Retain Copy option, specify whether a copy of the inspected content should be retained on the appliance.
    a. Select **Do not delete** if you do not want to delete inspected content. Select **Delete if disk space is needed** to delete inspected content when disk space is required. To specify a period of time to retain inspected content, select **Keep until incident has been closed for** and then choose the

desired period (days, week, months, quarters, or years) from the drop-down menu and enter the desired number. Click **Next** to continue.

8. Review the settings defined for the action. To save the settings, click **Finish**; to return to the previous screens in the wizard to make changes, click **Back**.

9.6.2 Remediation Actions

You can include remediation actions in policies. The system includes the following pre-defined remediation actions: copy, move, and delete. You can configure these actions to be performed by an incident reviewer or implemented automatically without any user intervention (see 9.2.1 "Creating a Discovery Policy" on page 144 for information). You can also create your own "custom" remediation actions (as described below).

About Remediation Actions

Before you run a scan that includes remediation actions, you should run some test scans and evaluate the results to make sure you are identifying the correct data. If you receive unexpected results, modify the policies and/or the locations specified in the scan to refine the results. Then, you can go back and include remediation actions in the policies associated with the scan.

Warning: The delete remediation action, when implemented on a file, cannot be undone. Though you can undo move actions, this might not be practical if dealing with many incidents. Exercise caution when using the move and delete actions. It is generally not recommended to execute these actions automatically unless you're certain about the setup and the likely results.

Creating a New Remediation Action

Any custom remediation actions you create are displayed in the Remediation Action screen (**Discover Data > Actions | Remediation).** Note that the Remediation Action screen does not display the pre-defined remediation actions; it only displays any custom actions you create.

A new remediation action is defined as a custom script that runs either on an appliance or agent. The Action Type setting determines whether the remediation action is intended to run on an appliance or an agent. Once selected, the Action Type cannot be changed.

You may create a remediation action object without uploading a script at creation time. However, you will see an indication in the Action list that the action is not fully defined, and you will not be able to use it in a policy until a script is uploaded. Once a script has been uploaded to the appliance, you can download the script at any time, allowing you to modify and re-upload the script at will.

Do not select any of the Script Options unless the script can truly handle these options. Doing so will cause the appliance to run the script with these options, and you may receive different results than expected.

To define a new remediation action:

1. From the DLP appliance management console, click **Discover Data > Actions | Remediation.**
2. Click the **Create Action...** button. The Create a New Remediation Action window is displayed.
3. Give the action a short name (<15 chars) and description (<256 chars), for example, describe the action to be performed.
4. From the Action Type drop-down menu, choose **Appliance** if the action is intended to run on an appliance; choose **Agent** if the action is intended to run on a Windows agent.
5. Click the Choose File button and then locate and open the pre-defined script to implement the action.
6. Enter any arguments for the script in the Script Arguments field.
7. Select the desired script options:
   a. Select **Requires a vault** if the script supports this option. If you enable this option and choose this action for a policy, the option for choosing a vault will be available for the policy. For example, if you want to move a file with your custom action to a designated vault, you would select this option.
   b. Select **Supports leaving text file with replacement message** if the script supports this option. If you enable this option and choose this action for a policy, the option for leaving a text file with message will be available for the policy upon execution of the action.
   c. Select **Support ability to Undo** if the script supports this option. If you enable this option and select this action for a policy, users will be able to undo the action (such as copy or move) while reviewing any incidents associated with this action.
8. Click **OK**.

9.6.3 Defining a Vault

You need to define at least one vault before you define a policy that includes a move, copy, or custom action that requires a vault. A vault is typically a secure directory on a file server in which you can store sensitive information.

To define a vault:

1. From the DLP appliance management console, click **Discover Data > Actions | Vaults.** The Vaults table will be displayed.

2. Click the **Create Vault...** button. The Create a New Vault window will be displayed.
3. Give the vault a short name (<15 characters) and description (<256 characters), for example, provide information about the file server that will contain the vault.
4. Enter the Universal Naming Convention (UNC) path for the vault/destination.
5. Enter the user name and password required to access the destination; re-enter the password to confirm it.
6. Enter the domain name for the destination. Click **OK**.

   Note: Make sure that permissions are correctly configured to allow access to the specified destination.

10 Backing Up the DLP appliance

The DLP appliance automatically creates a backup of system files and Incidents each night. After ten nights, the oldest backup is replaced with the newest, so a 10-day archive should be available. In addition, you can run a manual backup at any time. You can also export Incidents and System Logs using the management console user interface. The same is true for security certificates. You can also back up the file containing the data that triggered the Incident from the DLP appliance. Contact Blue Coat Systems technical support for more information.

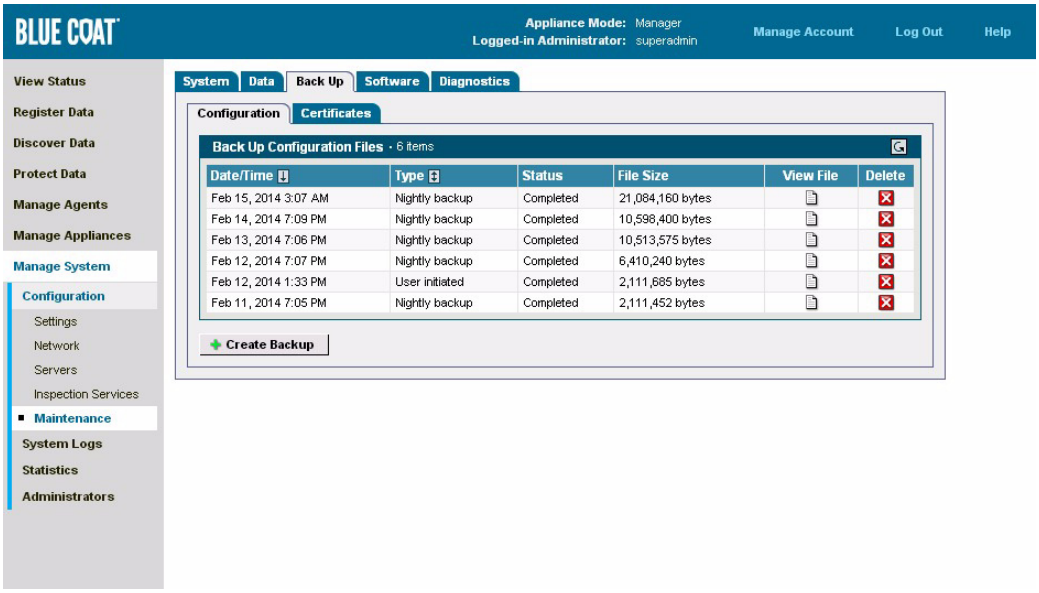


Figure 10.1: Backups are created nightly and appear in this list. Run a manual backup by clicking the **Create Backup** button.

10.1 Backing Up the System Configuration

This section describes how to perform a standard system configuration backup and how to back up the DLP appliance security certificates.

10.1.1 Performing a Standard Backup

You can manually back up the following files and databases:

- The DLP appliance database and configuration files
- Incidents (but not retained copies) and reports, system and event logs
- Registered data configuration (but not the actual external data) and access credentials

To back up the DLP appliance configuration files:

1. In the management console, click **Manage System > Maintenance | Back Up**.
2. Click the **Create Backup** button to start the backup routine.

   Backups are archived on the appliance, but should be saved on a machine other than the appliance:

   a. Click the **View** icon and when prompted, save the file to your local machine.

10.1.2 Backing Up the DLP appliance Security Certificates

If you have a DLP appliance configured for Manager mode, Blue Coat Systems recommends that you export your DLP appliance certificates to a secure location. If you ever need to restore or replace the appliance, having the original certificates means you will not need to re-sign the Inspectors and/or agents that report to it.

The difference between backing up your security certificates and exporting them is that the backup procedure includes all certificates, including private keys for the DLP Manager and Inspector. Exported certificates include only those used to register an Inspector.

To back up all DLP appliance certificates:

1. From the management console, click **Manage System > Maintenance | Back Up | Certificates**.
2. On the Certificates tab, click the **Back Up...** button and when prompted, save the XML configuration settings and certificates file (`dlp_certs.zip`) to a secure location.

10.1.3 Performing an Advanced Backup

An appliance automatically backs up the appliance configuration and database every night. The same level of backup is created when manually backing up configuration files from the user interface. Registered data and retained copies of Incident inspected files *are not included* in standard backups.

Backups are saved within the folder: `/var/cgn/copy/system_backups`

Backup Commands

To manually run the backup script, you need to log in to the appliance shell as root user using a tool such as PuTTY. Contact your support representative for the root password. Once logged in as root, review the options below and execute one of the backup commands provided.

To create a standard backup archive with the same contents as the nightly backup or as created from the user interface (the "default content"), enter:

```
# /usr/local/upgrade/backup.plx
```

To create a backup archive with the default content, *plus retained copies*:

```
# /usr/local/upgrade/backup.plx –-addcopies
```

Note: When you back up a large number of Incidents with the retained copies option enabled (that is, `--addcopies`), the archive can be very large and it may take a long time to complete, but the appliance will remain running during the backup.

For most installations, the backup options above are sufficient. Check with your support representative to determine whether or not you should use the additional options below.

To create a backup archive with *all available components* backed up (including configuration, database, retained copies, fingerprints, and SDI data), enter:

```
# /usr/local/upgrade/backup.plx --addcopies --addfp
```

or the simple equivalent:

```
# /usr/local/upgrade/backup.plx –-ALL
```

Note: Backing up fingerprints and SDI data (with the-`--addfp` option) or all components (with the `--ALL` option or `--addcopies --addfp` options) will shut down the appliance during the backup and restart the appliance when complete. The resulting backup file will likely be very large.

To create a backup archive with *only configuration files*, enter:

```
# /usr/local/upgrade/backup.plx --nodb
```

To view all options, enter:

```
# /usr/local/upgrade/backup.plx --help
```

Off-Site Storage

It is recommended that you periodically copy backup archives to a secure location off the appliance. If your appliance eventually retains so many file copies that disk space runs low, backup archives older than three months are automatically purged to free up space. In the most severe cases, an appliance will purge backup files more than three days old.

10.2 Restore the Appliance from a Backup

Note: Only restore a DLP appliance from a backup archive under the guidance of a support representative. Although the operation is usually fairly straightforward, situation-specific variables may arise and create complications.

Unless specified otherwise, the restore routine will restore everything from within the specified archive file that it finds. For example, restoring a standard nightly backup will also restore configuration settings and the database tables; whereas, restoring a manual backup with all options will restore all components.

Any restoration requires the appliance to be stopped. The restore routine will shut down the appliance for you automatically when it needs to, and will restart the appliance upon a successful restoration. If you shut down the appliance (e.g. via `cgnmgr stop`) before running either the backup or restore script, the script will leave the appliance shut down when complete. On the other hand, if the script shuts down a previously running appliance for you, then it will restart it when the restore operation is complete. Basically, the script leaves the appliance in the same running (or not) state that you had it in before running the script.

In general, you should only use a backup from the same appliance to restore the appliance. Make sure the backup for the appliance you are restoring is:

- From the same software version
- The same appliance model

10.2.1 Prior to Restoration

Before you restore an appliance, perform the following step and keep the following points in mind.

1. To run the restore script, you need to log in to the appliance as root user. Contact your support representative for the root password.
2. Only restore from a backup if the appliance firmware has not been changed since the backup was made.

3. Make sure the software version of the fresh install and the backup are the same. Verify this prior to restoration. In rare cases, restoration may be possible between minor releases.

10.2.2 Restoring an Appliance from a Backup File

Before you restore an appliance from a backup file, it is recommended that you first test the backup you intend to restore, as described below.

