



INSIGHT DLP APPLIANCE ADMINISTRATION GUIDE

SECTION 1 CONTENTS

Section 2 Introduction	5
Section 2.1 About the Appliance	5
Section 2.2 About Symantec DLP	6
Section 3 Conventions	7
Section 4 Prerequisites	8
Section 4.1 Hardware	8
Section 5 Default Settings	9
Section 6 Appliance Bootstrap.....	11
Section 6.1 Package Contents	11
Section 6.2 Rack the Appliance	11
Section 6.3 Network the Appliance.....	11
Section 6.4 Run Bootstrap Wizard	11
Section 7 Web Manager.....	13
Section 7.1 Screen Layout	13
Section 7.2 Info Page.....	15
Section 7.3 Device List.....	16
Section 7.4 Help.....	16
Section 7.5 Logout.....	16
Section 8 Appliance Management	17
Section 8.1 Accessing Servers.....	18
Section 8.1.1 Power Management	18
Section 8.1.2 Network Management.....	18
Section 8.1.3 Status Messages.....	19
Section 8.1.4 Updates.....	20

Section 8.2 Remote Appliance Management.....	21
Section 8.2.1 Adding a Remote Appliance.....	21
Section 8.2.2 Managing Remote Appliances	22
Section 9 DLP Server Management.....	23
Section 9.1 Power Management.....	23
Section 9.2 Network Management	23
Section 9.3 System Management.....	24
Section 9.4 Kerberos Configuration	25
Section 9.4.1 Basic Configuration	25
Section 9.4.2 Advanced Configuration	25
Section 9.5 System Backup.....	25
Section 9.5.1 Backup Retrieval	26
Section 9.6 User Impersonation.....	26
Section 9.7 Resetting Default Passwords	27
Section 9.7.1 Changing Passwords on Symantec DLP Servers.....	27
Section 9.8 Enforce Server (INSIGHT Directors Only).....	28
Section 9.8.1 INSIGHT DLP Solution Pack	28
Section 9.8.2 Accessing the Enforce Console	35
Section 9.9 Configure Data Insight (INSIGHT 2000/2100 Only)	36
Section 9.10 Configuring Network Monitor	37
Section 9.11 Configuring Email Prevent	37
Section 10 Updating Software	38
Section 10.1 OS Updates	38
Section 10.2 Symantec DLP Updates.....	38
Section 10.3 Oracle Updates (Enforce Only).....	39

Section 11 Integrating with an Existing Symantec DLP Infrastructure	41
Section 12 Napatech Cards	42
Section 13 Troubleshooting	43
Section 13.1 Root Access.....	43
Section 13.2 Using <i>tcpdump</i> to view traffic details.....	43
Section 13.3 Viewing logs.....	44
Section 13.4 Copying DLP files using WinSCP and the CLI	44
Section 14 Appendix A	45

SECTION 2 INTRODUCTION

This document describes the procedures required to set up and configure the INSIGHT DLP Appliance for Symantec Data Loss Prevention (DLP) utilizing the INSIGHT DLP Appliance Configuration Tool (IDACT). While you can read it in a linear fashion, it is best used as a non-linear reference document. As such, it is structured into sections for easy navigation. Sections 6 and 7 are particularly helpful for getting your Appliance(s) up and running quickly.

Symantec DLP documentation and this guide are available on the appliance by connecting to the **MGMT** port on the back of the Appliance, navigating to the Appliance's configured IP address (10 . 10 . 12 . 13) from your web browser, and choosing the **[Help]** link. Before you begin, it is beneficial to have a list of IP addresses, network gateway address, NTP servers, and DNS servers for your DLP environment available. A table is provided on [page 9](#) for your convenience. You may find it helpful to print the table and have your network team complete it prior to configuring your Appliance(s).

SECTION 2.1 ABOUT THE APPLIANCE

The INSIGHT DLP Appliance provides organizations a pre-packaged, pre-installed, and pre-configured Symantec DLP environment for swift deployment of data security protection.

Standardizing on a proven hardware-software platform, the Appliance simplifies and streamlines the Symantec DLP installation and configuration process by eliminating the need to procure and stage hardware, license and configure underlying operating systems and hypervisors, and test system interoperability. Deployment times are dramatically reduced, allowing you to focus on building your data security program.

With four available models, the INSIGHT DLP Appliance is scalable for unique network environments. Housing the Enforce Management Platform, Oracle database, and several key detection modules, the INSIGHT 2200 and INSIGHT 1200 Directors serve as the engine of your DLP solution. The INSIGHT 910, 610, and INSIGHT 310 Sensors extend DLP reach to include data-in-motion detection at single or multiple network egress points, or remote locations. Whether deployed together or separately, the INSIGHT Directors and Sensors combine Symantec DLP's unparalleled breadth of coverage with the rapid deployment and ease of use of a hardware-based system.

The diagram below illustrates the INSIGHT DLP Appliance concept:

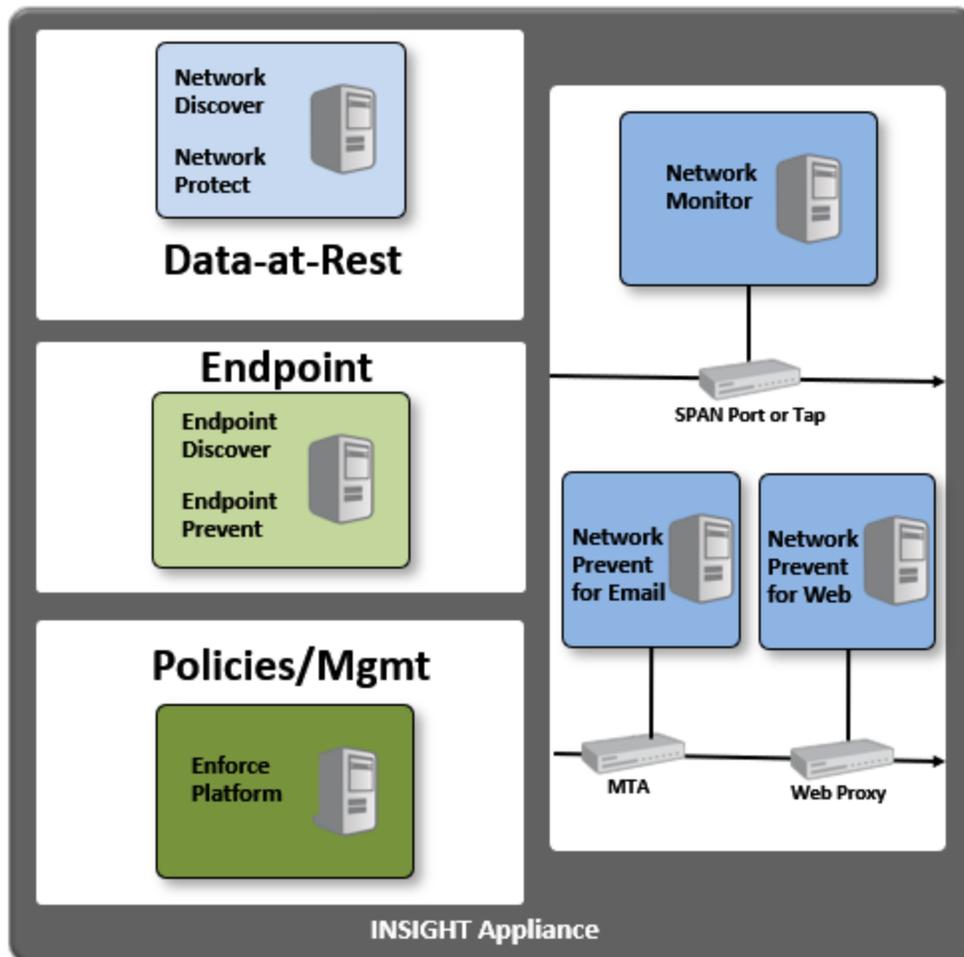


Figure 1 – INSIGHT Appliance Architecture

Note: references to the INSIGHT DLP Appliance refer to the physical hardware. Depending on the model, this can include a varying number of DLP servers. These DLP servers include the Enforce server (INSIGHT 1000, 1100, 1200 and INSIGHT 2000, 2100, 2200), and various detection servers (e.g. Network Monitor, Network Discover, etc.).

