Vormetric
Data Security™

Vormetric Data Security Manager (DSM)

DSM Common Criteria Addendum

Document Version 1.0

February 10, 2016

Vormetric Data Security Platform
Vormetric Data Security Manager
DSM Common Criteria Addendum v1.0

Contents

Preface

The *DSM Common Criteria Addendum* describes how to set up configure the Vormetric Data Security Manager.

About Common Criteria

The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for certification of the security of computer systems, networks, and application software. The certification ensures that the claims about the security attributes of the evaluated product were independently verified in the evaluated configuration operated in the specific environment.

Audience

The *DSM Common Criteria Addendum* is for systems administrators who install the Vormetric DSM and connect it to the network.

For more information

Supplementary product guidance can be found on the Vormetric website at:

http://www.vormetric.com

Assumptions

This document assumes that you have the following:

- Vormetric Data Security Manager (DSM), either virtual or physical version.
- Related VDS documentation.
- Basic knowledge of network configuration operations.

There are specific conditions that are assumed to exist in the Vormetric DSM operational environment. The following table lists the assumptions about the operational environment:

Table 1: Operational Environment

Objective	Assumption
Administration	There will be dedicated administrators that will be responsible for configuring and managing the DSM
Installation	The appliance will be installed, managed, and operated in a secure manner.
Competency	Personnel working as administrators shall be carefully selected and trained for proper operation of the appliance.
Access Control Products	One or more access control products will be deployed in th Operational environment to protect organizational assets.
Protected Environment	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
System Time	The Operational Environment will provide reliable time data.
Identification	The Operational Environment shall be able to identify an authorized user requesting access to the appliance.

The following table identifies assumptions applicable to the Vormetric DSM

Table 2: Vormetric DSM Assumptions

Assumption	Definition
Connectivity	The appliance will be able to establish connectivity to other ESM products in order to share security data.
Authentication	The Operational Environment will provide mechanisms to the DSM that reduce the ability of an attacker to impersonate a legitimate user during authentication.
System Time	The appliance will receive reliable time data from the Operational Environment.
Identification	The appliance will receive identity data from the Operational Environment.
Administration	There will be one or more competent individuals assigned to install, configure, and operate the appliance.

For support and troubleshooting issues

- help.vormetric.com
- support@vormetric.com

- (877) 267-3247

For Vormetric Sales:

- http://enterprise-encryption.vormetric.com/contact-sales.html
- sales@vormetric.com
- (888) 267-3732

DSM: Initial Configuration

1

This chapter describes how to configure the DSM v6000 appliance.

How to Access the DSM

The Vormetric Data Security Manager (DSM) is accessed locally via the command line interface (CLI) from a terminal device connected to through a serial port, and is administered remotely via a web interface over a secure session. The CLI access is intended for initial configuration and disaster recovery activities. Once the device is configured, it is administered via the remote Web Management Interface.

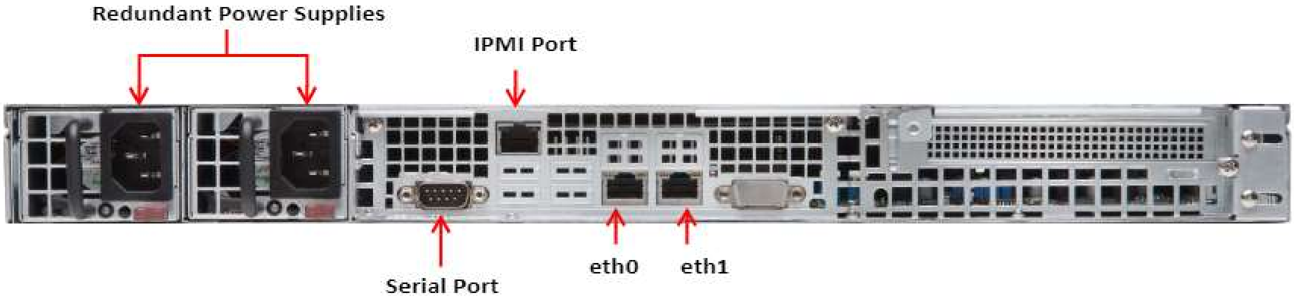
Accessing the CLI

The initial DSM configuration is done via the CLI. The CLI requires a physical connection to the DSM serial port, and is accessed directly via a terminal device connected to the DSM. This interface enforces user authentication.

To access the DSM CLI, you need connect through the console serial port with a DB-9 cable using a compliant terminal emulator program using the following parameters:

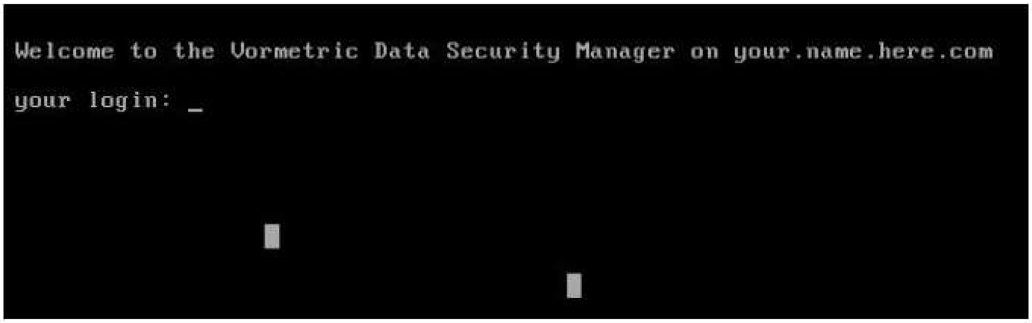
- Terminal Type: VT100
- Baud Rate: 9600
- Parity: None
- Data bits: 8

Figure 1: Connecting to the serial port



When successfully connected you will see the following screen:

Figure 2: Login screen



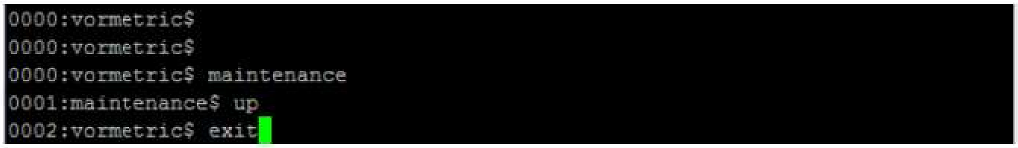
```
Welcome to the Vormetric Data Security Manager on your.name.here.com

your login: _
```

The login screen displays a welcome message and the host name as `your.name.here.com` since the appliance is still to be configured.

To terminate a CLI console session at any time, type `exit` at the main prompt or in any of the command menus, and press Enter. The CLI console will close and log you out.

Figure 3: Log out



```
0000:vormetric$
0000:vormetric$
0000:vormetric$ maintenance
0001:maintenance$ up
0002:vormetric$ exit
```

Configuring the DSM

This section describes how to configure the appliance host name, network settings, Network Time Protocol (NTP), LDAP, and Syslog servers, and how to generate a new certificate authority (CA) for the DSM. It also describes how to enable Common Criteria mode and verify web access.

To begin the configuration

1. Log in to the CLI console with the default user name and password.

   At the prompt, type:

   ```
   Login: cliadmin
   Password: cliadmin123
   ```

   After you login for the first time, you will be prompted to change the password. Refer to "Password Management" on page 28 for details about how to configure password settings.

   Next, you will be prompted to enter a password for the IPMI. The IPMI is disabled once the device is in CC mode.

   You are now accessing the CLI and will be presented with the `vormetric$` prompt on the console.

2. To check version information, navigate to the maintenance commands menu, type:

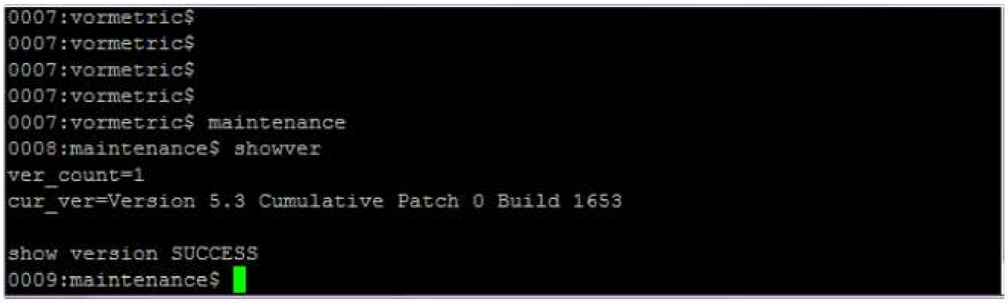
   ```
   0001:vormetric$ maintenance
   ```

   At the prompt, type:

   ```
   0002:maintenance$ showver
   ```

   Please visit the CCEVS Product Compliant List (https://www.niap-ccevs.org/Product/) to ensure the validated version of the product is used.

Figure 4: Software version check



```
0007:vormetric$
0007:vormetric$
0007:vormetric$
0007:vormetric$
0007:vormetric$ maintenance
0008:maintenance$ showver
ver_count=1
cur_ver=Version 5.3 Cumulative Patch 0 Build 1653

show version SUCCESS
0009:maintenance$
```

To back to the main menu, type `up`

Configure network settings

1. Navigate to the network commands menu, at the prompt, type:
   `0004:vormetric$ network`
2. Add the IP address for the DSM, type:
   `0005:network$ ip address init <DSM IP address>/<subnet mask (example: 16 or 24)> dev eth0`
   Example: `ip address init 10.3.1.1/16 dev eth0`
3. Optionally add the IP address for the default gateway, type:

`0005:network$ ip route add default table main.table dev eth0 via` [*Ethernet port eth0 or eth1*] *<IP address for the default gateway>*

Example: `0005:network$ ip route add default table main.table dev eth0 via eth0 10.3.1.8`

4. Verify the interface settings, type:
   ```
   0005:network$ ip address show
   ```
5. Verify the route settings, type:
   ```
   0005:network$ ip route show
   ```
6. To set the primary DNS server for the DSM, type:
   ```
   0005:network$ dns dns1 <ip address for dns server 1>
   ```
7. To set the search domain, type:
   ```
   0005:network$ dns search <search_domain>
   ```
8. Show the DNS settings, type:
   ```
   0005:network$ dns show
   ```
9. Return to the main menu, type:
   ```
   0005:network$ up
   ```
10. This will take you back to the main menu:
    ```
    0006:vormetric$
    ```

Set host name for the appliance

1. Navigate to the system commands menu, type:
   ```
   0006: vormetric$ system
   ```
2. To set the host name for your appliance, type:
   ```
   0006: system$ setinfo hostname <hostname>
   ```
3. To verify the host name setting, type
4. `0006:system$ setinfo show`

Configure NTP server

1. Navigate to the maintenance commands menu, type:
   ```
   0007:vormetric$ maintenance
   ```
2. Add a new ntpdate server, type:

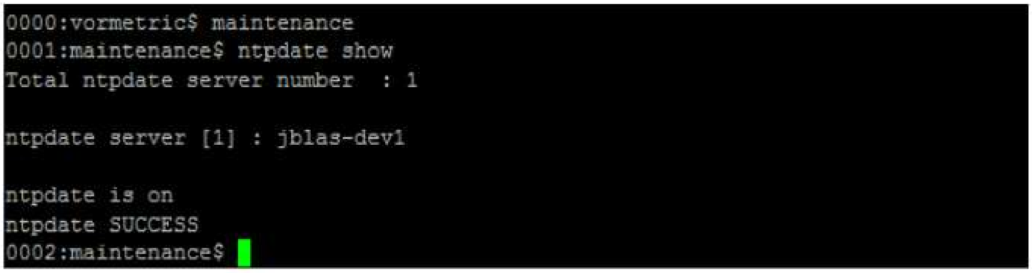
   `0008:maintenance$ ntpdate add` *<IP address/host name for the ntpdate server>*

   Repeat this step for each ntpdate server.
3. Activate the ntpdate server connection. Type,
   ```
   0008:maintenance$ ntpdate on
   ```
4. Show the current ntpdate settings. Type

```
0008:maintenance$ ntpdate show
```

You will see the following message:

Figure 5: NTP server configured



```
0000:vormetric$ maintenance
0001:maintenance$ ntpdate show
Total ntpdate server number  : 1

ntpdate server [1] : jblas-dev1

ntpdate is on
ntpdate SUCCESS
0002:maintenance$
```

Generate the DSM Certificate Authority

a. Navigate to the system commands menu, type,
`security genca`

b. Answer the following prompts:

- What is the name of your organizational unit? [departmentName]:
- What is the name of your organization? [mycompany]:
- What is the name of your City or Locality? [San Jose]:
- What is the name of your State or Province? [California]:
- What is your two-letter country code? [US]:

c. Return to the main menu. Type,
`up`

NOTE: The SHA-1 signature algorithm is not supported in CC mode for the DSM web certificate.

Common Criteria Mode

The Common Criteria mode ensures that your DSM appliance is operating within the Common criteria security specifications.

Checking Software Version

You can check which version of the DSM software is installed on your appliance from the web interface or the CLI.

From the web interface

1. On the web UI, click **System > About**.
2. The *About* window displays information about the software version installed.

From the CLI

1. Log on to the CLI console.
2. Navigate to the maintenance category commands, type:

   ```
   0001:vormetric$ maintenance
   ```

3. At the prompt, type:

   ```
   0002:maintenance$ showver
   ```

   The version information is displayed at the prompt.

FIPS Mode

The Vormetric DSM appliance runs in FIPS mode by default. There is no option to disable FIPS mode.

Ciphers and Protocols

The DSM supports the following ciphers and protocols for external communications:

1. TLS 1.0/1.1/1.2
   - TLS_RSA_WITH_AES_256_CBC_SHA,
   - TLS_RSA_WITH_AES_128_CBC_SHA
2. TLS 1.2
   - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
   - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384

Enabling CC Mode

To enable Common Criteria on your DSM appliance, you need to enable it via the CLI, and then ensure secure communications for administration of your appliance.

1. On the CLI console, navigate to the systems commands menu, type:

   ```
   0001:vormetric$ system
   ```

   To check CC mode status, type:

   ```
   0002:system$ security cc show
   ```

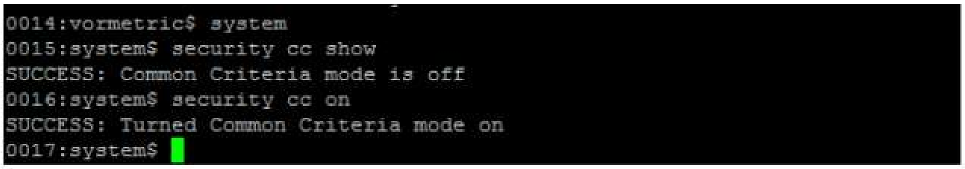
   If CC mode has not been turned on you will see a message that CC mode is off.

To turn CC mode on, type:

```
0002:system$ security cc on
```

You will see the following message:

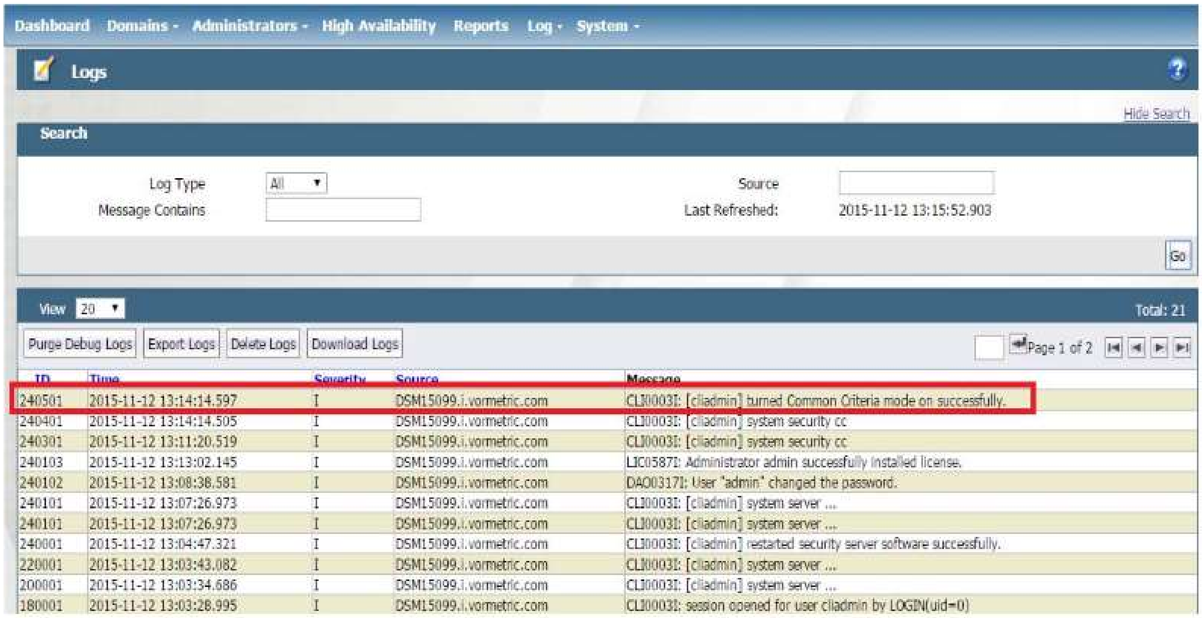
Figure 6: CC mode on



```
0014:vormetric$ system
0015:system$ security cc show
SUCCESS: Common Criteria mode is off
0016:system$ security cc on
SUCCESS: Turned Common Criteria mode on
0017:system$
```

A corresponding log entry is also created:

Figure 7: CC mode on log entry



Log Type: All
Message Contains:
Source:
Last Refreshed: 2015-11-12 13:15:52.903

View 20 Total: 21

ID	Time	Severity	Source	Message
240501	2015-11-12 13:14:14.597	I	DSM15099.i.vormetric.com	CLI0003I: [cliadmin] turned Common Criteria mode on successfully.
240401	2015-11-12 13:14:14.505	I	DSM15099.i.vormetric.com	CLI0003I: [cliadmin] system security cc
240301	2015-11-12 13:11:20.519	I	DSM15099.i.vormetric.com	CLI0003I: [cliadmin] system security cc
240103	2015-11-12 13:13:02.145	I	DSM15099.i.vormetric.com	LIC0587I: Administrator admin successfully installed license.
240102	2015-11-12 13:08:38.581	I	DSM15099.i.vormetric.com	DAO0317I: User "admin" changed the password.
240101	2015-11-12 13:07:26.973	I	DSM15099.i.vormetric.com	CLI0003I: [cliadmin] system server ...
240101	2015-11-12 13:07:26.973	I	DSM15099.i.vormetric.com	CLI0003I: [cliadmin] system server ...
240001	2015-11-12 13:04:47.321	I	DSM15099.i.vormetric.com	CLI0003I: [cliadmin] restarted security server software successfully.
220001	2015-11-12 13:03:43.082	I	DSM15099.i.vormetric.com	CLI0003I: [cliadmin] system server ...
200001	2015-11-12 13:03:34.686	I	DSM15099.i.vormetric.com	CLI0003I: [cliadmin] system server ...
180001	2015-11-12 13:03:28.995	I	DSM15099.i.vormetric.com	CLI0003I: session opened for user cliadmin by LOGIN(uid=0)

You must restart the DSM after enabling CC mode. The restart command stops and then starts the DSM software. It does not reboot the appliance. To restart the server:

1. Navigate to the system menu, type:

```
0005:vormetric$ system
```

2. At the system prompt, type:

```
0006: system$ server restart
```

You will see the following message:

```
Do you want to restart the server software ? (y/n):y
Restarting now...
Stopping Security Server...done.
Stopping the data store...done.
```

```
Starting Security Server...done.
SUCCESS: The security server software is restarted.
0010:system$
```

2. Disable IPMI:

   Navigate to the IPMI commands menu and type:

   ```
   0006:vormetric$ ipmi
   0007:ipmi$ disable
   ```

   Confirm that you want to turn off IPMI.

3. Disable CLI over SSH:

   Navigate to the network commands menu and type:

   ```
   0004:vormetric$ network
   0005:network$ ssh off
   ```

   You will see a warning informing you that the DSM LCLI will only be accessible via the serial port.

   Type `yes` and press Enter to continue.

Configuring the Login Banner

A banner with a default message, ‘Welcome to Vormetric Data Security Management Web GUI’ is displayed on the login screen. You can change this default banner message.

To configure the message from the web interface:

A banner with a message, ‘Welcome to Vormetric Data Security Management Web GUI’ is displayed on the login screen. You can change this default banner message after you log on to the system.

To configure the message from the web interface:

1. Log on to the Web Management Interface as an administrator of type System or All.
2. Select **System > General Preferences** in the menu bar.
3. In the **General Preferences** window, click the **Login Banner** tab.
4. Type the message you want to display on the login screen in the text box.
5. Click **Apply**.

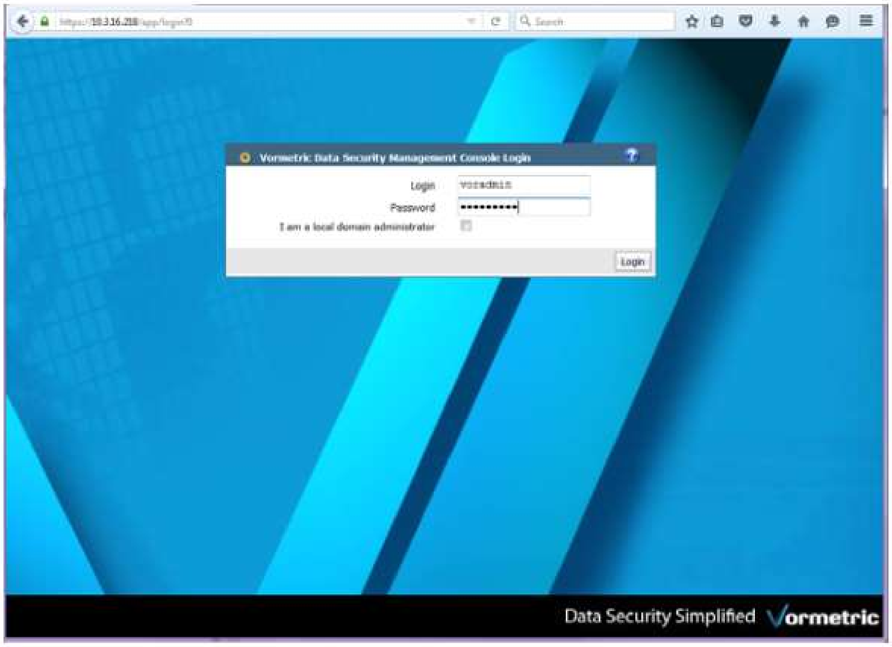
Verifying Web Access

Open a browser and confirm access over HTTPS to either the DSM hostname (if configured in DNS) or the IP address of the DSM. Example URL:

```
https://dsm.vormetric.com:8445
```

The default user name and password to log on to the DSM the first time; `admin` and `admin123`. You will be prompted to reset the password.

Figure 8: Web Management Interface



Vormetric Data Security Management Console Login

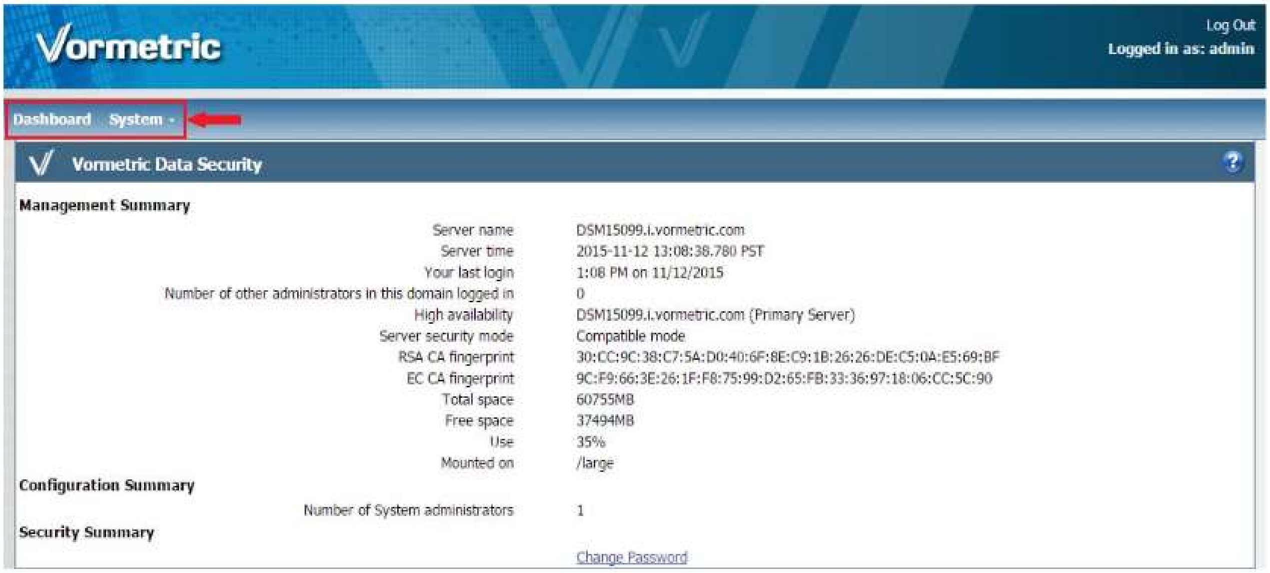
Login: voradmin

Password: ••••••••••

I am a local domain administrator □

The first time you log on to a DSM, the dashboard displays “License file not found" and you will see is the *Dashboard* and *System* tabs.