To restore a Manager or Stand-alone appliance (not Inspectors):

1. Log on to the DLP appliance as root using PuTTY or whatever SSH client you prefer.
2. Copy the backup file from its current location to a directory on the DLP appliance.
3. Change to the directory where you copied the backup.
4. Enter the following (to test the most recent nightly backup):

   ```
   # /usr/local/upgrade/restore.plx --nightly --test
   ```

5. After testing the most recent nightly backup, perform one of the steps below to restore an appliance from a backup.

   - To restore from a specific backup file, enter:

   ```
   # /usr/local/upgrade/restore.plx –f [FULL_PATH_OF_BACKUP_FILE]
   ```

   where <FULL_PATH_OF_BACKUP_FILE> is the full path and name of the file, for example,

   ```
   /var/cgn/copy/system_backups/appliance_backup.10.16.13
   ```

   - To restore the *latest file* within /var/cgn/copy/system_backups, enter:

   ```
   # /usr/local/upgrade/restore.plx --latest
   ```

   - To restore from the *most recent nightly backup*, enter:

   ```
   # /usr/local/upgrade/restore.plx --nightly
   ```

   - To restore everything within the latest backup *except retained copies*, enter:

   ```
   # /usr/local/upgrade/restore.plx --nightly --nocopies
   ```

   - To restore *only the configuration files* within the latest backup (without database information, registered data, or retained copies), enter:

   ```
   # /usr/local/upgrade/restore.plx --latest --nodb
   ```

   - To view all options, enter:

   ```
   # /usr/local/upgrade/restore.plx –-help
   ```

6. After restoring from a backup, you will need to re-crawl any content registered from uploaded files. Content registered in from a database or a file repository may be re-crawled immediately, or, if you have automatic re-crawling set, it will occur at the next scheduled interval.

7. From the management console, click **Registered Data > Files and Databases** and then the **Edit** button for each item on the RedList and GreenList for which the Data Type column shows (File Upload).
8. In the Edit Registered Content screen that appears, click the **Upload** tab, and then the **Update** icon and **Browse**... button to specify the location of the source file whose data was registered.

Useful Commands

Below are some useful commands related to restore operations.

To check for free disk space (make sure you have at least 50% free), enter:

```
df /var/cgn/copy/ -hP
```

To list restoration logs, enter:

```
ls -l /var/cgn/info/log/maintenance/restore*.log
```

To view the high-level log, enter:

```
tail /var/cgn/info/log/maintenance.log
```

10.3 Backing Up and Restoring Inspectors

You do not need to back up any appliances that are configured to run in Inspector mode. Inspectors do not require backup because the Manager automatically syncs the database and registered data information to its Inspectors.

To restore an Inspector, connect a replacement to the DLP Manager or manually reinstall the Inspector.

10.4 Enable/Disable SSH Access

To allow or disallow remote (command line) access to the DLP appliance:

1. From the management console, click **Manage System > Maintenance | Diagnostics | Tools**.
2. Click the **Enable/Disable SSH** button.

Note: If an error occurs during restoration using a backup file, SSH access is automatically enabled.

BLUE COAT

11 Data-Usage Incident Management and Reporting

DLP appliance Administrator's Guide

An incident is created when a policy's conditions are met and other exclusions, such as exception policies and the GreenList™, do not apply. When a data-usage incident occurs, the incident is posted to the Data-Usage Incidents screen.

Policy workflow actions can be configured to set up a review workflow for incidents. Incidents can also be configured to bypass the incident review workflow, and their status is marked Closed when the incident is created.

Open incidents can be assigned to specific personnel or groups (referred to as "assignees"), who can review incidents. Incident reviewers can review blocked transactions and approve blocked transactions to be sent (MTA-related incidents only). Assignees can change the Incident Status for incidents they address to "Resolved" or "Closed." Closed incidents can be reopened and the incident workflow can be re-performed for these incidents.

This chapter includes the following topics:

11.1 Policy Matches and Incidents

The diagram below shows the path required for a policy to trigger and execute an action, resulting in creation of an incident. Any other path will result in no action being taken and no incident created.

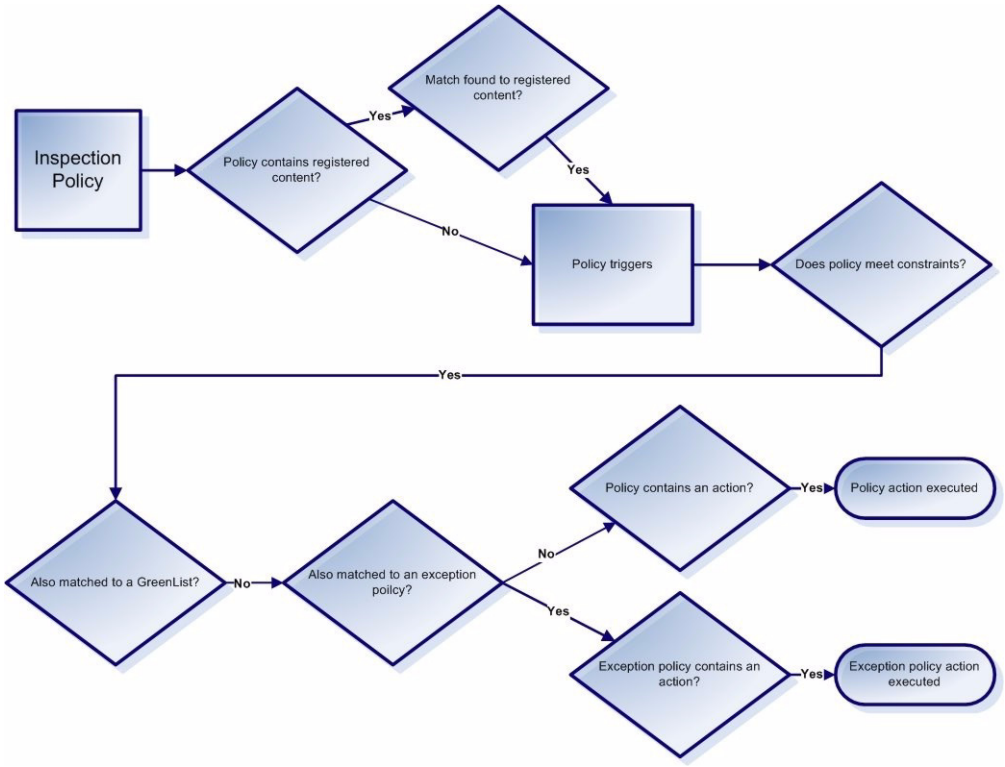


Figure 11.1: Path for a Policy to Trigger and Action to Execute.

When the policy action is set to None, a policy triggers but the policy action is not executed, nor is an incident created.

If the event does result in creation of an incident, only one incident can be created for each RedList™, pattern, or rule used in an active policy. If a transaction is found to violate more than one registered data object in a policy, or if it violates registered data objects in more than one policy, then multiple incidents can be created for a single

transaction. If a policy action is configured to send a notification when each incident is created, then a single transaction can lead to an Incident Reviewer receiving multiple alerts.

During content inspection, if the TCP data stream is not within the boundaries of a file and does not provide enough information to be processed as SMTP, HTTP, or FTP, it is processed as Other TCP. If a match is triggered by content in the data stream, the retained copy will be a binary file with a .bin extension. You can view this file with a viewer that displays binary files in a hexadecimal window, such as Free Hex Editor:

`http://www.hhdsoftware.com/hexeditor.html`.

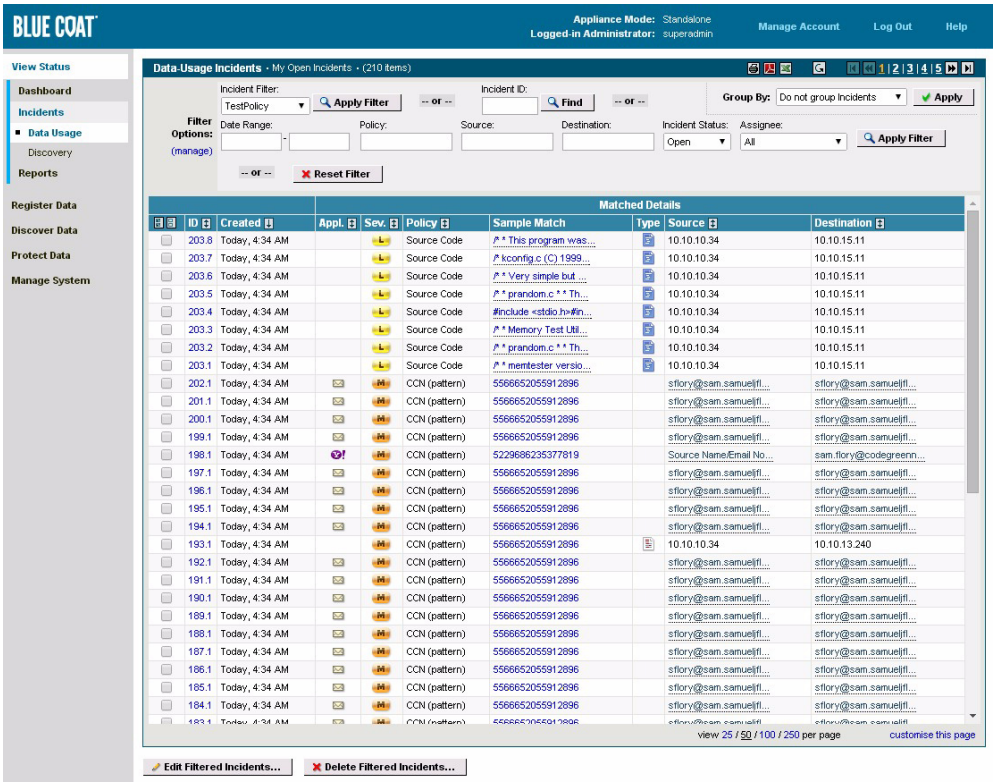


Figure 11.2: The Data-Usage Incidents screen can help you organize incident reviews and remediation actions.

Incidents are generally created for units crossing the network called transactions. A transaction is defined as a logical transfer of information. Often a transaction occurs via a single TCP transmission, however in a number of common cases (FTP, IM) a transaction can require multiple different TCP transmissions.

One transaction may have more than one policy match, leading to multiple incidents. Also, two different inspection services may inspect the same transaction and create different incidents for the same policy violation. In the Data-Usage Incidents screen, the incidents can be grouped and filtered in a number of different ways. Incidents can also be sorted by various criteria, including priority, status, and assignee.

Incident assignees can perform the following activities when working with incidents.

- They can customize their view of the incidents by grouping, filtering, and sorting incidents.
- They can access incidents assigned to them or their group and reassign incidents to themselves or others.
- They can group, filter, and sort their incident queue in various ways.
- They can choose the number of incidents to display on-screen.
- They can reprioritize the incidents in their queue.
- They can review information about the incident and view a copy of the data that led to the blocked transaction, when available.
- They can review the incident history and add comments.
- They can mark incidents as resolved and classify the incident into a resolution category.
- They can review a blocked transaction (using the MTA and ICAP inspection services) and approve the transaction to be sent (MTA only).
- In the rare case that there is a problem sending the MTA email after approval, they can retry sending it.
- They can review closed incidents and leave them closed or reopen them.

11.2 About Role-Based Access Control for Incidents

The incidents that are visible to Incident Reviewers on the Data-Usage Incidents screen depend on role-based access control.

Users with the role of Super Administrator have full access to view and find incidents, and they can delete incidents.

Incident Reviewers have access to the following incidents.

- All incidents assigned to them
- All incidents assigned to the Incident Reviewer groups to which they belong

If Incident Reviewers use the **Find** button to search for incident numbers on the Data-Usage Incidents screen, they will only be able to find incidents that they have authority to view.