SECTION 2.2 ABOUT SYMANTEC DLP

Symantec Data Loss Prevention stops critical data (e.g., IP, PII, PHI, PCI) from leaving your organization. It manages data loss policies, incident remediation, and risk reporting from a single web-based management console. Symantec DLP can improve visibility into data loss risk and deliver measurable risk reduction, help educate and protect well-meaning employees and third parties from accidentally leaking or losing confidential data, and ensure you are complying with data privacy regulations, such as HIPAA.

SECTION 3 CONVENTIONS

This document makes use of the following conventions:

- Buttons, menu items to press, or menu choices will be surrounded by brackets and in bold type.
Example: Press [**OK**] to continue
- Items such as IP addresses and commands to enter will be listed in **bold** type and using a `Courier` type face.
Example: Use the IP address of **10 . 10 . 12 . 14** to access the Enforce Console.
- Items needing specific attention will be in **bold** and *italic* type.
Example: Connect a network cable to the ***eth0*** Ethernet port on the back of the appliance.
- **Bold**, *Italic*, and underlined words and phrases indicate references to sections within this or other documents.
Example: See ***Defaults and Adapter Values*** for the default user name and password.
- Unless noted otherwise, all user name and password fields are ***case sensitive***.
-  **Notes** point out something important or useful.
-  **Cautions** tell you about commands or procedures that may have unwanted or undesirable side effects.
-  **Warnings** tell you about commands or procedures that could be dangerous to your files, your hardware, or even yourself.

SECTION 4 PREREQUISITES

SECTION 4.1 HARDWARE

- Management PC – The Management PC used to configure the Appliance must have access to the same network as the Appliance.
- Keyboard and monitor – A keyboard and monitor are necessary to complete the Bootstrap Wizard.

SECTION 5 DEFAULT SETTINGS

The following table is available to list and reference information for your DLP environment. You may find it helpful to print the table and have your network team complete it prior to configuring your Appliance(s).

Table 1 – INSIGHT Appliance IP address configuration table

DLP Component		IP Address	Network Mask	Default Gateway	NTP Server	DNS
INTERNAL NETWORK	<i>Appliance Hardware</i>					
	<i>Enforce</i>					
	<i>Detection_1:</i>					
	<i>Detection_2:</i>					
	<i>Detection_3:</i>					
	<i>Detection_4:</i>					
	<i>Detection_5:</i>					
	<i>Detection_6:</i>					

Table 2 – Default User Names and Passwords We recommend that you change these defaults during the initial configuration process.



The default SSH port is 30001

Table 2 – Default User Names and Passwords

Default User Names and Passwords		
Appliance, Enforce, and Detection Servers OS	User Name	appuser
	Password	Chang3m3!
Enforce Management Console	User Name	Administrator
	Password	Chang3m3!
Oracle User (Enforce OS Only)	User Name	oracle
	Password	Chang3m3!
Protect User (Symantec DLP Servers)	User Name	protect
	Password	Chang3m3!

NOTE: The default SSH port for all systems is port 30001

SECTION 6 APPLIANCE BOOTSTRAP

The INSIGHT DLP Appliance ships with a Bootstrap Wizard to assist in configuring the Appliance for your environment. This wizard automatically starts after the first boot.

SECTION 6.1 PACKAGE CONTENTS

The Appliance is shipped with the following components:

-
- | | |
|---------------------|------------------------------|
| • Appliance | • U/L Safety instructions |
| • Rack mounting kit | • Rack mounting instructions |
| • Quick Start Guide | • A/C power cord(s) |
-

SECTION 6.2 RACK THE APPLIANCE

Rack the Appliance prior to bootstrap configuration. Refer to the rack mounting kit instructions provided in the box for mounting the Appliance.

SECTION 6.3 NETWORK THE APPLIANCE

You will need to connect the Appliance to your network. The physical appliance is managed via the port labeled **MGMT**. To enable Symantec DLP components to access the network, connect a network cable to the port labeled **DLP**. We recommend you connect these two cables prior to running the Bootstrap Wizard.

SECTION 6.4 RUN BOOTSTRAP WIZARD

To access the bootstrap:

- 1) Plug a keyboard into an available USB port on the back of the Appliance.
- 2) Connect a monitor to the available VGA port.
- 3) Power on the appliance. You will see the system go through the basic boot functions. Once the appliance login prompt is displayed, enter the default Appliance credentials from **Table 2 – Default User Names and Passwords**.
- 4) Change the password for the default user.
- 5) When prompted, choose [Y]es to run the first boot wizard.

- 6) Enter your network information as prompted. For DNS and NTP you may provide multiple entries on one line. Separate them with a comma only.
Example: `0.pool.ntp.org,time.nist.gov`
- 7) Type `[Exit]` to end your session.



- Do not lose this password as it will be required to continue the setup.
 - On the INSIGHT 310 changing the hostname will cause the Appliance to reboot.
-

Continue the setup on the Appliance Web Manager by going to the IP address you set on port 5000 via https. For example: <https://<configured IP>:5000>



Once all systems are running and have been configured, run the update command from the CLI to install the latest available patches. See [Section 8.1.4](#)

SECTION 7 WEB MANAGER

All INSIGHT DLP Appliances include a Web Manager to make configuration and maintenance easier. From the Web Manager you are able to:

- Start/Stop/Restart DLP Servers
- Configure DLP Server Networking information
- Enable/Disable auto-start
- Enable/Disable promiscuous mode for Network Monitor
- Manage your INSIGHT Appliance infrastructure from one system (See [Section 8](#))
- Configure backup time for Enforce
- Perform a variety of other tasks

To access the Web Manager, begin by navigating to `https://<configured_IP>:5000`. Be sure to use the IP address of the appliance as configured during the bootstrap process.

At the login screen, use the default user name and password for the Appliance. See [Table 2 – Default User Names and Passwords](#) for the default username and password if you didn't change it during the bootstrap process.

SECTION 7.1 SCREEN LAYOUT

The following screen captures are provided as a general reference. Your web interface may not look exactly the same. The Device list is the primary page for modifying system properties and performing configuration tasks.

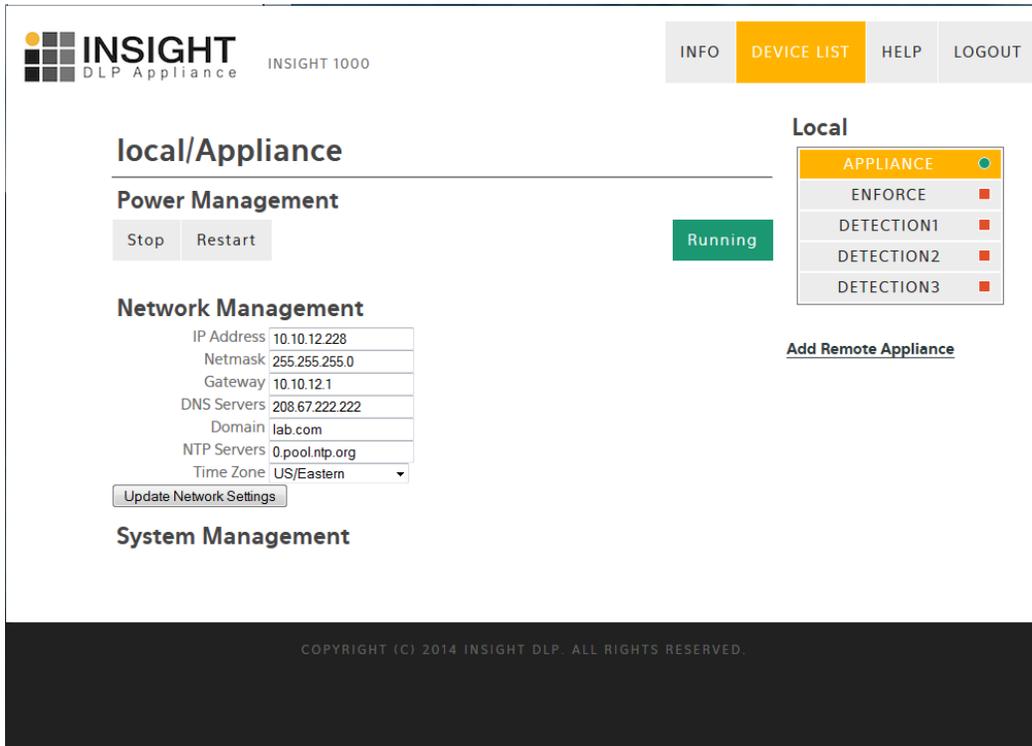


Figure 2 – Device List

Within the Device List page is the Appliance Sidebar.