Figure 9: DSM dashboard on first login



Management Summary

Server name	DSM15099.i.vormetric.com
Server time	2015-11-12 13:08:38.780 PST
Your last login	1:08 PM on 11/12/2015
Number of other administrators in this domain logged in	0
High availability	DSM15099.i.vormetric.com (Primary Server)
Server security mode	Compatible mode
RSA CA fingerprint	30:CC:9C:38:C7:5A:D0:40:6F:8E:C9:1B:26:26:DE:C5:0A:E5:69:BF
EC CA fingerprint	9C:F9:66:3E:26:1F:F8:75:99:D2:65:FB:33:36:97:18:06:CC:5C:90
Total space	60755MB
Free space	37494MB
Use	35%
Mounted on	/large

Configuration Summary

Number of System administrators	1

Security Summary

You need to click **System** and select **License**, then **Upload the license file**. After uploading your license file, you will see all the other tabs.

You must have a valid license to configure hosts and register agents with a Vormetric DSM. Once your license expires because it reaches its expiration limit, the agent under that license will continue to operate until the protected host is rebooted or un-registered. However, new agents cannot be registered without a valid license, and the existing agent will need to be re-registered with a valid license.

Licenses are provided by Vormetric Customer Support and are uploaded to the DSM. The term of a license begins when you register the agent using that license.

Uploading a License file

1. Log on to your DSM as a DSM administrator of type System or All. Other administrator types can view the license in the Web Management Interface, but they cannot upload a license file.
2. Get a license file from Vormetric Customer Support.
3. Select **System > License** in the menu bar. The *License* window opens.
4. Click **Upload License File**. The *Upload License File* window opens.
5. Enter the full path of the license file in the **License File** field or click **Browse** to locate and select the license file.
6. Click **Ok**.

Web Management Interface & CLI

2

The DSM comes with a built-in web server that implements a browser-based graphic user interface called the Web Management Interface (formerly referred to as the Management Console). This web interface enforces authentication and implements role-based access control.

CLI access is intended for initial configuration and disaster recovery activities. Once the DSM has been configured and is operational, the remote Web Management Interface should be used instead.

Once the appliance is configured, it is administered via the web interface. The CLI is also used to reboot the appliance.

This chapter describes an overview of the Web Management Interface and the CLI commands that are used for initial configuration and management of the DSM appliance.

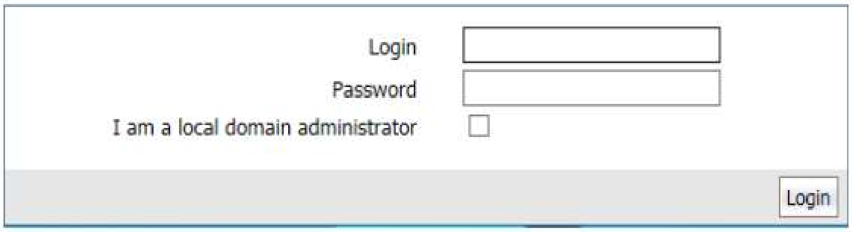
Accessing the Web Management Interface

Open a browser and enter the IP address assigned to the DSM. The DSM Web management Interface Login screen opens. Log on with the default DSM System Administrator account credentials:

user name: `admin`

password `admin123`

Figure 1: Login screen



This administrator/password combination; `admin/admin123` can be used only once. The first time that the `admin` administrator logs in, the password must be reset. We recommend that you use this account only to log on to the DSM Web Management Interface to initially create other DSM administrator accounts. After this operation, you should not use the `admin` account instead, use the newly created accounts for any further configuration operations. The first time you log on to a DSM, the dashboard displays “License file not found" and you will only see the *Dashboard* and *System* tabs. The other menu options become available once the license file is uploaded.

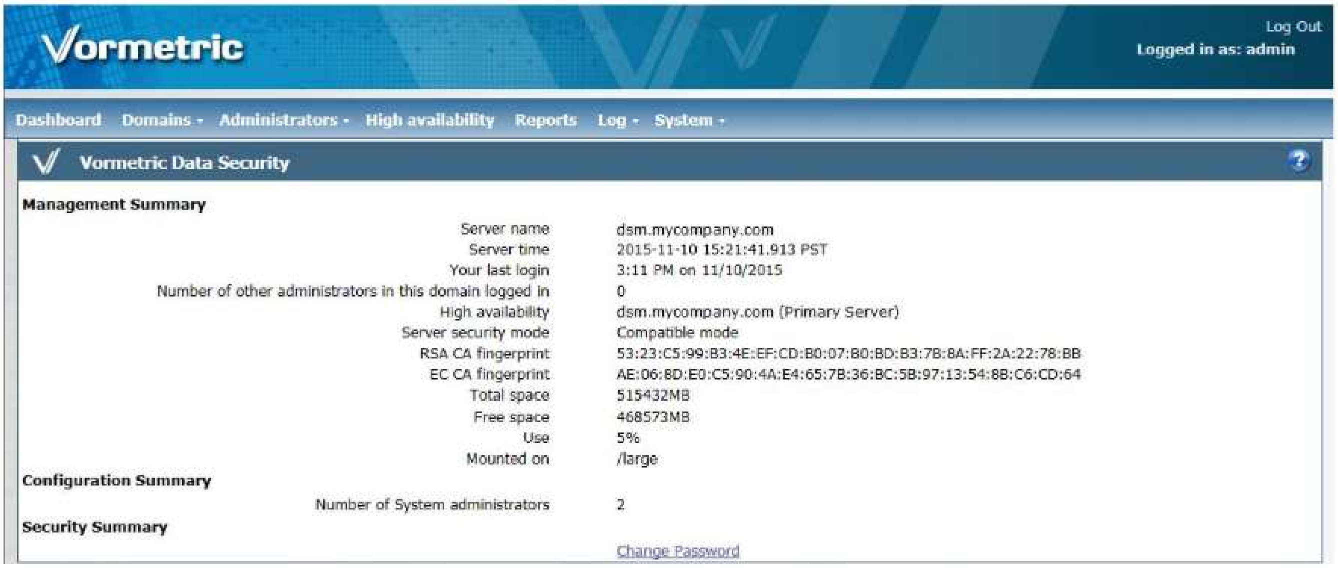
NOTE: It is recommended that you always use the latest version of Internet Explorer or Chrome browser to access the Web Management Interface.

To log out of the Web Management Interface at any point during your session, click **Log Out** on the top right corner of the interface. Logging out will take you back to the Login screen of the Web Management Interface.

Overview of the Web Management Interface

The Web Management Interface lets you manage, and administer your Vormetric protected data.

Figure 2: Web Management Interface



Management Summary

Server name	dsm.mycompany.com
Server time	2015-11-10 15:21:41.913 PST
Your last login	3:11 PM on 11/10/2015
Number of other administrators in this domain logged in	0
High availability	dsm.mycompany.com (Primary Server)
Server security mode	Compatible mode
RSA CA fingerprint	53:23:C5:99:B3:4E:EF:CD:B0:07:B0:BD:B3:7B:8A:FF:2A:22:78:BB
EC CA fingerprint	AE:06:8D:E0:C5:90:4A:E4:65:7B:36:BC:5B:97:13:54:8B:C6:CD:64
Total space	515432MB
Free space	468573MB
Use	5%
Mounted on	/large

Configuration Summary

Number of System administrators	2

Security Summary

Change Password

Web Management Menu Options

When you log on to the DSM, the top right corner displays the name of the administrator who is logged on. The availability of the various menus depends on the DSM administrator type and privileges and whether the administrator is currently inside or outside of a domain.

The following menu items are available when an administrator of type System or All logs on, but is *not* logged onto a domain:

Dashboard

The Dashboard provides a summary of the DSM activity. this menu is available to everyone who logs on to the DSM.

- The Management Summary displays the server name, the current server time, the last time this administrator logged in, whether any other administrators are logged into the domain, the security certificates, and the disk space usage on the DSM.
- The Configuration Summary displays how many administrators are available for this DSM. If you are logged into a domain, it displays the number of administrators in the domain, the number of hosts and host groups, the number of symmetric and asymmetric keys, the number of key groups and the number of online and offline agents.
- The Security Summary displays the number of attempts to access the DSM that were denied in the past hour, the number of access attempts that were denied in the past 24 hours, and the number of access attempts that were denied in the past week starting from the date indicated.

Domains

The Domains menu lets you create and delete domains, and switch to a domain. An administrative domain is a logical partition that is used to separate administrators, and the data they access, from other administrators.

Administrators

The Administrators menu lets you create and delete administrators, as well as assign and remove administrators from domains. The availability of

High Availability

The High Availability menu lets you configure a failover DSM to enable high availability.

Reports

The Reports menu lets you view and download reports about; the number of Systems, Domain, and Security administrators authorized to administer the DSM, that status of the DSM, the number of security domains, the license usage by domain, a system-level view of all licenses, and a system-level summary of the DSM.

If you are logged into a domain, you can view and download reports about keys, keys and their usage by policies, policies, policies and their keys, policies and their usage by host, hosts and their status, guard points, certificates, license usage summary by domain, license usage by host, host registrations and unregistrations, audit reports on hosts with their guard point status.

Log

The Log menu contains the Logs and Syslog sub-menus. The Logs sub-menu opens the Logs window where system events are recorded in log files. The information displayed in the table is determined by the log settings on each host. You can:

- Purge Debug Logs: Removes all DEBUG level messages from the Log window and the Security Server database.
- Export Logs: Saves the Management Web Management Interface log to a file.
- Delete Logs: Removes the entire Security Server log database.
- Download Logs: Collects all the logs used in the maintenance and configuration of the Security Server installation and writes them to a ZIP file.

The Syslog sub-menu opens the Syslog window. You can add or delete a syslog server from this window. The **System->General Preferences->System->Syslog Enabled** checkbox must be selected before you can transmit data to the syslog servers. Syslogs are domain-specific. If syslogs are configured in a domain, only the events that take place in that domain will be logged to the syslog server.

- Administrators of type System Administrator or All can enable or disable syslog forwarding when outside of a domain.
- Administrators of type System Administrator or All can configure syslog servers for system-level events when outside a domain.
- Administrators of type Domain Administrator, Domain and Security Administrator, or All can configure syslog servers for domain-level events when inside a domain.

System

The System menu lets you configure DSM preferences and tasks:

- **General preferences**—the number of objects displayed based on the object type. For example, you can set a preference that displays all configured policies on one Web page, rather than just 20 per page.
- **System preferences**—enable syslog messaging, enable super administrators, and shorten the update interval when pushing changes to the same policy to hosts on different servers.
- **Password preferences**—how long a password must be, the types of characters that a password must contain, and password duration. Password preferences also configure how the DSM responds to repeated failed login attempts.
- **Log preferences**—log maintenance parameters on the DSM. For example, you can set the interval to wait before moving agent log entries from temporary buffers on the DSM to the DSM log database, and consequently to the log viewer. You can set the log level settings for the different agents.
- **Network Diagnostics**—a set of diagnostic tools are provided to troubleshoot and analyze the Security Server network. The tools are:

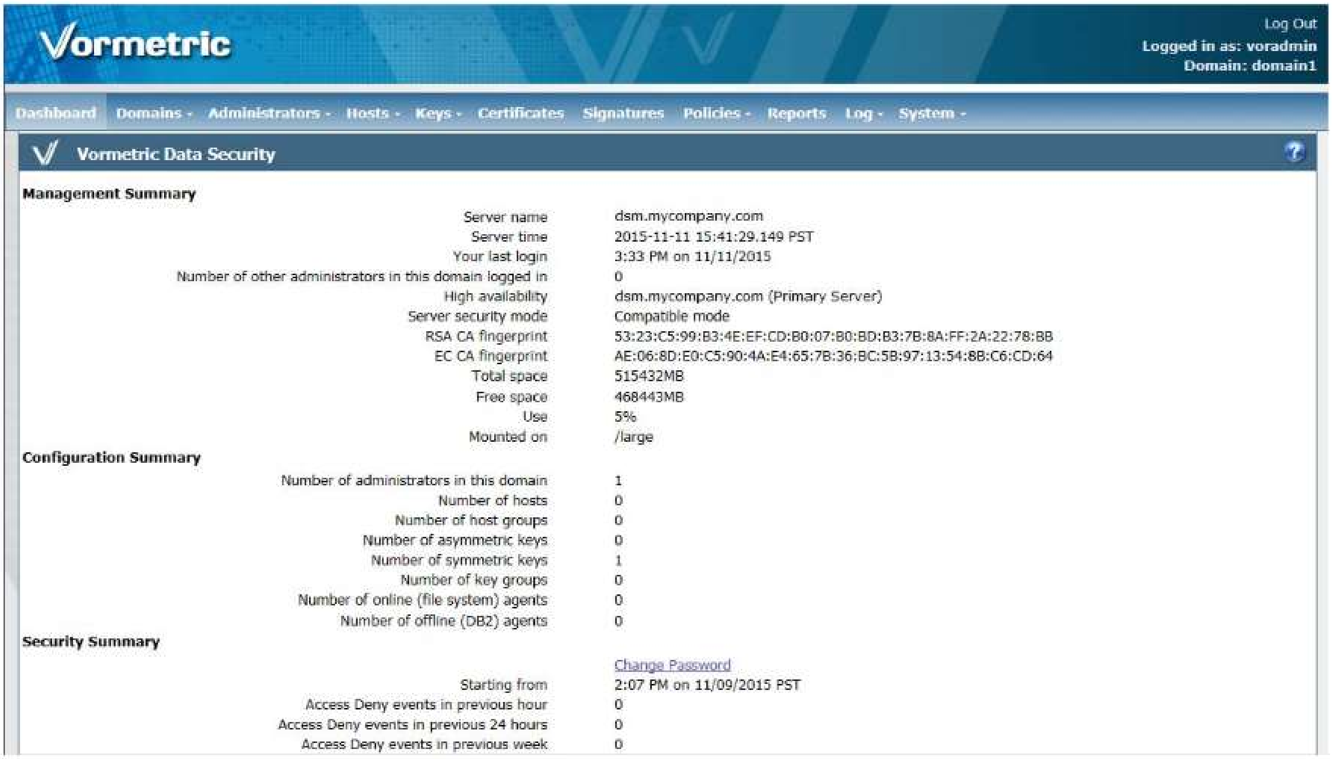
  - ping
  - ipAddress
  - arping
  - arp
  - traceroute
  - checkport
- **Wrapper Keys**—create wrapper keys to encrypt and secure a DSM system backup.
- **Backup and Restore**—create a backup of the DSM system configuration that can be used to restore the system in the event of a software crash recovery or a system change.
- **Software Upgrade**—contains two sub-menus; Upgrade and Patch list. You can upgrade your DSM software to a newer version. You can also view details about the software patches applied to your system and click on a specific patch to view details about it.
- **Web Server Certificate**—you can configure the DSM to validate with an external certificate authority (CA).
- **Upload RSA Configuration File**—enable multi factor authentication when logging on to the DSM to enhance security.
- **LDAP**—configure an LDAP server to import user information. The DSM can be integrated with Lightweight Directory Access Protocol (LDAP) directory services such as Active Directory (AD) and OpenLDAP. This feature allows the DSM Administrator to import user criteria instead of recreating it from scratch.
- **License**—view information about the licenses on the system:
  - Issued to: name of licensee
  - Multiple Domain Enabled: When checked, you can have more than one domain

  If you have any expired licenses, they are listed on the top left of the page.
- **About**—view a summary of the following information about the DSM appliance:
  - Version
  - Cumulative Patch
  - Build
  - Install Type
  - Product Type
  - Serial Number
  - Part Number
  - HSM Disabled

Web Management Menu Options inside a domain

When you log on to the DSM, and switch to a domain the top right corner shows the name of the administrator who is logged on and the name of the domain. The following additional menu items are available when an administrator of type System or All logs in and switches to a domain:

Figure 3: Web Management Interface when logged into a domain



Management Summary

Server name	dsm.mycompany.com
Server time	2015-11-11 15:41:29.149 PST
Your last login	3:33 PM on 11/11/2015
Number of other administrators in this domain logged in	0
High availability	dsm.mycompany.com (Primary Server)
Server security mode	Compatible mode
RSA CA fingerprint	53:23:C5:99:B3:4E:EF:CD:B0:07:B0:BD:B3:7B:8A:FF:2A:22:78:BB
EC CA fingerprint	AE:06:8D:E0:C5:90:4A:E4:65:7B:36:BC:5B:97:13:54:8B:C6:CD:64
Total space	515432MB
Free space	468443MB
Use	5%
Mounted on	/large

Configuration Summary

Number of administrators in this domain	1
Number of hosts	0
Number of host groups	0
Number of asymmetric keys	0
Number of symmetric keys	1
Number of key groups	0
Number of online (file system) agents	0
Number of offline (DB2) agents	0

Security Summary

	Change Password
Starting from	2:07 PM on 11/09/2015 PST
Access Deny events in previous hour	0
Access Deny events in previous 24 hours	0
Access Deny events in previous week	0

Hosts

The Hosts menu has the following sub- menus:

- Hosts—The Hosts menu lets you add and delete hosts, and also import hosts to add multiple hosts in a batch operation.
- Host Groups—The Host Groups menu lets you create and delete host groups. You can also edit host group settings.
- Host Password Challenge & Response—generate a host password to access encrypted guard point data when a connection to a DSM is not available. The host administrator generates a challenge string that the DSM administrator enters in the Challenge/Response field. The DSM administrator then provides the host administrator with the response (password) so that the host administrator can access the encrypted guard point data.

Keys

The Keys menu has the following sub-menus:

- Agent Keys—provides an overview of the encryption keys for the File System Agent. You can also export and import symmetric keys between DSMs.

Signatures

The Signature Sets page displays current signature set status, lets you create new signature sets, modify existing signature sets, sign signature sets, and delete signature sets. Signature sets are configured in an online policy as part of a process set to verify the integrity of a process before it is allowed access to guarded data.

Policies

Policies are displayed on the Policy page. Policies can be modified or deleted. The Policies menu has the following sub-menus:

- Manage Policies—create new File System Agent policy. Delete selected policy or policies from the system.
- Policy Wizard—the Policy Wizard helps to create sample policies to protect a particular application environment. It can create an encryption key, sample policies, hosts and guard point.
- Import/Export Policies—DSM File System Agent policy files can be exported and then imported by other Security Servers.

Accessing the DSM Command Line Interface (CLI)

The DSM CLI commands are used to configure the DSM.

NOTE: The CLI is intended for initial configuration. Once DSM has been configured and is operational, the remote Web Management Interface should be used instead.

The commands are grouped into the following categories or *submenus*. Log on to the DSM as a DSM CLI administrator, then enter a ? at the command line prompt to list the categories:

```
0000:vormetric$ ?
maintenance  System maintenance utilities
network      Networking configuration
system       System configuration
user         User configuration
exit         Exit
```

To enter a category, enter a name or just the first few letters of the name. To display the commands for that category, enter a ?. For example, the category `maintenance` is used to provide maintenance utilities:

```
0001:vormetric$ main
0038:maintenance$ ?
showver      Show the installed VTS version
ntpdate      Set ntp services
date         Set system date
time         Set system time
gmttimezone  Set system time zone
diag         OS diagnostics
up           Return to previous menu
exit         Exit
```

You can use the <Tab> key to complete a category, command, or argument. Enter enough characters to uniquely identify a category, command, or argument, and then press the <Tab> key to complete the command.

Every command has usage and example input. Type the command without a value:

```
0039:maintenance$ ntpdate
usage: ntpdate {sync | add SERVER_ADDRESS | delete SERVER_ADDRESS | on |
off | show }

0040:maintenance$ date
month=Mar day=17 year=2015
Show system date SUCCESS

0041:maintenance$ time
hour=11 min=11 sec=36 zone=PDT
Show system time SUCCESS
```

```
0042:maintenance$ gmttimezone
usage: gmttimezone {list|show|set ZONE_NAME}
0044:maintenance$
```

You must enter the submenu to execute the submenu commands. For example, the `reboot` command is in the system submenu, so you would type `system`, then type `reboot`. To return to the main level when finished, enter `up`.

Other supported DSM CLI navigation methods are:

- Enter a question mark (`?`) to display the next command or argument that is expected.
- Enter "`up`" to return to the top level so that you can enter another category. You can enter another category only from the top level.
- Enter "`exit`" at any time to end the current DSM CLI session.

A complete description of the DSM CLI commands can be found in the DSM Administrators Guide.

Additional DSM Configuration

3

This chapter describes additional configuration operations such as adding a syslog server, generating cryptographic keys, password configuration, and manual system clock configuration for the DSM appliance.

Adding a Syslog Server

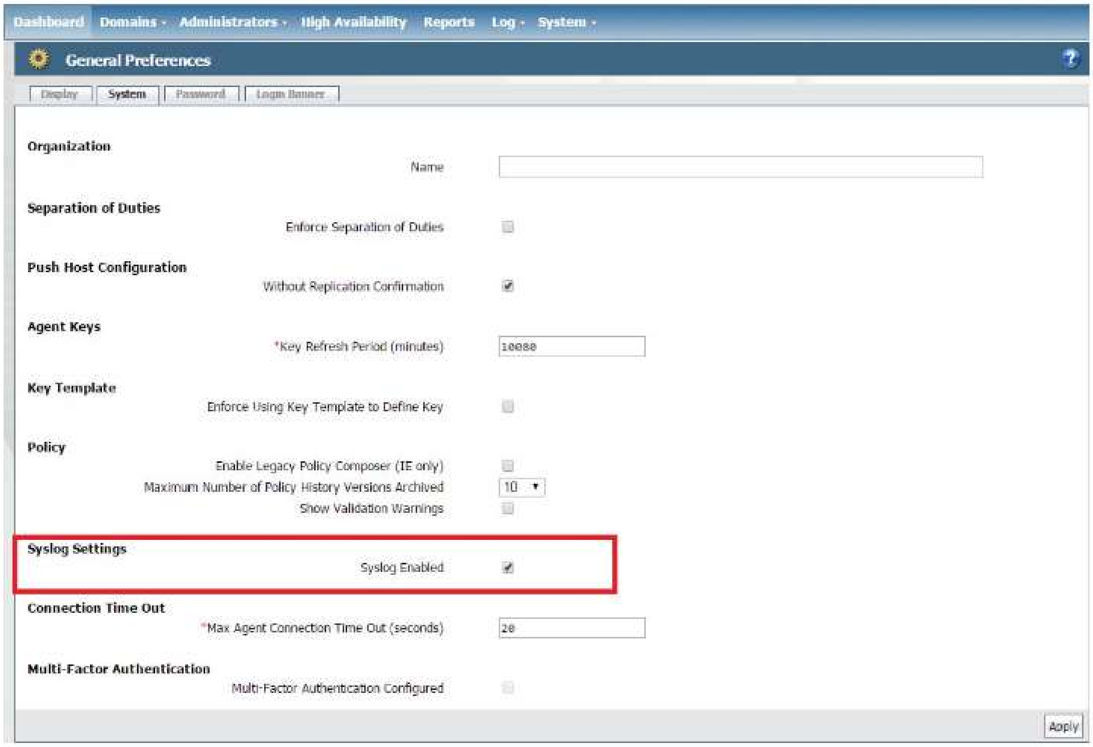
The syslog server connection requires TLS secure channel for Common Criteria.

1. Verify that one or more syslog servers are accessible from the DSM system. Record the syslog transport protocols and port numbers of the syslog server(s). You will need this information later.
2. Set the severity level at which to send messages to the syslog server. In CC mode, the log level *must* be set to either DEBUG or INFO.
   Severity levels in the *Log Preferences* window are DEBUG, INFO, WARN, ERROR, and FATAL. Severity levels are cumulative, so each level includes the levels below it. For example, FATAL logs only FATAL messages, whereas WARN logs WARN, ERROR, and FATAL messages. Log on to the Web Management Interface as an administrator of type System Administrator or All.
3. Select **System > General Preferences**. The *General Preferences* window opens to the **General** tab.
4. Click the **System** tab, and then select **Syslog Enabled**.

