THALES

Vormetric Data Security Platform

Vormetric Data Security Manager (DSM)

Installation and Configuration Guide

Release 6

Version 6.1.0

Documentation v2
August 06, 2018

Vormetric Data Security Platform
Installation and Configuration Guide
Vormetric Data Security Manager (DSM)

Thales Data Security includes a restricted license to the embedded IBM DB2 database. That license stipulates that the database may only be used in conjunction with the Thales Vormetric Security Server. The license for the embedded DB2 database may not be transferred and does not authorize the use of IBM or 3rd party tools to access the database directly

Contents

Preface

The *Data Security Manager (DSM)* Vormetric Data Security Manager (DSM) describes how to install and configure the DSM hardware and virtual appliances, including the V6100 DSM with Hardware Security Module (HSM). This document is intended for system administrators who install the DSM and connect it to a network.

DOCUMENTATION VERSION HISTORY

The following table describes the documentation changes made for each document version.

Documentation Changes

Document Version	Date	Changes
6.0.2 v3	02/02/2018	This release contains important security fixes.
6.0.2 v4	03/01/2018	This release introduces support for DSM key attributes to be propagated to VAE and support for a DSM AWS image.
6.0.3 v1	05/24/2018	GA release of v6.0.3This release introduces support for nShield Connect Integration, Automatic registration of LDT/Docker hosts, Bring Your Own Encryption Keys (BYOK). Provides the ability to create non-KMIP domains with a DSM KMIP license installed, Additional REST APIs, and Thales branding on GUI, CLI, and documentation.
6.1.0 v1	07/20/2018	V6000 and virtual appliances can now be HSM-enabled by connecting them to an nShield Connect appliance. DSM is now available in the Azure marketplace.
6.1.0 v2	08/06/2018	Removed extraneous text.

ASSUMPTIONS

This documentation assumes that you have knowledge of your computer network as well as network configuration concepts. For the hardware appliance, you'll also need access to the data center where your DSM hardware appliance will be racked and cabled.

For more information about what's new in this release, refer to the *DSM 6.0.2 Release Notes*. Refer to the *DSM Administrators Guide* for how to administer your DSM Appliance and to the various agent guides for information about Vormetric Data Security Agents.

SERVICE UPDATES AND SUPPORT INFORMATION

The license agreement that you have entered into to acquire the Thales products (“License Agreement") defines software updates and upgrades, support and services, and governs the terms under which they are provided. Any statements made in this guide or collateral documents that conflict with the definitions or terms in the License Agreement, shall be superseded by the definitions and terms of the License Agreement. Any references made to “upgrades” in this guide or collateral documentation can apply either to a software update or upgrade.

SALES AND SUPPORT

For support and troubleshooting issues:

- http://help.thalesesecurity.com
- http://support.vormetric.com
- support@thalesesecurity.com
- (877) 267-3247

For Thales Sales:

- http://enterprise-encryption.vormetric.com/contact-sales.html
- sales@thalesesec.net
- (408) 433-6000

1 The Data Security Manager (DSM)

The Data Security Manager (DSM) is the central component in the Vormetric Data Security Platform (VDS Platform). The DSM provides centralized management of data security policies and encryption keys that enable corporations to secure their data in physical as well as virtual environments. With the DSM you can:

- Define security policies to encrypt files and directories and control access to that encrypted data
- Create, store and manage DSM encryption keys, efficiently
- Provide centralized key management for third-party platforms, and securely store X.509 certificates, symmetric keys, and asymmetric keys
- Provide strong separation of duties, ensuring one administrator does not have complete control over data security policies, encryption keys, and DSM administration
- Create administrative domains for different business units or different customers to share the DSMs protection but, with complete separation of administrators and the data they control
- Provide continuous availability by clustering DSMs to ensure access to DSM policies and keys
- Provide flexible administration via a web-based management console, command line interface (CLI), and application programming interfaces (API) including REST and SOAP.

This guide describes how to install and configure the DSM V6100 and V6000 hardware appliances, and the DSM virtual appliance.

This chapter contains the following sections:

DSM Overview

The DSM is available as either a hardware appliance with a Hardware Security Module (model V6100), a hardware appliance (model V6000), or a virtual appliance.