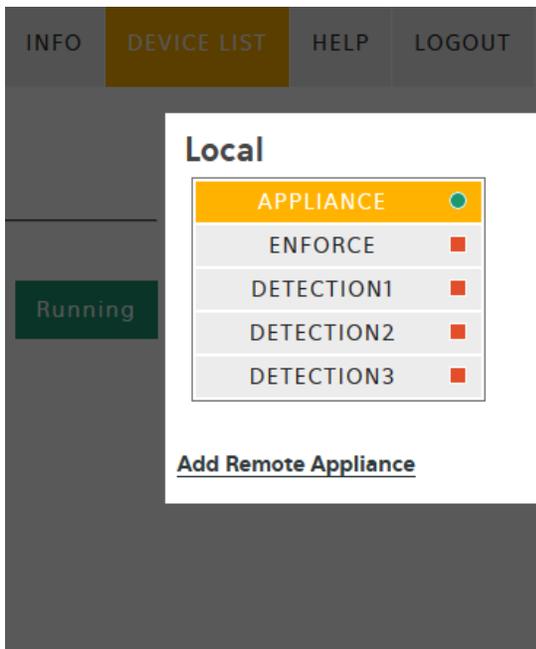


Figure 3 – Appliance Sidebar

Server information display page (main area).

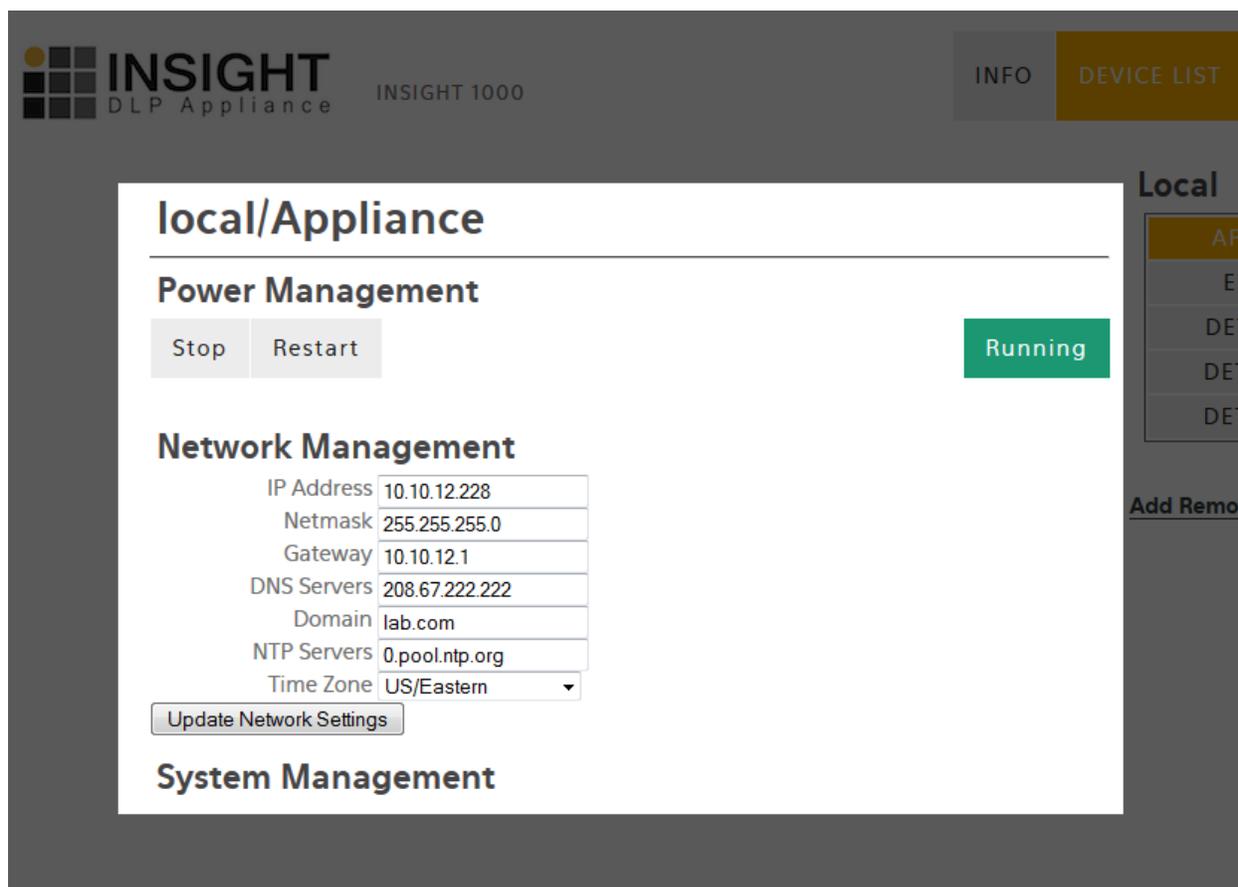


Figure 4 – Server Management

SECTION 7.2 INFO PAGE

The info page gives you an overview of the Appliance you are currently logged in to. The **Appliance Key** is the key needed when adding an appliance to be managed. See [Section 8.2](#) for remote management.

Managed by indicates whether the device is being managed by another INSIGHT Appliance. If it is, the IP address to the managing Appliance is provided as a hotlink.

Promiscuous Interface enabled on indicates which local detection server has had the span port enabled. It does not show remote Appliance Members' promiscuous mode statuses.

Appliance Version and **WebUI Version** indicate which version of the IDACT software is running on the Appliance. You will need this information when opening a support case.

Appliance Key : 0761d70839ac7d3851e376eb203a544b
Managed By :
Promiscuous Interface enabled on :
Appliance Version : INSIGHT release v2.0.0
WebUI Version : 1.0

Figure 5 – Info Page

SECTION 7.3 DEVICE LIST

The Device List page allows you to easily access, select, and configure the Appliance, as well as the Symantec DLP servers. For information on configuring Symantec DLP Servers see [Section 9](#). For configuring the Appliance see [Section 8](#).

SECTION 7.4 HELP

The Appliance ships with this administration guide and the full Symantec DLP documentation bundle for the installed version of DLP. The help page has links to these documents and links for INSIGHT Support.

SECTION 7.5 LOGOUT

Pressing the [**Logout**] button will log the user off the Appliance and return you to the login page.

SECTION 8 APPLIANCE MANAGEMENT

Users can manage the Appliance in one of two ways: using the Web Manager or using the command line interface (CLI). Most actions are available in both management interfaces.

The CLI of the INSIGHT DLP Appliance can be accessed two ways: by plugging a keyboard and monitor in to the Appliance directly or by using SSH to remotely access the Appliance. If connecting via SSH use either the hostname or IP address, as specified in the Web Manager interface, with a port of 30001. The INSIGHT console provides a list of commands available to the user. You can get a list of available commands by typing **help** or **?**. Issuing **help <topic>** will provide a short description of the command.

Command	Description
bash	Drops to the Bash prompt as the protect user on the Appliance.
clearreg	Clears out any management registration for this appliance.
cron	This call is meant for contab, and should not be run from the CLI.
exit	Exits the Appliance CLI.
list	Lists the available systems on the appliance.
multihomed	Disables the networking capabilities as the systems are multi-homed.
network	Reconfigures the Appliance Hardware Networking Information.
restart	Restarts the specified VM
service_restart	Restarts the web UI service.
shell	Initiates a root shell to the appliance. You will need to be with INSIGHT support to get the proper challenge response to run this command.
singlehomed	Enables the networking capabilities as the systems are single-homed.
start	Starts the specified VM
stop	Stops the specified server or Appliance

testnet	testnet IP/FQDN Performs common troubleshooting procedures (such as ping and traceroute) to the specified host.
update	Updates the hardware and all running VMs to current.
update_winadmin	Updates the CLI management password on the Appliance. Run this to sync password changes done within Windows to the AppMgmt account. On INSIGHT 2000 and 2100 only.