   This enables communication between the DSM and the syslog server.

NOTE: You must have the **Syslog Enabled** box selected from outside a domain; otherwise, the **Apply** button will not be selectable from within a domain.

Figure 1: Enable Syslog setting



Organization
Name

Separation of Duties
Enforce Separation of Duties □

Push Host Configuration
Without Replication Confirmation ☑

Agent Keys
*Key Refresh Period (minutes) 10080

Key Template
Enforce Using Key Template to Define Key □

Policy
Enable Legacy Policy Composer (IE only) □
Maximum Number of Policy History Versions Archived 10 ▾
Show Validation Warnings □

Syslog Settings
Syslog Enabled ☑

Connection Time Out
*Max Agent Connection Time Out (seconds) 20

Multi-Factor Authentication
Multi-Factor Authentication Configured □

5. Click **Apply**.
6. Select **System > Log Preferences**. The *Log Preferences* window opens to the *Server* tab.
7. Set the **Logging Level** property.

   The level you select affects the number of messages that are displayed in the *Logs* window, and these messages are also sent to the syslog server.

   Redundant syslog failure messages are filtered so that only one out of every fifty redundant messages is sent to `/var/log/messages` and the *Logs* window. All redundant syslog failure messages are sent when the level is set to DEBUG.
8. Click **Apply**.
   - If you are configuring a syslog server to receive system-level log data, remain logged in (for example, ‘system-level’ is when you are not in a domain).
   - If you are configuring a syslog server to receive domain-level log data, and are logged in as an administrator of type All, remain logged in and enter the domain to be configured.
   - If you are configuring a syslog server to receive domain-level log data, and are logged in as an administrator of type System Administrator, log out and log back in as a user of type Domain Administrator, or All, and enter the domain to be configured.
9. Select **Log > Syslog**. The **Syslog Server** window opens.
10. Click **Add** and enter the following information:

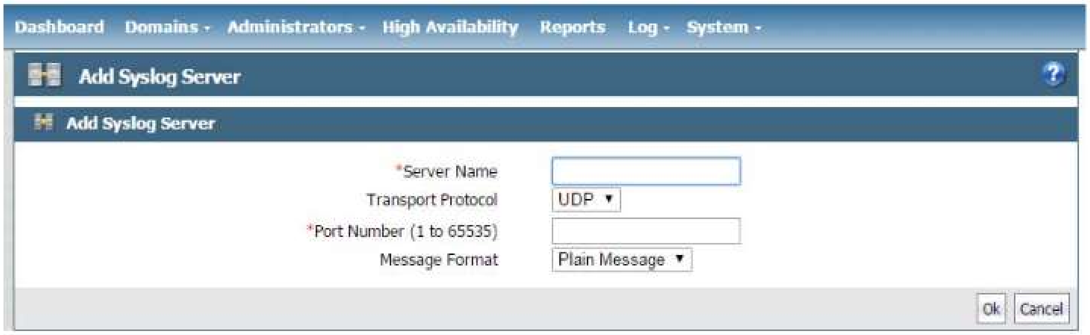
a. **Server Name:** The host name or FQDN of a syslog server. Use the network name of a syslog server which is accessible to the primary server and all the failover servers in the HA cluster.

b. **Transport Protocol:** Select TLS from the drop down. If you select TLS, a field appears for you to browse to a Certificate.

c. **Certificate:** Click **Choose File** to import the syslog certificate. This is required for Common Criteria.

NOTE: The SHA-1 signature algorithm is not supported in CC mode for Syslog certificate.

Figure 2: Add Syslog server



Add Syslog Server

Add Syslog Server

*Server Name

Transport Protocol: UDP

*Port Number (1 to 65535)

Message Format: Plain Message

NOTE: If you add a syslog certificate when using TLS protocol, you must do a `system > server restart` from the CLI. After restart, verify that the syslog server is logging messages as expected.

d. **Port Number:** The port number the transport protocol uses to connect to the syslog server. Enter a value between 1 and 65535. There is no default.

e. **Message Format:** Select Plain Message, CEF, or RFC5424.

NOTE: You may configure multiple syslog servers but only one instance of a syslog server name is allowed in the DSM database.

11. Click **Ok**.

12. Do a task on an agent system that normally generates a syslog entry, such as accessing a guard point. Check the `/var/log/messages` file on the syslog server for DSM log entries.

NOTE: If the syslog server becomes temporarily unavailable, the syslog messages will not be forwarded to the syslog server. When the connection is re-established there is no reconciling of the differences between the syslog server and the local audit records.

Supported Syslog Formats

The DSM supports the following log formats:

- Plain Message
- Common Event Format (CEF)
- RFC5424
- Log Event Extended Format (LEEF)

Refer to "Supported Syslog formats" on page 76 for details about these supported formats.

Configuring Cryptographic Functions

Once the DSM appliance is set to CC mode, it will be configured to use the appropriate cryptographic ciphers and no manual configuration is required.

Generating Keys

Keys are stored or cached in three different ways and have different effects:

Creating a symmetric key

1. Log on to the Web Management Interface as an administrator of type Security Administrator with `Key` role permissions or type All.
2. Select **Keys > Vormetric Agent Keys > Keys** in the menu bar.

   The **Add Vormetric Agent Key** window opens.
3. Select the **Symmetric** tab.
4. Complete the field in this window by using the information in Table 1.

Table 1: Symmetric Key Fields

Field	Description
Name	Enter a name for the key in the **Name** field. This field is mandatory. The maximum number of characters is 64.
Description	(Optional) Enter a phrase or string in the **Description** text-entry box that helps you to identify the key. The maximum number of characters is 256.
Algorithm	Select an encryption algorithm from the **Algorithm** list. Select either `AES128` or `AES256`. The default is `AES256`.

Field	Description
Key Type	Select the location for the generated key from the **Key Type** scroll-list. Your choices are **Stored on Server** and **Cached on Host**. The default is **Stored on Server**. **Stored on Server** keys are downloaded to non-persistent memory on the host. Each time the key is needed, the host retrieves the key from the DSM. Stored on Server requires a constant network connection to the DSM. **Cached on Host** downloads and stores (in an encrypted form) the key in persistent memory on the host. The cached keys are used when there is no network connection between the host and DSM. All hosts using the same encryption key can access encrypted data on other hosts that use the same key. The **Unique to Host** checkbox is displayed when **Cached on Host** is selected.
Unique to Host	This check box is displayed when the **Key Type** is set to **Cached on Host**. When enabled, this check box uses a token that is stored in the host record on the DSM to make the encryption key unique. The unique host encryption key is downloaded to the host and stored in an encrypted manner using the host password. These keys are used for locally attached devices, as files encrypted by them can be read by only one machine. Therefore, do not enable this checkbox for cloned systems, RAID configurations, clustered environments, or any environment that uses host mirroring. The **Unique to Host** checkbox can be enabled only when the **Key Type** is set to **Cached on Host** and the **Key Creation Method** is set to **Generate**.
Key Creation Method	Select if the key is to be generated automatically using a random seed or if it is to be generated by importing a file. Your choices are **Generate** and **Manual Input**. **Generate** is the default. The **Unique to Host** check box is disabled when **Key Creation Method** is set to **Manual Input**.
Key String	This list is displayed when **Key Creation Method** is set to **Manual Input**. Enter a hex string [0-9,a-f,A-F] for the key in the **Key String** text-entry box. - Enter 32 hex characters (128 bits) if the selected algorithm is AES128. - Enter 64 hex characters (256 bits) if the selected algorithm is `AES256`.

5. Click **Ok**.

Displaying and Modifying Key Configuration

Symmetric and asymmetric keys have the following informational items:

- Name
- Description
- Creation and expiration dates
- Algorithm
- Key Type
- Key-specific options
- The public-key portion of an asymmetric key can be exported

You can change the following key information of symmetric and asymmetric keys:

- Description (both symmetric and asymmetric keys)
- Creation date of manually generated symmetric keys
- Expiration date
- Key type

To display and modify key information:

1. Log on to the Web Management Interface as an administrator of type Security Administrator with `Key` role permissions or type All.
2. Select **Keys > Vormetric Agent Keys > Keys** in the menu bar.

   The **Vormetric Agent Keys** window opens and displays all the configured keys and their properties. The table lists a special key; clear_key that is available by default and is provided to remove encryption from guarded files and restore the files to their original unencrypted form. This key cannot be deleted.
3. (Optional) Enter all or part of a key name and select a key type in the **Search** panel to display only the keys that match.

   The **Show Search** label located below the **Keys** banner opens the **Search** panel. You can enter a string and/or limit the search to a specific type of key, and click **Go** to display only those keys that match the search criteria. Click **Hide Search** to conceal the **Search** panel.
4. In the **Name** column, click the key that you want to modify.

   The **Edit Vormetric Agent Key** window opens. The content of this window changes based on the type of key being modified. The Agent Key fields are detailed in Table 2.

Table 2: Edit Vormetric Agent Key window field information

Field	Description
Name	Name assigned to the key when it was first created.
Description	(Optional) Text description of the key. Enter a phrase or string in the **Description** text-entry box that helps you to identify the key. The maximum number of characters is `256`.
Algorithm	Algorithm you had selected when you created the key. Select the following symmetric key algorithms `AES128`, `AES256`.
Key Type	If a symmetric key algorithm is configured, `Stored on Server` or `Cached on Host` can be displayed. `Stored on Server` keys are downloaded to non-persistent memory on the host. Each time the key is needed, the host retrieves the key from the DSM. `Cached on Host` downloads and stores (in an encrypted form) the key in persistent memory on the host. For symmetric keys without `Unique to Host` enabled, you can toggle between `Cached on Host` and `Stored on Server` only. You can enable/disable `Unique to Host` only when configuring a new key. When you switch between `Stored on Server` and `Cached on Host` symmetric keys, the configuration change is pushed to the host.

5. Click **Ok** if you are applying changes.
6. If you are viewing a symmetric key type, click **Back** to return to the **Keys** window.
7. If you are viewing an asymmetric key type, click **Click to Export**.

   The **File Download** window opens.
8. Click **Open** to display the public key component of the asymmetric key in a Web browser.

   How the public key is displayed depends on your Web browser and what it does with files of type `.xml`. The key data can be displayed as raw XML code in a Web browser page, or, if your system is configured with an XML editor, the editor can be opened and the formatted XML file displayed.
9. Click **Save** to save the public key component of the asymmetric key.

   The **Save As** dialog box opens.

   a. Specify a path and name for the file.

   b. Click **Save**.

      The **Download Complete** dialog box opens.

   c. Click **Open** to display the public key component of the asymmetric key in a Web browser or click **Close**.
10. Click **Back** to return to the **Keys** window.

Encryption keys can be stored exclusively on the DSM, downloaded to the host, or downloaded to the host and stored in non-persistent memory. The keys can also be downloaded and stored (in an encrypted form) in persistent memory on the host for use when there is no network connection between the host and DSM. If the host password is configured using challenge-response authentication, run the vmsec challenge utility, then contact your DSM administrator with the challenge string, and enter the response string provided by the DSM administrator. Afterwards, you can read and write encrypted data without corrupting it.

Deleting keys

Warning! Do not delete keys without first backing them up. All data that has been encrypted with deleted keys cannot be restored or accessed once the keys are lost.

To delete keys:

1. Log on to the Web Management Interface as an administrator of type Security with `Key` role permissions, type Domain and Security, or type All.
2. Select **Keys > Vormetric Agent Key > Keys** in the menu bar.

   The *Vormetric Agent Keys* window opens.

3. Enable the **Selected** checkbox for those keys you want to delete.
4. Click **Delete**.

Password Management

In order to confirm to Common Criteria specifications, your password policy must conform to the following rules:

1. Passwords must be composed of a subset of the following character sets:
    - standard ASCII alphabet characters: a-z, A-Z
    - integers: 0-9
    - a set of special characters: !@#$%^&*(){}[]
2. The DSM administrator shall define the minimum password length. The minimum password length is an integer between 16v and the limit of the operating system.
3. The DSM administrator shall define the composition rules for characters used to create passwords.
4. Passwords must expire after the duration defined by the DSM administrator.
5. New passwords must contain a minimum number of character changes from the previous password as defined by the DSM administrator.
6. Passwords shall not be reused within the limit defined by the DSM administrator.

All of these settings must be defined on the *Password* tab of the *General Preferences* page on the Web Management Interface.

Configuring Password Attributes

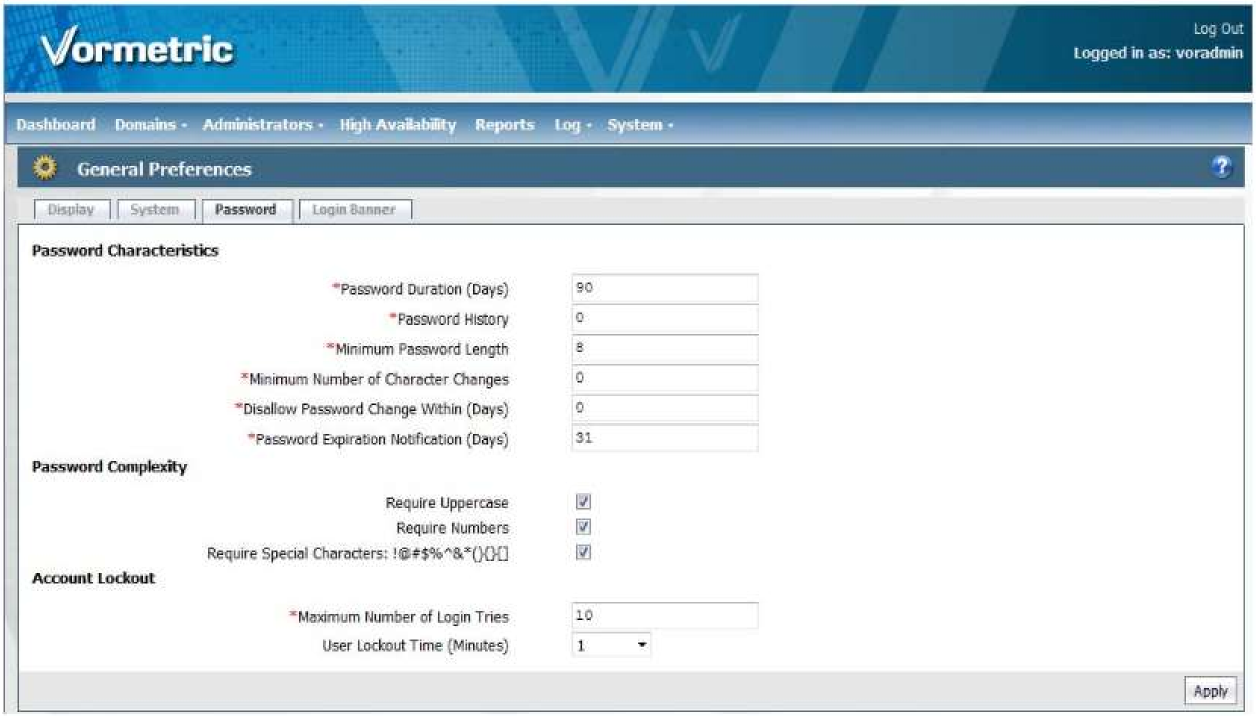
Settings under the *Password* tab affect all passwords used to access the DSM.

Password preferences are applied to both administrator passwords and host system passwords. The password characteristics and complexity can be configured from the Web Management Interface.

To set DSM password preferences:

1. Log on to the Web Management Interface as an administrator of type Security Administrator or type All with Host role permissions.
2. Select **System > General Preferences**. The *General Preferences* window opens.
3. Select the **Password** tab.
4. Change the values displayed in the attribute text-entry boxes or scroll-list.

Figure 3: Password Preferences



Password Characteristics

*Password Duration (Days) 90
*Password History 0
*Minimum Password Length 8
*Minimum Number of Character Changes 0
*Disallow Password Change Within (Days) 0
*Password Expiration Notification (Days) 31

Password Complexity

Require Uppercase ☑
Require Numbers ☑
Require Special Characters: !@#$%^&*(){}[] ☑

Account Lockout

*Maximum Number of Login Tries 10
User Lockout Time (Minutes) 1

The following is a list of attributes you can configure, and their values:

Password Characteristics

- **Password Duration:** Passwords expire after the number of days set by an administrator. The password expiration interval is applied globally to each administrator account. If the administrator does not change the password prior to the expiration, the administrator must reset the password immediately the next time the administrator logs in. The expiration interval is an integer between 7 and 365. The default is 90. 'Password Duration' must be set to a value greater than 'Password Expiration Notification'.
- **Password History:** The DSM maintains a password history. You cannot use the same password more than once per the set limit. The default is 4.
- **Minimum Password Length:** Sets the minimum number of characters, including blank spaces that must be in a password. The minimum password length is an integer between 8 and the limit of the operating system. The default is 8.
- **Minimum Number of Character Changes:** Sets the minimum number of characters, including blank spaces, that constitute a password change.
- **Disallow Password Change Within (Days):** Sets the number of days you must wait before you can change the password again.

- **Password Expiration Notification:** Sets the number of days prior to the password expiration at which to begin telling the administrator that their password is about to expire. Administrators are notified of the impending expiration at the Web Management Interface login. The notification interval is an integer between 6 and 31. The default is 31.

Password Complexity

- **Require Uppercase:** When enabled, requires at least one uppercase alphabet character in the administrator password. This is enabled by default.
- **Requires Numbers:** When enabled, requires at least one integer in the administrator password. This is enabled by default.
- **Requires Special Characters:** When enabled, requires at least one special character. (i.e., !@#$%^&*(){}[])

Account Lockout

- **Maximum Number of Login Tries:** Sets the maximum number of unsuccessful login attempts before disabling access for a set interval of time. The Management Console becomes inoperable and ignores further login attempts by a administrator for the specified interval. The range is between 1 and 10 and the default number of tries allowed is 3.
- **User Lockout Time:** The interval to wait before re-enabling the Management Console Web interface and allowing administrators to login. The default is 30 minutes.

Changing User Passwords

When a DSM System Administrator changes the password of an administrator of type Domain Administrator, Security Administrator, or All, the Domain Administrator, Security Administrator, or All account is disabled in every domain of which they are a member, and they must be enabled in every domain of which they are a member at the time the password is changed, by a different administrator of type Domain Administrator, Domain and Security Administrator, or All before they can again enter a domain. A disabled administrator can log on to the DSM, but the domain selection radio buttons are opaque and cannot be selected, so the administrator cannot enter any domain and cannot modify the DSM configuration.

To change another administrator's password:

1. Log in as an administrator of type System Administrator or All.
2. Check that the administrator is not currently logged into the Web Management Interface because their login session becomes inactive when the password changes.

   If you are changing the password of another System Administrator, you can check the DSM log.

If you are changing the password of a Domain Administrator or Security Administrator, have a Domain Administrator switch to each domain in which the administrator is a member and check the DSM log of each domain.

3. Select **Administrators > All**. The *Administrators* window opens.
4. Select an administrator in the Login column. The *Edit Administrator* window opens.
5. Enter the password and then click **Ok**.

   The password is applied to the administrator. If the administrator is currently logged on to a Web Management Interface session, the login becomes inactive and the administrator must log back into the Web Management Interface to resume operation.
6. For administrators of type Domain Administrator, Security Administrator, or All, have a different administrator of type Domain Administrator, Domain and Security Administrator, or All re-enable the administrator's domains.

Configuring Management Session Timeouts

The CLI is default session timeout is set to 30 minutes and is not configurable.

The session timeout period can be configured from the Web Management Interface. To set the timeout period:

1. Log on to the Web Management Interface as an administrator of type System or All.
2. Select **System > General Preferences** in the menu bar.
3. In the *General Preferences* window, on the **Display** tab page, select an option from the **Management Web Management Interface Timeout** drop down list to set the time period after which the Web Management Interface will time out. The options are
   - 5 minutes
   - 20 minutes
   - 1 hour
   - 2 hours
   - 8 hours
4. Click **Apply**.

When an administrator changes the Web Management Interface timeout value, the new timeout value applies:

- to the current login session only if you navigate to another page from the **General Preferences > Display** page.

or

- to subsequent administrator login sessions after you log out and then log in again.

You can also configure the interval allowed for establishing a network connection between DSMs and hosts. Changes to this value are applied immediately for DSM to host connections; however, they are not pushed to hosts until changes to host configurations occur, such as adding guard points or changing Host Settings, or, not until the individual hosts query the DSM for updates, which can be initiated by restarting the `vmd` process on the host system. To set the interval:

1. Log on to the Web Management Interface as an administrator of type System or All.
2. Select **System > General Preferences** in the menu bar.
3. In the *General Preferences* window, on the **System** tab page, enter a number in the **Max Agent Connection Time Out** field. The allowed range is 1 to 600 seconds. The default is 20.

Manually Configuring the System Clock

You must have the correct time set and synchronized with servers and other DSM units because several system functions, such as certificate exchange, are highly time sensitive.

1. Navigate to the maintenance commands menu. At the prompt type:

   ```
   0001:vormetric$ maintenance
   ```

2. Show the current timezone settings. At the prompt type:

   ```
   0002:maintenance$ gmttimezone show
   ```

3. Set the country and city where the DSM resides. At the prompt type:

   ```
   0002:maintenance$ gmttimezone set <country/city>
   ```

4. Set the date. At the prompt type,

   ```
   0002:maintenance$ date <mm/dd/yyyy>
   ```

5. Set the time. At the prompt type:

   ```
   0002:maintenance$ time <hh:mm:ss>
   ```

   Where hh is 00 to 23.

6. Verify your settings. Type,

   ```
   0002:maintenance$ time
   0002:maintenance$ date
   ```

7. Return to the main menu. Type,

   ```
   up
   ```

User Management

4

DSM Administrator Types and Roles

The Vormetric Data Security Manager (DSM) provides three types of administrators: System Administrator, Domain Administrator, and Security Administrator. Within the Security Administrator role there are five permissions: audit, key, policy, host and challenge and response. The DSM implements identity based authentication using passwords for the different administrator accounts.

- The DSM System Administrator type operates outside of domains. It creates domains and assigns administrators of the Domain Administrator role to the domains.
- The Domain Administrator type primarily serves to assign administrators into a domain.
- Security Administrators exists inside a domain, and is responsible for managing hosts, policies, keys, and audit settings.

Each DSM administrative type is allowed to do specific administrative tasks. By default, a DSM administrator is assigned one administrator type and is allowed to do the tasks for only that one administrator type. This approach requires at least three administrators, each assigned to a different type. Combined administrator type assignments can also be configured:

- DSM administrator of type All. Such administrators can operate both inside and outside of global domains. When an administrator of type All enters a domain, that administrator can do DSM Domain Administrator and DSM Security Administrator tasks. When an administrator of type All exits the domain, the administrator can do DSM System Administrator tasks.
- DSM administrator of type Domain and Security. The DSM Domain and Security Administrator can do every task that is allowed an administrator inside a domain. For example, the DSM Domain and Security Administrator can add administrators to the domains of which they are a member, but they cannot create new administrators.

Table 1: Administrator types and roles

Type	Permissions
DSM System Administrators. This administrator cannot do any security procedures in any domain.	Upgrade DSM software Backup and restore DSM database Add and delete all administrators Reset passwords for all administrators Add and delete all domains Assign one Domain Administrator to each domain Configure syslog server for system-level messages Install license file Configure DSM preferences View logs Configure High Availability (HA)
DSM Domain Administrators. This administrator cannot remove domains and cannot do any of the domain security roles.	Add and remove administrators (Domain, Security, All) to and from domains Configure Security Administrator roles (Audit, Key, Policy, Host, Challenge & Response) Configure syslog server for application-level messages View DSM preferences View logs
DSM Security Administrators. Do the data protection work specified by their roles. Different roles allow them to create policies, configure hosts, audit data usage patterns, apply guard points, and do other duties.	Configure signature sets Configure keys and key groups Configure online and offline policies Configure hosts and host groups Assign host passwords (manually or generated) Apply guard points Share a host with another domain Export the DSM public key Import symmetric keys View DSM preferences View logs
DSM Domain and Security Administrators.	Domain Administrator and Security Administrators capabilities combined. Administrators of this type are deleted from the DSM database upon switching from relaxed to strict domain mode.
All.	System, Domain, and Security Administrators capabilities combined. Administrators of type All are deleted from the DSM database upon switching from relaxed to strict domain mode.