The DSM stores data security policies, encryption keys, and audit logs in a a virtual or hardened appliance that is physically separated from the VTE Agents. Security teams can enforce strong separation of duties over management of the system by requiring the assignment of key and policy management to more than one data security administrator so that no one person has complete control over the security of data.

Figure 1: DSM V6000 Appliance without HSM (rear view)

Figure 2: DSM V6100 Appliance with HSM (rear view)

The DSM integrates key management, data security policy management, and event log collection into a centrally managed platform that provides high availability and scalability to thousands of Vormetric Transparent Encryption (VTE) Agents. This enables data security administrators to manage standards-based encryption across Linux, UNIX, and Windows operating systems in both centralized and geographically distributed environments. The DSM supports IPv4 and IPv6 addresses.

IPMI

The V6000 and V6100 DSM hardware appliances support the Intelligent Platform Management Interface (IPMI). IPMI is a computer interface specification for autonomous computer subsystems. It provides remote access to the V6000 and V6100 hardware appliances. It allows administrators to remotely monitor appliance health (temperature, power consumption, physical drive status, chassis intrusion), perform remote cold boots (power off and power on),

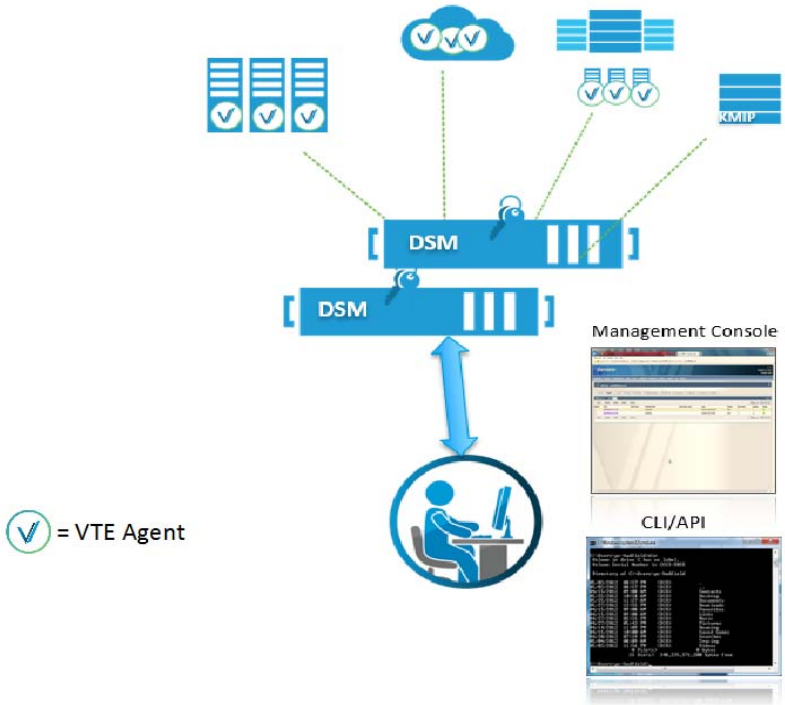
and access the DSM CLI from a remote location. IPMI is not supported by the DSM virtual appliance or hardware appliances earlier than V6000/V6100.

As of this release, IPv6 addresses are supported on DSM hardware appliances. However IPv6 addresses cannot be configured via the IPMI CLI. To configure an IPv6 address using IPMI, you must access the IPMI management console UI.

Although not necessary for DSM maintenance and operation, some administrators may find the IPMI features useful. IPMI activation and best practices are described in "IPMI" on page 145.

DSM Deployment

Figure 3: The DSM in a VTE environment



A VTE environment consists of a DSM and one or more VTE Agents residing on your protected hosts. A protected host contains the data to be protected, and can be on-site, in the cloud, or a

hybrid of both. The VTE Agents communicate with the DSM and implement security policies on their protected host systems.

Communication between agents and the DSM is encrypted and secure. DSM Administrators establish access and manage encryption policies through the Management Console, a browser-based interface to the DSM.

VTE achieves security with complete transparency to end users with little impact to application performance. It requires no changes to your existing infrastructure and supports separation of duties between data owners, system administrators, and security administrators.