The Assignee filters also depend on role. For Incident Reviewer, Assignee = All means assignees within the Incident Reviewer groups to which they belong.

Incident export is also based on roles. Export is based on the incidents that can be viewed in the Data-Usage Incidents screen. This means that a Super Administrator can export the entire set of incidents, but other Incident Reviewers (such as incident admins) can only export incidents assigned to them or their groups.

Note: If incident redaction is enabled (**Manage System > Administrators | Roles)**, the Incident Reviewer will not be able to see information about the source/destination information and/or sensitive data when viewing incident details and exporting incidents.

Super Administrators have no restrictions. They can view and export incidents assigned to all assignees and groups, and they can export the entire set of incidents. Incident redaction does not apply to Super Administrators.

11.3 Displaying Incident Details

You can display the details recorded for an incident, including the workflow settings, by clicking the incident ID in the Data-Usage Incidents screen. The Edit Incidents Details dialog box for the selected incident will be displayed. To display the incident details in-line, below the Data-Usage Incidents list, click the "pin" button in the upper-right side of the Edit Incident Details dialog box. A confirmation dialog box will be displayed. Click OK to proceed.

11.4 The Incident Management Workflow

The incident management interface was built using the following basic workflow. Each step in the workflow has three different incident states associated with it: Incident Status, Approval Status, and Transaction Status. Policy actions are configured to determine whether the incident will undergo a review workflow or be auto-closed, whether email transactions will be blocked if a policy match is found that leads to an incident, and who the assignee or group of assignees will be. The policy action also assigns a default incident severity and review priority.

- **Step 1:** Policy action is executed and the incident is created with the appropriate states assigned. If the policy action is configured so incidents do not undergo a workflow, the incident is auto-closed at this stage, although it can be reopened and sent for a full review at a later step in the workflow.

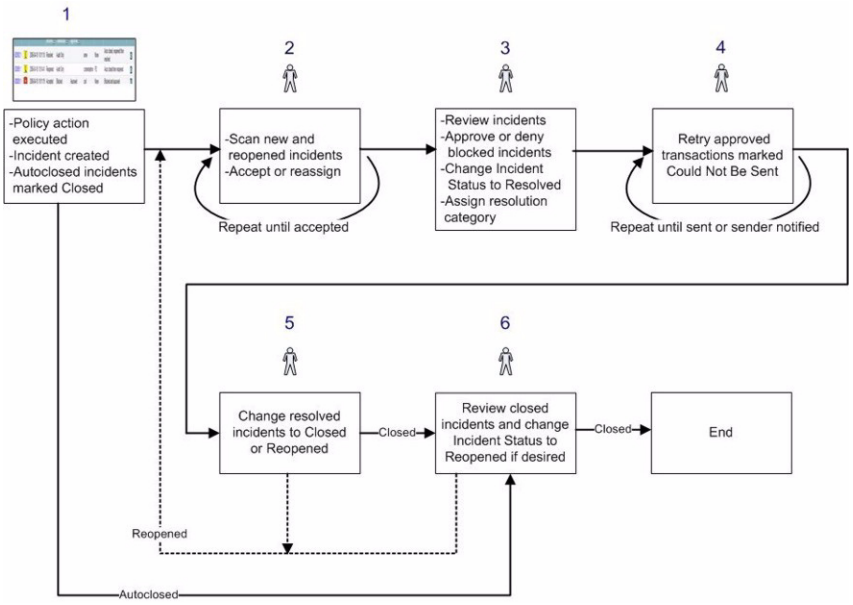


Figure 11.3: Incident Management Workflow.

- **Step 2:** The assignee looks over each assigned incident and either accepts it as an assignment or reassigns it to another Incident Reviewer. The incident can be reassigned any number of times, until an assignee finally accepts the incident.
- **Step 3:** The assignee reviews the details of each incident. If the incident involves a temporarily blocked email, the assignee is asked to approve or deny the incident. If this is the only incident associated with the email transaction, the email will be placed in the send queue when the assignee approves it. However, if the email transaction led to more than one incident that involves blocking, all of the blocked incidents in the transaction group must be approved before the email transaction will be placed in the send queue. The exception to this is if the assignee invokes an override option at the time of approval of one of the incidents. The override allows the email to be sent regardless of the Approval Status of the other incidents.
- **Step 4:** (Applies only to cases where an email transaction was blocked and then approved.) If for some reason forwarding the approved email fails, the Transaction Status will appear as Could Not Be Sent. If an assignee finds this status while reviewing incidents, a Super Administrator should be notified to make sure that MTA and the forwarding or rerouting server are working properly. The assignee can retry the email, and, if that does not help, may need to compose an email to the sender that the blocked email was not able to be sent.
- **Step 5:** The assignee changes incidents that are resolved to the Closed status. This step allows independent review of resolved incidents, if desired. This step is also necessary to make one last check that all resolved incidents that involved blocked email have been properly sent. If there is any problem with the resolved incident, it can be sent through the review workflow again by marking it Reopened.
- **Step 6:** Assignees can review incidents marked Closed to look for any irregularities, marking the incidents Reopened, if necessary, to send them back for review.

This is also the step in which incidents that were automatically closed by the policy action can be reviewed and sent for a full review, if desired. If a reopened incident involves email that has already been sent (through approval or override), then it can no longer be blocked, but the incident can be re-categorized for purposes of record keeping.

11.4.1 Incident Status

Incident Status reflects the life cycle of the incident. It has the following values shown in the table below.

Table 11.1: Incident Status Values.

Value	Description
All	Assignee selects this value to view all incidents, regardless of their status.
Open	Assignee selects this value when an incident needs to be resolved.
Accepted	Indicates that the logged-in user has taken responsibility for the incident.
New	(Automatic) Status when incident is first created.
Reopened	Assignee selects to reopen a resolved or closed incident and initiate a new workflow.
Resolved	Assignee selects this value when the assignee has dealt with the incident.
Closed	Assignee selects this value when the incident is judged to be resolved correctly.

Incident Status also appears in the list of filters on the Data-Usage Incidents screen.

The value Open is a container for Incident Status values All, Open, New, Reopened, and Resolved. By default, only open incidents are displayed in the Data-Usage Incidents screen. Closed incidents, or a single Incident Status value in the Open category, can be displayed by changing the filters.

When actions are created, a default Incident Status of New or Closed can be assigned. If an action assigns a default Incident Status value of Closed, the incidents are logged but do not appear in the Data-Usage Incidents screen unless the assignee specifically sets the Incident Status filter to review closed incidents.

11.4.2 Resolution Category

When assignees mark incidents Resolved or Closed, they can also assign a resolution category to the incident. The following values are possible.

Table 11.2: Resolution Category Values.

Value	Description
None	Assigned when the value of Incident Status is New. Assignees can also select this value if no other category is appropriate.
Invalid	Assignee selects this value if the incident was a false positive. In other words, when the policy was created, it was not the intention to catch this kind of text or file. Items in this category should be reviewed for the possibility of adding GreenList™ or exception policies to reduce the number of false positives.
Duplicate	Assignee selects this value if the incident is judged to be a duplicate of another incident.
Authorized	Assignee selects this value if the incident was a correct policy match, but the assignee judges it to be an acceptable transaction or authorizes the specific transaction to continue.
User Error	Assignee selects this value if the incident was a correct policy match, and the transaction violates policy, but the assignee judges that the user sent it by mistake.
Prohibited	Assignee selects this value if the incident was a correct policy match, the transaction violates policy, and the assignee considers the transaction to be unacceptable, or, in the case of email blocking, wants to keep the email blocked.

11.4.3 Transaction Status

When the MTA or ICAP inspection service is enabled and a policy action is configured to block SMTP or HTTP/HTTPS transactions, respectively, the Transaction Status variable shows the state of the incident. In the case of the MTA inspection service, email is held by the DLP appliance, and then forwarded or rerouted when approved. The transaction status reflects the status of the email on the MTA server, as described in the following table.

Table 11.3: Transaction Status Values.

Value	Description
Audit Only	Assigned when the action is not configured for blocking only. When incidents are created, they are assigned a Transaction Status value of Blocked or Audit Only.
Blocked	Assigned when the incident is created (if the policy action is configured to block email).
In Send Queue	When the Approval status is changed to Approved, the email enters the send queue and takes on this value.
Sent	Email was sent successfully from the send queue.
Could Not Be Sent	Email was not sent successfully from the send queue because the appliance cannot connect to the forwarding or reroute MTA. This could be because the link between the MTA and the forwarding or reroute server went down, or the forward or reroute MTA went down. If the user clicks the **Retry** button, the email returns to the send queue and the value, "In Send Queue," is assigned to the incident's state.

In the case of the ICAP inspection service, once a transaction is blocked, it cannot be unblocked. Blocked HTTP transactions will show a transaction status of Blocked.

11.4.4 Approval Status

When the policy action is configured to block email transactions upon creation of an incident, then one step in the incident workflow requires the assignee to approve or deny the email transaction by clicking an **Approve** or **Deny** button.

Approval Status values are assigned automatically on the basis of a blocked transaction's location in the workflow and the assignee's decision to approve or deny, as shown in the following table.

Table 11.4: Approval Status Values.

Value	Description
Needs Approval	Assigned when the incident is created and the policy action is configured to assign a workflow.
Approved	Assigned when the assignee clicks the **Approve** button.
Denied	Assigned when the assignee clicks the **Deny** button.
Bypassed	Assigned when an incident is in the Needs Approval state and the assignee approves another incident in the same transaction and uses the override option to allow the transaction to be sent.
None	No value when an email transaction is not blocked (Audit Only)

11.5 Incident Severity and Incident Priority

If assignees have a large number of incidents to review, they need some way to organize and prioritize the incidents. There are two ways to classify incidents in terms of their importance and urgency: incident severity and priority.

Incident severity is intended to reflect the sensitivity of the data being transmitted. Highly confidential data with serious consequences if leaked would be assigned a High severity. Data that should be monitored, but is not so highly sensitive, would be assigned a Low or Medium severity.

A default incident severity of High, Medium, Low, or Info can be automatically assigned by the policy action. Incidents can be sorted by incident severity, or incident severity can be used as a filter to limit the incidents that are viewed. Incident severity can also be modified by assignees, if individual policy matches are judged to have greater or lesser sensitivity.

Incident priority is intended for use by the assignee in categorizing the urgency of review. A default priority of P1, P2, P3, or None can be assigned by the policy action. This value can also be changed by the assignee. This value appears in a column in the summary table, so it can be used for sorting, but it cannot be used as a filter.

Incident severity and incident priority may not match in some cases. For example, an incident rated as High severity might take five hours to review, while a Medium-severity incident might take five minutes, so the priority of the Medium-severity incident might be set at P1 and the High-severity incident at P2.

The assignee can use incident severity and incident priority together when viewing incidents. For example, an assignee can set the severity filter so only the High-severity incidents are displayed, and then sort on priority to determine the priority of incidents for that level of severity.

11.5.1 About Email Notifications Regarding Incident Updates

You can configure email notifications to be sent automatically when certain incident updates occur (for example, when the incident severity, priority, or status is changed by another administrator). See 3.5.5 "Configure Incident Management Notifications" on page 29 for information.

11.6 States at Each Step in the Workflow

This topic contains more technical details for each step in the basic incident review workflow. At each step of the workflow, the incident has values for Incident Status, Approval Status, and Transaction Status associated with it. The following sections describe the states assigned at each step of the workflow.

In the figures in this topic, italics are used to denote values that have not changed from the previous step in the workflow.