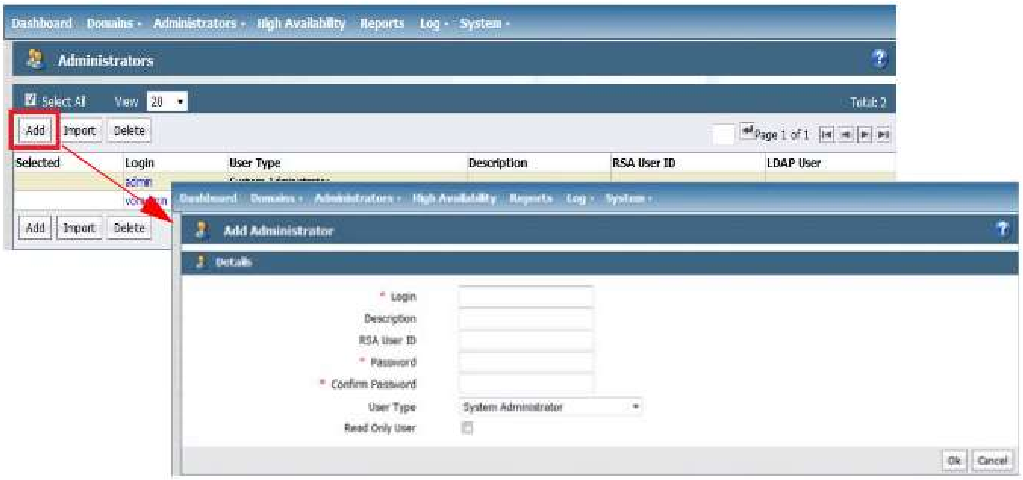
CLI Administrators

CLI administrators do tasks related to set up and operate the DSM installation—they do not administer the DSM from the Web Management Interface.CLI administrators are system users with login accounts. That is, they are entered in /etc/passwd and they have directories under /home. The password requirements for both CLI and DSM administrators are set by the password policy in the Web Management Interface.

Creating a DSM administrator

1. Log on to the Web Management Interface as the DSM System Administrator or as DSM administrator of type All.
2. Click **Administrators** and click **Add**.

Figure 1: Adding an administrator



User Type: System Administrator

3. Enter the following details into the corresponding fields:

   a: **Login**—Choose a name. Only one instance of an administrator name is allowed.

   b: **Description**—(Optional) Enter a phrase or string that helps you to identify the administrator. This field is optional. The maximum number of characters is 256.

   c: **RSA User ID**—(Optional) Enter the RSA user name in the RSA User Name field.

   d: **Password**—Enter a password for the administrator to log on to the Web management Interface.

   e: **Confirm Password**—re-type the password you entered for this administrator.

   f: **User Type**—Select System Administrator, Domain Administrator, Security Administrator, Domain and Security Administrator, or All from the drop-down menu.

The first time an administrator logs on to the Web Management Interface on a newly created DSM Administrator account, they are prompted to change the password. They cannot use the same password that was used to create the account.

4. Click **Ok**. A new DSM Administrator is created. The *Administrators* windows opens with the name and type of the new administrator added to the table.

Configuring LDAP

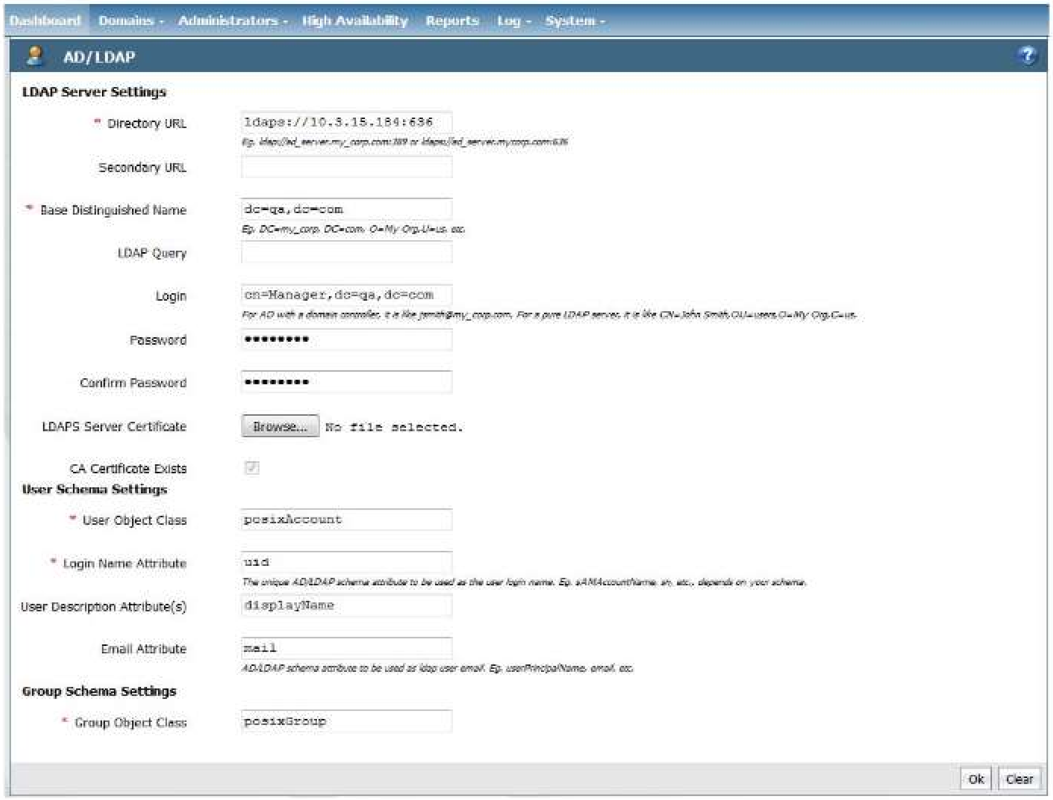
LDAP users can be imported as DSM administrators. An LDAP server must be configured and authenticated before any information can be imported. The LDAP server connection requires TLS secure channel for Common Criteria.

NOTE: The SHA-1 signature algorithm is not supported in CC mode for LDAP certificate.

Configure LDAP server settings

1. Log in to the Web Management Interface and select **System > LDAP**.

Figure 2: Adding an LDAP server



LDAP Server Settings

* Directory URL	ldaps://10.3.15.184:636 *Eg. ldap://ad_server.my_corp.com:389 or ldaps://ad_server.mycorp.com:636*
Secondary URL	
* Base Distinguished Name	dc=qa,dc=com *Eg. DC=my_corp, DC=com, O=My Org,U=us, etc.*
LDAP Query	
Login	cn=Manager,dc=qa,dc=com *For AD with a domain controller, it is like jsmith@my_corp.com. For a pure LDAP server, it is like CN=John Smith,OU=users,O=My Org,C=us.*
Password	••••••••
Confirm Password	••••••••
LDAPS Server Certificate	No file selected.
CA Certificate Exists	☑

User Schema Settings

* User Object Class	posixAccount
* Login Name Attribute	uid *The unique AD/LDAP schema attribute to be used as the user login name. Eg. sAMAccountName, sn, etc., depends on your schema.*
User Description Attribute(s)	displayName
Email Attribute	mail *AD/LDAP schema attribute to be used as ldap user email. Eg. userPrincipalName, email, etc.*

Group Schema Settings

* Group Object Class	posixGroup

2. Enter the URL of the LDAP server in the **Directory URL** field. If a secure LDAP URL is specified here, then its LDAPS Server Certificate in PEM format must also be entered in LDAPS Server Certificate.

   Example:

   ldaps://ldapserver.mycorp.com:636

NOTE: The default LDAPS port is 636.

3. (Optional) Enter the URL of an alternate LDAP server, in the **Secondary URL** field. This alternate LDAP server will be used if the primary LDAP server is unreachable. If you enter a secure LDAP path, you should browse to the location of a certificate in the **LDAPS Server Certificate** field and upload the certificate for that server.
4. If you enter a secure LDAP path, you should browse to the location of a certificate in the LDAPS Server Certificate field and upload the certificate for that server.
5. Enter a **Base Distinguished Name**. For example, if you use Active Directory with a domain name such as “mycorp”, your base DN would be DC=mycorp, DC=com
6. (Optional) Enter up to a 256 character string to filter searches, in the **LDAP Query** field.

7. Enter the LDAP user login name in the **Login** field.

   Example: If your domain name is “mycorp” and using Active Directory with a domain controller your login name might be:

   jsmith@mycorp.com

8. Enter the LDAP password in the **Password** field. Enter it again in **Confirm Password**.

9. **LDAPS Server Certificate**: If a secure LDAP path was entered in the Directory URL field, click Browse and navigate to the location of the Root CA Certificate. The CA certificate must be in PEM format. This field does not allow direct user input to avoid typographic errors.

NOTE: If LDAPS is used for the Directory URL or Secondary URL fields, you must upload a certificate in the LDAPS Server Certificate field. The certificate must be in PEM format

10. The **CA Certificate Exists** box will be checked if the LDAPS Server Certificate has been uploaded to the DSM.

User Schema Settings

1. Enter the “Object Class” attribute in the **User Object Class** field.

   For example: user or person

2. Enter the user attribute containing the unique user ID in the **Login Name Attribute** field. This is the AD/LDAP schema attribute to be used as the LDAP user login name.

   For example: sAMAccountName or commonName

NOTE: If a Login Name already exists in the Vormetric DSM database, the Import function will not overwrite existing users with the same login name.

3. (Optional) Enter the user attributes desired in the **User Description Attribute(s)** field. To enter multiple attributes, separate values with a semicolon.

   For example: name or description

4. (Optional) **Email Attribute**: This is the AD/LDAP schema attribute to be used as LDAP user email. For example: userPrincipalName or mail

Group Schema Settings

1. Enter the group “Object Class” attribute in the **Group Object Class** field.

   For example: group or posixGroup

2. Click **OK** to save the settings on the page, or click **Clear** to clear the form. You can also click **Clear** any time later to delete the AD/LDAP settings.

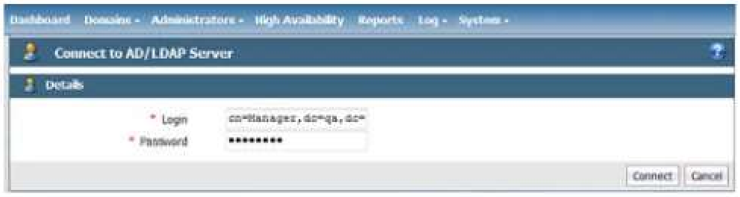
Importing LDAP users

The **Import** function allows Administrators to import data from an LDAP server such as Active Directory (AD) or OpenLDAP. Once an LDAP server has been identified and configured, the DSM Administrator can import the desired values. To set up access to an AD/LDAP repository, see "Configuring LDAP".

To import values from an LDAP directory:

1. Select the **Administrators > All** tab. Click **Import**.

Figure 3: Connecting to an LDAP server



* Login cn=Manager,dc=qa,dc=

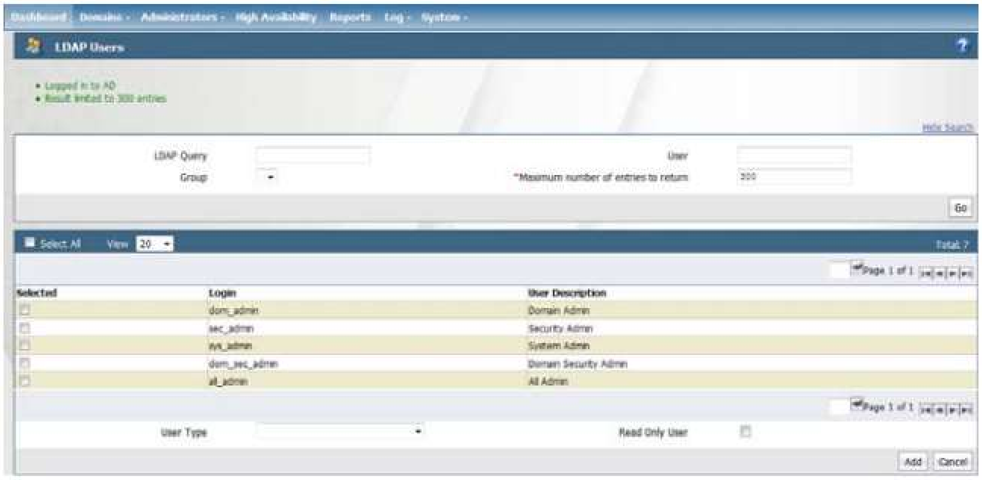
* Password ••••••••

2. Enter the **Login ID** and **Password**. If the Login and Password were entered under LDAP Server Settings on the AD/LDAP Details window, these values will be populated and do not need to be re-entered. You may also enter a different Login and Password in place of these stored values when you import administrators.
3. Click **Connect**. The LDAP Users window displays LDAP user names.

Selecting LDAP administrators

The following search option are available on the *LDAP Users* window:

Figure 4: LDAP users



- Logged in to AD
- Result limited to 300 entries

LDAP Query

Group

User

*Maximum number of entries to return: 300

View: 20

Selected	Login	User Description
□	dom_admin	Domain Admin
□	sec_admin	Security Admin
□	sys_admin	System Admin
□	dom_sec_admin	Domain Security Admin
□	all_admin	All Admin

User Type

Read Only User □

- **LDAP Query**—Use the field to filter searches using the LDAP query language. Results depend on how the LDAP service is set up. See RFC2307 for full details on syntax.
- **Group**—Select a group from the drop down list.
- **User**—Enter a user name.
- **Maximum number of entries to return**— Limits the maximum number of records to import or display. The default value is 300. The minimum value is 1 and the maximum value is 10,000. A high integer value may result in a delay depending on the database size.
- **Go**—Click to refresh the screen
- **Select All**—Click to select all values on that page
- **View**—Select a value from this drop down box to control how many values appear on any page
- **Selected**—Click to select individual values.
- **User Type**—Select a value from this drop down box to define the type of Administrator or role of the values you import.
- **Add/Cancel**—Select to add or cancel your selections.

Deleting a DSM administrator

DSM administrators of type System or All can delete other administrators of any type—except for the default *admin* administrator and themselves.

If the administrators to be deleted are members of a domain, they must first be removed from that domain (even if the domain has been deleted), before they can be deleted.

To remove an administrator from a domain:

1. Log in as an administrator of type Domain Administrator, Domain and Security Administrator, or All.
2. Remove the administrator you want to delete from every domain of which they are a member.

To delete an administrator

1. Log in as a DSM administrator of type System Administrator or All.
2. Select **Administrators > All**.
3. In the Administrators window, enable the **Selected** check box of the administrator(s) to be deleted.
4. Click **Delete**.
5. You are prompted to verify that you want to proceed with this operation.
6. Click **Ok**. The selected administrators are deleted from the DSM Management Web Management Interface and cannot access the DSM.

Modifying an administrator

1. Log in as a DSM administrator of type System Administrator or All.
2. Select the **Administrators** tab.
3. Select the administrator name in the **Login** field. You *cannot* modify the administrator login name.
4. (Optional) Edit the description of the administrator in the **Description** field.
5. In the **Password** and **Confirm Password** fields, edit the password for the DSM administrator.
6. You *cannot* edit the type for the administrator.
7. Click **Ok**.

Administrative Domains

Administrative types in the DSM apply to Administrative Domains. An administrative domain is a logical partition that is used to separate administrators, and the data they access, from other administrators. Administrative tasks are performed in each domain based upon each administrator’s assigned role. There are two types of administrative domains; global domains and restricted domains. Domain or Security Administrators assigned to a global domain are restricted to their assigned domains but can be assigned to multiple domains. Domain and

Security Administrator assigned to a restricted domain are restricted to that particular domain they cannot be assigned to multiple domains.

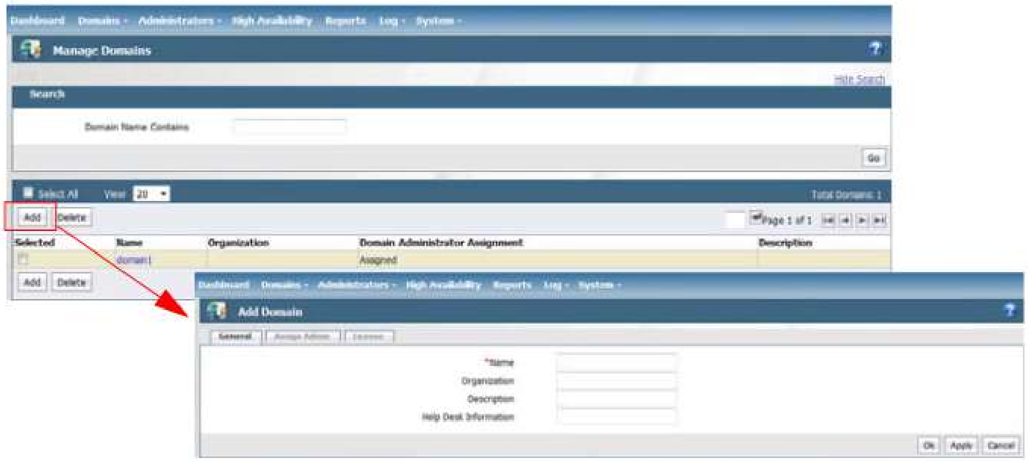
DSM administrators of type System can add and delete domains. However, they are not members of domains. A domain is a group of one or more DSM-protected hosts under the control of an assigned DSM Domain Administrator. Before a protected host can be administered, it must be placed in a domain.

Adding Domains

1. Log in as a DSM administrator of type System Administrator or All.
2. Click **Domains > Manage Domains** to bring up the *Manage Domains* window.

   If you are in a domain click **Exit Domain** to exit the domain and then click **Manage Domains**.
3. Click **Add**. The *Add Domain* window opens.

Figure 5: Adding a domain



Selected	Name	Organization	Domain Administrator Assignment	Description
□	domain1		Assigned	

4. Under the **General** tab, provide a name for the domain.

   a. **Name**: Enter a name of up to 64 characters for the new domain.

   b. **Organization**: (Optional) Enter the name of the organization responsible for or administered by this domain.

   c. **Description**: (Optional) Enter a phrase or string of up to 256 characters to help identify the domain.

   d. **Help Desk Information**: (Optional) Enter the phone number to call to get the response string for challenge-response authentication. If you leave this box empty, the default message is "Please contact a Security Server administrator for a response." (Note: The term "Security Server" refers to the DSM.)
5. Click **Apply** to save the domain information.

6. Click the **Assign Admin** tab to assign an administrator. If you do not assign an administrator when you add the domain, you can edit the domain later to add an administrator. However, you cannot switch to the domain until you assign an administrator.
7. Click the **License** tab to allocate licenses or license hours per agent on this domain. This is optional.
8. Click **Ok**. The *Domains* window opens with the name and description of the new domain.

After the domain is created and has an assigned DSM Domain Administrator, hosts can be added to it.

Deleting Domains

Before you delete a domain, back up security objects such as keys, policies, and logs. Without the keys, you cannot restore or access encrypted data. When you delete a domain, all the log data for that domain is also removed from the DSM database.

1. Log in as a DSM administrator of type Security or All.
2. Switch to the domain to be deleted.
3. Delete all the policy, key, and host configurations.
4. Logout.
5. Log in as an administrator of type Domain Administrator, Domain and Security Administrator, or All.
6. Switch to the domain to be deleted.
7. Delete all administrators that are assigned to that domain.

   You can delete all but one Domain Administrator; which is the administrator that you are currently logged in as.
8. Log out.
9. Log in as an administrator of type System Administrator or All.
10. Select **Domains > Manage Domains**.
11. In *Domains* window, enable the **Selected** check boxes for the domains to be deleted.
12. Click **Delete**. You are prompted to verify that you want to proceed with this operation.
13. Click **Ok**.

The deleted domain will no longer appear in the domains table in the *Domains* window.

Assigning administrators to domains

A DSM System Administrator creates other DSM administrators and can assign only one administrator of type Domain Administrator or Domain and Security Administrator to a domain. After these administrators are assigned to a domain, they can log on to the Web Management Interface and add additional Domain Administrators or Domain and Security Administrators to the domain. The Domain Administrator can add only existing Domain Administrators, Security Administrators, and Domain and Security Administrators to the domain.

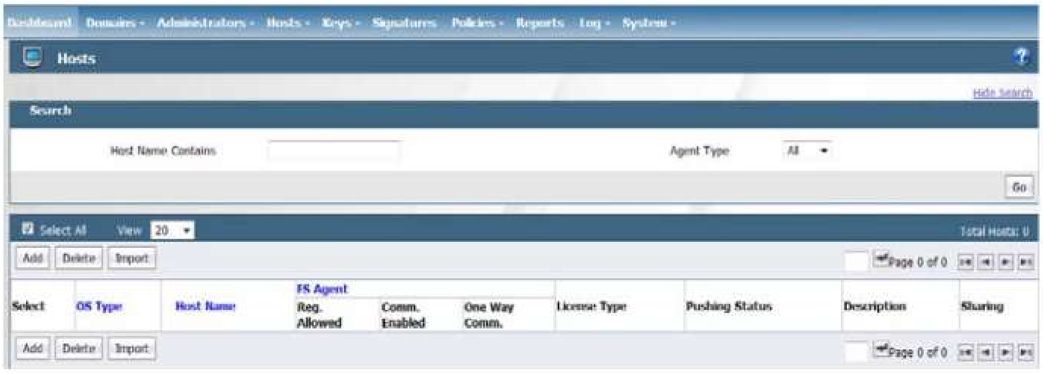
Installing Agents on Hosts

5

A “protected host” is a computer system on which Vormetric Transparent Encryption (VTE) Agents (also called File System Agents) are running. The agent on a protected host may protect data on that host, or data on other devices connected to that host.

To see all the protected hosts in the DSM database, log on to the DSM as an administrator of type Security, type Domain and Security, or type All, and enter a domain and click **Hosts > Hosts**. The *Hosts* window has a table listing names of the protected hosts in the DSM database and the following details about each protected host:

Figure 1: Hosts page



Host Name Contains

Agent Type: All

☑ Select All View 20 Total Hosts: 0

Select	OS Type	Host Name	FS Agent			License Type	Pushing Status	Description	Sharing
			Reg. Allowed	Comm. Enabled	One Way Comm.				

Table 1: DSM *Hosts* Window Table Details

Column	Description
Select	Select this checkbox to select the host for deletion. Multiple check boxes can be selected at one time.
OS Type	Values may be `Unknown`, `AIX`, `HPUX`, `Linux`, `Solaris`, or `Windows`. `Unknown` indicates that the host has not been registered or is an unsupported type.
Host Name	The name of the host in the DSM database.

Column	Description
FS Agent	This column consists of three sub-columns of check boxes: - **Reg. Allowed**—the host can register and be configured to run File System (VTE) Agent software. - **Comm. Enabled**—a policy can be applied to a host. **Reg. Allowed** must be enabled before you can set **Comm. Enabled**. - **One Way Comm.**—indicates that the agent was registered with One-Way Communication enabled between the Agent and the DSM.
License Type	Perpetual, Term, Hourly
Pushing Status	Status for pushing policy and configuration changes to locally assigned hosts. Status is specific to the local DSM. Run the Management Web Management Interface on a failover DSM to see the push status of the hosts assigned to that server. **Done**—the host has the latest policy and configuration changes. **Pending**—an update is in progress or is queued for download to the host. **N/A**—the local host is disabled or the host is being administered by a different server.
Description	(Optional) Text to help you identify the host.
Sharing	Indicates if the host is shared with another domain. The column may have a value of `Shared`, `External`, or blank. - `Shared` indicates that the host is in the current domain and, if the Security Administrator has the correct roles, it can be fully configured. The shared host is visible only in the domain with which it is being shared. - `External` indicates that host is administered in another domain. You can assign the host a VTE Agent guard point, but you cannot change the host configuration. - A blank value indicates that the host is not shared.

Adding Hosts to the DSM

Hosts must be registered with the DSM database using the *Certificate Fingerprint* method.

The Certificate Fingerprint method requires adding the host name or IP address for each protected to the DSM database before registering the agent. After registration, the Agent Installer must pass the CA certificate to the DSM Security Administrator to verify that the protected host and DSM share valid certificates.

To add a host

1. Determine the manner in which you want to address the host. That is, FQDN, host name, or IP number.
   - If FQDN, verify that DNS is configured and working on the DSM.

- If host name, use the host CLI command to link IP numbers with host names, or edit `/etc/hosts` directly.

2. Log on to the Management Web Management Interface as an administrator of type Security with `Host` role permissions, type Domain and Security, or type All.
3. Switch to the domain where you will add the host.
4. Select **Hosts > Hosts** in the menu bar. The *Hosts* window opens.
5. Click **Add**. The *Add Host* window opens.
6. Enter the following information:

a. **Host Name**—Enter the IP address, host name or FQDN (54 character max).