2

DSM V6100 Hardware Appliance

The DSM V6100 appliance comes with a Hardware Security Module (HSM). The HSM safeguards and manages DSM objects (example: certificates and keys) with strong authentication and crypto-processing. This chapter describes how to set up and configure the V6100 hardware appliance.

In a V6100 high availability (HA) environment, all systems must be V6100s, they cannot be combined with any other appliance type or version of DSM. As of the v6.0.2 release, the DSM supports full disk encryption for enhanced security, and dynamic IP addressing via DHCP.

Figure 4: V6100 DSM hardware appliance

Front

Back

This chapter contains the following sections:

DSM V6100 Overview

The V6100 includes a FIPS 140-2 Level 3 cryptographic HSM. The HSM is managed by a set of smart cards known as the Administrator Card Set (ACS), which are read using a card reader. The DSM software provides a Remote HSM Administration feature, to remotely manage the V6100 appliance. With remote HSM administration, the card reader does not need to be connected directly to the V6100 appliance instead, it is connected to a laptop or PC, outside the data center, which in turn, is connected to the V6100 appliance over a secure channel.

Remote HSM Administration

Advantages

- Eliminates the need for administrators to be physically present in the lab to administer the DSM
- Eliminates the need for physical mode switch changes for HSM administration
- Enables administrators to present smart cards remotely from a PC or laptop
- Enables operational simplicity and efficiency

Requirements

Remote HSM Administration only applies to the V6100 appliances that have DSM software v6.0 or later installed. Remote administration needs to be turned on from the CLI before you can begin to use it.

To use the remote HSM administration feature, the following are required:

- a remote card reader or trusted verification device (TVD) and smart cards set. These must be ordered separately, contact your Thales Sales representative for more information.
- V6100 appliance with DSM software (v6.0 or later)
- Client system (e.g. laptop, PC outside the data center) on which to install the remote administration software and connect the TVD.

See “Enable remote administration” on page 27 for details.

NOTE: If you choose not to enable remote HSM administration, you can continue to use the original card reader and card set that came with your DSM V6100 appliance.

Administrator Card Set (ACS)

The ACS is used to secure and manage the HSM. It creates a logical boundary called a Security World, within which keys can be securely managed. You must create an ACS for your V6100 DSM environment.

The ACS must be initialized when you setup your primary DSM server. The ACS smart cards, read with a card reader (trusted verification device, TVD) are required to carry out administrative operations for example;

- Initial DSM configuration, specifically generating certificate authority using the DSM CLI command `system security genca`
- Generating a certificate or Master Key rotation
- Replacing the ACS

These are just a few of the administrative operations that require the ACS, see table 9, "V6100 Operations that require the ACS", for complete list of operations that require the ACS.

To configure remote HSM management for your DSM deployment, you must have a remote smart card reader (TVD) and the associated set of smart cards. Contact Thales Sales and Support for more information about ordering these accessories. See "Supported Upgrade Paths" for configuration and setup information.

Security World

A Security World is a logical security grouping of a DSM appliance and its associated objects and the Administrative Card Set (ACS) that is used to create and manage that appliance and its associated objects. In the case of a high availability deployment, all the DSM appliances and their associated objects in the cluster, are members of the same Security World.

The ACS is required to access a DSM, and in an HA environment, the same ACS is required to access the failover DSM nodes. The ACS creates the Security World to which the DSM belongs. In an HA deployment, all DSMs in the same cluster belong to the same Security World and require the same ACS to carry out administrative functions, for example, adding new DSMs to a cluster. Each card set consists of a number of smart cards, ***N***, of which a smaller number, ***K***, is required to authorize an action. That required number ***K*** is known as the quorum.

ACS

The ACS is created when the primary DSM is configured. During ACS creation, you must choose the total number of smart cards contained in your ACS (a minimum of two, recommended is at least three, maximum is 64). This number is called ***N***. You must then choose a smaller number of cards from this set of ***N***, which are required to authorize an administrative action. This required number is called ***K***, and is known as the *quorum*.

For example, if you have a single DSM, you can choose to have 6 cards in your ACS (N=6), and 4 cards to authorize an administrative action (K=4).

Before configuring your DSM, decide both N and K. Remember that in a distributed HA environment, you may want K cards at each geographic location so you don't have to ship cards to the different location to perform an administrative task. However, you may also want to have K+1 cards in case one card goes bad or is unavailable.