Step 1: Incident is created and states are assigned

In the first step of the workflow, following a policy match, an incident is automatically created. The values for Incident Status, Approval Status, and Transaction Status are automatically assigned, and their values are as shown in the figure below. If email blocking was configured in the policy action for SMTP transactions, then Transaction Status has the value Blocked; otherwise, Transaction Status has the value Audit Only.

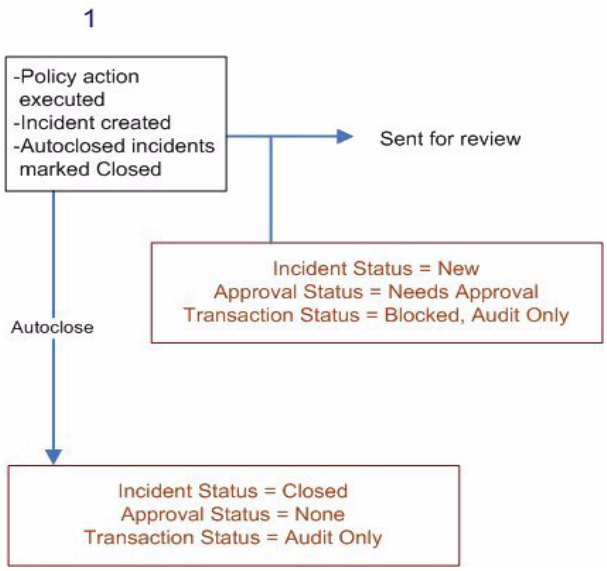


Figure 11.4: Incident States After Step 1 of the Workflow.

If the policy action was configured to automatically close the incident, then Incident Status is marked Closed. Because this incident will not go through review, Approval status has the value None because it is not applicable. Transaction Status has the value Audit Only. The resolution category is marked Auto-closed. These auto-closed incidents can be reopened in the last stage of the workflow and be submitted to full review at that point. This feature works well when you only want to review a small number of incidents, such as in the case where a policy is producing many false positives, or in the early stages of creating and testing policies, when you are not interested in a formal review process for incidents.

Step 2: Accept or reassign incidents

In the second step of the workflow, assignees view open incidents assigned to them in the Data-Usage Incidents screen. For each incident, assignees have the option of changing the Incident Status to Accepted or reassigning the incident to another assignee. This step of the workflow is iterative until the Incident Status is changed to Accepted.

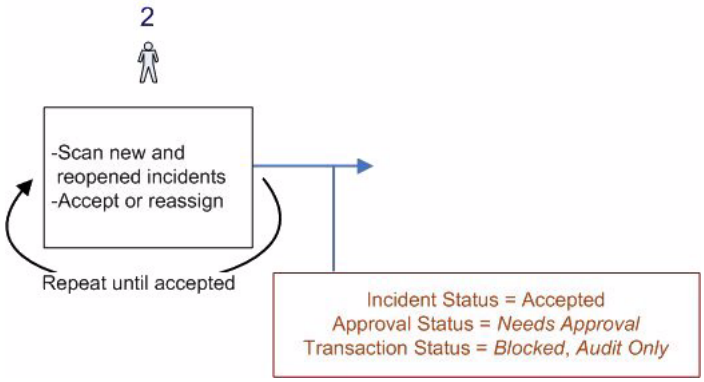


Figure 11.5: Incident States After Step 2 of the Workflow.

The values for Approval Status and Transaction Status remain the same as for the previous step in the workflow.

Step 3: Approve or deny transactions

In the third step of the workflow, the assignee looks at the details of the policy match that led to the incident, approves or denies blocked email transactions, marks the Incident Status Resolved, and assigns a resolution category.

Note: This step of the workflow does not apply to blocked ICAP transactions, which cannot be approved or denied.

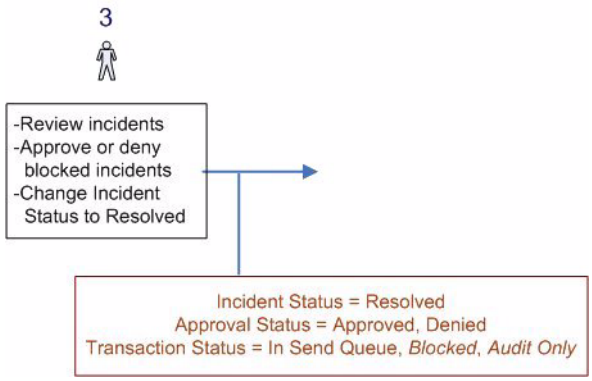


Figure 11.6: Incident States After Step 3 of the Workflow.

In the case where the Transaction Status for an email incident has the value Blocked, the assignee is presented with **Approve** and **Deny** buttons, to allow the email to be sent or keep it blocked, respectively. Clicking **Approve** changes the Approval Status value to Approved, and clicking **Deny** changes the Approval Status to Denied. What happens next depends on the number of incidents that are associated with that transaction. When the transaction contains only one blocked incident, the Transaction Status value is changed to In Send Queue. When the transaction contains more than

one blocked incident, then all of the incidents must be approved before the Transaction Status value changes from Blocked to In Send Queue. The exception to this is if the assignee invokes an override option at the time of approval of one of the incidents. The override allows the email to be sent regardless of the status of the other incidents. In that case, if the Approval Status of other incidents associated with the transaction have the value Needs Approval, and then the Approval Status for those overridden incidents changes to Bypassed.

In the case of policy incidents that were not set up for blocking, the assignee still reviews the policy match details that led to the incident. Because the transaction has already left the network, the Transaction Status retains its value of Audit Only.

In all cases, once the incident has been reviewed, and approved or denied, if applicable, the assignee changes the Incident Status to Resolved and assigns a resolution category to the incident.

For approved email placed in the send queue, the Transaction Status will continue to change as appropriate. If the email is sent successfully, the value of Transaction Status will change to Sent. In the rare case that the email cannot be sent successfully, the value of the Transaction Status will change to Could Not Be Sent.

Step 4: Review transaction status of approved email

In the fourth step of the workflow, assignees check the Data-Usage Incidents screen for approved email whose Transaction Status value is Could Not Be Sent.

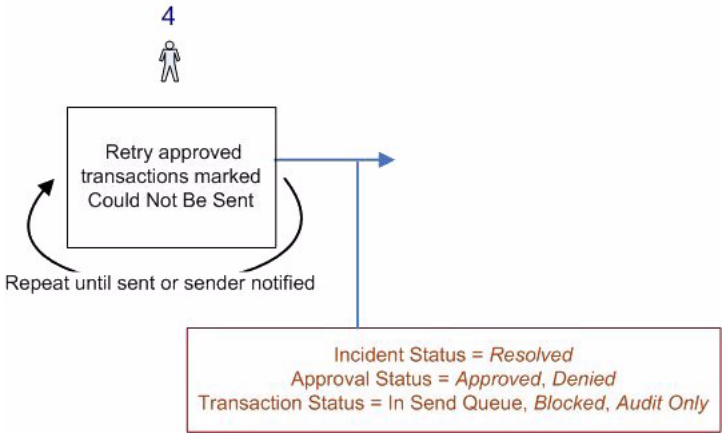


Figure 11.7: Incident States After Step 4 of the Workflow.

Alternatively, if there are still problems with sending the email, the assignee may want to notify the sender that the email was not transmitted.

Step 5: Close incidents

In Step 5 of the workflow, assignees change the Incident Status of resolved incidents to Closed. The assignee can also change the value of the resolution category or even change the value of Incident Status from Resolved to Reopened, to make another pass through the review workflow.

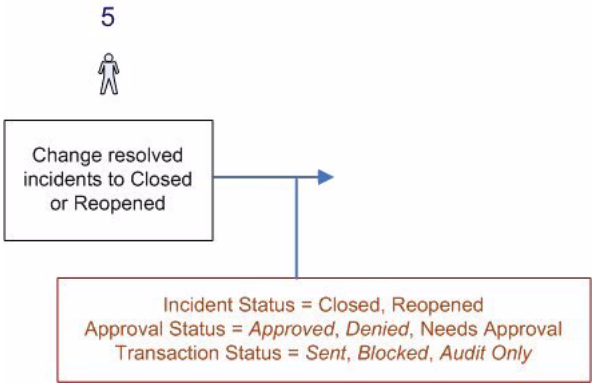


Figure 11.8: Incident States After Step 5 of the Workflow.

If the Incident Status value changes to Reopened, the Approval Status is automatically changed to Needs Approval, and the workflow commences from Step 2. The Transaction Status does not change as a result of this step.

Step 6: Review closed incidents

In Step 6 of the workflow, assignees can review incidents marked Closed to look for any irregularities, marking the incidents Reopened if necessary to send them back for review. This is also the step in which incidents that were automatically closed by the policy action can be reviewed and sent for a full review, if desired.

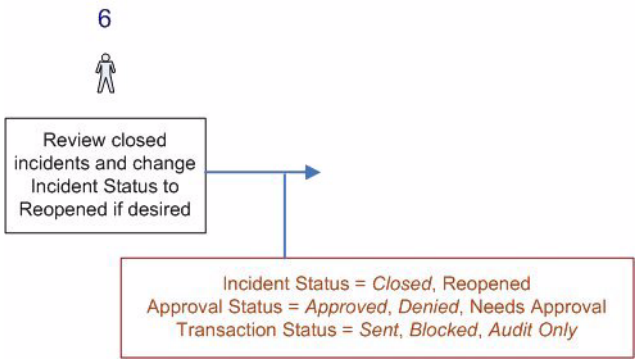


Figure 11.9: Incident States After Step 6 of the Workflow.

If the Incident Status value changes to Reopened, the Approval Status is automatically changed to Needs Approval, and the workflow commences from Step 2. The Transaction Status does not change as a result of this step.

11.7 Examples of Incident Management

Below are some typical examples of the ways incidents can be handled using the basic workflow.

Example 1: Automatically close incidents

(Applies to all inspection services.)

The auto-closed response is useful when a policy has a high probability of producing false positives, in other words, incidents that you wish had not been created. Rather than having to review and mark each false positive, assignees could instead review the closed incidents for that policy and open the ones that look like bona fide violations.

The auto-close response is also useful for creating an audit trail about data that does not necessarily need to be reviewed. The incidents are logged and can be analyzed for trends and so on, but do not undergo a full incident review.

Studying the false positives could also be valuable in that it would provide information on how to reduce them, including the following options.

- The policy can be made more restrictive.
- A GreenList™ can be created to protect RedList™ matches from becoming incidents.
- Exception policies can be created so the main policy remains general and the exceptions are enumerated.

In summary, a policy action can be configured to automatically close incidents. In this case, the incident is logged, the transaction is unaffected, and there is no approval or denial required in the workflow. Auto-closed incidents can be re-opened by the assignee in Step 5 of the workflow, at which point they will go through the full workflow review process.

Example 2: Email transaction allowed, but incident undergoes review

(Applies to the Packet Monitor and MTA inspection services.)

You may not want to block email for a particular policy, but still want the incident to undergo review and assignment to a resolution category as a means of improving policies and procedures.

In this case, the policy action is configured so that when an incident is created, the Incident Status is automatically set to New to initiate a workflow. Because the blocking option is not selected, the Transaction Status is set to Audit Only, and the Approval Status is blank.

Assignees filter the incidents in the Data-Usage Incidents screen to view new incidents assigned to them. For the Audit Only incidents, they review the details of the policy match, assign a resolution category, and set the Incident Status to Resolved.

Example 3: Transaction blocked, incident undergoes review

(Applies to the MTA and ICAP inspection services.)

ICAP blocking can be used to block download or upload of HTTP data, including Webmail. This requires that the ICAP inspection service be configured with a supported proxy server and enabled. Multiple policies could be created that would respond differently based on web page content. For example, obscene or hateful web sites could be blocked, with notifications sent to the user accessing the web page and to an Incident Reviewer. Webmail can also be blocked. There is no approval process like there is for SMTP mail.