NOTE: Host names that include an underscore are rejected by the Management Web Management Interface.

b. Select a **Password Creation Method.** This is the password you use to unlock a guard point when there is no server connection.

- **Generate** (challenge-response)—dynamic password. Each time a host password is required, the DSM Security Administrator requests a new password from a DSM Administrator.
- **Manual**—static password that is entered each time a host password is required. Select **Manual**, then enter and re-enter the password in the **Password/Confirm Password** fields.

c. **Automatically Assign to a Server**—Optional. Select to automatically assign the host to a DSM during host registration. Automatic host assignment is a load-balancing function in an HA cluster. If servers in the HA cluster are physically distributed over great distances, you may not want to use this option because hosts can be assigned to distant servers with slow connections. By default, hosts are assigned to the primary DSM when they are added. If you leave it unchecked, you can specify the server to explicitly assign the host later in the **Hosts for High Availability Server** window.

d. **Description**—Optional. Enter text that helps you to identify the host. The maximum number of characters is 256.

e. **License Type**—Choose the type of license that will run on this host. Options are **Perpetual**, **Term**, and **Hourly**, depending on the system license. For instance, if only a Term license is installed on the system, only Term appears in the box.

f. **Registration Allowed Agents**—Select the agents that will run on the host system. The agent must be selected here before you can register that agent with the DSM. Only the agents you have a license for will display here.

g. **Communication Enabled**—Select this to enable communication between the DSM and the agent. This can also be done later by going to the *Edit Host* page.

7. Click **Ok**. The host has been added to the DSM.

The host administrator (with root access) installs the agent software on the host and registers the agent with DSM, as described in the *Vormetric Agent Installation and Configuration Guide*.

Deleting hosts

When you delete a host in the Web Management Interface, you are deleting the host record and configuration from the DSM database only. The agent installations on the host continue to run, complete with the applied policies. To completely remove an agent host, run the software removal utility on the host system after you delete the host record in the Web Management Interface.

When you delete a host you also delete that host from any host groups for which it may be a member.

NOTE: Only DSM administrators of type Security, type Domain and Security, or type All can add and delete hosts. If the host is shared with other domains, the DSM administrator must be in the same domain in which the host was first created in order to delete it.

NOTE: Do not unregister or delete the VTE Agent while locks are applied. The locks stay in effect after the agent is unregistered and, without agent credentials, the DSM cannot administer that VTE Agent and it cannot disable the locks. You must boot the host into single-user mode and manually modify the agent configuration to disable the locks.

To remove everything associated with a host, including the agent software that runs on the host:

1. Apply a rekey policy and run `dataxform` on the host files that you want unencrypted.
2. Disable the locks for the host in the *Edit Host* window, **General** tab.
3. Remove all the guard points for the host in the *Edit Host* window, **Guard FS** tab.
4. Select **Hosts > Hosts** in the Management Web Management Interface menu bar.
5. The *Hosts* window opens.
6. Enable the **Select** check box of each host to be deleted.
7. Click **Delete**.

   A dialog box opens that asks if you are sure you want to proceed with the operation.
8. Click **Ok**.
9. The host administrator with root permissions must log on to the host system and delete the agent software.

   The *Host Groups* window opens. All configured host groups are displayed.

10. Enable the selection check boxes of those host groups that you want to delete.

    The selection check boxes are located in the **Select** column of the *Host Groups* window.

11. Click **Delete**.

    You are prompted to verify the deletion.

12. Click **Ok**.

Policy Management

6

The DSM Security Administrator creates policies that protect data. Policies govern access to, and encryption of, the files in Vormetric-agent-protected directories. These directories are called 'guard points'.

A DSM policy is a set of rules that specifies which users and processes can access guard point files

Policy Rule Criteria and Effects

Policy Rules consist of five *criteria*, which specify the attributes of an access attempt, and *effects*, which define whether that access is permitted or denied, and whether encryption or decryption is required.

Table 1: Policy Rule Criteria

Criteria	Action
Resource	Specifies which files and/or directories in a guard point are to be blocked. Example: `/secure_dir/financials`
User	Specifies a which users or groups of users can access the files.
Process	Specifies executables that can operate on the files.
When	Specifies the time range when files can be accessed.
Action	Specifies the allowed file action. Example: read, write, remove, rename, make directory.

Table 2: Policy Rule Effects

Effect	Action
Permit	Permit access to the data.
Deny	Deny access to the data.
Apply Key	Encrypt data written into guard point with the key specified in the *Key Selection Rules* tab. Decrypt data that is accessed using the same key.

Effect	Action
Audit	Creates an entry in the Message Log that describes what is being accessed, when it is being accessed, the security rule being applied.

Every time a user's application tries to access a guard point file, VTE tests that access attempt against the criteria of each rule. For example, suppose user `Harry` wants to access and modify a file called `secret`, using the command `cp`, at 3AM. For `Harry` to be successful, there must be a rule that allows access to `secret` (*resource*), by user `Harry` (*user*), using the command `cp` (*process*), at 3AM (*when*), and includes the permission `write` (*action*).

A blank criteria field specifies a value of *All*. If *User* is blank, the rule applies to all users; if *When* is blank, the rule applies to all times; if *Process* is blank, the rules applies to all executables, and so on. *Effect* can never be blank. It must have at least a *permit* (allow access) or *deny* (deny access).

A policy can have multiple rules. Rules are evaluated much like firewall rules; they are evaluated in order, from first to last, and evaluation stops when a rule is found for which all the criteria are met. The effect for that rule is then enforced. Therefore, you must carefully order a policy's rules to achieve the desired result.

The DSM provides a warning to users about potential conflicts in the following cases:

1. If a newly created rule, or an updated rule is identical to an existing rule,

   a: the following message is displayed for a new rule:

   The new security rule <*rule number*> has been added, but the security rule <*rule number*> has same object sets as security rule <*rule number*> with similar effect. The security rule <*rule number*> may not take effect. Please review security rules carefully before proceeding.

   b: the following message is displayed for an updated rule:

   The new security rule <*rule number*> has been updated, but security rule <*rule number*> has same object sets as security rule <*rule number*> with similar effect. The security rule <*rule number*> may not take effect. Please review security rules carefully before proceeding.

2. If all sets (resource, user, process, or time) to which the rule applies are identical, but the effects are contradictory,

   a. the following message is displayed for a new rule:

   The new security rule <*rule number*> has been added, but the security rule <*rule number*> has same object sets as security rule <*rule number*> with conflict effect. The security rule <*rule number*> may not take effect. Please review security rules carefully before proceeding.

   b. the following message is displayed for an updated rule:

   The new security rule <*rule number*> has been updated, but security rule <*rule number*> has the same object sets as security rule <*rule number*> with conflict effect. The security rule <*rule number*> may not take effect. Please review security rules carefully before proceeding.

3. If a security rule is a superset of subsequent security rule, then the subsequent security rule will not get executed. The Policy Composer detects the superset security rule and gives out a warning message for the subsequent security rule,

   a. the following message is displayed for a new rule:

   The new security rule <*rule number*> has been added, but the security rule <*rule number*> object sets supersede security rule <*rule number*> object sets. The security rule <*rule number*> may not take effect. Please review security rules carefully before proceeding.

   b. the following message is displayed for an updated rule:

   The new security rule <*rule number*> has been updated, but the security rule <*rule number*> object sets supersede security rule <*rule number*> object sets. The security rule <*rule number*> may not take effect. Please review security rules carefully before proceeding.

Creating and Configuring Policies

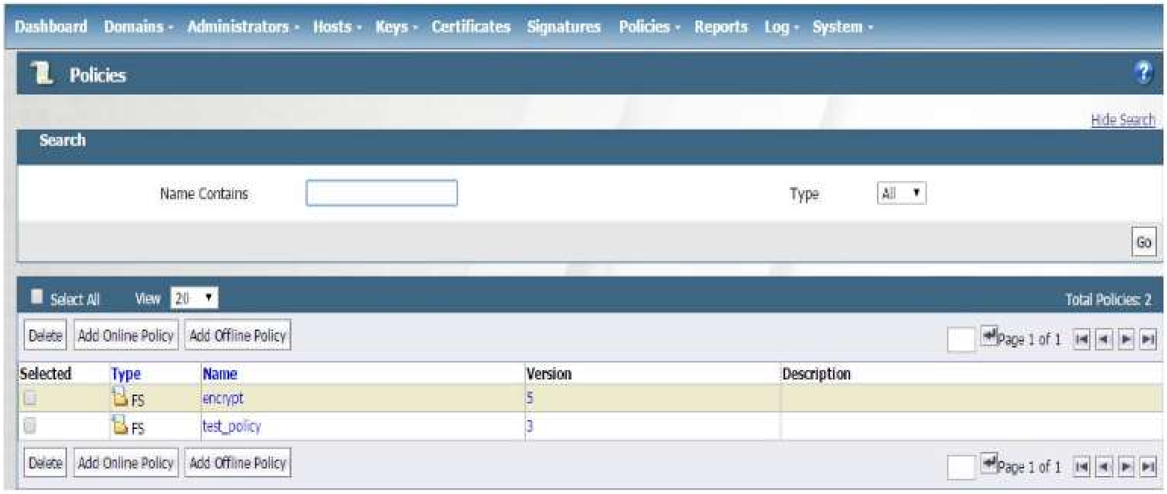
Access the Domain to be Protected

1. Log on to the Web Management Interface as a DSM administrator with DSM Security Administrator privileges to the domain containing your protected host.
2. Switch to the domain containing the host you want to protect. Click **Domains > Switch Domains.** The **Switch Domains** window opens.
3. Select the domain containing the protected host and click **Switch to domain**. The domain to which you switched, is displayed in the upper right corner of the Web Management Interface.

Naming Your Policy

1. Click **Policies > Manage Policies** to list the policies available to this domain. In this example, there are two policies.

Figure 1: Policy Management window



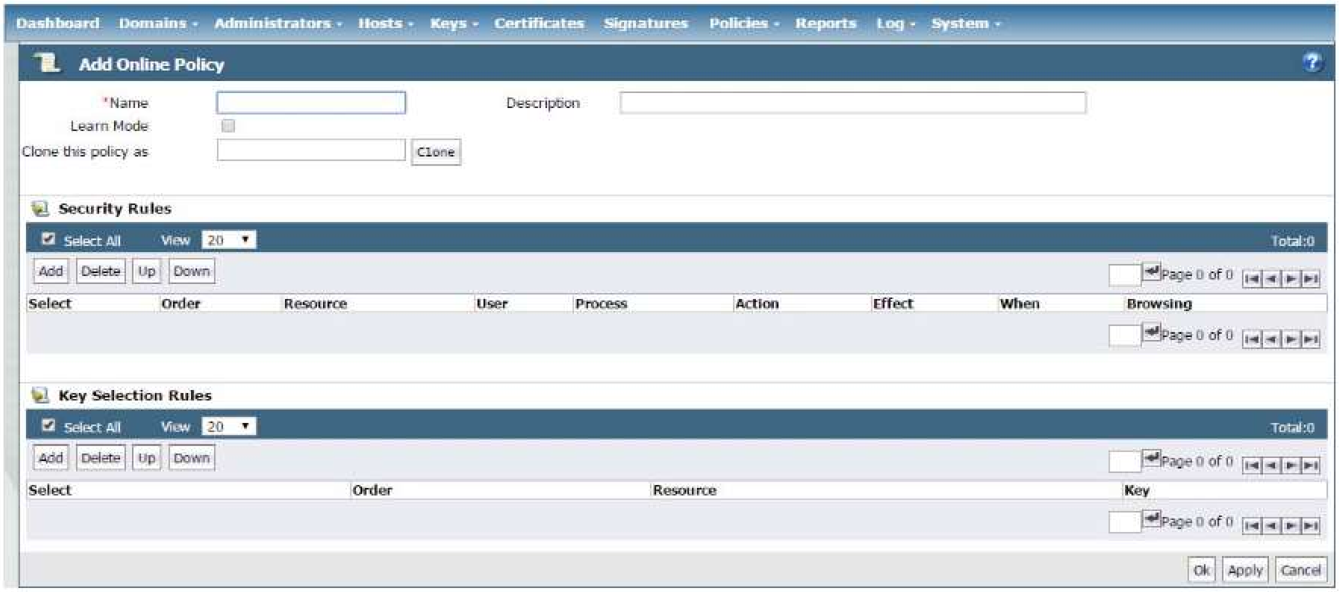
Name Contains:

Type: All

Selected	Type	Name	Version	Description
☐	FS	encrypt	5	
☐	FS	test_policy	3	

2. Click **Add Online Policy**. The *Add Online Policy* window opens.

Figure 2: Add Online Policy window



*Name:

Learn Mode: ☐

Clone this policy as:

Description:

Select	Order	Resource	User	Process	Action	Effect	When	Browsing

Select	Order	Resource	Key

3. Add an Online Policy by selecting and entering the following information.

   a. Give your policy a **Name** (for example, `basic-access-policy)` and optional **Description**.

   b. **Learn Mode** (*Optional)*. This mode permits a policy to be tested without actually denying access to the guard point. In Learn Mode, all actions that would have been denied are instead permitted, but logged. This allows you to test policies by tracking how rules are evaluated, without enforcing the policy. Monitor the log to determine how data is being accessed, then modify the policy accordingly.

   A **deny** statement in Effect must include **apply_key** when Learn Mode is enabled. This option generates a warning each time an access attempt is made that matches any security rule in the policy. This warning is sent as a log message and it can be viewed in the Web Management Interface (if it's configured to accept warnings).

Learn Mode is recommended for policies that restrict by application (process), as many applications use multiple binaries that may not be known to the creator of the policy at time of creation.

c. **Clone this policy as** (*Optional)*. Type in a new policy name and clicking **Clone**. This creates a clone of the original policy.

4. Clicking **Ok** at this point creates a blank policy called `basic-access-policy`. This policy has no rules. If you want to add rules to the policy before creating it, click **Add** instead of Ok. The **Add Security Rule** window opens.

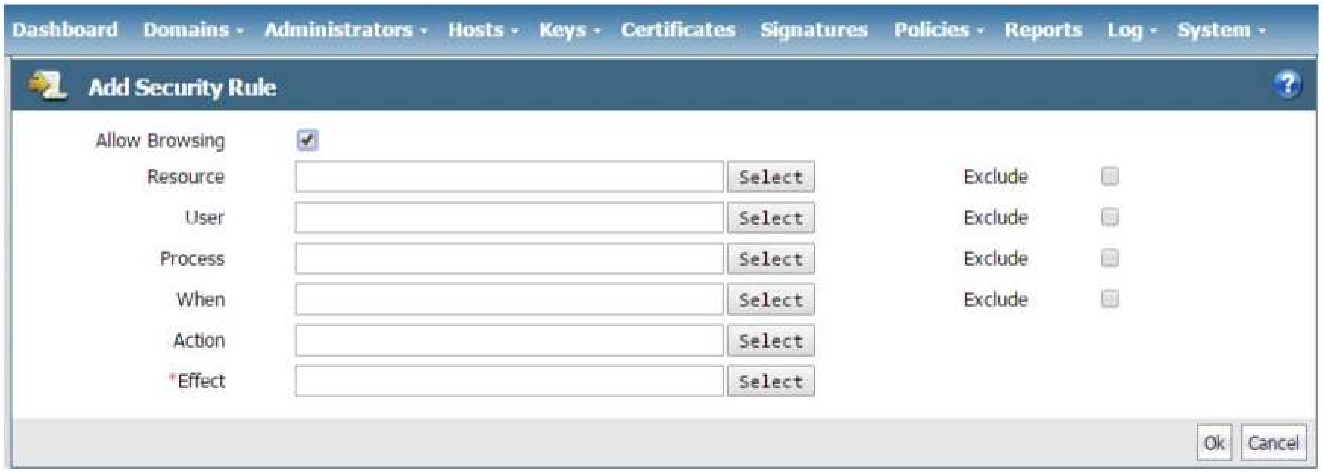
Adding Security Rules to a Policy

Rules specify how the DSM will respond to an access request.

To add security rules to a policy:

1. Open the **Add Security Rule** window if it is not displayed. Click the policy name (example: **basic-access-policy**) in the **Policies** window if the policy has already been created. Click **Add** in the **Security Rules** panel.

Figure 3: Add security rule window



NOTE: This section walks you through adding the criteria by clicking the Select button. If the criteria has already been defined and you know the names of them, you can type their names in the text boxes.

2. **Resource** (Optional)—specifies the hosts, files and directories that a user or process will be permitted or denied access to. Though not mandatory, if you define a resource that resource should exist in the guard point.

a. To specify ***all*** resources, leave **Resource** blank.

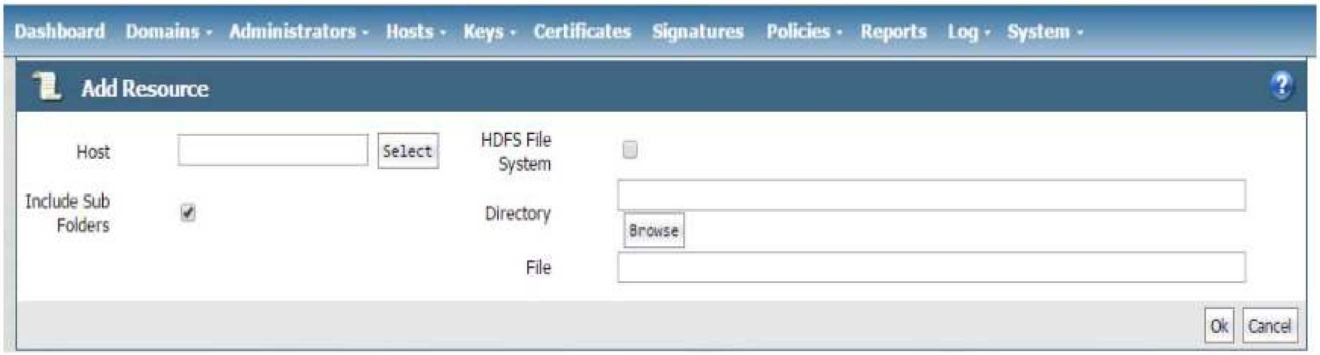
To define specific resources in a guard point, select **Resource**. The **Select Resource Set** window opens.

b. Click **Add** to create a Resource Set.

The **Add Resource** window opens. A Resource Set is a named collection of directories, files, or both, that a user or process will be permitted or denied access to.

c. Click **Add**. Here you specify the **Host**, **Directory** and **Files** on which to apply the rule.**Security Rules** panel. The **Add Security Rule** window opens.

Figure 4: Add resource window



Host

Include Sub Folders ☑

HDFS File System □

Directory

File

A resource is a combination of a directory, a file, and patterns or special variables.

Host is the hostname containing the directory. Enter the hostname and click **Browse** to browse for the directory.

HDFS File System, select this check box if the resource is located on a host that is part of a HDFS cluster group.

Directory is appended to the guard point. If the guard point is `/mnt/remote2` and the directory is `/remoteDir`, then the policy applies to the files and directories in `/mnt/remote2/remoteDir`.

The asterisk and question mark can be used to indicate one to many characters (*), or exactly one character (?). Directory examples:

`sales/` — Access limited to `sales` directory under the guard point.

`*sales/` — Access limited directories that end in “`sales`” under the guard point.

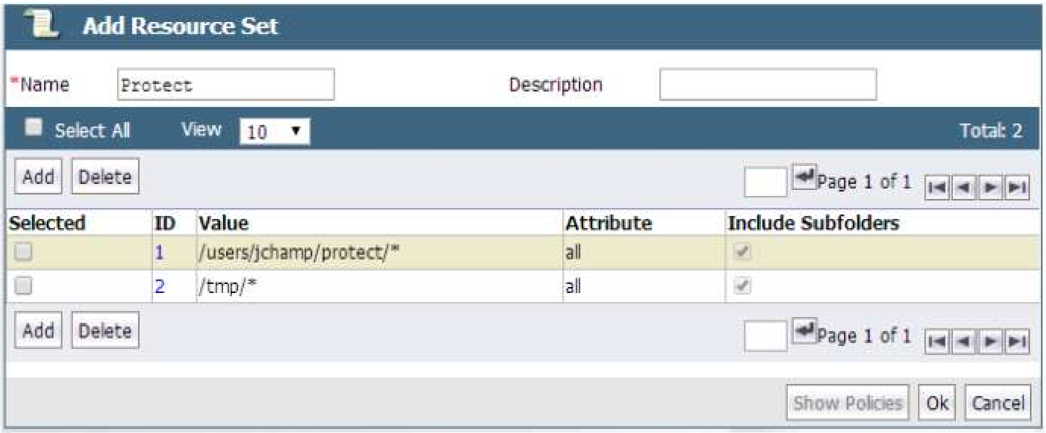
`*/sales` — Access is granted to any directories named "`sales`" anywhere.

File is the filename and can include variables or patterns.

Include subfolders finds all occurrences of the resource pattern under the guard point and applies policy protection to them. For example, if the guard point is at *a/b* and the resource is defined as *c/*.txt* and **Include subfolders** is checked, then every occurrence of **.txt* anywhere under the guard point is protected (example: *a/b/c/d/*.txt*). If **Include subfolders** is not checked, then only *a/b/c/*.txt* is protected.

d. Click **Ok** to add your desired resources to the Resource Set.

Figure 5: Add Resource Set window



Add Resource Set

*Name: Protect

Description:

□ Select All View 10 Total: 2

Add Delete Page 1 of 1

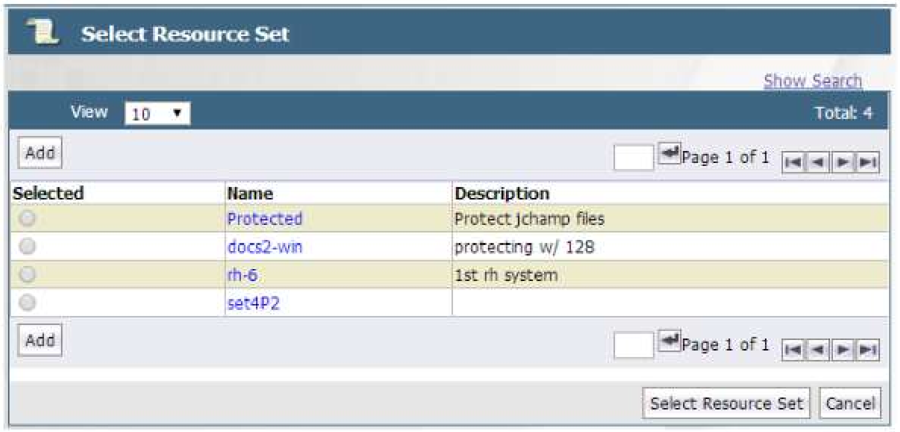
Selected	ID	Value	Attribute	Include Subfolders
□	1	/users/jchamp/protect/*	all	☑
□	2	/tmp/*	all	☑

Add Delete Page 1 of 1

NOTE: You can also create or select Resource Sets directly, without first creating a policy, by clicking **Policies > Manage Policies > Resource Sets** to bring up the **Resource Sets** window.

e. Once you have added all resources to your resource set, click **Ok**. The **Select Resource Set** window opens with the new resource set added.

Figure 6:



Select Resource Set

Show Search

View 10 Total: 4

Add Page 1 of 1

Selected	Name	Description
○	Protected	Protect jchamp files
○	docs2-win	protecting w/ 128
○	rh-6	1st rh system
○	set4P2	

Add Page 1 of 1

f. Select the resource set for this policy and click **Select Resource Set**. The **Edit Security Rule** window opens with the resource added (in this example, **Protected**).

g. Check the **Exclude** box to the right of the **Resource** text-entry box to include all host resources *except* those resources in the resource set. Uncheck the box to include just the resources in the resource set.

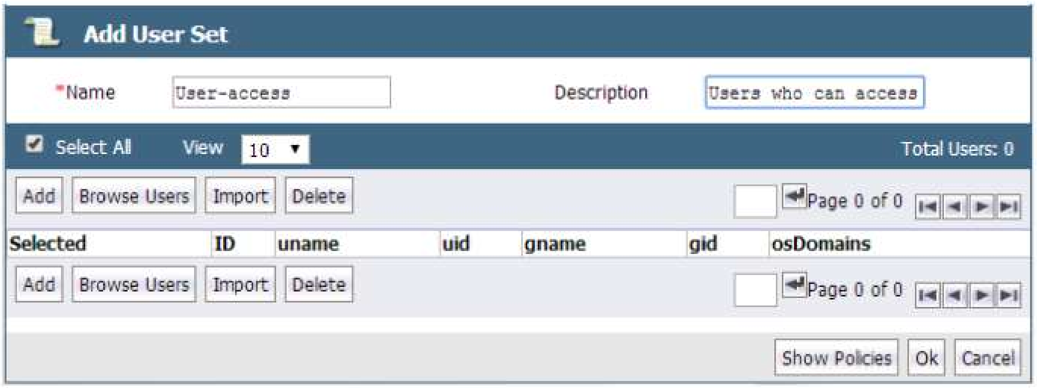
3. Specify the **User** criteria. **User** allows you to specify the users that are permitted or denied guard point access.

   a. To specify *all* users, leave **User** blank.