The web-based Server Management area is accessed by selecting the Device List button from the top of the screen.

SECTION 8.1 ACCESSING SERVERS

The Device List page provides an overview of the current Appliance networking configuration along with a listing of the available Symantec DLP servers. Depending on the model, there could be as many as 7 Symantec DLP servers on any one Appliance. If the Appliance is a designated management server, remote Appliances will be listed on the right-hand side of the screen in the Appliance Sidebar. See [Section 8.2](#) for more details on remote management.

SECTION 8.1.1 POWER MANAGEMENT

Clicking the Device List button will display the local Appliance configuration page. You can stop or restart the Appliance from this page. By doing so, any running DLP servers will be suspended, and the server will be cleanly shutdown or restarted. The Symantec DLP servers will resume when the Appliance is powered back on.

SECTION 8.1.2 NETWORK MANAGEMENT

Networking for the Appliance can be handled in the Web Manager interface or from the CLI. Select a server from the Appliance Sidebar to access the network management page for that server.

To change the networking from the CLI, log in via SSH or with a keyboard and mouse. Once authenticated, issue the **network** command to start the networking wizard.

Available to change are the following:

- Hostname (CLI ONLY) - Hostname of the Appliance
- IP Address - The IP address for the server
- Netmask - Subnet mask for the IP address entered above
- DNS Servers - Internal or external DNS servers referenced by IP address. For multiple DNS servers, separate them with a comma.
Example: **4 . 2 . 2 . 2 , 208 . 67 . 222 . 222**
- Domain - Internal domain name.
Example: **company.local** or **company.com**
- NTP Servers - Network Time Protocol servers for keeping the server time synchronized. As with DNS, separate multiple values with a comma.
Example: **0.pool.ntp.org, time.nist.gov**
- Time Zone - Drop-down list for time zones of the servers.

Once the fields in the web GUI have been configured, press [**Update Network Settings**] to make the changes. A red box will outline any fields with errors.

SECTION 8.1.3 STATUS MESSAGES

The Web Manager provides a quick view of the health status of the DLP servers. To refresh the status of the server, click the name of the server in the Appliance Sidebar. For servers which are currently running and manageable, there is a  (green circle) next to the name within the Appliance Sidebar. By clicking on the name of the server, you'll see a green status of **Running**.



Running

Servers in a stopped state will have a  (red square) in the Appliance Sidebar and status of **Not Running**.



Not Running

Options available in this state are to **Start** the server and **enable/disable autostart**.



You will not be able to change networking information on a system that is not running.

A system not currently manageable is indicated by a  (yellow square). Within the primary server listing, the status will be **Management Down**.

Management Down

The **Management Down** status indicates the server is in the process of starting or stopping and will be changing to a **Not Running** or a **Running** state. If you see the **Management Down** status for longer than 15 minutes, contact support.

SECTION 8.1.4 UPDATES

The operating system of the Appliance and the operating systems of the Symantec DLP Servers can be updated from the command line interface, or by using the **[Update]** button under **System Management** on the web interface of each Appliance.



To update the Operating System the Appliance needs unproxied Internet access via port 80.

If your organization utilizes a proxy, an exception must be made to allow all DLP servers access to the Internet. At a minimum, they will need access to reach `repo.insightdlp.com` via port 80.

Alternatively, you can add proxy information from the CLI of each Appliance using the **proxy** command. This will apply the given information to the Appliance and all systems running on that particular Appliance.

To update the operating system of the Appliance and the operating systems of all *running* DLP servers:

- 1) Log in to the CLI of the Appliance either via SSH or via console.
- 2) Issue the **update** command. The OS of the Appliance and running DLP servers will be updated.

Alternatively

- 3) Log in to the Web Manager of each Appliance.
- 4) Click **[Device List]** and click **[Update]** at the bottom of the page.



Any systems that do not have Internet access and any systems that are powered off will indicate a failure.

SECTION 8.2 REMOTE APPLIANCE MANAGEMENT

Beginning with IDACT version 2.0, users can manage multiple INSIGHT DLP Appliances from one web-based console. While any Appliance can be designated the main manager, we recommend using the largest INSIGHT Appliance model in the environment. For example, if you have one INSIGHT 2200, 4 INSIGHT 610s, and 6 INSIGHT 310s, we recommend designating the INSIGHT 2200 as the primary management Appliance. Appliances do not have to be centrally managed and all Appliances in an organization do not need to be managed by one system. For example, consider the following scenario:

The organization has 2 data centers across the globe. The North America data center has one INSIGHT 2200, 2 INSIGHT 610s, and 2 INSIGHT 310s. The other data center has 3 INSIGHT 610s and 2 INSIGHT 310s. Because of the change control rules for each data center, the devices must be managed by local staff. DLP traffic, however, can pass to the Enforce server located on the INSIGHT 2200 via a secured network. To enable easy management for local administrators, the Appliances have been broken up into 2 logical groups. For the North America data center, the INSIGHT 2200 is the manager. The other data center designated an INSIGHT 600 to locally manage the Appliances.

SECTION 8.2.1 ADDING A REMOTE APPLIANCE

Once you have determined how you want to manage the Appliances, you can begin by adding Appliances to the designated manager. Before adding Appliances, you must give primary networking information to the Appliance via the Bootstrap utility. See [Section 6.4 above](#). To add a remote Appliance:

1. Open a web browser and navigate to the Web Manager address of the designated management server.
2. Log in and click [**Device List**].
3. Click the [**Add Remote Appliance**] link at the bottom of the Appliance Sidebar.
 - You will be asked for two items: Server Name and Host/Address. The Server Name can be anything you want to call the Appliance. This will show up under the Local listing on the Appliance Sidebar and can be changed later.
 - We recommend a descriptive name such as "Remote_Site" or "Branch_Location". You can use either the hostname or IP address. If using the host name, it must be available to the server via DNS. Longer names will be truncated on the Appliance Sidebar.
4. Once both items have been entered, click [**Check for Appliance**].

- If the Appliance can be found with the provided information, you will be asked for the Appliance Key. If the Appliance is not found, you will be given an error and be prompted to modify the connection data.
 - If the Appliance you are adding is already being managed by another Appliance, the system will notify you of which system is already managing the Appliance, but it will still let you continue. Continuing is not recommended as it can create confusion.
5. Open a new browser window and navigate to the Web Manager address of the Appliance you are adding.
 6. Log in and copy the Appliance Key from the Info page.
 7. Paste the key in the management Appliance browser window in the appropriate field. Click **[Add New Appliance]** to complete the process.
 - You will now see the new Appliance listed in the Appliance Sidebar. If you have not already, you may now log out of the remote Appliance window.

Continue this process until all your remote Appliances have been added.

SECTION 8.2.2 MANAGING REMOTE APPLIANCES

Once you have added your Appliance(s) to your designated management Appliance, you will see them listed under the Local Appliance within the Appliance Sidebar.

To access the DLP servers on the remote Appliance, click **[Show]** next to the remote Appliance and click on the remote system you wish to access. See [Section 6](#) and [Section 8](#) for details on modifying settings.

To change the display name of the remote Appliance, click the name of the remote Appliance in the Appliance Sidebar. From this page you can also modify the Host/IP address.

To remove an Appliance from the management server, click on the name of the remote Appliance in the Appliance Sidebar. Click the **[Remove Remote Appliance]** link.

SECTION 9 DLP SERVER MANAGEMENT

Please note: all DLP servers running on the INSIGHT DLP Appliance have a custom certificate for inter-DLP communication generated by INSIGHT. If you are using the Appliance as an augmentation to an existing DLP infrastructure, you **must** change this certificate. This information can be found in the ***Symantec Data Loss Prevention Administration Guide*** under the heading, ***About the sslkeytool utility and server certificates***.