For SMTP mail monitored by the MTA inspection service, when an information leak would be extremely serious, email transactions can be blocked pending review, at which point they can be approved or denied. If they are approved, they are sent at that point. This case should be reserved for information leaks with very serious consequences and should only be enforced after a policy has been tested and false positives eliminated to the extent possible. Blocking email means a delay in transmission even if approved, and it requires the review process to occur soon after the email was sent, otherwise the normal flow of corporate communication outside the network could be seriously disrupted. Although you can configure the policy action to send an automatic notification to the sender of the email warning that the transaction has been blocked and auto-notify an Incident Reviewer, there must then be staff dedicated to responding to the concerns of the sender.

For both ICAP and MTA blocking, the policy action would be configured to block the email and open a workflow. For MTA blocking, the policy action should also be configured to send a notification to one or more assignees so they can approve or deny the email in a timely fashion.

Email transaction blocked, transaction includes more than one incident

(Applies to the MTA inspection service.)

It is possible for one email transaction to trigger more than one policy match, such that several incidents are created for the same transaction. In this case, the reviewer has the following choices when reviewing a single incident related to a blocked email.

- Approve the incident and select the option to bypass the other incidents and allow the transaction to be forwarded.
- Approve the incident but leave the transaction blocked until all incidents have been approved.

Below are some cases where more than one incident can be created for a single email transaction.

- Multiple attachments matching one policy
- Multiple attachments matching multiple policies
- A container attachment (such as a zip file) matching one or more policies

- Email body or attachment matching more than one registered data object used in a group rule in a single policy

11.8 Variations on the Workflow

There is a great deal of flexibility built into incident management on the DLP appliance, and you do not have to follow all the workflow steps as they are laid out. For example, if your policies do not block email and you do not need to follow up on whether approved email was sent or not, you might want to bypass the Resolved state and just mark the incident Closed and then assign a resolution category.

The values for Incident Status, Approval status, and Transaction Status cannot be configured. In other words, you cannot add, remove, or change the names of values. You can make any changes to the workflow as long as you do not need more values for states than what are provided, and as long as the new workflow is consistent with the automatic assignment of values that occurs. In most cases, the easiest way to vary the workflow will be to simplify it, that is, you do not use all the values that are provided. In this case, because values cannot be deleted, you would have to instruct assignees not to use certain values. For example, you might tell incident reviewers that they should never assign the value Closed for Incident Status.

If you design your own workflow, you should create a workflow diagram similar to the one shown for the default workflow (Figure 11.3), and mark the values for all of the states that will be assigned at the end of each step in the workflow. Once you have made this decision and are sure that you can use at least a subset of the existing values, it will not be hard to map the workflow onto the UI when you create policy actions and review incidents.

11.9 About Incident and Report Filters

When viewing incidents on the Data-Usage Incidents screen, filters can be used to constrain the incidents that are displayed in the summary table. These filters can be selected by clicking the **customize this page** link.

When report templates contain query constraints, those constraints can also be used as filters on the Data-Usage Incidents screen. These report filters have the same name as the report template in which they are used and are available for selection along with incident-management filters. Report filters can only be created and edited as part of a report template's query constraints.

Advanced filters are shared between the data-usage incident filters and reports. Incident and report filters can be constrained on the same categories as those available for creating query constraints in reports:

- Severity
- Incident Status
- Transaction Status
- Approval Status
- Assignee
- Policy
- Source
- Destination
- Incident Tag
- Incident Type
- Date Range
- Number of Matches

Once you select a filter, it will remain in effect. During a session, you can return to the default filters by clicking the **customize this page** link and then the **reset to default filters** link in the Customize the Incident Table dialog box.

Note: The changes made to the displayed filters and displayed columns are saved for each user.

For instructions on creating advanced filters and custom report templates, see 11.11 “About Query Constraints and Filters” on page 200.

11.10 About Reports

Reports allow you to examine incidents that result from policy matches.

Reports are generated from report templates. Predefined report templates are provided with the DLP appliance and generate the most popular reports.

You can create custom report templates, which will generate reports by querying the incident log and grouping the data on a single category that you choose. You can use optional query constraints to limit the data set. For example, you might want to generate a monthly report that shows all incidents grouped by policy, and another monthly report that shows only email incidents grouped by the email address of the sender.

When you generate a report from a template, you can drill down on one category and group it into subcategories. For example, if your main chart displays incidents grouped by policy, then you might wish to look further at the policy that led to the most incidents, breaking it down by protocol, or looking at the sources or destinations of the transactions.

Drill down is ideally used for exploratory data mining, in which you are looking at the data in various ways to try to find patterns that will tell you why certain kinds of inci-

dents are occurring. For scheduled reports that will be generated at regular intervals, it may be easier to construct a custom report with query constraints.

11.10.1 About Charts and Tables

To use, view, and create new reports, click **View Status > Reports**. The Reports screen will be displayed.

You can generate the report as a chart, as a summary or detail table, or both. You can print a report using the Print Preview functionality in your web browser, or you can export the chart and table to a PDF file. You can export the data related to a report's summary table or detail table to a CSV file. Exporting, printing, and saving are done on the screen that displays the generated report.

Charts can be of the following types:

- Pie chart
- Vertical bar chart
- Horizontal bar chart

There are two types of tables:

- Summary table—Shows grouped data categories to match the chart. The data are displayed as links to allow drilling down.
- Detail table—Displays the individual incidents included in the data set.

If you would like to export the logs for incidents that were included in the report, you should generate a detail table.

Summary tables are usually displayed with links. Clicking a link generates a drill-down report using the subcategory displayed in the Drill-Down Options pane at the bottom of the generated report page. Changing the category will change the report that is generated when you click the link. You can generate the same drill-down report by clicking any pie slice in a pie chart or any bar in a bar chart.

Note: Predefined reports of the type "System Logs" do not display data in charts.

11.10.2 About Role-Based Access Control for Reports

Incident data used in reports are subject to two constraints that are outside the control of the user:

- Role-based access control

  This applies to users with the role of Incident Reviewer and limits the incidents included in the report data set.

- Incident redaction

  If incident redaction is enabled, then source and destination information will be suppressed for users logged in as an Incident Reviewer when reports are generated or report data is exported.

These restrictions apply to dashboard charts, predefined report templates, and reports generated from custom report templates.

When Incident Reviewers generate reports, the data set used for the report is automatically limited to the following conditions.

- Incidents assigned to the user currently logged in, or
- Incidents assigned to the Incident Reviewer groups to which the user belongs, or
- Incidents assigned to other users in the same Incident Reviewer groups as the logged-in user.

If **Individual Assignee** or **Group Assignee** is selected as a grouping category for a report, the breakdown in the generated report will show only data for these incidents.

Likewise, in query constraints, a user with the role of Incident Reviewer can select a subset of these incidents, but cannot include more.

Super Administrators have full access to incident data with no role constraints.

11.11 About Query Constraints and Filters

You can constrain the incidents displayed on the Data-Usage Incidents screen by creating advanced incident filters. You can constrain the data included in reports by selecting an existing advanced incident or report filter, by creating new query constraints, or both.

Either advanced incident filters or report filters can be applied as a basis for building a query in a new custom report template. Once you save the new template, the query constraints in that template are saved as a new report filter under the name of that report template.

The following examples demonstrate when you might want to use a query constraint. For example, you might want to view only incidents created for transmissions sent from a particular employee. You can do this by setting query constraints.

- Generating a report at the end of each month that includes only that month's incidents.
- Viewing incidents related to email sent from a particular employee.
- Viewing incidents created for outbound documents of the AutoCAD file type, even though the policy applied to all file types.
- Viewing incidents for FTP transmissions only.
- Viewing only incidents that triggered the Notify High action.

The following query constraints contain a text box with an asterisk, where you can specify a group of objects by entering a portion of their names with the wildcard * at the beginning or end of the string.

- Policy
- Registered Data
- Source User
- Destination User
- Inspected File/File Name
- Action
- Assignee
- Incident Tag

You can also use this text box to enter renamed or deleted objects that do not appear in the selection list.

To create an advanced incident filter using a new query:

1. Click **View Status > Incidents > Data Usage | Manage** and then click the **Create Filter...** button.
2. Type a description (name) for the filter.
3. Select **Create a new Query** as the initial constraint.
4. Use the **Select** drop-down menu to select the desired category (e.g. Inspection Service). Then use the provided drop-down menus and/or text box(es) to specify the desired parameter(s) for the selected category. Click the **+** (plus sign) button to add the selected category and parameter(s). Repeat this step to define other categories.
5. When finished, click the **OK** button to save the new filter.

Note: The procedure for creating a custom report is similar to the above procedure. Click **View Status > Reports**. Then click the **Create Report** button.

When creating the filter, if you choose more than one category, the categories are connected with AND logic. For example, if you select Inspection Service = Packet Monitor and Protocol = SMTP, the list of incidents would contain only incidents created as a result of inspection of SMTP traffic coming through the Packet Monitor port. If you choose more than one value for the same category, the values are connected with OR logic. For example, if you choose Protocol=HTTP and Protocol=SMTP, the list of incidents would contain incidents from either protocol.

As another example, suppose you set up an advanced filter with query constraints for content, policy, and protocol. The logic of the query constraint will be the following:

```
content AND policy AND protocol
```

However, suppose you include two query constraints for policy. Then the logic becomes:

```
content AND (policy1 OR policy2) AND protocol
```

TIP: If the Packet Monitor inspection service is enabled together with either the MTA or ICAP inspection service, then two incidents may be created for the same policy violation, one for each inspection service. To control the display of incidents, set an advanced filter for the MTA and ICAP inspection services (if enabled) to eliminate duplication of incidents, and then create another advanced filter for Packet Monitor that excludes SMTP (for MTA) and HTTP (for ICAP) to view incidents that do not overlap.

11.12 Scheduling Reports

You can create reports and schedule them to run at specified intervals, for example, hourly, daily, or monthly. You can select one or more of the predefined report templates or any custom report templates you created for a scheduled report. In addition, you can select the desired report format and select users you want to receive copies of the report.

To create a scheduled report:

1. From the Reports screen (**View Status > Reports**), click the **Create Scheduled Report** button. The Create a New Scheduled Report Wizard will be displayed.
2. Type name for the report in the **Name** field. (You must specify a unique name for each scheduled report.)
3. Select the desired schedule for the report (e.g., hourly, daily, etc.). Click **Next** to continue.
4. Select the report template(s) you want to use for the report.
   - To select one or more reports from the list, Shift-click to select a range of reports in the **Available Reports** list; Ctrl-click to select more than one non-contiguous report in the list. Click the down-arrow button. The selected report(s) moves to the **Selected Reports** list.
   - To select and move all the reports, click the double-arrow down button. (You can move one or more reports or all reports back to the **Available Reports** list by selecting the desired report(s) and clicking the up-arrow button or clicking the double-arrow up button, respectively.)
5. Choose the desired format for the report (Adobe® PDF or CSV file) from the **Format** drop-down menu. Click **Next** to continue.

6. A default report subject and description are automatically entered.
   a. To change the text, select the text in the desired field and enter the desired text.
   b. To configure the report to be emailed even when the report contains no data, check the **Send email even when report is empty** box. Click **Next** to continue.
7. Select the system users you want to receive the emailed reports. Similar to the reports selection screen, select the desired users from the **Eligible Users** list and then click the right-arrow button to move the selected user(s) to the **Selected Admins** list. Click the double-arrow button to move all users to/from the **Selected Admins** list. Click **Next** to continue.
8. Review the summary of the settings for the scheduled report.
   - If you need to modify the settings, click the **Back** button to return to the configuration screens.
   - To accept the displayed settings and create the scheduled report, click the **Finish** button. Once created, the scheduled report appears in the Scheduled Reports table.