   To define specific users, select **User**. The **Select User Set** window opens.

b. Click **Add** to create a *User Set*. A User Set is a named collection of users that are permitted or denied guard point access. The **Add User Set** window opens.

Figure 7: Add User Set window



Add User Set

*Name: User-access

Description: Users who can access

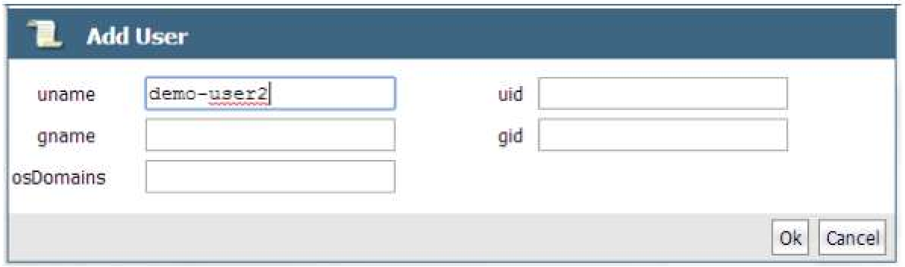
☑ Select All View 10 ▼ Total Users: 0

Selected	ID	uname	uid	gname	gid	osDomains

c. Enter a **Name** (for example, `User-access`) and optional **Description**.

d. Click **Add**. The *Add User* window opens. You must specify at least one field.

Figure 8: Add User window



Add User

uname: demo-user2

uid:

gname:

gid:

osDomains:

uname—login name.

uid (*UNIX only*)—user identification number.

gid (*UNIX only*)—user group number. Enter only the primary group ID number of the user.

gname—comma-separated list of group names.

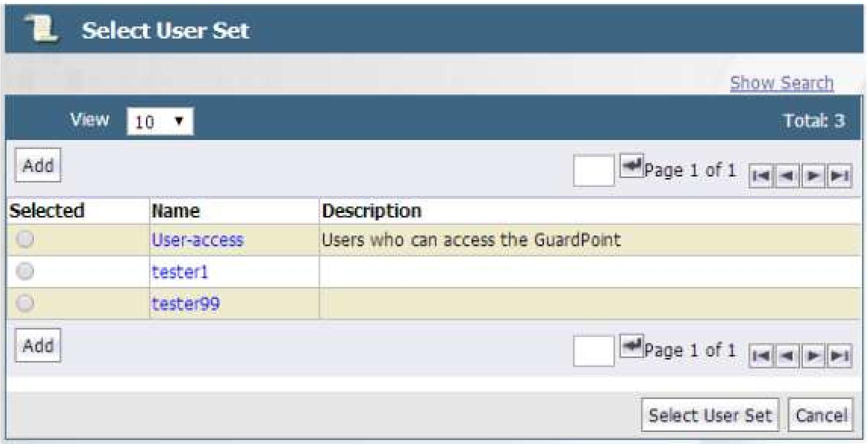
osDomain (*Windows only*)—network domain of the user. Multiple domain names, separated by commas, may be entered. Enter the string **`localhost`** to configure a generic domain.

e. Click **Ok** to add this user to the User Set.

f. Add as many users to the User Set as needed by repeating steps **c** through **e**.

g. Click **Ok**. The **Select User Set** window opens with the new User Set added.

Figure 9: Select User Set window



View 10 ▼ Total: 3

Selected	Name	Description
○	User-access	Users who can access the GuardPoint
○	tester1	
○	tester99	

h. Select the User Set for this policy and click **Select User Set**. The **Edit Security Rule** window opens with the new User Set resource added (in this example, **User-access**).

i. Check the **Exclude** box to the right of the **User** text-entry box to include all host users *except* those users in the User Set. Uncheck the box to include just the users in the User Set.

You can also create or select User Sets directly, without creating a policy, by clicking **Policies > Manage Policies > User Sets** to bring up the **User Sets** window.

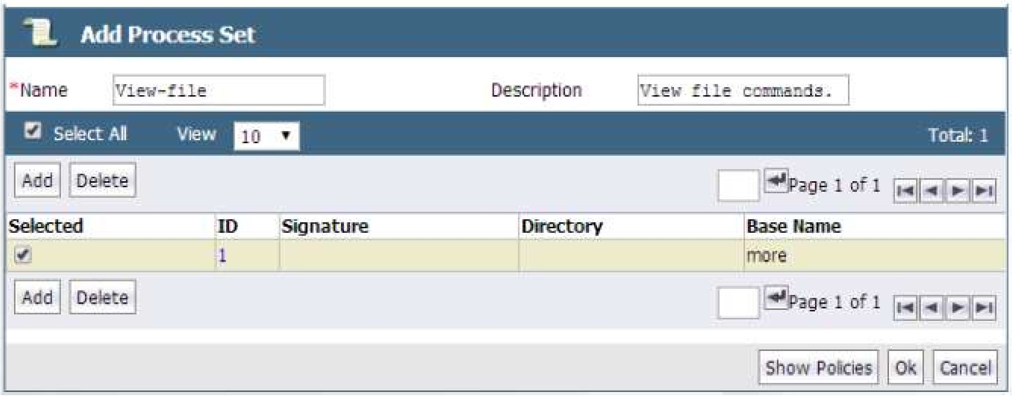
4. Specify the **Process** criteria. **Process** allows you to specify the executables that are permitted or denied access to the guard point data.

a. To specify *all* processes, leave **Process** blank.

To define specific processes, select **Process**. The **Select Process Set** window opens.

b. Click **Add** to create a *Process Set*. A Process Set is a named collection of processes that are permitted or denied access to the guard point data. The **Add Process Set** window opens.

Figure 10: Add Process Set window



*Name View-file

Description View file commands.

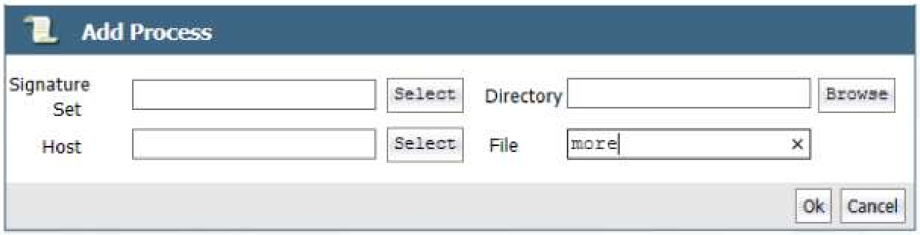
☑ Select All View 10 ▼ Total: 1

Selected	ID	Signature	Directory	Base Name
☑	1			more

c. Enter a **Name** (for example `View-file`) and optional **Description**.

d. Click **Add**. The *Add Process* window opens.

Figure 11: Add Process window



File: more

Signature Set—collection of signed files and/or directory names. Files that are signed confirm software integrity and guarantee that code has not been altered since it was cryptographically signed. If you created a signature set to use with this policy, select the signature set from the scroll-list. Otherwise, you must first create a signature set.

Host—host of the directory or executable and activates the **Browse** function.

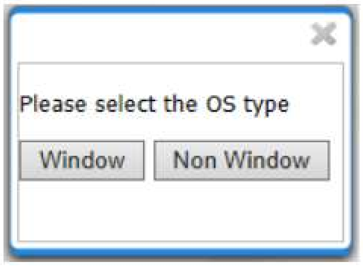
Directory—directory path information. It may be a full path, a relative path,

or left blank.

File—name of the executable. The `more` command is used in the example.

Click **Ok** to add this process to the Process Set. If you get a pop-up message asking you to select the OS type, click **Windows** for Window hosts and **Non-Windows** for Linux/UNIX hosts.

Figure 12: OS type Pop-up



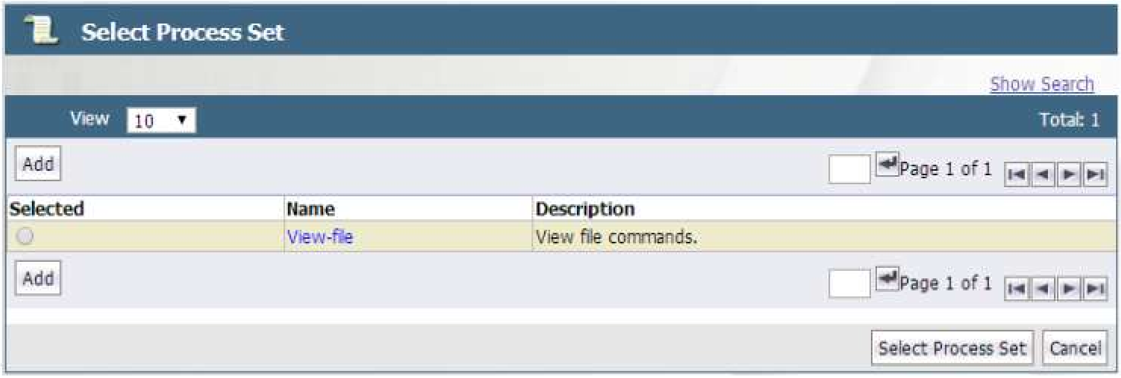
Please select the OS type

e. The **Add Process Set** window opens with the **`more`** command added.

f. Repeat steps c to e to add additional process sets.

g. Click **Ok**. The **Select Process Set** window opens with the new Process Set(s) added.

Figure 13: Select Process Set window



Selected	Name	Description
○	View-file	View file commands.

h. Select the Process Set for this policy and click **Select Process Set**. The **Edit Security Rule** window opens with the new Process Set added (in this example, **View-file**).

i. Check the **Exclude** box to the right of the **Process** text-entry box to include all host processes *except* those users in the Process Set. Uncheck the box to include just the processes in the Process Set.

You can also create or select Process Sets directly, without creating a policy, by clicking **Policies > Manage Policies > Process Sets** to bring up the **Process Sets** window.

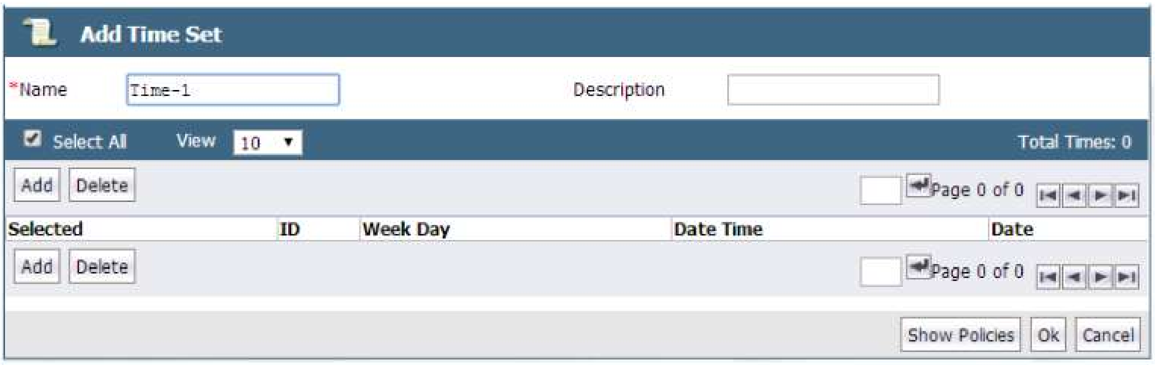
5. Specify the **When** criteria. **When** enables you to specify when guard point access is allowed.

a. To specify *all* times, leave **When** blank.

To define specific allowable times, select **When**. The **Select Time Set** window opens.

b. Click **Add** to create a **Time Set**. A Time Set is a named collection of times when guard point access is permitted or denied. The **Add Time Set** window opens.

Figure 14: Add Time Set window



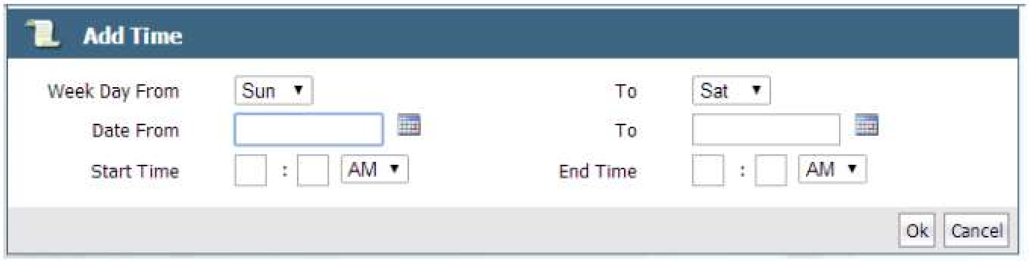
*Name: Time-1
Description:

Selected	ID	Week Day	Date Time	Date

c. Enter a **Name** (for example `Time-1`) and optional **Description**.

d. Click **Add**. The **Add Time** window opens.

Figure 15: Add Time window



Add Time

Week Day From	Sun ▾	To	Sat ▾
Date From		To	
Start Time	: AM ▾	End Time	: AM ▾

Week Day From - To is a range of weekdays days during which access is denied or permitted.

Data From - To is a range of dates during which access is denied or permitted.

Start Time - End Time is a range of times during which access is denied or permitted.

NOTE: Time is set to the protected host clock, not the DSM clock.

e. Click **Ok** to add this time range to the Time Set.

Repeat steps c through e to add additional time sets. Add as many times to the Time Set as needed.

f. Click **Ok**. The **Select Time Set** window opens with the new Time Set added.

g. Select the Time Set for this policy and click **Select Time Set**. The **Edit Security Rule** window opens with the new Time Set resource added (in this example, `Time-1`).

h. Check the **Exclude** box to the right of the **When** text-entry box to include all times *except* those times in the Time Set. Uncheck the box to include just the times in the Time Set.

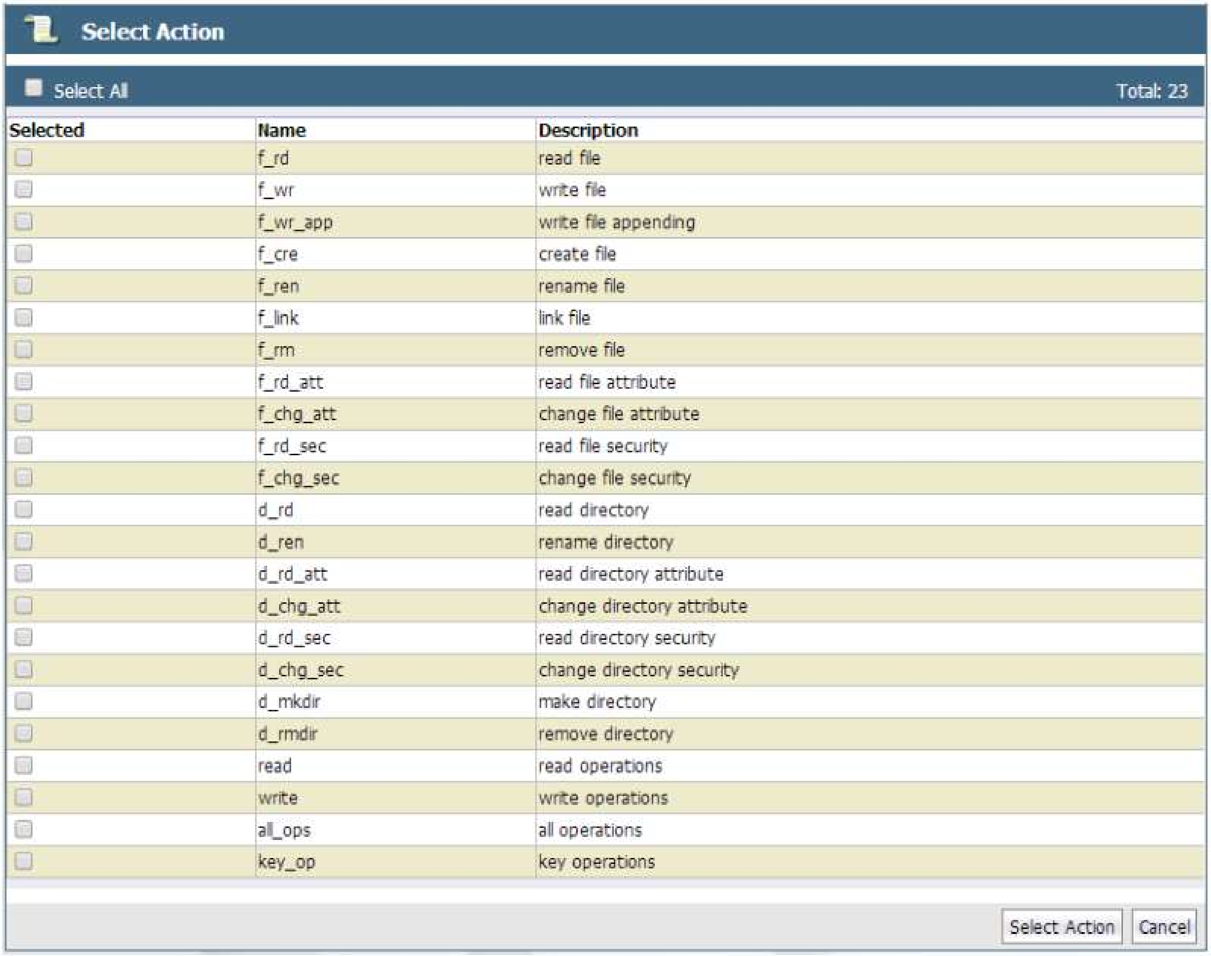
You can also create or select Time Sets directly, without creating a policy, by clicking **Policies > Manage Policies > Time Sets** to bring up the *Time Sets* window.

6. Specify the **Action** criteria. **Action** allows you to specify the type of file and directory action allowed in a guard point.

To specify *all* actions, leave **Action** blank.

To specify allowable actions, select **Action**. The *Select Action* window opens.

Figure 16: Select Action window



Select Action

□ Select All Total: 23

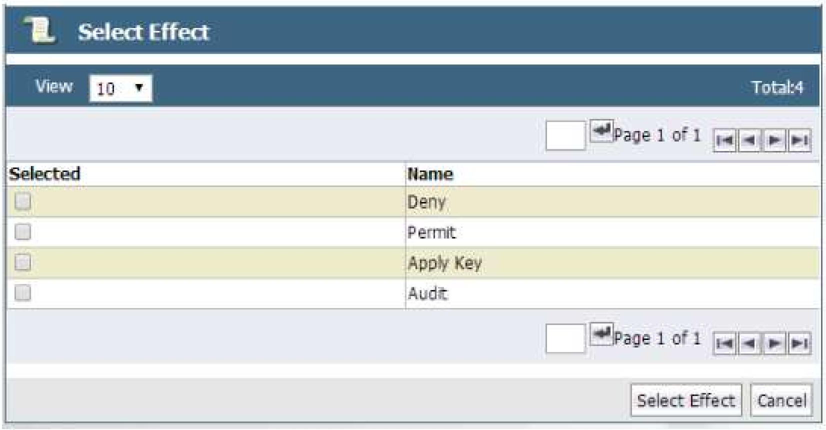
Selected	Name	Description
□	f_rd	read file
□	f_wr	write file
□	f_wr_app	write file appending
□	f_cre	create file
□	f_ren	rename file
□	f_link	link file
□	f_rm	remove file
□	f_rd_att	read file attribute
□	f_chg_att	change file attribute
□	f_rd_sec	read file security
□	f_chg_sec	change file security
□	d_rd	read directory
□	d_ren	rename directory
□	d_rd_att	read directory attribute
□	d_chg_att	change directory attribute
□	d_rd_sec	read directory security
□	d_chg_sec	change directory security
□	d_mkdir	make directory
□	d_rmdir	remove directory
□	read	read operations
□	write	write operations
□	all_ops	all operations
□	key_op	key operations

i. Select the allowable actions, and click **Select Action**. The **Add Security Rule** window opens with the allowable actions.

7. Specify the **Effect** for each security rule. **Effect** is the action that occurs when the attempted access matches all the criteria in the rule.

a. Select **Effect**. The **Select Effect** window opens.

Figure 17: Select Effect window



Selected	Name
□	Deny
□	Permit
□	Apply Key
□	Audit

Deny—Denies the access attempt to the resource.

Permit—Grants the access attempt to the resource.

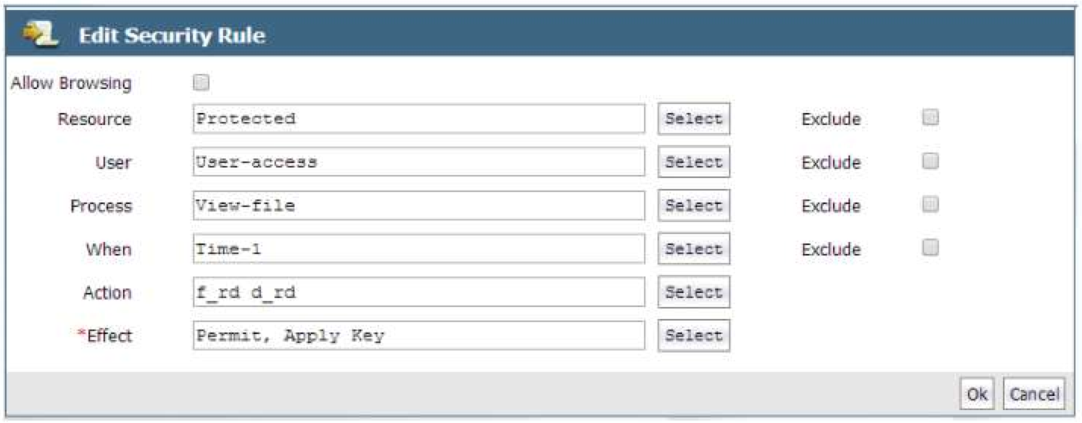
Audit—Used in conjunction with **permit** or **deny**, **audit** creates an entry in the Message Log that describes what is being accessed, when it is being accessed, and the security rule being applied.

Apply Key—Applies an encryption key to data in a guard point. Data copied into the guard point is encrypted with the key specified in the **Key Selection Rules** panel and data that is accessed in the guard point is decrypted using the same key.

NOTE: If you select **Apply Key**, you must also specify the key rules to apply for encrypting and decrypting the resources.

b. Select desired effects and click **Select Effect**. The *Edit Security Rule* window opens with all criteria and the effects displayed.

Figure 18: Edit Security Rule window

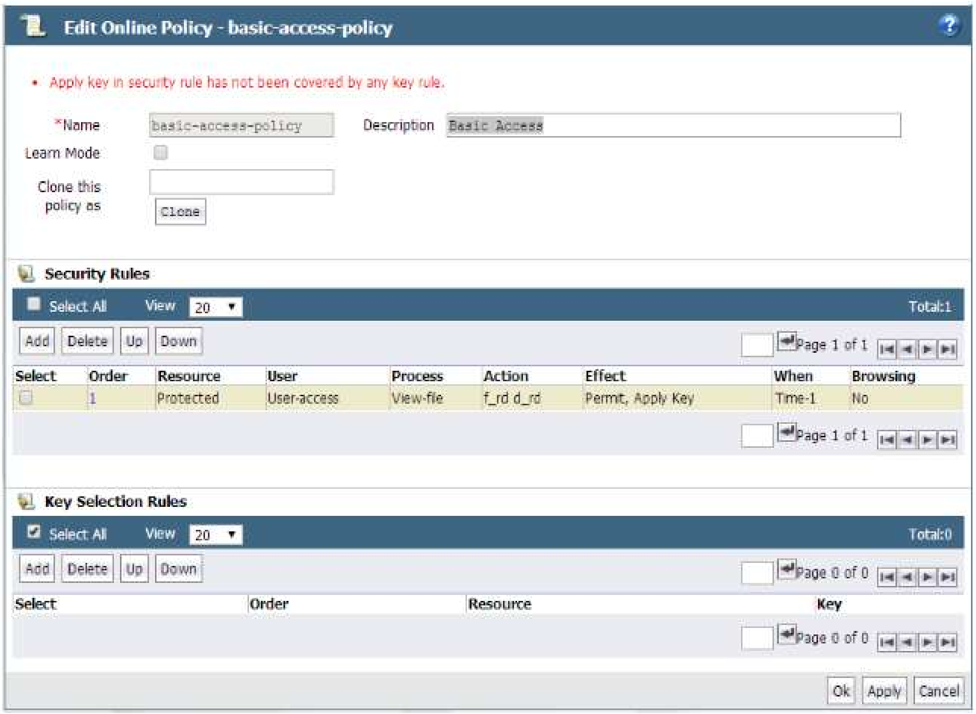


Allow Browsing	□	
Resource	Protected	Exclude □
User	User-access	Exclude □
Process	View-file	Exclude □
When	Time-1	Exclude □
Action	f_rd d_rd	
*Effect	Permit, Apply Key	

c. Click **Ok**. The **Add Online Policy** window opens.

d. If you did not enter **Apply Key** to **Effect**, click **Ok**. The *Edit Online Policies* window opens, `basic-access-policy` can now be applied to a guard point.