Replace or remove the factory-installed certificate if using this Appliance as an augmentation of an existing DLP infrastructure.

SECTION 9.1 POWER MANAGEMENT

Within the web manager screen, different power options will be available based upon the power status of the server. See **Section 8.1.3** for status messages. The different options, their function, and when they are available are listed here:

	Start	Stop	Restart	Power [†]	Autostart
Description	Power the server on	Gracefully shut down the server	Gracefully restart the server	Forcibly shut down the server	Tells the Appliance to automatically start the DLP server when the Appliance boots
Availability	DLP server is in a stopped state	DLP server is running	DLP server is running	System is on	Available regardless of power state



[†] ***This is equivalent to pulling the power out of a computer and should only be used as a last resort. Data loss may occur.***

SECTION 9.2 NETWORK MANAGEMENT

Networking for the Appliance and Symantec DLP servers is handled in the Web Manager interface. Select a server from the Appliance Sidebar to access the network management page for that server. The DLP servers will have pre-populated values taken from the Appliance bootstrap configuration process. The following are available to change:

- Hostname
 - Hostname for the DLP server.



- **Not available for the Appliance. Use the CLI to change the Appliance hostname.**
 - **The Symantec DLP server will be rebooted if this value is changed.**
-

- IP Address
 - The IP address for the server
- Netmask
 - Subnet mask for the IP address entered above
- DNS Servers
 - Internal or external DNS servers referenced by IP address. For multiple DNS servers, separate them with a comma.
 - Example **4 . 2 . 2 . 2 , 208 . 67 . 222 . 222**
- Domain
 - Internal domain name.
 - Example: **company.local** or **company.com**
- NTP Servers
 - Network Time Protocol servers for keeping the Appliance and DLP server time synchronized. As with DNS, separate multiple values with a comma.
 - Example: **0.pool.ntp.org, time.nist.gov**
- Time Zone
 - Drop-down list for time zones of the servers.

Once the fields have been configured, press [**Update Network Settings**] to make the changes. A red box will outline any fields with errors. Remember: if the hostname has changed, the system will reboot.

SECTION 9.3 SYSTEM MANAGEMENT

System management options are available for some Symantec DLP server components. Each INSIGHT DLP Appliance can have **one** Symantec DLP Network Monitor server. This server requires a dedicated network interface card (NIC) to receive traffic. This NIC is labeled as **SPAN** on the rear of the Appliance. If you choose to use this component of the DLP suite, you must ensure your TAP or SPAN traffic is aggregated to one port and plugged into the NIC labeled **SPAN**. Once the SPAN has been provisioned, choose a DLP Server to enable promiscuous mode traffic. Once a system has been enabled for promiscuous mode traffic, the DLP server will be listed on the Info page. See [Section 7.2](#).



Only one DLP server per Appliance can have promiscuous mode enabled.

To enable promiscuous mode, click on one of the DLP servers from the Appliance Sidebar. Scroll down to System Management and click [**Enable Monitor**]. Once enabled on the Appliance, the button will not be available for any other DLP servers on the same physical Appliance.

To disable promiscuous mode, click on the DLP server where the feature is enabled. Scroll down to System Management and click [**Disable Monitor**].

SECTION 9.4 KERBEROS CONFIGURATION

On the INSIGHT 2100 and INSIGHT 1100, these settings are made available for the Enforce server. Kerberos configuration can be set to allow users to sign in using their Active Directory credentials. There are two options available for Kerberos setup: Basic and Advanced configuration.

SECTION 9.4.1 BASIC CONFIGURATION

Basic configuration is the easiest way to setup Kerberos for Active Directory authentication. Enter a list of hosts using their fully qualified domain names (FQDN) with one host per line. The first line will be considered the primary server. Once the [**Update Kerberos Configuration**] button is pressed, the `krb5.conf` file will be created and placed in `/etc/` as `/etc/krb5.conf`. It is now up to you to configure Enforce to point to this file location. Refer to the Symantec DLP Administration guide for instructions on configuration.

SECTION 9.4.2 ADVANCED CONFIGURATION

Advanced Configuration mode allows you to enter the Kerberos data directly. After submitting the Kerberos configuration file while in the Basic setting, the system will automatically convert to Advanced mode. Take extra care upon entering this information to ensure all settings are valid.

SECTION 9.5 SYSTEM BACKUP

All INSIGHT Appliance Enforce servers have an automated backup utility which backs up the Symantec DLP Enforce server program files, indexes, log files, and the Oracle database daily. An email is sent at the end of the backup process with statistics regarding the backup. The System Backup area allows you to enable or disable the backup as well as specifying when the backup occurs. Change the drop-down menus to set the time and date for the backups and press [**Set Backup Time**] to configure.

The system will also check the table size within the Oracle database on Enforce to ensure you are not running out of space within the data files. An email with the Oracle table size and percentage of free space is sent daily as well.

Below the backup time is the email address configuration section. This allows you to specify the TO and FROM addresses of the emails the system sends. Once the email addresses have been entered, click **[Update Email Addresses]** to apply. For information on accessing the backup files see [Section 9.5.1](#). Multiple TO email addresses may be specified by separating them with a comma.

Logs of the backups (if enabled) and Oracle database size checks are stored on the Enforce server. To retrieve the log files, log in via SSH to the Enforce server and become the **protect** user. (See [Section 9.6](#) for details on user impersonation.) Navigate to `/var/log/SymantecDLP/INSIGHT` to find a list of log files.

SECTION 9.5.1 BACKUP RETREIVAL

A user may import or export files to the DLP Servers via SCP over the default SSH port. For Windows computers, the use of a file transfer client is required. INSIGHT DLP recommends WinSCP as a secure means of transferring files to or from the Appliance. It is up to the user to retrieve the backup files daily as they will be overwritten at every backup interval. It is left as an exercise for the user to script this retrieval should it be desired.

Backup files are accessible from the Enforce server in the `/backup/` directory. To access the backup files:

- For Windows clients: Log in to the Enforce server with WinSCP or another similar tool.
- For Linux clients: SSH to the Enforce server as the default user (See [Table 2 – Default User Names and Passwords](#))
- Navigate to `/backup/`
- Copy all tar.gz files to a secure location

SECTION 9.6 USER IMPERSONATION

Impersonating users is a powerful tool in the Linux world. By impersonating users, you can gain access to files, directories, and commands you may not otherwise have access to. The default user can impersonate, or **su**, the following users:

- oracle (Enforce only)
- protect

The **protect** user owns all the Symantec DLP files and processes. Following the Symantec DLP documentation, there may be times when it is necessary to login as the **protect** user. The **oracle** user owns and runs all the Oracle files and processes. One typically needs to be **oracle** for troubleshooting or applying Oracle updates as per the DLP documentation.

Accessing these accounts can be done one of two ways.

- 1) By impersonating the user from an already logged in default user session
- 2) By logging in as **protect** directly via SSH

Before logging in via SSH, you will need to change the **protect** user password. To learn how to reset passwords on the INSIGHT DLP Appliance see [Section 9.7](#).

SECTION 9.7 RESETTING DEFAULT PASSWORDS

The INSIGHT DLP Appliance ships with default passwords. These passwords can be found in [Table 2 – Default User Names and Passwords](#). It is strongly recommended that users change these default passwords as soon as possible.

SECTION 9.7.1 CHANGING PASSWORDS ON SYMANTEC DLP SERVERS

Depending on the INSIGHT DLP Appliance model, some user accounts may not exist on the system.

SECTION 9.7.1.1 RESET **APPUSER** ACCOUNT

- Log in to any DLP server as the default user
- Issue the command **passwd** and follow the prompts. You have now changed the password for the **appuser** user.

SECTION 9.7.1.2 RESET **PROTECT** ACCOUNT

- Log in to any DLP server as the default user
- Issue the command **sudo su - protect**
You will note the prompt changes from saying **appuser@...** to **protect@...**
- Issue the command **passwd** and follow the prompts. You have now changed the password for the **protect** user.