To send a scheduled report to specified users:

1. Click the Send button beside the report. A confirmation dialog box is displayed.
2. Click **OK** to proceed.

To edit a scheduled report:

1. Click the **Edit** button beside the report. The Edit Scheduled Report dialog box is displayed.
2. Edit the report's settings as desired (click the tabs at the top of the dialog box to navigate through the configuration screens).
3. Click the **Apply** and **OK** buttons when finished.

To delete a scheduled report:

1. Click the **Delete** button beside the report. A confirmation dialog box will be displayed.
2. Click **OK** to proceed.

11.13 Data-Usage Incident Logs

You can print and export data-usage incident logs.

11.13.1 About Exported Data-Usage Incident Logs

When you export filtered or unfiltered incidents displayed on the Data-Usage Incidents screen to a PDF or CSV file, the exported data is saved in a file named filtered-incidents.pdf or incidents.zip (which contains the incidents.csv file).

When you export a report with a detail table to a CSV file, the incidents that provided the data for the report are downloaded to a CSV file named "report.csv."

Not every column in the exported incident log pertains to every incident, so some cells may be blank. This section describes how to save and export incidents logs.

11.13.2 Save and Delete Incidents and Logs

You can save a copy of all Date-Usage Incidents, all Discovery Incidents, and all Agent Activity Logs (if you are running the CI Agent on endpoints). Note that saved incidents do not include the original file (or email) that triggered the policy match. Use these exports for archival or reference purposes; they are not intended to serve as the basis for a system restore. In addition, you can delete all incidents and all Agent Activity Logs.

To save all Data-Usage or Discovery Incidents:

1. In the management console, click **Manage System > Maintenance | Data.**
2. Click either the **Export All Data-Usage Incidents** or the **Export all Discovery Incidents** button (depending on the type of incidents you want to export).
3. When prompted, choose the location where you want to save the file.

To save all Agent Activity Logs:

1. In the management console, click **Manage System > Maintenance | Data.**
2. Click the **Export All Agent Activity Logs** button.
3. When prompted, choose the location where you want to save the file.

To delete all incidents or Agent Activity Logs:

1. In the management console, click **Manage System > Maintenance | Data.**
2. Click either the **Delete All Incidents** or the **Delete All Agent Activity Logs** button (depending on the data you want to delete).

Note: When deleting incidents, all data-usage and discovery incidents will be deleted.

To save individual incidents:

1. In the management console, click **View Status > Incidents > Data Usage** or **Discovery**, depending on the type of incidents you want to export.
2. Choose the Filter options you want, click **Apply Filter**, and after the results appear click the **Export list to CSV file** or the **Export list to PDF file** button, depending on the file type you want.
3. Save the file to your local machine.

11.13.3 Save Incident Files

Content that triggered a policy match is stored on the DLP appliance that detected the file (this may be the DLP Manager or an Inspector). You can view and/or save the content for individual incidents, or log in to the DLP appliance and use the file system to copy all files to a secure location.

Note: To view or copy files from the appliance you need to log in to the DLP appliance using a SSH client. See 10.4 "Enable/Disable SSH Access" on page 179 for more information.

Content files on the appliance cannot be correlated with the Incident details except through the management console. In addition, the files can not be "re-associated" with an incident, for example, as part of a system restore. Files are renamed and both the metadata and content are kept in separate files.

To save a file associated with an incident:

1. In the management console, click **View Status > Incidents**.
2. To view Data Usage Incidents, click **Data Usage**; to view Discovery Incidents, click **Discovery**. Depending on your selection, the Data Usage Incidents or the Discovery Incidents screen appear.
3. In the screen that appears, choose the filter options that you want and click **Apply Filter.**
4. In the list that appears, click the ID of the incident whose content you want to save. The Edit Incident Details window appears.
   a. For Data Usage Incidents:
      - Click the down arrow button and then click **Download Original Email...** or **View Email**... in the drop-down menu.
      - If you select **View Email**..., the email containing the areas in the document that matched the registered data appears.

- If you select **Download Original Email...**, the email is downloaded to your local machine.

b. For Discovery Incidents:

- Click the down arrow button and then click **Download Original File...** or **View File**... in the drop-down menu.
- If you select **View File**..., the areas in the document that matched the registered data appear.
- If you select **Download Original File...**, the Discovery Incidents are downloaded to your local machine.

11.13.4 Printing Data-Usage Incident Report Logs

To print out the current contents of the Data-Usage Incidents screen:

1. Click the **Print this list** button at the top of the Data-Usage Incidents screen. The Print dialog box will be displayed.
2. Select the desired printing options and then click **OK**.

11.14 About Webmail

The following types of Webmail can potentially be identified.

- Google Mail
- AOL Mail
- Yahoo! Mail
- Hotmail
- MSN Live Mail (Full and Light)

Webmail that cannot be identified as such is classified as an HTTP transaction. When Webmail can be identified in an HTTP stream, it is classified as a special type of email, in the following ways.

- When you view details of an incident, the protocol tab is labelled Email, and the Email Properties pane contains special fields for Webmail.
- You can view the unformatted original transaction and the formatted email message (if the policy action was configured for copy retention).
- If you export incidents, several fields in the exported file provide information about the Webmail:
  - Provider (e.g., Google, AOL)
  - Service (e.g., Classic, Beta)
  - Data Context (file, stream)
  - Host Name (value sent in Host header in Webmail request)

Note: For transactions sent from AOL Mail with Rich Text enabled (the default), when an incident is logged to a matched rule or fingerprint violation on the

body of the message, two incidents will be logged. This is because in AOL mail, when Rich Text is on, there is both a PlainBody and a RichBody section, each containing the body data.

BLUE COAT

12 Discovery Incident Management

DLP appliance Administrator's Guide

An incident is created when a policy's conditions are met and other exclusions, such as exception policies and the GreenList™, do not apply. When a Discovery incident occurs, the incident is posted to the Discovery Incidents screen.

Policy workflow actions can be configured to set up a review workflow for incidents. When you configure policies for Discovery scans, you can specify default settings for all incidents that are created by a policy with a given workflow action (see 9.6 "Configuring Actions" on page 169 for information).

For Discovery incidents associated with files found on CIFS file shares or resulting from CI Agents scans, you can specify remediation actions you'd like to be performed on discovered data that matches a policy scan. You can choose for the specified action to be performed manually by the person reviewing the incident or to be performed automatically, without any user interaction.

Incidents can be assigned to specific personnel or groups (referred to as "assignees"), who can review incidents. If an incident includes a remediation action that is not configured to be executed automatically, the assignee can choose to execute the remediation action or ignore the action. Assignees can change the incident status for incidents they address to "Resolved" or "Closed." Closed incidents can be reopened and the incident workflow can be re-performed for these incidents.

This chapter includes the following topics:

12.1 Policy Matches and Incidents

The diagram below shows the path required for a policy to trigger and execute an action, resulting in creation of an incident. Any other path will result in no action being taken and no incident created.

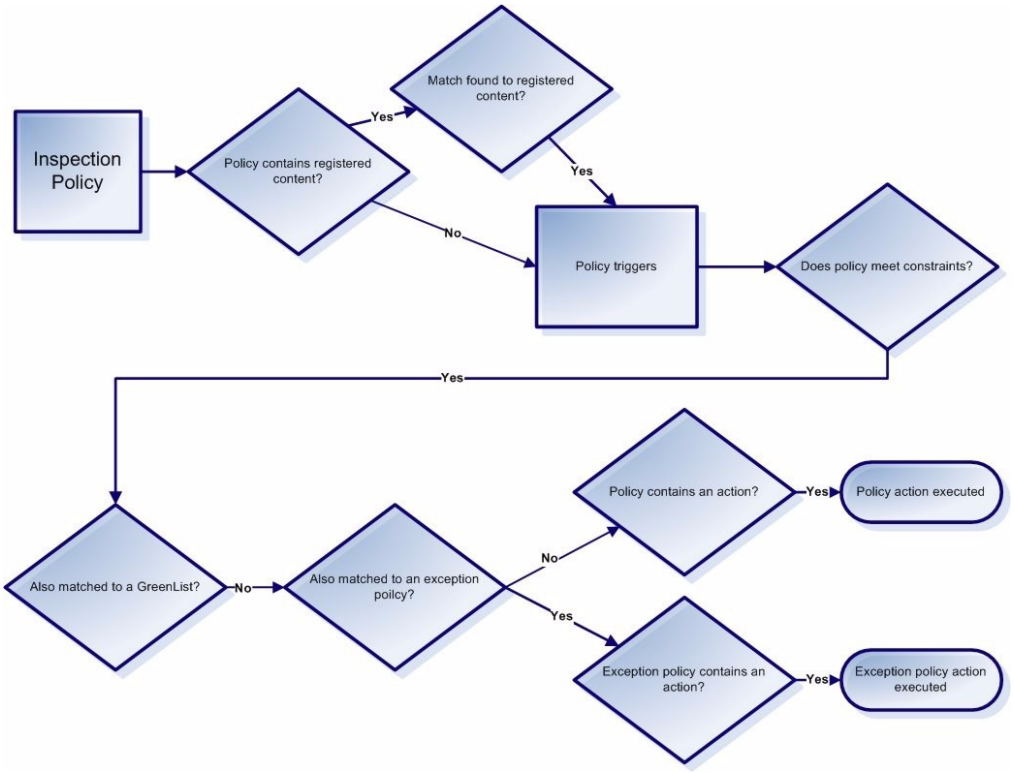


Figure 12.1: Path for a Policy to Trigger and Action to Execute.

When the policy action is set to None, a policy triggers but the policy action is not executed, nor is an incident created.

For file-based (as opposed to database) content, if the event does result in creation of an incident, one incident is created per file. The incident information shows the file that triggered the incident.

Database discovery is table-centric. When you perform a Discovery scan on a database, one incident will be created for each table in each scanned database. Incident data resulting from database scans are also table-centric. For example, incident information for a database-related incident identifies the table that triggered the incident and the incident details identify the column that triggered the incident.

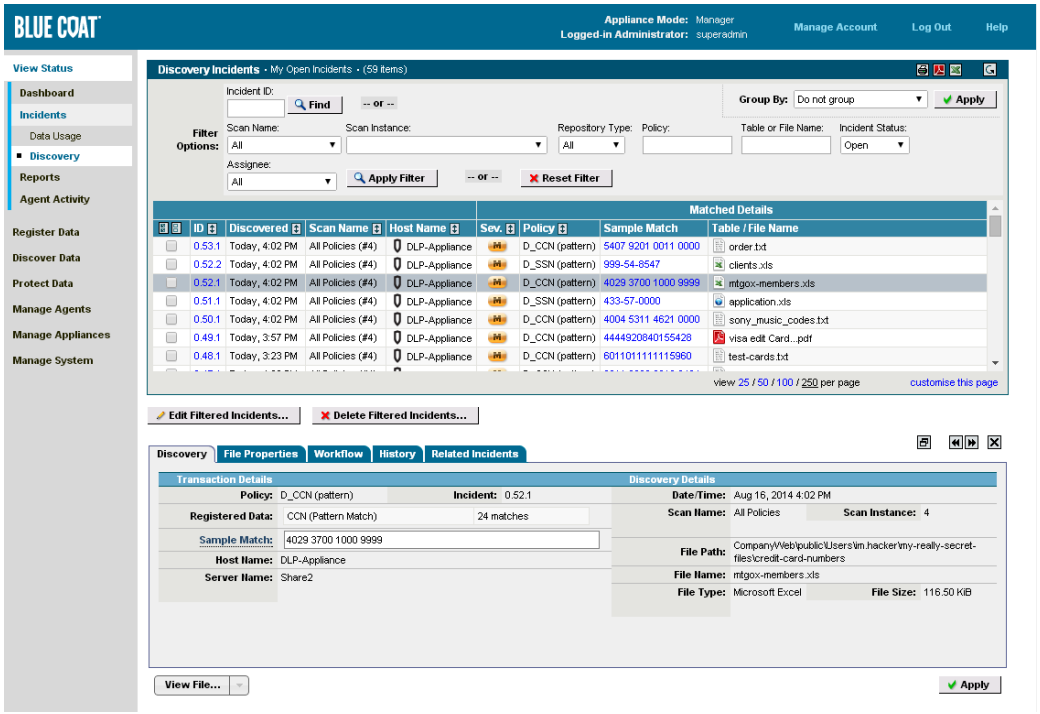


Figure 12.2: The Discovery Incidents screen can help you organize incident reviews and remediation actions.