Figure 19: Edit Online Policies window



- Apply key in security rule has not been covered by any key rule.

*Name: basic-access-policy
Description: Basic Access
Learn Mode: □
Clone this policy as:

Security Rules

Select	Order	Resource	User	Process	Action	Effect	When	Browsing
□	1	Protected	User-access	View-file	f_rd d_rd	Permit, Apply Key	Time-1	No

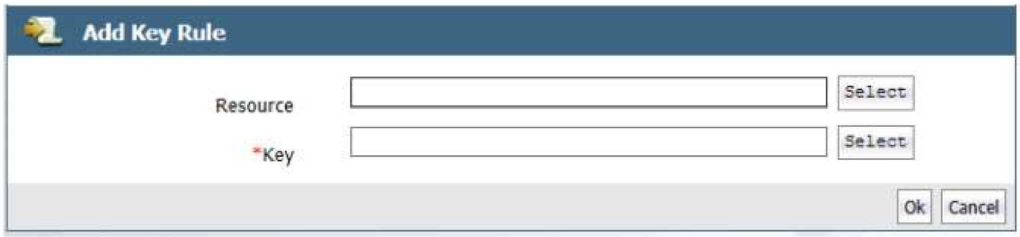
Key Selection Rules

Select	Order	Resource	Key

e. If you entered **Apply Key** to **Effect**, you must set up your *Key Selection Rules*. Click **Add** in the **Key Selection Rules** panel at the bottom of the *Add Online Policy* window.

The **Add Key Rule** window opens.

Figure 20: Add Key Rule window

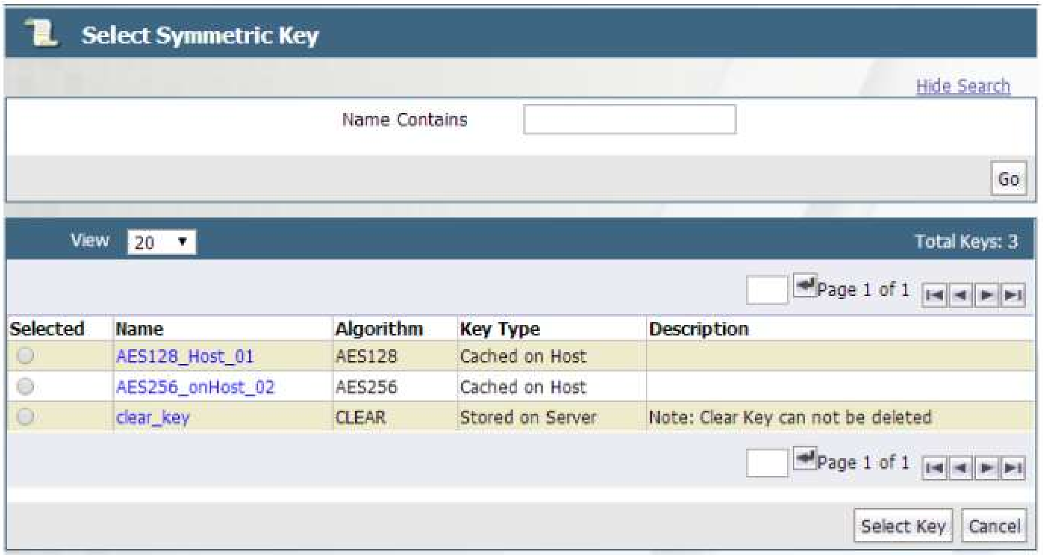


Resource—(Optional) Opens the **Resource Set List** window from which you can select or create the resource set whose members are to be encrypted. If you do not specify a resource set in the **Key Selection Rules** tab, encryption is applied to the resources specified in the **Security Rules** tab.

Key—Enables you to enter a key name, or, if selected, the **Select Symmetric Key** window opens allowing you to select an existing key.

f. Select a **Resource**, if desired, then select **Key**. The **Select Symmetric Key** window opens.

Figure 21: Select Symmetric Key window



Selected	Name	Algorithm	Key Type	Description
○	AES128_Host_01	AES128	Cached on Host	
○	AES256_onHost_02	AES256	Cached on Host	
○	clear_key	CLEAR	Stored on Server	Note: Clear Key can not be deleted

g. Select a key and then click **Select Key**. The **Add Key Rule** window opens with the key added. Click **Ok**. The **Edit Online Policy** window opens.

h. Add as many security rules as required to implement the desired policy by repeating steps **c** through **g**.

The last rule of the policy is called a *default security rule* or a *catchall rule*. This rule catches any access attempt that is not matched by other security rules.

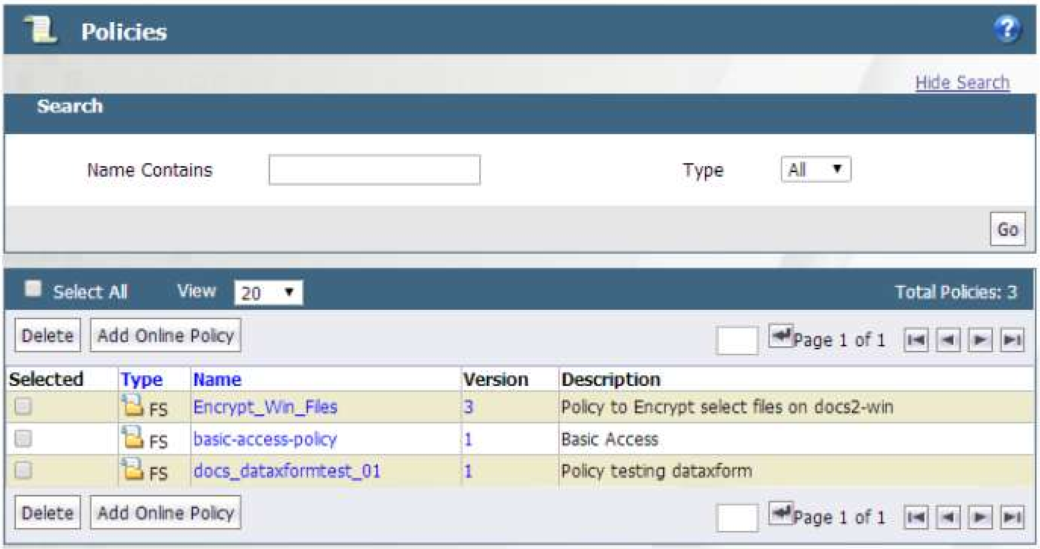
To create a default security rule, leave all criteria fields blank with the exception of **Action** and **Effect** on the **Security Rules** tab:

- Set **Action** to **all_ops**
- Set **Effect** to **deny audit**

This security will match any attempt to access any data on the host. After creating this rule, click **Ok** in the **Edit Online Policy** window.

The **Policies** window opens and `basic-access-policy` can be applied to a guard point.

Figure 22: Policies window



Name Contains: (blank)

Type: All

Select All

View: 20

Total Policies: 3

Selected	Type	Name	Version	Description
□	FS	Encrypt_Win_Files	3	Policy to Encrypt select files on docs2-win
□	FS	basic-access-policy	1	Basic Access
□	FS	docs_dataxformtest_01	1	Policy testing dataxform

Displaying Policies

Policies are displayed in the *Policies* window. Policies displayed can be selected for modification or deletion.

To display policies:

1. Log on to the Web Management Interface as an administrator of type Security with `Policy` role permissions, type Domain and Security with `Policy` role permissions, or type All.
2. Select **Policies** in the menu bar.

   The number of times a File System, or *online*, policy has been changed is displayed in the **Version** column of the **Policies** window. This number indicates the current revision only. It cannot be used to roll-back to a previous version. Restore a backup to revert to a previous online policy version. The version count starts at zero when the online policy is initially created and increments by one each time it is saved thereafter. Backup, or *offline*, policies display `N/A` only.

Viewing and selecting policies in the policy window

- (Optional) The **Show Search** label located below the **Signature Sets** banner opens the **Search** panel. You can enter all or part of a policy name and/or limit the search to policies that are used by a specific type of agent (All or FS). Click **Go** to display only those policies that match the search criteria. Click `Hide Search` to conceal the **Search** panel.
- **Select All**—Selects all the policies that are displayed on the current Web browser page. Select this checkbox to select all the policies on the current page at one time. If you have enabled the

Select checkbox for many individual policies, a quick way to deselect them is to enable and then disable the **Select All** checkbox.

- **View**—A scroll-list from which to select the maximum number of policies to display on the current page. Up to 200 policies can be displayed on one page. Displays up to the specified number of policies on one Web page, regardless of the display number specified in the preferences.

Navigation buttons are displayed in the **Policies** window. Use these buttons to advance between pages.

Creating a GuardPoint

A GuardPoint is a Vormetric-agent-protected directory. A GuardPoint is created after the VTE agent is installed on a host, and a policy has been created and applied to a directory on that host. The policy applies to all files and folders under the GuardPoint. The VTE Agent intercepts any attempts to access anything in the GuardPoint, and uses the DSM policy to grant or deny the access attempt.

Check that no one is using the directory before making it a GuardPoint. If a user is accessing a file or folder in the directory when it is made into a GuardPoint, that user can continue to use data in memory rather than use the actual data in the GuardPoint. Users should save their work, close applications that are running in the directory, and exit the directory before a GuardPoint is applied. When users re-enter the directory, they will use protected data and the VTE Agent will work as per the applied policy.

To change a policy or rekey a GuardPoint, be prepared to temporarily stop access to the GuardPoint. Changing policies for a GuardPoint requires an interruption of service because the transition process entails disabling one policy and then enabling another policy. The GuardPoint must be inactive during the transition period to ensure GuardPoint integrity. The same rule applies to moving a host between host groups when it includes a change in policies. Coordinate policy changes during a maintenance outage window.

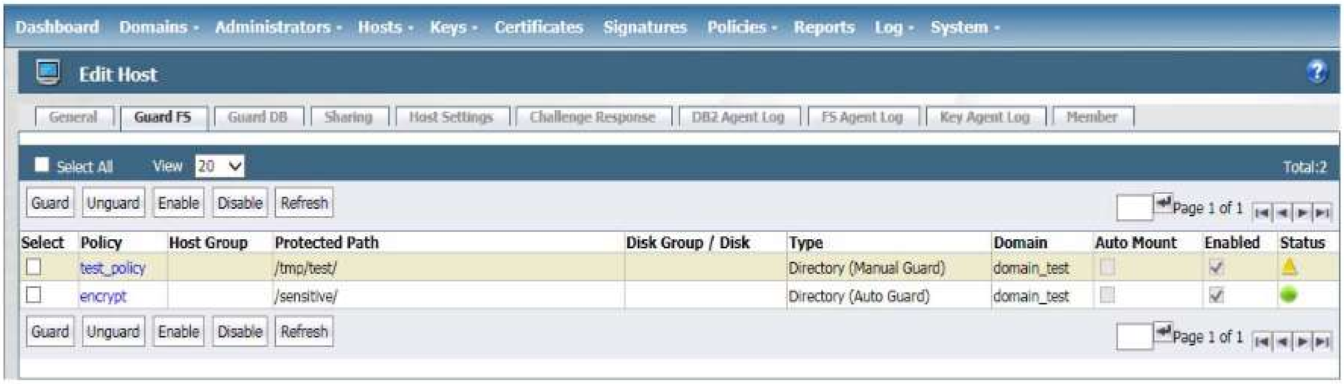
Applying a Policy to Create a GuardPoint

1. Log on to the Management Console as an administrator of type Security with Host role permissions, type Domain and Security, or type All.
2. Select Hosts > Hosts in the menu bar. The Hosts window opens.
3. Click the target host in the Host Name column. The Edit Host window opens to the General tab for the selected host.

The Registration Allowed check box must be selected for the VTE Agent running on the target host to register itself with the DSM. The Communication Enabled check box must be selected for the DSM to push policy and configuration changes to the host, and for the DSM to accept VTE Agent policy evaluation requests.

4. Select the Guard FS tab. This tab displays applied policies in a tabular format:

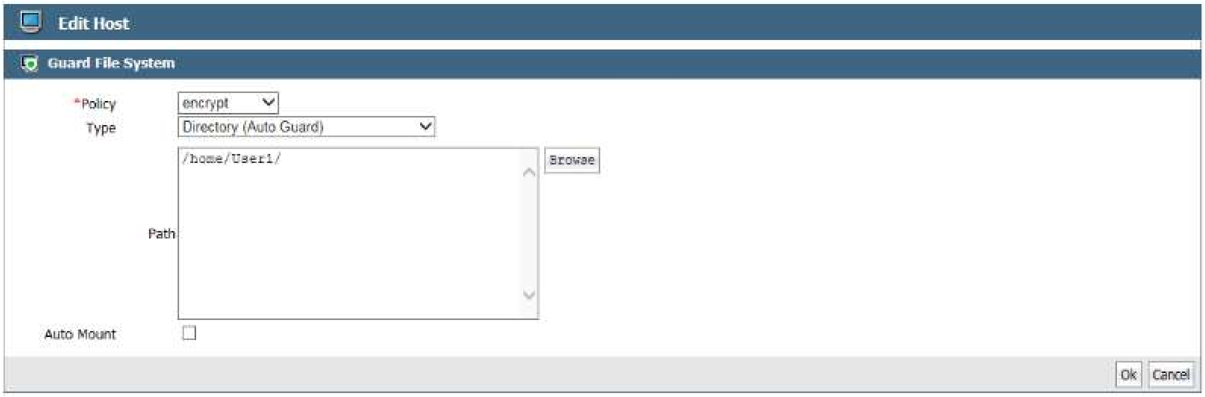
Figure 23: Guard FS tab: Policies



Select	Policy	Host Group	Protected Path	Disk Group / Disk	Type	Domain	Auto Mount	Enabled	Status
□	test_policy		/tmp/test/		Directory (Manual Guard)	domain_test	□	☑	⚠
□	encrypt		/sensitive/		Directory (Auto Guard)	domain_test	□	☑	●

5. Click Guard. The Guard File System window opens.

Figure 24: Guard File System



*Policy: encrypt
Type: Directory (Auto Guard)
Path: /home/User1/
Auto Mount □

a: Select a policy to apply from the Policy drop-down menu. You must select a policy before you can browse the agent file system.

Later, when you select directories to configure as GuardPoints, if you select multiple directories, they will all be configured with the selected policy.

b: Select the type of GuardPoint to apply in the Type drop-down menu.

UNIX choices are:

- Directory (Auto Guard)
- Directory (Manual Guard)
- Raw or Block Device (Auto Guard)

- Raw or Block Device (Manual Guard)

Windows choices are:

- Directory (Auto Guard)
- Raw or Block Device (Auto Guard).

Make selections as follows:

- For file system directories, select Directory (Auto Guard) or Directory (Manual Guard)
- For raw or block devices, select Raw or Block Device (Auto Guard) or Raw or Block Device (Manual Guard).
- For file system directories that are to be manually guarded and unguarded in order to failover to a different node in a cluster, select Directory (Manual Guard).
- For raw devices that are to be manually guarded and unguarded in order to failover to a different node in a cluster, select Raw or Block Device (Manual Guard).

c: Select the Auto Mount check box, if applicable, to indicate that the GuardPoint is a UNIX automount. The Auto Mount check box disappears when Directory (Manual Guard) or Raw or Block Device (Manual Guard) is selected because only regular mounts are supported by these types.

d: Enter the full paths of one or more directories in the Path text-entry box and click Ok to apply the policy to the target GuardPoint. Enter one path per line in the Path text-entry box. Enter part of a directory path in the Path text-entry box and click Browse to jump to the specified point. From there, you can use the browser to descend further into the directory hierarchy and select one or more directories to be guarded.

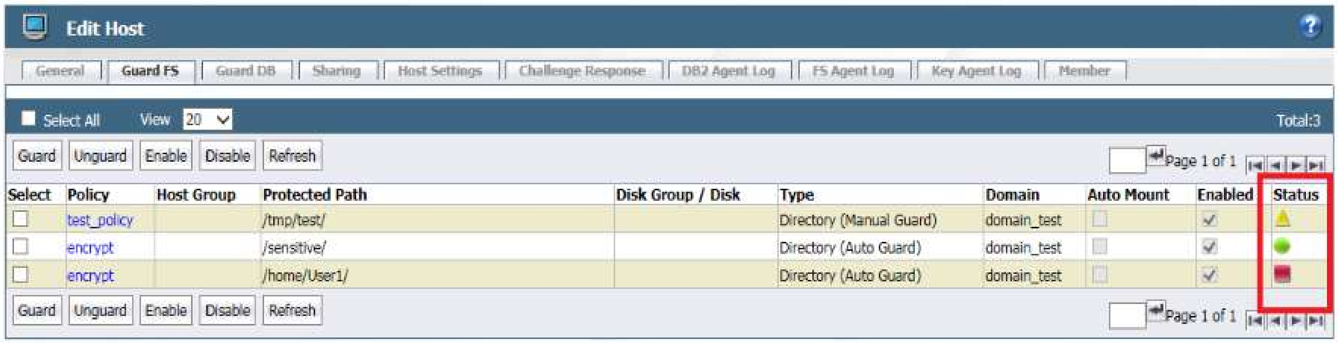
Configured GuardPoints are displayed as folders overlaid with a shield. If you suspect that the GuardPoint status is incorrectly indicated, note that the agent status displayed in the window shows the status as it is configured in the DSM database. It is not a real-time indication of the actual status. For actual status, log onto the agent system and run VTE Agent utilities, like “vmsec status” and “secfsd -status guard”. Compare the two to ensure that the GuardPoint status on the DSM and VTE Agent match. If the two do not match, go with what you see on the agent. The shield indicates a configured GuardPoint only. The GuardPoint can be enabled or disabled and the shield will still be displayed. The shield remains displayed until the GuardPoint is unguarded (deleted).

e: Click OK. The Guard File System window opens to display the selected values.

6. Click OK. The Edit Host window is updated to display the new GuardPoint or GuardPoints.

   Observe the GuardPoint status column:

Figure 25: GuardPoint Status



Select	Policy	Host Group	Protected Path	Disk Group / Disk	Type	Domain	Auto Mount	Enabled	Status
□	test_policy		/tmp/test/		Directory (Manual Guard)	domain_test	□	☑	▲
□	encrypt		/sensitive/		Directory (Auto Guard)	domain_test	□	☑	●
□	encrypt		/home/User1/		Directory (Auto Guard)	domain_test	□	☑	■

- A green circle indicates an active and healthy connection to the agent system.
- A red square indicates that a policy has been configured but not applied on the agent system; that a GuardPoint is disabled or is in the process of being disabled; or that a communication error has occurred between the DSM and agent systems.
- A yellow triangle indicates that an attempt to delete a GuardPoint is still pending. The DSM awaits confirmation from the agent before it deletes the GuardPoint from the DSM. A yellow triangle also indicates a GuardPoint of type Directory (Manual Guard) or Raw or Block Device (Manual Guard) that is not mounted on the host system.

Wait a moment then click the Refresh button to update the display. The red square should change to a green circle.

7

Audit Logs

System events are recorded in various log files and displayed in the Web Management Interface. Several log files are generated during software installation and while using the DSM. You can view logs files directly in an editor, or you can view log entries on the Web Management Interface. The information displayed in the *Logs* window is determined by the log settings of each host.

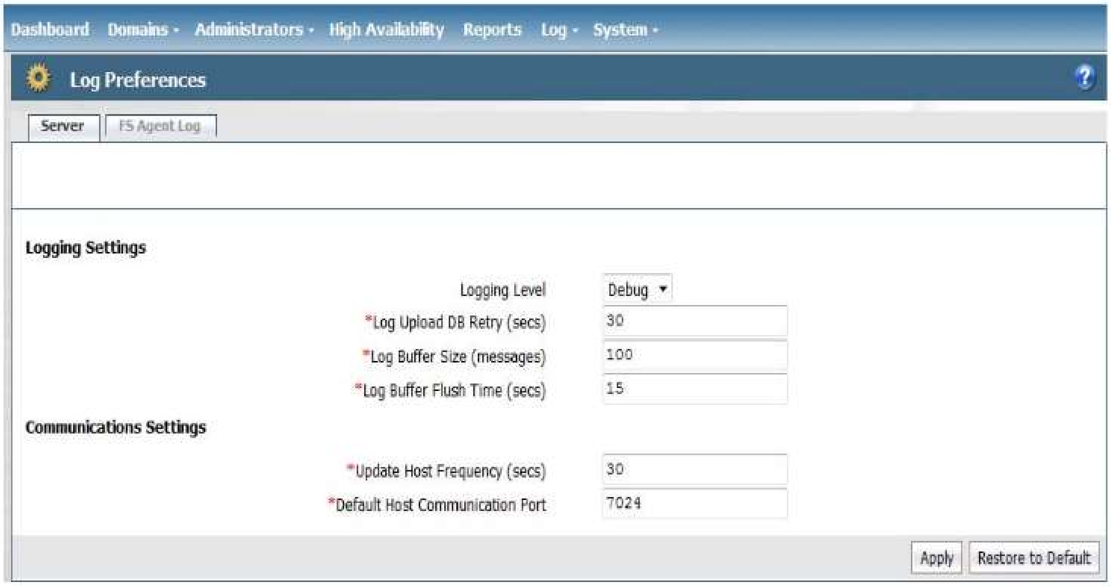
Log Preferences

The **System > Log Preferences** page lets you set logging preferences for the VTE agents. There are 4 different logging levels that can be set to choose the level of information to be collected. In the CC mode, the log level ***must*** be set to either DEBUG or INFO.

Setting server log preferences

The **Server** tab displays information about the current DSM configuration.

Figure 1: Log Preferences - Server



Logging Settings

Logging Level: Debug
*Log Upload DB Retry (secs): 30
*Log Buffer Size (messages): 100
*Log Buffer Flush Time (secs): 15

Communications Settings

*Update Host Frequency (secs): 30
*Default Host Communication Port: 7024

You can configure the following attributes:

- **Logging Level**: Sets the severity level of the DSM. This information is displayed in the 'Logs' window. The choices are DEBUG, INFO, WARN, ERROR, and FATAL. Each level includes the levels below it. For example, FATAL logs only fatal errors, whereas WARN logs warnings, ERROR and FATAL conditions. The default is INFO. See Table 1 below.
- **Log Upload DB Retry (secs)**: The interval before resuming the transfer of agent log data that had been uploaded, and is stored in system files, into the log viewer database after a failure, such as after losing the connection to the database. The default is 30 seconds.
- **Log Buffer Size (messages)**: The maximum number of entries to place in the DSM log. When this limit is reached, or when Log Buffer Flush Time has elapsed, the entries are moved to the log viewer database. The default is 100 entries.
- **Log Buffer Flush Time (secs)**: The interval to wait before moving log entries in the server log buffers to the log viewer database. The default is 15 seconds.
- **Update Host Frequency**: The interval between scans of the queue to see if any changes have been made to the host configuration on the DSM. Any changes are pushed to the host. The default interval between scans is 30 seconds.
- **Default Host Communication Port**: The port number on the DSM and on the file agent through which the communicate. When you change the Default Host Communication Port number, the new port number is applied to all new hosts that are added after the configuration change is made. Existing file agent hosts are unaffected. The change is visible in the Communication Port display in the General tab of each new host. If you change the Communication Port number for an existing host, you must restart the file agent process that runs on that host.

Upload Logging Settings

- Maximum Number of Messages to Upload At Once: Limits the number of messages sent to the DSM at one time. When the specified number of log entries is reached, those entries are uploaded to the DSM. The default is 1000.
- Upload Messages At Least Every (seconds): The maximum interval to wait before the agent is to upload messages to the DSM. Use this attribute to update the log viewer even when the Maximum Number of Messages to Upload At Once has not been reached. You can lower the interval if there is little agent activity. The default is 10 seconds.
- Upload Messages At Most Every (seconds): The minimum interval to wait before the agent is to upload messages to the DSM. You can increase the interval if there is considerable agent activity, so the agents do not flood the network with log messages. The default is 1.
- Normal Time Out (seconds): The maximum interval of time the agent is to wait for the DSM to acknowledge a backup or restore request and upload related message data. If the agent cannot connect to the DSM within the specified interval, the agent will try again after the interval configured by the Upload Messages At Least Every attribute. The default is 2 seconds.