SECTION 9.7.1.3 RESET **ORACLE** OS ACCOUNT (ENFORCE ONLY)

- Log in to any DLP server as the default user
- Issue the command `sudo su - oracle`
You will note the prompt changes from saying `appuser@...` to `oracle@...`
- Issue the command `passwd` and follow the prompts. You have now changed the password for the `oracle` user.

SECTION 9.7.1.4 RESET ORACLE DATABASE ACCOUNT (ENFORCE ONLY)

The password for Symantec DLP to access the database can be changed via a script. This script will also allow you to change the `protect` account on the Enforce OS. We recommend using this script to change both the OS-level password and the Oracle database-level password at the same time. This script will synchronize the new Oracle database password with the Symantec DLP software. This is important to allow DLP to continue to access the Oracle database.

- As the default user SSH to the Enforce server
- Change directories to `/etc/appliance`
- Issue the command: `sudo ./ProtectPWDChange.sh`
- Follow the prompts. If no input is given for a particular password, the default of `protect1` will be used.

SECTION 9.8 ENFORCE SERVER (INSIGHT DIRECTORS ONLY)

The INSIGHT 2000 and INSIGHT 1000 ship with the Enforce console as part of the Appliance. This houses the Oracle database, detection policies, and is the main administration console for the Symantec DLP system.

SECTION 9.8.1 INSIGHT DLP SOLUTION PACK

Prior to leaving the factory, a Solution Pack was installed on all INSIGHT DLP Enforce servers. The solution pack is based on the Health Care Solution Pack from Symantec.

SECTION 9.8.1.1 POLICIES

The INSIGHT DLP Appliance Solution Pack does not provide any policies out of the box. This is due to a bug in the way Symantec DLP handles Discover scans with solution pack-installed policies. You may add your own via the **[Add Policy]** button.

SECTION 9.8.1.2 RESPONSE RULES

The INSIGHT DLP Solution Pack provides the following *automated* rules.

Table 3 – Automated Response Rules

Rule	Action	Conditions
Block SMTP Email Note: Only available with Network Prevent for Email.	Block SMTP Message Set Status: Escalated	When Severity Is Any Of High Protocol or Endpoint Monitoring Is Any Of SMTP
Block Web Communication Note: Only available with Network Prevent for Web.	Block HTTP/HTTPS Request Set Status: Escalated	When Protocol is any of HTTP, SSL, IM:MSN, IM:AIM, IM: Yahoo, FTP, NNTP And Severity Is Any of High
Remove Web Content Note: Only available with Network Prevent for Web.	Remove HTTP/HTTPS Web Content Set Status: Escalated	When Protocol is any of HTTP, SSL, IM:MSN, IM:AIM, IM: Yahoo, FTP, NNTP And Severity Is Any of High
Quarantine SMTP Email Note: Only available with Network Prevent for Email.	Modify SMTP Message Change Header 1 name to "X-CFilter-Quarantine" and the value to "Yes". Set Status: Escalated	Protocol or Endpoint Monitoring Is Any Of SMTP And Severity Is Any of Medium
Block Copy to Removable Media Note: Only available with Endpoint Prevent.	Endpoint: Block Set Status: Escalated	When Severity Is Any of High
Notify End User Note: Only available with Endpoint Prevent.	Endpoint: Notify	When Severity Is Any of Medium
Quarantine Stored File (on network file share) Note: Only available with Network Protect.	Protect: Quarantine File Set Status: Escalated	When Severity Is Any of High
Copy Stored File (on network file share) Note: Only available with Network Protect.	Protect: Copy File	When Severity Is Any of Medium
Notify and Resolve	Send Email Notification (to sender) Set Status: Resolved	When Severity Is Any of Low

	Set Resolution Attribute: Automatically Resolved	
Resolve with No Action	Set Status: Resolved Set Resolution Attribute: Automatically Resolved	When Severity Is Any of Info
Notify of Critical Incident	Send Email Notification (to manager) Send Email Notification (to sender) Set Status: Escalated	When Severity Is Any of High

The INSIGHT DLP Solution Pack provides the following **manual** (Smart) response rules.

Table 4 – Manual (Smart) Response Rules

Rule	Action	Conditions
Notify Sender	Send Email Notification (to sender)	Manually Executed
Notify Manager	Send Email Notification (to manager)	Manually Executed
Escalate for Investigation	Set Status: Investigation	Manually Executed
Dismiss, Bus. Process Issue	Set Status: Dismissed Set Dismissal Reason Attribute: Bus. Process Issue	Manually Executed It is recommended that you add comments to the incident indicating next steps.
Dismiss, False Positive	Set Status: Dismissed Set Dismissal Reason Attribute: False Positive	Manually Executed
Resolve, Business Issue	Set Status: Resolved Set Resolution Attribute: Business Issue	Manually Executed It is recommended that you add comments to the incident indicating next steps.
Resolve, Education Issue	Set Status: Resolved Set Resolution Attribute: Education Issue	Manually Executed It is recommended that you add comments to the incident indicating next steps.
Resolve, Employee Oversight	Set Status: Resolved	Manually Executed

	Set Resolution Attribute: Employee Oversight	It is recommended that you add comments to the incident indicating next steps.
Resolve, One-time Event	Set Status: Resolved Set Resolution Attribute: One-time Event	Manually Executed
Escalate to ISM	Set Status: Escalated	Manually Executed

SECTION 9.8.1.3 USERS AND ROLES

The INSIGHT DLP Solution Pack provides the following roles.

Table 5 – Solution Pack Roles

Role	Description	Access	Permissions
Audit	The Audit role ensures that compliance regulations are being met. Users in this role develop strategies for risk reduction at the Business Unit level and can view incident trends and risk scorecards.	All incidents All policies	<ul style="list-style-type: none"> View incidents and reports Look up attribute View all custom attributes Folder Risk Reporting Incident Reporting API
ISM	The InfoSec Manager role provides second-level incident response. This role is used to manage escalated incidents within the Information Security team.	All Escalated, Investigation, Resolved, or Dismissed incidents All policies	<ul style="list-style-type: none"> View incidents and reports Remediate incidents Look up attributes Edit all custom attributes Folder Risk Reporting
ISR	The InfoSec Responder Role provides first-level incident response for specific policies. This role is used to find broken business processes and distribute incidents to the extended remediation team.	New and Escalated incidents All policies	<ul style="list-style-type: none"> View incidents and reports Remediate incidents Perform attribute lookup View or edit some custom attributes Folder Risk Reporting Incident Reporting API Incident Update API
Policy Author	Policy Author is provided as a role to write policies with no access to sensitive data.	All incidents All policies	<ul style="list-style-type: none"> Author policies Author response rules View incidents Remediate incidents

			<ul style="list-style-type: none"> • View some incident attributes • View some custom attributes • Folder Risk Reporting API
Reporting	The Reporting role provides User Risk reporting and API access.	All incidents All policies	<ul style="list-style-type: none"> • User Reporting • Remediate incidents • Perform attribute lookup • View all custom attributes • Folder Risk Reporting
Sys Admin	The System Administrator role is enabled to encourage users to use roles other than Administrator.	All incidents All policies	<ul style="list-style-type: none"> • User administration • System administration • View incidents and reports • No access to incident details • No access to incident attributes • Discover scan control • Root content enumeration • Credential management • Export Web archives

The INSIGHT DLP Solution Pack provides the following configured user.

Table 6 – Solution Pack Users

User	Role	Description
Administrator	Global administrator	Default system administrator. This user cannot be disabled or removed.

SECTION 9.8.1.4 ATTRIBUTES

The INSIGHT DLP Solution pack provides the following attribute groups.

Table 7 – Attribute Groups

Status Group	Status
Open	New Escalated

	Investigation
Closed	Resolved
Dismissed	Dismissed

The INSIGHT DLP Solution Pack provides the following custom attributes:



To populate some of these attributes, you will need to create a connection to your directory service. See the Symantec documentation for more details.

Table 8 – Custom Attributes

Resolution	Dismissal Reason	Assigned to	Business Unit
Employee Code	First Name	Last Name	Phone
Sender Email	Manager Last Name	Manager First Name	Manager Phone
Manager Email	Region	Country	Postal Code

SECTION 9.8.1.5 PROTOCOLS

The INSIGHT DLP Solution Pack provides the following additional protocols.