In the Discovery Incidents screen (**View Status > Incidents > Discovery**), the incidents can be grouped and filtered in a number of different ways. Incidents can also be sorted by various criteria, including by severity, policy, and assignee.

Incident assignees can perform the following activities when working with incidents.

- They can customize their view of the incidents by grouping, filtering, and sorting incidents.
- They can access incidents assigned to them or their group and reassign incidents to themselves or others.
- They can group, filter, and sort their incident queue in various ways.
- They can choose the number of incidents to display on-screen.
- They can re-prioritize the incidents in their queue (based on incident severity).
- They can review information about the incident and view a copy of the data that led to the incident, when available.
- They can review the incident history and add comments.

- For incidents that include remediation actions that require implementation after review, they can implement the remediation actions.
- They can mark incidents as resolved and classify the incidents into resolution categories.
- They can review closed incidents and leave them closed or reopen them.

12.2 About Role-Based Access Control for Incidents

The incidents that are visible to Incident Reviewers on the Discovery Incidents screen depend on role-based access control.

Users with the role of Super Administrator have full access to view and find incidents, and they can delete incidents.

Incident Reviewers have access to the following incidents.

- All incidents assigned to them
- All incidents assigned to the Incident Reviewer groups to which they belong

If Incident Reviewers use the **Find** button to search for incident numbers on the Discovery Incidents screen, they will only be able to find incidents that they have authority to view.

The Assignee filters also depend on role. For Incident Reviewer, Assignee = All means assignees within the Incident Reviewer groups to which they belong.

Incident export is also based on roles. Export is based on the incidents that can be viewed in the Discovery Incidents screen. This means that a Super Administrator can export the entire set of incidents, but Incident Reviewers can only export incidents assigned to them or their groups.

Note: If incident redaction is enabled (**Manage System > Administrators | Roles)**, the Incident Reviewer will not be able to see information about the sensitive data when viewing incident details and exporting incidents.

Super Administrators have no restrictions. They can view and export incidents assigned to all assignees and groups, and they can export the entire set of incidents. Incident redaction does not apply to Super Administrators.

12.3 Displaying Incident Details

You can display the details recorded for an incident, including the workflow settings, by clicking the incident ID in the Discovery Incidents screen. The Edit Incidents Details dialog box for the selected incident will be displayed. To display the incident details in-line, below the Discovery Incidents list, click the “pin” button in the upper-right side

of the Edit Incident Details dialog box. A confirmation dialog box will be displayed. Click **OK** to proceed.

12.3.1 Viewing File Properties for Incidents Generated from Agent-Based Scans

When assignees review incidents resulting from agent-based discovery scans, the File Properties tab is available in the Edit Incidents Details dialog box (or the in-line incident-details display). When selected, the File Properties screen displays the following information about the file that matched a policy and triggered the incident.

Table 12.1: File Properties.

Value	Description
File Path	Displays the path of the scanned directory.
File Name	Displays the name of the file that triggered the incident.
File Type	Display's the file's type, for example, Microsoft PowerPoint.
File Attributes	Identifies the file's attributes, which could include: Read Only, Hidden, System, etc. Attributes associated with the file are checked.
File Owner	Displays the name of the file's owner.
Permissions	Displays the permission information associated with the file.

12.4 The Incident Management Workflow

The incident management interface was built using the following basic workflow. Each step in the workflow has the following different incident states associated with it: Incident Status and Review Status. Policy actions are configured to determine whether the incident will undergo a review workflow or be auto-closed, and who the assignee or group of assignees will be. The policy action also assigns a default incident severity and review priority.

- **Step 1:** Policy action is executed and the incident is created with the appropriate states assigned. If the policy action is configured so incidents do not undergo a workflow, the incident is auto-closed at this stage, although it can be reopened and sent for a full review at a later step in the workflow.

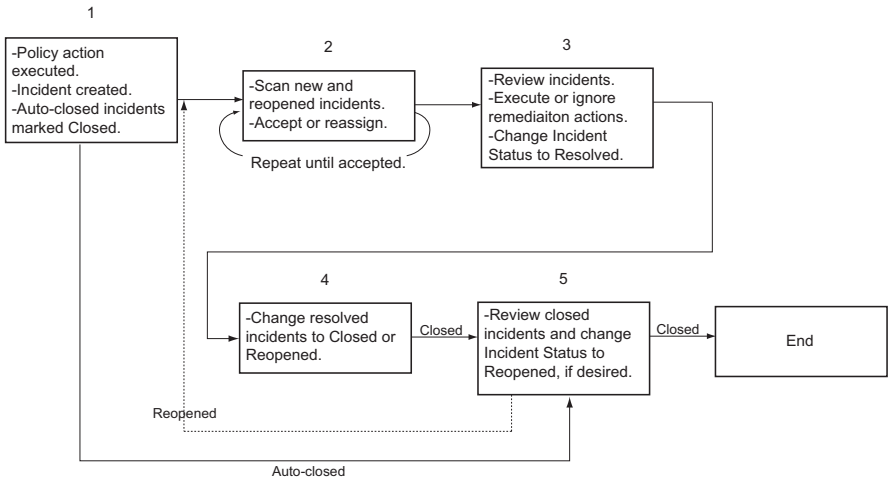


Figure 12.3: Discovery Incident-Management Workflow.

- **Step 2:** The assignee scans each assigned incident and either accepts it as an assignment or reassigns it to another Incident Reviewer. The incident can be reassigned any number of times, until an assignee finally accepts the incident.
- **Step 3:** The assignee reviews the details of each incident. This is the step at which the Incident Reviewer can implement a remediation action (if the policy included such action).
- **Step 4:** The assignee changes incidents that are resolved to the Closed status. This step allows independent review of resolved incidents, if desired. If there is any problem with the resolved incident, it can be sent through the review workflow again by marking it Reopened.
- **Step 5:** Assignees can review incidents marked Closed to look for any irregularities, marking the incidents Reopened, if necessary, to send them back for review. This is also the step in which incidents that were automatically closed by the policy action can be reviewed and sent for a full review, if desired.

12.4.1 Incident Status

Incident Status reflects the life cycle of the incident. It has the following values shown in the table below.

Table 12.2: Incident Status Values.

Value	Description
All	Assignee selects this value to view all incidents, regardless of their status.
Open	Assignee selects this value when an incident needs to be resolved.
Accepted	Indicates that the logged-in user has taken responsibility for the incident.
New	(Automatic) Status when incident is first created.
Reopened	Assignee selects to reopen a resolved or closed incident and initiate a new workflow.
Resolved	Assignee selects this value when the assignee has dealt with the incident.
Closed	Assignee selects this value when incident is judged to be resolved correctly.

Incident Status also appears in the list of filters on the Discovery Incidents screen.

The value Open is a container for Incident Status values All, Open, New, Reopened, and Resolved. By default, only open incidents are displayed in the Discovery Incidents screen. Closed incidents, or a single Incident Status value in the Open category, can be displayed by changing the filters.

When actions are created, a default Incident Status of New or Closed can be assigned. If an action assigns a default Incident Status value of Closed, the incident is logged but does not appear in the Discovery Incidents screen unless the assignee specifically sets the Incident Status filter to review closed incidents.

12.4.2 Resolution Category

When assignees mark incidents Resolved or Closed, they can also assign a resolution category to the incident. The following values are available.

Table 12.3: Resolution Category Values.

Value	Description
None	Assigned when the value of Incident Status is New. Assignees can also select this value if no other category is appropriate.
Invalid	Assignee selects this value if the incident was a false positive. In other words, when the policy was created, it was not the intention to discover this kind of data. Items in this category should be reviewed for the possibility of adding GreenList™ or exception policies to reduce the number of false positives.
Duplicate	Assignee selects this value if the incident is judged to be a duplicate of another incident.
Authorized	Assignee selects this value if the incident was a correct policy match, but the assignee judges it to be an acceptable instance or authorizes the specific instance to exist.
User Error	Assignee selects this value if incident was a correct policy match, and the data violates policy, but the assignee judges that the user had the data by mistake.
Prohibited	Assignee selects this value if the incident was a correct policy match, the data violates policy, and the assignee considers the data to be prohibited.

12.4.3 Remediation Status

When a remediation action is configured upon creation of an incident, one step in the incident workflow allows the assignee the option of implementing the remediation action or ignoring the action. When an incident includes a remediation action, two types of status information are provided regarding the remediation action: review and remediation status. The remediation status value is either blank or "Complete," which is displayed when the remediation action has been implemented. The values for review status are described in the following table.

Table 12.4: Remediation Review Status Values.

Value	Description
Awaiting Review	Indicates that a remediation action has been included in the incident and the remediation action has not yet been implemented.
Executed Manually	Indicates that the remediation action included for the incident was executed manually (typically by an Incident Reviewer).
Executed Automatically	Indicates that the remediation action included for the incident was executed automatically.

12.5 Incident Severity and Incident Priority

If assignees have a large number of incidents to review, they need some way to organize and prioritize the incidents. There are two ways to classify incidents in terms of their importance and urgency: incident severity and priority.

Incident severity is intended to reflect the sensitivity of the data. Highly confidential data with serious consequences if leaked would be assigned a High severity. Data that should be monitored, but is not so highly sensitive, would be assigned a Low severity.

A default incident severity of High, Medium, Low, or Info can be automatically assigned by the policy action. Incidents can be sorted by incident severity, or incident severity can be used as a filter to organize and/or limit the incidents that are viewed. Incident severity can also be modified by assignees, if individual policy matches are judged to have greater or lesser sensitivity.

Incident priority is intended for use by the assignee in categorizing the urgency of review. A default priority of P1, P2, P3, or None can be assigned by the policy action. This value can also be changed by the assignee and can be displayed in a column in the Discovery Incidents screen. Incidents can be sorted by priority and priority can also be used as a filter.

Incident severity and incident priority may not match in some cases. For example, an incident rated as High severity might take five hours to review, while a Medium-severity incident might take five minutes, so the priority of the Medium-severity incident might be set at P1 and the High-severity incident at P2.

The assignee can use incident severity and incident priority together when viewing incidents. For example, an assignee can set a filter so only High-severity incidents are displayed, and then sort on priority to determine the priority of incidents for that level of severity.

12.5.1 About Email Notifications Regarding Incident Updates

You can configure email notifications to be sent automatically when certain incident updates occur (for example, when the incident severity, priority, or status is changed by another administrator). See 3.5.5 "Configure Incident Management Notifications" on page 29 for information.

12.6 States at Each Step in the Workflow

This topic contains more technical details for each step in the basic incident review workflow. At each step of the workflow, the incident has values for Incident Status and Review Status. The following sections describe the states assigned at each step of the workflow.