- Shutdown Time Out (seconds): The maximum interval of time the agent is to wait for the DSM to acknowledge job completion and upload related message data. If the agent is unable to upload the log messages within the specified interval, they are left on the agent system. The agent will resend the messages at the beginning of the next job. The default is 30 seconds.
- Drop If Busy: Select to slow log message generation and drop log files during periods of extreme logging.

NOTE: The Upload to Server check box must be enabled in order to configure these options.

Duplicate Message Suppression Settings

- Threshold: Used when the Duplicates value is set to Suppress. Specifies the maximum number of duplicate messages the agent is to send to the DSM within the amount of time specified by the Interval parameter. The default is 5 messages. The maximum is 100.
- Interval: Used when the Duplicates value is set to Suppress. Specifies the time period in which the number of duplicate messages, specified by Threshold, can be uploaded to the DSM. Once Interval is exceeded, the count specified by the Threshold parameter starts again. The default is 600 seconds (10 minutes). The maximum is 3600.

Log message levels

The detail and extent of information logged is determined by the selected log level. The agent supports five log levels as listed in Table 1.

Table 1: The Supported Log Levels

Severity	Description
DEBUG	The DEBUG level provides detailed information about events that are intended for support engineers and developers.
INFO	The INFO level provides general information that highlights the progress of the application.
WARN	The WARN level designates potentially harmful situations.
ERROR	The ERROR level designates error events that might still allow the application to continue running.
FATAL	The FATAL level designates very severe error events that will presumably lead the application to quit.

Log levels are cumulative. The level that you select not only generates log entries for events that occur at that level, but all the levels below. For example, the WARN level also includes events that occur on the ERROR and FATAL levels.

Supported Syslog formats

Refer to chapter 3, “Adding a Syslog Server” on page 21, for details about how to add a Syslog server.

The following log formats are supported:

Plain Message

The following is an example of a Plain Message formatted log message. The table following the message describes the components of the message.

```
12-07-201216:53:02Local7.Debug10.3.32.2312012-12-08 01:01:58.709
vormetric:SOURCE[linux64-32231.qa.com]:DAO0445I:Administrator voradmin added
SysLog Host 10.3.25.168.
```

Table 2: Syslog message parameters and descriptions

Parameter	Description
`12-07-201216:53:02`	Date and time
`Local7.Debug`	Message priority
`10.3.32.231`	Sending machine’s IP address
`2012-12-08 01:01:58.709`	Date and time of logged event
`vormetric`	Originator tag
`SOURCE[linux64-32231.qa.com]`	Source of message
`DAO0445I`	Unique message ID
`Administrator voradmin added SysLog Host 10.3.25.168`	Plain text message of the logged event

Common Event Format (CEF) log format

Vormetric syslog supports Common Event Format (CEF) log format. The Vormetric CEF format is specified in the Arcsight “Common Event Format” standard.

The following is an example of a CEF formatted log message.

```
<27> 2012-10-16T16:01:44.030Z centos-6-0 CEF:0|Vormetric, Inc.|vee-
fs|5.1.0.9026|CGP2604E| Reject access|7|logger=CGP spid=6362 cat=[ALARM]
pol=AuditAllExceptLp uinfo=lp,uid\=4,gid\=7\\lp\\ sproc=/bin/ls
```

```
act=read_dir_attr gp=/Guard filePath=/datafiles/file.dat denyStr=DENIED
showStr= Code (1M)
```

Table 3: CEF Log Format parameters and descriptions

Parameter	Description
`<27>`	A standard syslog facility/priority code
`2012-10-16T16:01:44.030Z`	Date and time
`centos-6-0`	The host name of the machine sending the message.
`CEF:0`	Version of the CEF
`Vormetric, Inc.`	Sending device vendor
`vee-fs`	Sending device product
`5.1.0.9026`	Sending device version
`CGP2604E`	Unique message ID
`Reject access`	Name: A human-readable and understandable description of the event.
`7`	Severity: An integer that reflects the importance of the event. Only numbers from 0 to 10 are allowed, where 10 indicates the most important event.
`logger=CGP spid=6362 cat=[ALARM] pol=AuditAllExceptLp uinfo=lp,uid\=4,gid\=7\\lp\\ sproc=/bin/ls act=read_dir_attr gp=/Guard filePath=/datafiles/file.dat denyStr=DENIED showStr= Code (1M)`	Extension: A collection of key-value pairs. The keys are part of a predefined set. The standard allows for including additional keys. An event can contain any number of key-value pairs in any order, separated by delimiting characters.

RFC5424

Vormetric syslog supports RFC5424 log format.

An example of an RFC5424 formatted log message follows. Components of the message are described in the table following the message example:

```
<30>1 2012-12-07T21:44:04.875Z t3-normaluser.i.vormetric.com vee-FS 0
CGP2603I [CGP@21513 sev="INFO" msg="Audit access" cat="\[AUDIT\]"
pol="normaluser-only-aes256" uinfo="normaluser,uid=2001,gid=1\\other\\"
sproc="/usr/bin/cat" act="read_attr" gp="/export/home/normaluser/test"
filePath="/test.txt" denyStr="PERMIT" showStr="Code (1M)"]
```

Table 4: CEF Log Format parameters and descriptions

Parameter	**Description**
`<30>1`	A standard syslog facility and priority code
`2012-12-07T21:44:04.875Z`	Date and time
`t3-normaluser.i.vormetric.com`	The host name of the machine sending the message.
`vee-FS`	Sending device product
`0`	Process ID field having no interoperable meaning, except that a change in t he value indicates that there has been a discontinuity in syslog reporting.
`CGP2603I`	Unique message ID
`[CGP@21513 sev="INFO" msg="Audit access" cat="\[AUDIT\]" pol="normaluser-only-aes256" uinfo="normaluser,uid=2001,gid=1\\ other\\" sproc="/usr/bin/cat" act="read_attr" gp="/export/home/normaluser/test" filePath="/test.txt" denyStr="PERMIT" showStr="Code (1M)"]`	Structured data field: Provides a mechanism to express information in a well-defined, easily parseable and interpretable data format. This field consists of the Structured Data (SD) Element, SD-ID, and SD-Parameter.

Log Event Extended Format (LEEF)

Vormetric syslog supports Log Event Extended Format (LEEF). The LEEF header is pipe ("|") separated and attributes are tab separated.

Viewing Logs

The entries displayed in the Message Log depend on the administrator type (System, Domain, Security, All), the domain in which the administrator is working, and, for Security Administrators, the administrator roles (Audit, Key, Policy, Host, Challenge & Response) that have been assigned.

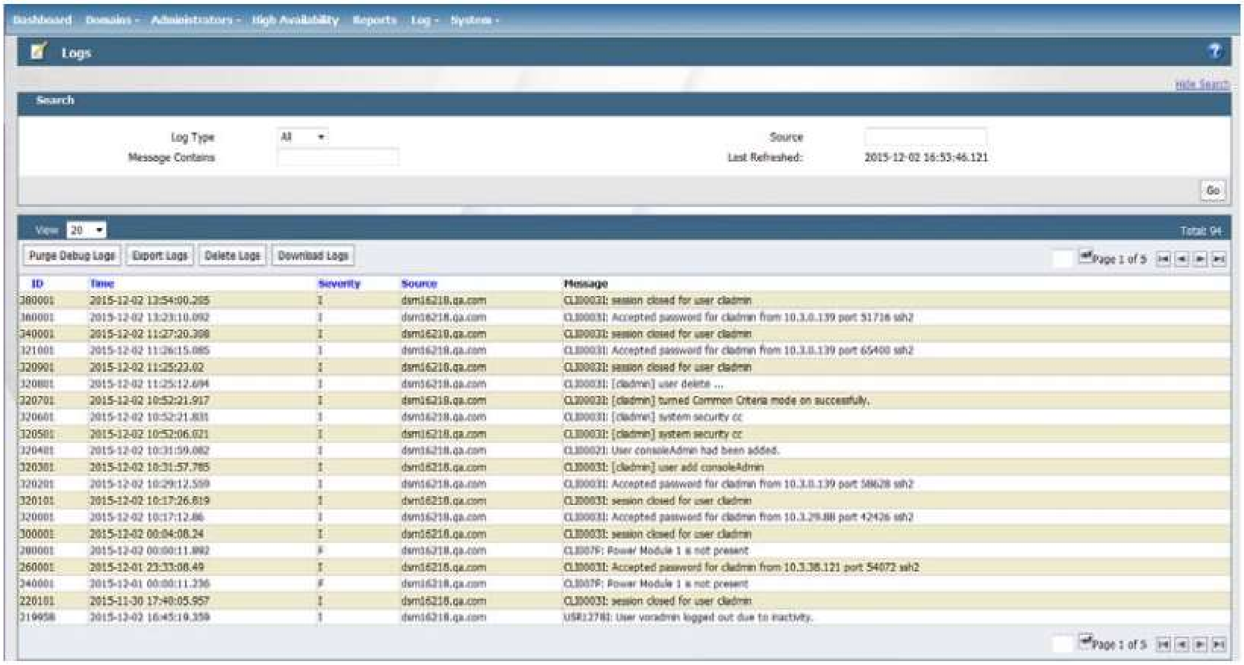
An administrator of type DSM System Administrator cannot view the log entries that an administrator of type DSM Domain Administrator or DSM Security Administrator (and vice versa). By design, entries exported to a syslog log file will have gaps in the number sequence depending on the domains and roles of the DSM administrators who are actively logged on.

As a System Administrator, you will see log entries such as the administrators that have logged into the Web Management Interface, the administrators that have been created, and policy evaluation.

The Logs page

The *Logs* page lets you purge, export, delete, or download log files.

Figure 2: Logs page



Log Type: All
Message Contains:
Source:
Last Refreshed: 2015-12-02 16:53:46.121

View: 20

ID	Time	Severity	Source	Message
380001	2015-12-02 13:54:00.205	I	dsm16218.qa.com	CLI0003I: session closed for user cladmin
360001	2015-12-02 13:23:10.092	I	dsm16218.qa.com	CLI0003I: Accepted password for cladmin from 10.3.0.139 port 51716 ssh2
340001	2015-12-02 11:27:20.308	I	dsm16218.qa.com	CLI0003I: session closed for user cladmin
321001	2015-12-02 11:26:15.085	I	dsm16218.qa.com	CLI0003I: Accepted password for cladmin from 10.3.0.139 port 65400 ssh2
320901	2015-12-02 11:25:23.02	I	dsm16218.qa.com	CLI0003I: session closed for user cladmin
320801	2015-12-02 11:25:12.694	I	dsm16218.qa.com	CLI0003I: [cladmin] user delete ...
320701	2015-12-02 10:52:21.917	I	dsm16218.qa.com	CLI0003I: [cladmin] turned Common Criteria mode on successfully.
320601	2015-12-02 10:52:21.831	I	dsm16218.qa.com	CLI0003I: [cladmin] system security cc
320501	2015-12-02 10:52:06.021	I	dsm16218.qa.com	CLI0003I: [cladmin] system security cc
320401	2015-12-02 10:31:59.082	I	dsm16218.qa.com	CLI0002I: User consoleAdmin had been added.
320301	2015-12-02 10:31:57.785	I	dsm16218.qa.com	CLI0003I: [cladmin] user add consoleAdmin
320201	2015-12-02 10:29:12.559	I	dsm16218.qa.com	CLI0003I: Accepted password for cladmin from 10.3.0.139 port 58628 ssh2
320101	2015-12-02 10:17:26.819	I	dsm16218.qa.com	CLI0003I: session closed for user cladmin
320001	2015-12-02 10:17:12.86	I	dsm16218.qa.com	CLI0003I: Accepted password for cladmin from 10.3.29.88 port 42426 ssh2
300001	2015-12-02 00:04:08.24	I	dsm16218.qa.com	CLI0003I: session closed for user cladmin
280001	2015-12-02 00:00:11.882	F	dsm16218.qa.com	CLI007F: Power Module 1 is not present
260001	2015-12-01 23:33:08.49	I	dsm16218.qa.com	CLI0003I: Accepted password for cladmin from 10.3.38.121 port 54072 ssh2
240001	2015-12-01 00:00:11.236	F	dsm16218.qa.com	CLI007F: Power Module 1 is not present
220101	2015-11-30 17:40:05.957	I	dsm16218.qa.com	CLI0003I: session closed for user cladmin
219958	2015-12-02 16:45:19.359	I	dsm16218.qa.com	USR1278I: User voradmin logged out due to inactivity.

- **Purge Debug Logs**: Removes all DEBUG level messages from the Log window and the Security Server database.
- **Export Logs**: Saves the Management Web Management Interface log to a file.
- **Delete Logs**: Removes the entire Security Server log database.
- **Download Logs**: Collects all the logs used in the maintenance and configuration of the Security Server installation and writes them to a ZIP file.

Entries are displayed based upon the following criteria:

- Event time and sequence
- Severity of the event
- Log type (i.e., agent, server, or both)
- Source of the event i.e. DSM or agent host name
- Log message text

The DSM log displays:

- DSM configuration changes that have occurred. Only an indication that a change has occurred is provided. Specific information about each change is not provided.
- Authorized and unauthorized access attempts to directories protected by the Transparent Encryption Agent, as specified in the policy and log settings of the host.

Example audit log

```
CGP2601I: [SecFS, 0] [AUDIT] Policy[allowAllOps_fs]
User[root,uid=0,gid=0\root,bin,daemon,sys,adm,disk,wheel\]
Process[/bin/cat] Action[write_app] Res[/opt/apps/apps1/doc/file2.txt]
Key[aes128] Effect[PERMIT Code (1U,2U,3R,4M)]
```

Codes are provided in the file system audit logs that identify actions by the policy enforcement engine. The code follows the number of the rule being processed.

Transparent Encryption Agent Error Codes:

A: The Action component of a security rule failed to match.

M: All security rule components match and, unless overridden, the Effect for that security rule is applied.

P: The Process component of a security rule failed to match.

R: The Resource component of a security rule failed to match.

T: The time specified in the When component of a security rule failed to match.

U: The User component of a security rule failed to match.

Refer to the audit log example above. The first and second Security Rules fail because of a mismatch in the User component (1U, 2U). The third Security Rule fails because of a Resource component (3R) mismatch. However, all the rules in the fourth Security Rule match (4M), and the actions defined in the policy, such as use an encryption key, are applied.

Sample Audit Logs

Audit Server Connection

Establishment and dis-establishment of communications with audit server:

```
LOG1318W: Syslog message back logged: qa-syslog:1515 (TCP)
(org.productivity.java.syslog4j.SyslogRuntimeException:
java.net.ConnectException: Connection refused)
```

```
LOG0668W: Route to syslog server DOWN: qa-syslog:1515 (TCP)
(java.net.ConnectException: Connection refused)
```

Audit configuration modifications:

```
119924 2015-09-17 13:37:08.799 I sys29088.qa.com CGP2601I: [SecFS, 0]
PID[0] [AUDIT] Policy[EncryptionPolicy]
User[root,uid=0,gid=0\root,bin,daemon,sys,adm,disk,wheel\]
Process[/bin/cat] Action[read_file] Res[/manual-
guard/encryptedfile.txt] Key[EncryptionKey] Effect[PERMIT Code (1M)]
119923 2015-09-17 13:37:08.799 I sys29088.qa.com CGP2603I: [SecFS, 0]
PID[0] [AUDIT] Policy[EncryptionPolicy]
User[root,uid=0,gid=0\root,bin,daemon,sys,adm,disk,wheel\]
Process[/bin/cat] Action[read_attr] Res[/manual-
guard/encryptedfile.txt] Effect[PERMIT Code (1M)]
```

Configuration of external audit storage location:

```
19964  2015-09-16 17:09:19.074  I  dsm15243.qa.com  DAO0445I:
Administrator domadmin added SysLog Host 10.3.48.240.
```

Syslog connection failure:

```
1420863 2016-01-11 10:53:43.872 W toe LOG1318W: Syslog message back
logged: 10.3.15.156:1514 (TCP) (The Security Server was unable to
contact 10.3.15.156.)
```

TLS connection established:

```
1633101 2016-01-11 10:44:05.348 I toe COM1376I: 10.3.15.241:8521 >
toe:8445 TLS connection established with cipher
suite:TLS_RSA_WITH_AES_256_CBC_SHA
```

TLS connection closed:

```
1632501 2016-01-11 10:44:05.811 I toe COM1377I: toe:37290 >
10.3.15.156:1514 TLS connection closed
```

TLS connection failed:

```
164331 2016-01-11 11:00:12.235 W toe COM1375W: 10.3.15.241:8603 >
toe:8448 TLS connection failed, reason:handshake_failure
```

Authentication

Installing a license:

```
19905 2015-09-15 16:44:09.26 I dsm15243.qa.com LIC0587I: Administrator
admin successfully installed license.
```

Administrator password change:

```
19904 2015-09-15 16:41:42.643 I dsm15243.qa.com DAO0317I: User "admin"
changed the password.
```

User log in record:

```
19903 2015-09-15 16:41:30.345 I dsm15243.qa.com DAO0267I: User "admin",
a SYSTEM_ADMIN logged in at 2015-09-15 16:41:30.337 from client with IP
address 10.3.0.166; trusted channel established.
```

Failure to login:

```
19921  2015-09-16 15:46:08.115  E  dsm15243.qa.com  USR0632E: User
"sysadmin" failed to login from client with IP address 10.2.5.117.

19920  2015-09-16 15:46:08.113  E  dsm15243.qa.com  DAO0297E:
Administrator "sysadmin" failed to login at 2015-09-16 15:46:08.087 from
client with IP address 10.2.5.117.
```

Failure to login. In this instance (null) refers to the local host and not a remote machine:

```
CLI0006E: FAILED LOGIN 1 FROM (null) FOR cliadmin, Authentication
failure
```

Establishment/termination of a session:

```
199912 2015-09-21 19:02:59.534 I dsm15243.qa.com USR1277I: User
secadmin logged out.
```

Establishment/termination of a session:

```
19906 2015-09-15 17:45:42.957 I dsm15243.qa.com USR1278I: User admin
logged out due to inactivity.
```

Unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state:

```
279929 2015-09-17 13:28:34.881 I dsm49252.qa.com DAO0268I:
Administrator "voradmin" account is locked due to multiple failed login
attempts.
```

Configuration of authentication failure threshold value:

```
DAO0268I: Administrator "voradmin" account is locked due to multiple
failed login attempts.    DAO0269I: Administrator "voradmin" account is
unlocked.
```

Acceptance of tested secret or password during login:

```
1701738 2016-01-14 12:46:19.623 I toe DAO02671: User "all_admin", a
ALL_ADMIN logged in at 2016-01-14 12:46:19.619 from client with IP
address 10.3.27.199; trusted channel established.
```

Rejection of tested secret during login for non-LDAP user:

```
1701737 2016-01-14 12:46:10.18 E toe USR0632E: User “admin” failed to
login from client with IP address 10.3.27.199
```

Identification of changes to defined quality metrics:

```
1701740 2016-01-14 12:47:51.953 I toe DAO0305I: Administrator
"all_admin" updated the password policy to "360 days duration;4 password
history;8 minimum length;0 minimum number of character changes;disallow
change with 0 days;31 days expiration notification;uppercase
required;numbers required;special characters required".
```

Management of users that belong to a particular role:

```
19922  2015-09-16 15:53:30.665  I  dsm15243.qa.com DAO0406I: Domain
Administrator Admin removed user jsmith from the domain.
```

```
19921  2015-09-16 15:53:15.256  I  dsm15243.qa.com DAO0405I:
Administrator Admin added user jsmith with roles [KEY_CUSTODIAN,
POLICY_ADMINISTRATOR, SERVER_ADMINISTRATOR, DOMAIN_ADMINISTRATOR,
CHALLENGE_RESPONSE_ADMINISTRATOR] to the domain domain1.
```

```
19920  2015-09-16 15:53:09.819  I  dsm15243.qa.com DAO0424I:
Administrator Admin disabled user jsmith in the domain.  DAO0425I:
Administrator Admin enabled user jsmith in the domain {2}.
```

Modification of an administrator role:

```
17017442016-01-14 12:52:57.846I toe DAO1281I: Administrator "all_admin"
assigned roles [KEY_CUSTODIAN, POLICY_ADMINISTRATOR,
SERVER_ADMINISTRATOR, CHALLENGE_RESPONSE_ADMINISTRATOR] to user
"security" in the domain "CC" to replace old roles [AUDIT_CUSTODIAN,
KEY_CUSTODIAN, POLICY_ADMINISTRATOR, SERVER_ADMINISTRATOR,
CHALLENGE_RESPONSE_ADMINISTRATOR].
```

Adding an administrator to a DSM:

```
17017422016-01-14 12:51:17.063I toe DAO0089I: Administrator "all_admin"
added a new administrator "admin1" of user type "SYSTEM_ADMIN" into the
Security Server.
```

Failure for HTTPS:

```
2781601 2016-01-14 16:14:23.375 W toe COM1375W: 10.3.27.199 > toe:8448
TLS connection failed, reason:handshake_failure
```

LDAP server

Connecting to an LDAP Server:

```
159916 2015-09-17 14:44:30.527 I dsm15243.qa.com DAO0267I: User
"user1", a DOMAIN_SECURITY_ADMIN logged in at 2015-09-17 14:44:30.522
from client with IP address 10.3.0.167; trusted channel established.
```

Rejection of tested secret during login for LDAP user:

```
17017312016-01-14 12:42:31.956E toe USR1351E: LDAP User "all_admin"
failed to login from client with IP address 10.3.27.199. Reason: [LDAP:
error code 49 - Invalid Credentials]
```

Policy Logs

Creation of a policy:

```
19958 2015-09-16 16:15:12.921 I dsm15243.qa.com DAO0280I: Administrator
"secadmin" created online policy "EncryptionPolicy".
```

Modification of a policy:

```
19959 2015-09-16 16:15:18.447 I dsm15243.qa.com DAO0282I: Administrator
"secadmin" updated online policy "EncryptionPolicy"
```

Deletion of a policy:

```
19961 2015-09-16 16:18:04.211 I dsm15243.qa.com DAO0281I: Administrator
"secadmin" deleted online policy "EncryptionPolicy".
```

Transmission of policy to Access Control products:

```
119905 2015-09-17 11:24:02.546 I sys29088.qa.com VMD3883I: [vmd, 16192]
PID[16192] Certificates for the vmd agent expire in 364 days
119904 2015-09-17 11:24:02.545 I sys29088.qa.com VMD3640I: [vmd, 16192]
PID[16192] STARTED on linux PORT 7024 VERSION: 5.1.1.21
119902 2015-09-17 11:24:01.544 I sys29088.qa.com VMD3781I: [vmd, 16192]
PID[16192] Successfully received and implemented a new security
configuration.
119901 2015-09-17 11:24:01.348 I sys29088.qa.com POL4553I: [vmd, 16192]
PID[16192] Internal initialization successful.
```

Definition of object attributes:

```
99964 2015-09-17 11:36:11.28 I dsm15243.qa.com DAO0560I: Administrator
"secadmin" created resource set "EncryptTextFiles".
```

Association of attributes with objects:

```
99964 2015-09-17 11:36:11.28 I dsm15243.qa.com DAO0560I: Administrator
"secadmin" created resource set "EncryptTextFiles".
```

Definition of subject attributes where the guard point /home/data is the subject and the security attribute is the policy "encrypt-all"

```
17017282016-01-14 12:37:57.043ItoeDAO0229I: Administrator "all_admin"
added guard point "/home/data/" with policy "encrypt-all" on host
"linux3805".
```

Policy push from DSM:

```
17017262016-01-14 12:29:15.289 I toe COM0314I: The Security Server was
able to successfully send security configuration changes to the agent on
host linux3805
```

Policy implemented from agent:

```
18799072016-01-14 12:29:34.323I linux3805 VMD3781I: [vmd, 2096]
PID[2096] Successfully received and implemented a new security
configuration.
```

How to Contact Support

In the event of software failures such as:

- Failure of the DSM software to start
- Unreachable DSM services
- Inability of DSM to reach other services (such as LDAP or Syslog)
- Operating System Kernel panics
- System hangs

OR

For hardware failures please follow the RMA process to return your appliance to Vormetric for analysis and receiving a functioning replacement hardware appliance. Hardware failures typically tend to be:

- hard disk failures
- power module failures
- Unresponsive system (e.g. mother board failures)

Contact Vormetric technical support at:

- help.vormetric.com
- support@vormetric.com
- (877) 267-3247