Table 9 – Additional Protocols

Protocols
TCP: Telnet
TCP: SSH
TCP: SSL
TCP: Pop3
TCP: IRC
TCP: EDonkey
TCP: Gnutella
TCP: BitTorrent
TCP: Napster
TCP: DirectConnect
TCP: FastTrack

SECTION 9.8.1.6 ALERTS

Alerts have been populated for some of the more useful alert codes. Enter an email address to be alerted of any of the following:

Table 10 – Custom System Alerts

Code	Name	Description
1007	{0} restarts excessively	Process {0} has restarted {1} times during last {2} minutes
1014	Low disk space	Hard disk space is low. Symantec Data Loss Prevention server disk usage is over {0}%.
1205	Incident limit reached for Policy "{0}"	The policy "{0}" has found incidents in more than {1} messages within the last {2} hours. The policy will not be enforced until the policy is changed, or the reset period of {2} hours is reached.
1401	Invalid license	The ICAP channel is not licensed or the license has expired. No incidents will be detected or prevented by the ICAP channel.
1403	Out of memory Error (Web Prevent) while processing message	While processing request on connection ID{0}, out of memory error occurred. Please tune your setup for traffic load.
1500	Invalid license	The SMTP Prevent channel is not licensed or the license has expired. No incidents will be detected or prevented by the SMTP Prevent channel.
1800	Incident Persister is unable to process incident Incident	Persister ran out of memory processing incident {0}.
1802	Corrupted incident received	A corrupted incident was received, and renamed to {0}.
1815	Low disk space on incident server	Hard disk space for the incident data storage server is low. Disk usage is over {0}%.
2111	Runaway lookup detected	One of the attribute lookup plug-ins did not complete gracefully and left a running thread in the system. Manager restart may be required for cleanup.
2202	License has expired	One or more of your product licenses has expired. Some

		system feature may be disabled. Check the status of your licenses on the system settings page.
2203	License about to expire	One or more of your product licenses will expire soon. Check the status of your licenses on the system settings page.
2300	Low disk space	Hard disk space is low. Symantec Data Loss Prevention Enforce Server disk usage is over {0}%.
2301	Tablespace is almost full	Oracle tablespace {0} is over {1}% full.
2302	{0} not responding	Detection Server {0} did not update its heartbeat for at least 20 minutes.
2309	System statistics update failed	Unable to update the Enforce Server disk usage and database usage statistics. Please look at the Enforce Server logs for more information.
2500	Unexpected Error Processing Message	{0} encountered an unexpected error processing a message. See the log file for details.



For more information on Solution Packs, see the Symantec documentation.

SECTION 9.8.2 ACCESSING THE ENFORCE CONSOLE

Once all DLP components have been configured and are running, access the Enforce Console of your DLP environment.

- 1) Go to: https://<enforce_ip_address> where the <enforce_ip_address> is the IP address you configured while setting up the Enforce Server.



If the Appliance is an add-on to an existing DLP infrastructure containing an existing Enforce server, follow the [Integrating with an Existing Symantec DLP Infrastructure](#) to remove the custom inter-DLP communication certificate from the detection server(s).

- 2) Use the default information provided in **Table 2 – Default User Names and Passwords** for the default username and password.
- 3) After logging in, you may be presented with the Symantec Data Loss Prevention End User License Agreement (EULA). You must read and complete the **[Name]**, **[Title]**, and **[Company]** fields and press **[I Accept]** to continue.
- 4) After accepting the EULA, you will be immediately directed to the **System Overview** section.
- 5) Click **[Settings]** then click **[Configure]**.
- 6) Under the **License** section, click **[Browse]** to choose your Symantec DLP SLF file. This was provided to you by Symantec after your purchase of Symantec Data Loss Prevention. If you do not have this file, please contact your Symantec sales representative, Symantec Partner / reseller sales representative, or Symantec Technical Support to receive another copy of the file.
- 7) Once you've chosen the DLP SLF file, click **[Open]** on the dialog box.
- 8) The path to your DLP SLF file should be filled out by the system.
- 9) Click **[Save]** near the top of the screen.
- 10) You will now be able to register your detection servers by following the **Registering a detection server** steps detailed in the Symantec Data Loss Protection Installation guide available from Symantec.



INSIGHT DLP recommends changing the default Administrator password for Enforce.

SECTION 9.9 CONFIGURE DATA INSIGHT (INSIGHT 2000/2100 ONLY)

Data Insight is an advanced Data-at-Rest scanning component of Symantec DLP. The INSIGHT DLP Appliance has one (1) instance of Data Insight installed on the INSIGHT 2000 or 2100 only. To access and configure Data Insight, perform the following tasks.



- **The Data Insight server is shipped with a Windows Server 2008 R2 Standard edition license. You will find this product key sticker affixed to the outside lid or chassis of the INSIGHT 2000/2100 Appliance.**
 - **You will need Internet access to complete the registration process.**
-

- 1) Log in to the web interface of the INSIGHT 2000/2100 and configure the Data Insight server as you would any other DLP system.
- 2) Using another computer with the Windows operating system or a program that can use RDP (Remote Desktop Protocol), connect to the Data Insight system via the IP address or hostname configured in step 1. Refer to **Table 2 – Default User Names and Passwords** for the default credentials.
- 3) If prompted, trust the computer and log in with the Administrator credentials.

- 4) You may be presented with a pop-up indicating that Windows is not yet activated. If so, click **[Activate Now]**. If you are not presented with this pop-up,
 - a. Right click on **[Computer]** on the desktop and choose **[Properties]**.
 - b. Click the **[Activate Windows now]** link at the bottom of the window.
 - c. Select **[Activate Windows online now]**.
- 5) Locate the product key sticker affixed to the INSIGHT 2000/2100 Appliance lid or chassis. This key will need to be entered into the **[Product Key]** field *exactly as written*.
- 6) Press **[Next]** to complete the activation process.

SECTION 9.10 CONFIGURING NETWORK MONITOR

One Symantec Data Loss Prevention Network Monitor server can be configured for any one INSIGHT DLP Appliance. From the Web UI, choose the detection server you wish to use as the Network Monitor server. Click **[Enable Monitor]** under **System Management**. See [Section 9.3](#) for more information.



Only one DLP server per Appliance can have promiscuous mode enabled.

Follow the documented steps for adding a Network Monitor server in the Symantec DLP documentation. When choosing the network interface on which to monitor traffic, choose **eth1** from within the Enforce console.

SECTION 9.11 CONFIGURING EMAIL PREVENT

To allow the Network Prevent Email server to pass email through, you need to change how the Linux firewall (iptables) handles traffic. The Symantec DLP documentation contains a list of commands for doing this on the Prevent Email server. On the INSIGHT Appliance, you must preface the commands with **sudo**. The save command is different as well since we're not going to overwrite iptables's configuration, but instead allow iptables to save its running configuration instead.

To facilitate getting the Prevent Email server running quickly, the commands are listed here in order. Within an SSH session to the Prevent Email server, you can copy and paste this entire block as the default user.

```
sudo iptables -N Vontu-INPUT
sudo iptables -A Vontu-INPUT -s 0/0 -p tcp --dport 25 -j ACCEPT
sudo iptables -I INPUT 1 -s 0/0 -p tcp -j Vontu-INPUT
sudo iptables -t nat -I PREROUTING -p tcp --destination-port 25 -j
REDIRECT --to-ports=10025
sudo /etc/init.d/iptables save
```

If you want to remove this iptables entry, issue the following command:

```
sudo iptables -t nat -D OUTPUT -o lo -p tcp --destination-port 25 -j REDIRECT --to-ports=10025
```

SECTION 10 UPDATING SOFTWARE

There are three primary software groups that can be updated:

- 1) OS updates
- 2) Symantec DLP updates
- 3) Oracle patches

Care must be taken when applying updates as data loss could occur. We recommend making a backup prior to applying any updates.

SECTION 10.1 OS UPDATES

To update the Operating Systems for the INSIGHT DLP Appliance and resident DLP servers see [Section 8.1.4](#). When applying OS updates, you not only receive updates to the operating system but also to the IDACT software. Check the INSIGHT Support Portal for notices about available updates, security patches, and bug fixes as they become available.