Step 1: Incident is created and states are assigned

In the first step of the workflow, following a policy match, an incident is automatically created. The values for Incident Status and Review Status are automatically assigned, and their values are as shown in the figure below.

If no remediation action is included with the incident, the Review Status and Remediation Actions fields are blank. In the example below, the incident includes a remediation action that has not yet been executed, so the Review Status = Awaiting Review.

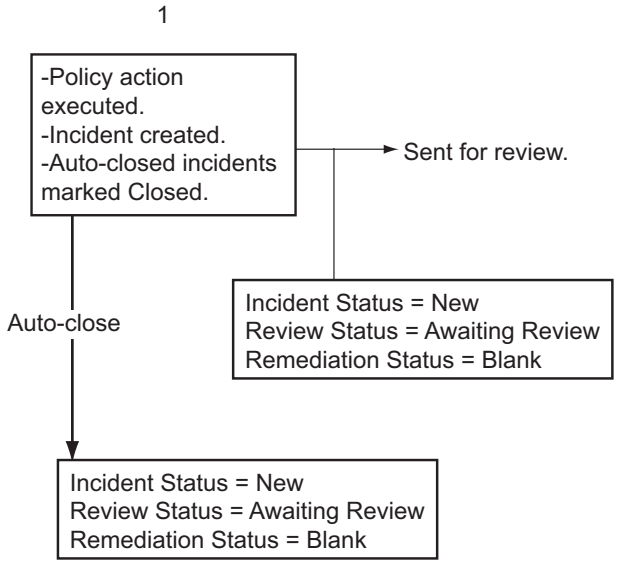


Figure 12.4: Incident States After Step 1 of the Workflow.

If the policy action was configured to automatically close the incident, then Incident Status is marked Closed. The resolution category is marked auto-closed. These auto-closed incidents can be reopened in the last stage of the workflow and be submitted to full review at that point. This feature works well when you only want to review a small number of incidents, such as in the case where a policy is producing many false positives, or in the early stages of creating and testing policies, when you are not interested in a formal review process for incidents.

Step 2: Accept or reassign incidents

In the second step of the workflow, assignees view open incidents assigned to them in the Discovery Incidents screen and, for each incident, have the option of changing the Incident Status to Accepted or reassigning the incident to another assignee. This step of the workflow is iterative until the Incident Status is changed to Accepted.

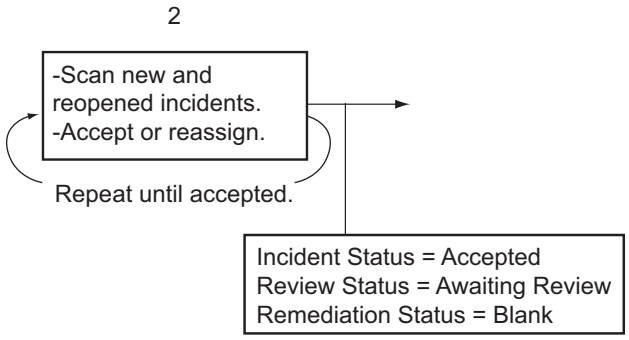


Figure 12.5: Incident States After Step 2 of the Workflow.

The Review and Remediation Status remain the same as for the previous step in the workflow.

Step 3: Review Remediation Actions

In the third step of the workflow, the assignee looks at the details of the policy match that led to the incident, implements or ignores indicated remediation actions, marks the Incident Status Resolved, and assigns a resolution category.

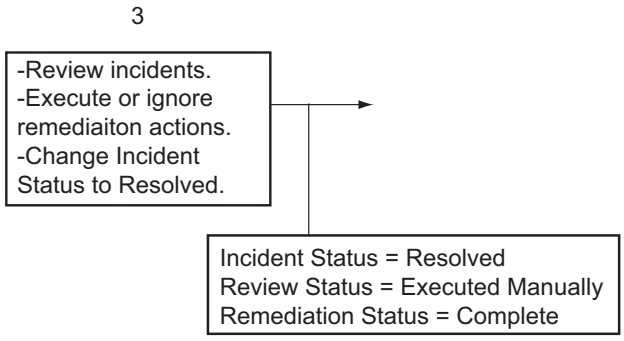


Figure 12.6: Incident States After Step 3 of the Workflow.

In the case where a remediation action for an incident was specified and the option for reviewing the action was selected during policy creation (see 9.2.1 "Creating a Discovery Policy" on page 144), the indicated action appears in the Remediation Actions column.

As an example, if an incident has a copy action included with it, "Awaiting Review" is displayed in the Review Status column on the Discovery Incidents screen and "Copy" is displayed in the Remediation Actions column. During incident review, a **Copy** button is presented in the Edit Incidents Details dialog box (or the in-line display) for the incident. If the Incident Reviewer decides to implement the copy remediation action by clicking the **Copy** button and then the **Apply** button, a message is displayed to indicate that the remediation action has been started. On the Edit Incident Details | Workflow screen, Remediation Action = pending. After the copy action has completed and the file containing the data that matched a policy has been copied to the vault, Remediation Action = Complete (OK) and the path to the vault and the copied file is displayed. On the Discovery Incidents screen, the Review Status field = Executed Manually and the Remediation Status field = Complete.

In the case of policy incidents that were not set up for remediation actions, the assignee still reviews the policy match details that led to the incident. In all cases, once the incident has been reviewed, the assignee changes the Incident Status to Resolved and assigns a resolution category to the incident.

Step 4: Close incidents

In Step 4 of the workflow, assignees change the Incident Status of resolved incidents to Closed. The assignee can also change the value of the resolution category or even change the value of Incident Status from Resolved to Reopened, to make another pass through the review workflow.

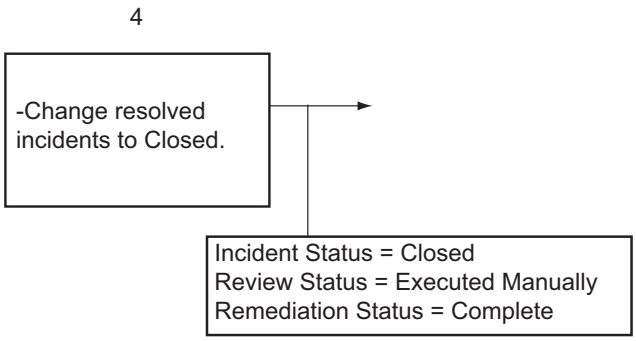


Figure 12.7: Incident States After Step 4 of the Workflow.

The Review Status does not change as a result of this step.

Step 5: Review closed incidents

In Step 5 of the workflow, assignees can review incidents marked Closed to look for any irregularities, marking the incidents Reopened, if necessary, to send them back for review. This is also the step in which incidents that were automatically closed by the policy action can be reviewed and sent for a full review, if desired.

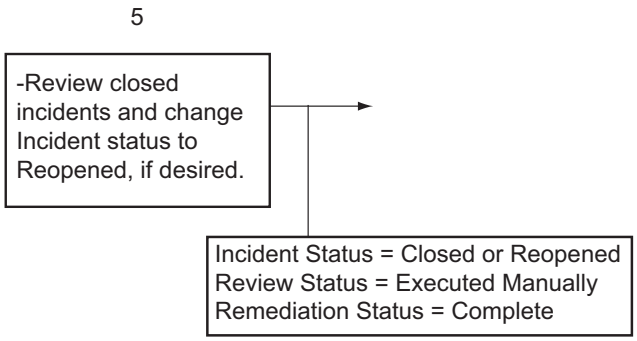


Figure 12.8: Incident States After Step 5 of the Workflow.

If the Incident Status value changes to Reopened, the workflow commences from Step 2. The Review Status does not change as a result of this step.

12.7 Examples of Incident Management

The example below provides information about automatically closed incidents. See "Step 3: Review Remediation Actions" on page 219 for an example showing implementation of a remediation action.

Example 1: Automatically close incidents

(Applies to all inspection services.)

The auto-closed response is useful when a policy has a high probability of producing false positives, in other words, data that you wish had not been discovered. Rather than having to review and mark each false positive, assignees could instead review the closed incidents for that policy and open the ones that look like bona fide violations.

The auto-close response is also useful for creating an audit trail about data that does not necessarily need to be reviewed. The incidents are logged and can be analyzed for trends and so on, but do not undergo a full incident review.

Studying the false positives could also be valuable in that it would provide information on how to reduce them, including the following options.

- The policy can be made more restrictive.
- A GreenList™ can be created to protect RedList™ matches from becoming incidents.
- Exception policies can be created so the main policy remains general and the exceptions are enumerated.

In summary, a policy action can be configured to automatically close the incident. In this case, the incident is logged, the data is unaffected, and there is no user intervention required in the workflow. Auto-closed incidents can be re-opened by the assignee in Step 5 of the workflow, at which point they would go through the full workflow review process.

12.8 Variations on the Workflow

There is a great deal of flexibility built into incident management on the DLP appliance, and you do not have to follow all the workflow steps as they are laid out.

The values for Incident Status and Review Status cannot be configured. In other words, you cannot add, remove, or change the names of values. You can make any changes to the workflow as long as you do not need more values for states than those that are provided, and as long as the new workflow is consistent with the automatic assignment of values that occurs. In most cases, the easiest way to vary the workflow will be to simplify it, that is, you do not use all the values that are provided. In this case, because values cannot be deleted, you would have to instruct assignees not to use certain

values. For example, you might tell them that they should never assign the value Closed for Incident Status.

If you design your own workflow, create a workflow diagram similar to the one shown for the default workflow (Figure 12.3), and mark the values for all of the states that will be assigned at the end of each step in the workflow. Once you have made this decision and are sure that you can use at least a subset of the existing values, it will not be hard to map the workflow onto the UI when you create policy actions and review incidents.

12.9 About Incident Filters

When viewing incidents on the Discovery Incidents screen, filters can be used to constrain the incidents that are displayed in the Discovery Incidents screen. These filters can be selected and managed using by clicking the **customize this page link**.

Discovery incidents can be filtered based on the following categories:

- Incident Type
- Repository Type
- Table Name/File Name
- Date Range
- Severity
- Incident Status
- Scan Name/Instance
- Policy
- Assignee
- Managed Host
- Database Name/File Path
- Incident Tag
- Inspected Computer
- Review Status
- Number of Matches

The following policy filters provide a text box. You can specify a group of objects by entering a portion of the object name with the * wildcard at the beginning or end of the name/string.

- Policy
- Database/File Path
- Managed Host

The following examples demonstrate when you might want to use incident filters. For example, you might want to only view incidents created with certain policies.

You can also use incident filters to view only incidents:

- With a High severity
- Resulting from a certain scan and/or scan instance
- Resulting from file or database scans (Repository Type)

Once you apply a filter, it will remain in effect. During a session, you can return to the default filters by clicking **the customize this page** link and then the **reset to default filters** link in the Customize the Incident Table dialog box.

Note: The changes made to the available filters and displayed columns are saved for each user.

12.10Discovery Incident Logs

You can print and export Discovery incident logs.

12.10.1 About Exported Discovery Incident Logs

When you export filtered or unfiltered incidents displayed on the Discovery Incidents screen to a PDF or CSV file, the exported data is saved in a file named discovery-incidents.pdf or discovery-incidents.zip (which contains the discovery-incidents.csv file).

Not every column in the exported incident log pertains to every incident, so some cells may be blank. See 11.13 "Data-Usage Incident Logs" on page 204 for instructions on saving (exporting) Discovery incidents logs.

12.10.2 Printing Discovery Incident Report Logs

To print out the current contents of the Discovery Incidents screen:

1. Click the **Print this list** button at the top of the Discovery Incidents screen. The Print dialog box will be displayed.
2. Select the desired printing options and then click **OK**.