The ACS is created during primary DSM configuration. While generating the certificate, you are prompted to insert a smart card into the reader and to provide an optional passphrase for each card. If a passphrase is specified, it will be required for subsequent card usage. That is, not only will the card holder have to provide the smart card, but also the passphrase required for that card. Repeat this procedure for each card in your ACS (N number of times). On completion of the ACS creation, distribute the cards to the appropriate card holders.

ACS Guidelines

Once you create your ACS, you can never change N and K. You can create a replacement ACS, but N and K remain the same. Use these guidelines to carefully select the card set.

- The ACS is crucial: an unusable card set will prevent you from performing administrative operations that require the ACS.
- The ACS for the DSM(s) in a standalone or HA environment is created when the primary DSM is configured. You *must* define N and K before you set up your primary DSM, and you must decide whether or not to use pass phrases for each card in the ACS.
- You can only create an ACS on the primary DSM, it cannot be created on failover DSMs
- Do not create an ACS where K is equal to N because an error on one card would render the whole card set unusable.
- Certain administrative tasks on a DSM require only a quorum (K) of smart cards. If you are creating a distributed HA environment, you'll probably want enough smart cards to access each of the distributed DSMs in your environment plus maybe one extra in case one of the cards goes bad.
  For example, if you have four distributed DSMs and the quorum, K, is two, you will need at least three smart cards at each DSM location. This means, that the total number of smart cards, N, must be at least twelve.
- Choose the optimal K to N ratio for your situation. You cannot change the K or N of your ACS after initial creation.
  A higher K to N ratio provides greater security, but less convenience. For example if you choose K to be nine and N to be ten, nine cards must be available to perform an administrative task on any DSM in the system, and you will have one extra in case one of those nine are not available. On the other hand, making sure those nine cards are available can provide more logistical problems.

A lower K to N ratio provides slightly less security, but more convenience. For example if you have a one primary and three geographically distributed failover DSMs, and you choose K to be three and N to be sixteen, then you could distribute four cards to each DSM location and only three of those cards need be available.
You should choose enough smart cards to support all of your DSMs, plus a backup card in case one of the cards gets damaged, or is unavailable. However, a higher N increases the risk of others gathering enough cards to access the DSM. You want K to be high enough to provide a level of security that you are comfortable with, but not so high as to be logistically difficult.

- In some cases, it is desirable to make K greater than half the value of N (for example, if N is seven, to make K to be four). Such a policy makes it harder for a potential attacker to obtain enough cards to access the DSMs. Choose values of K and N that are appropriate to your situation.
- Smart cards have a unique identification number, it can be very useful to document the ID number of each card, which ACS group that card belongs to, the security officer a card belongs to, the passphrase, and any additional information you consider useful for your situation.
- Pass phrases are optional for each card. An ACS can have some cards with pass phrases and some with no pass phrase. Pass phrases can be different for each card.
- Create a security policy to manage the card set and to keep it well protected. No single person should have access to more than one card (separation of duties).

V6100 Operations that require the ACS

The following table outlines the operations that require the smart card (ACS) set. Once remote HSM administration is configured, the mode switch located on the back panel of the V6100 appliance is moved to the operational '**O**' position and physical toggling of the mode switch is no longer required (except where indicated in the table below).

Additionally, from v6.0 onwards, even if remote administration is not enabled, as long as the mode switch is in the 'O' position, physical toggling of the mode switch is no longer required.

Table 1: v6100 Physical Presence Requirements with remote administration enabled

Scenario	DSM Server	Smart Cards Required	HSM Switch change	DSM CLI Command	Notes
Primary DSM Setup: initialize security world	Primary	Set of N	Automatic	`security genca`	Run the genca command after the basic networking configuration