SECTION 10.2 SYMANTEC DLP UPDATES

As Symantec releases updates to the DLP software, the INSIGHT DLP team tests these releases on currently supported INSIGHT DLP Appliances. Once a new version or patch is officially supported by INSIGHT DLP, a notice is posted within the INSIGHT Support Portal. DLP updates and patches are available from Symantec File Connect.



Upgrading to an unsupported version of Symantec DLP will invalidate your INSIGHT DLP Appliance support!

It is *imperative* that users check the supported version of Symantec Data Loss Prevention prior to updating. Not doing so may lead to your support being nullified and your DLP system being in an unstable state.

To verify your Symantec DLP version check within the DLP console under [**System > Servers > Overview**]. Alternatively you can SSH to the Enforce server and look at the **Manager.ver** file located in `/opt/SymantecDLP/Protect/`.

Once you have verified the desired version of Symantec DLP is supported, follow the Symantec Upgrade guide for updating Linux versions. You will be asked for the Oracle program directory; enter the following:

```
/opt/oracle/product/<version>/db_1
```

Where <version> can be determined by running the following command on the Enforce server as the *oracle* user:

```
$ORACLE_HOME/OPatch/opatch lsinventory | awk '/^Oracle Database/{print $NF}'
```

When the directions tell you to run the post upgrade script as root, do the following:

- 1) Log in via SSH to the DLP Server being upgraded as the default user.
- 2) Change directory to `/etc/SymantecDLP-Updates/<NEW_DLP_VERSION>`
- 3) Run the script using the **sudo** command.
Example: **sudo ./12.0.1_upgrade_root_script.sh**
- 4) The script will complete and you can now logout.

SECTION 10.3 ORACLE UPDATES (ENFORCE ONLY)

Oracle updates can be applied by the default user. As with Symantec DLP updates, you *must* check the INSIGHT Support Portal to verify that the update being applied has been tested and is supported. Only the Oracle Patch Set Updates (PSU) provided by Symantec should be used.



- **Applying unsupported Oracle PSUs will invalidate your INSIGHT Appliance support.**
 - **ONLY use PSUs supplied by Symantec via File Connect.**
-

Follow the documentation provided by Symantec to apply the Oracle PSU. Refer to [Section 9.6](#) on how to gain access to the *oracle* user.

Prior to updating Oracle, ensure the version of Oracle you are running is supported with the updates you want to apply. To determine the Oracle version run:

```
$ORACLE_HOME/OPatch/opatch lsinventory | awk '/^Oracle Database/{print $NF}'
```

Alternatively there is a script located in the Oracle home directory called `ora_version.sh`. Run this as the *oracle* user and it will print the current Oracle version.

SECTION 11 INTEGRATING WITH AN EXISTING SYMANTEC DLP INFRASTRUCTURE

The INSIGHT DLP Appliance makes use of a custom inter-DLP communication certificate for Enforce to securely communicate with the detection servers on the INSIGHT DLP Appliances. When adding a detection server on an INSIGHT DLP Appliance to an existing, non-INSIGHT Enforce server controlled environment, you **must** remove the custom certificate and restart the **VontuMonitor** service.

1. Log in to the detection server(s) via SSH as the **appuser**.
2. Follow [Section 9.6](#) to assume the role of **protect**.
3. Change directories to **/opt/SymantecDLP/Protect/keystore** by issuing:
`cd /opt/SymantecDLP/Protect/keystore`
4. Remove the file called **monitor.sslKeyStore** by issuing the command:
`rm monitor.sslKeyStore`
5. Restart the **VontuMonitor** service by:
`/etc/init.d/VontuMonitor restart`
6. Type **exit** to return to the **appuser** profile.
7. Type **exit** again to exit the SSH session.

Your detection server is now ready to be registered to your existing Symantec DLP Enforce server. See the [Registering a detection server](#) steps detailed in the Symantec Data Loss Protection Installation guide available from Symantec.

SECTION 12 NAPATECH CARDS

Some Small Sensor Appliances ship with Napatech cards built-in. These cards have been configured to automatically load the drivers needed at boot time. Some small changes need to be done on the configuration of the Network Monitor server within DLP for the Napatech cards to start capturing. Refer to the hardware guide which shipped with the sensor Appliance to determine which port should be used on your Napatech card.

In the Advanced Server settings page of the Napatech-enabled Small Sensor Appliance, enable the Napatech packet capture by setting the following flag to **true**:

PacketCapture.IS_NAPATECH_ENABLED

Update the value of the path to the Napatech driver tools directory by entering the path in the field for the following entry:

PacketCapture.NAPATECH_TOOLS_PATH

The path on the Small Sensor Appliance is:

/opt/napatech/bin

Restart the services on the Network Monitor server for the changes to be applied.

When using an Appliance with a Napatech card, you do **not** need to click the [**Enable Monitor**] button under System Management on the Appliance Web UI.

SECTION 13 TROUBLESHOOTING

The following are some troubleshooting steps and commands which can assist with common issues.

SECTION 13.1 ROOT ACCESS

The default user has root access to the following Linux commands. Accessing commands as root other than the commands listed below will require a support case. To get more information about a command, while on a SSH session, issue the command `man <command_name>` to display the manual entry for the command. Press `q` to exit the manual program.



To gain CLI access to an INSIGHT 300, log in as the default user, and enter `bash` as the command.

Issuing the `sudo` command before any of the following commands will execute that command as root.

Command	Example	Result
man	<code>man tcpdump</code>	Display the manual entry for running tcpdump
shutdown	<code>sudo shutdown -r -t 10</code>	Restart the system in 10 seconds
ntpdate	<code>sudo ntpdate 0.pool.ntp.org</code>	Update the time from the server 0.pool.ntp.org
ntpd	<code>sudo vi /etc/ntp.conf</code>	Edit the NTP configuration file
tcpdump	<code>sudo tcpdump -i eth1 port 80</code>	Dump network traffic from NIC eth1, filtering on only port 80 traffic, to the screen
yum update	<code>sudo yum update</code>	Update system software
route	<code>route</code>	Shows the system's IP routing table
ifconfig	<code>ifconfig</code>	Displays the network adapter and associated data
iptables	<code>sudo iptables -L</code>	Shows the current iptables configuration
service	<code>sudo service ntpd restart</code>	Restarts the ntpd daemon

SECTION 13.2 USING TCPDUMP TO VIEW TRAFFIC DETAILS

Tcpdump is a CLI tool which is useful for troubleshooting a component like Network Monitor. The tool allows the user to view the details of the TCP traffic the server is sending and receiving. Tcpdump is

available on all Detection servers, Enforce and the Appliance itself. This is often important when verifying the type of traffic of being spanned or sent by a network TAP or span port to Symantec DLP Network Monitor. By default, tcpdump gives you information about the source IP or destination IP and port number by printing out packet headers.

SECTION 13.3 VIEWING LOGS

DLP logs can be

- Downloaded directly from the Enforce console by navigating to System > Server > Logs
- Accessed at the CLI via the default DLP user in `/var/log/SymantecDLP`. See [Section 9.6](#) for information on accessing resources as the default DLP user.
- The default user is restricted from accessing OS-level logs. Please open a support case if access to these logs is required.

SECTION 13.4 COPYING DLP FILES USING WINSCP AND THE CLI

Users can access the DLP system as the default Symantec user (`protect`) from the command line. The easiest way to move DLP-related files to and from the Symantec DLP software is with this user.

- Connect to Enforce with WinSCP and navigate to the desired DLP directory on the right-hand pane.
- Drag the file from the left pane representing your local machine or source directory to the right pane representing the Enforce server.
- Open an SSH session and connect to Enforce and login with your `protect` user credentials.

Alternatively log in with the default user and change to the `protect` user. See [Section 9.6](#) for information on accessing resources as the default DLP user.

SECTION 14 APPENDIX A

Figure 1 – INSIGHT Appliance Architecture	6
Figure 2 – Device List	14
Figure 3 – Appliance Sidebar.....	14
Figure 4 – Server Management.....	15
Figure 5 – Info Page	16