Scenario	DSM Server	Smart Cards Required	HSM Switch change	DSM CLI Command	Notes
Any subsequent change requiring operator to run 'genca' on an already configured DSM and established Security World	Primary	None	No	`security genca`	Example would be if the Hostname changed for the DSM. Note, this would also require re-registering all agents.
Replacement of smartcard	Primary	Original K + new N	No	`hsm replaceacs`	Requires a complete new set of N to be created. Requires K from original set of N be inserted before creating new set of N. Note that N cannot be changed.
Certificate generation or Master Key rotation	Primary	Any 1 of N	No	`security gencert`	Requires any 1 card of total set N to be inserted.
Creating DSM Backup	Primary	None	No	via web UI or CLI	DSM wrapper keys for backup/restore.
Restoring DSM Backup into same Security World.	Primary	None	No	via web UI	DSM wrapper keys for backup/restore.
Restoring DSM Backup into a different Security World	Primary	Set of K (of the security world used to create the backup)	Automatic	`config restore <name>`	Upload package from the Web UI, then follow instructions to use CLI to complete operation.
Initial setup for a Failover DSM	Failover	Set of K	Automatic	`ha convert2failover`	First time the DSM is joined to a primary DSM in an HA cluster. (Do not run 'genca' on failovers).
Subsequent DSM failover conversion in the same Security World	Failover	None	No	`ha convert2failover`	This is typically done during upgrades or when manipulating the DSM HA cluster configuration.
Subsequent failover conversion if moving to a different Security World	Failover	Set of K	Automatic	`ha convert2failover`	This is the same as an initial failover conversion.
Convert a Failover DSM to a Primary DSM	Failover	None	No	`ha convert2primary`	Take care to avoid having multiple primary DSMs in the cluster.

Scenario	DSM Server	Smart Cards Required	HSM Switch change	DSM CLI Command	Notes
Zeroize – Wiping out the HSM – Factory Reset	Any	None	Automatic	`config load default`	Restores DSM to default factory settings. DSM can then be initialized as Primary or Failover as per above.
DSM Reset	Any	None	Automatic	`config reset`	Retains network configuration, but erases all other DSM data (Keys, Policies). The DSM can then be initialized as Primary or Failover as per above.*
DSM Software Upgrade**	Any	None	No	`via web UI`	

*See Appendix D, "Reset DSM Appliance and Remove All Data" for more information about using this command.

**Except when upgrading from DSM software v5.3.1 to v6.0, a quorum and physical toggling of the switch are required while doing an upgrade.

Configuring a V6100 Appliance

This section describes how to configure a new V6100 appliance with DSM software v6.0.2. Follow the procedure described in "Specifications, Racking, and Cabling for the V6000 and V6100", to install the physical appliance.

After installation and configuration, the DSM must have connectivity to all hosts that have Vormetric Transparent Encryption Agents installed.

As of v6.0.2, DSM appliances have DHCP enabled by default on the `eth0` interface for fresh installations. If a DSM appliance is upgraded to v6.0.2, DHCP must be enabled manually, see "Upgrading the DSM" on page 107 for more details. The next sections describe how to configure the DSM appliance with DHCP enabled, or if you choose to turn it off, how to configure the appliance using static IP addressing.

Configuring DSM via DHCP

DHCP support is available for all the DSM interfaces; `eth0` (enabled by default), `eth1`, and `bond0`. The DSM DHCP implementation configures the interface IP address, subnet mask, router (default gateway), DNS server, and the search domain. It does not configure a host

name, an NTP server, or Time Zone for the DSM appliance, these have to be manually configured via the CLI.

You can choose to turn off dynamic IP addressing and use static IP addressing instead, see "Configuring DSM via Static IP Addressing". DHCP is managed via the CLI, the DHCP CLI commands are available in the Network category of commands and are described in detail in the *DSM Administrators Guide*.

The DSM appliance `eth0` interface is now DHCP-enabled by default. This section describes how to configure the DSM appliance with DHCP enabled. You must have a DHCP Server properly configured to ensure that the DSM appliance gets the correct IP address.

After accepting the license agreement and changing the CLI administrators password, you need to set the host name and configure an NTP server. The following sections describe the procedures to configure the DSM using DHCP:

Configure appliance with DHCP enabled

1. Assemble required information using the checklist (page 13)
2. "Specify host name resolution method" on page 15, if required
3. "Configure DSM ports" on page 16, if applicable
4. "Configure the hostname" on page 27
5. "Configure NTP, time zone, date, time" on page 26
6. "Enable DHCP on `bond0` interface:" on page 26, if you choose to use this feature
7. "Generate DSM Certificate Authority and create ACS" on page 28
8. "Configuring High Availability for V6100" on page 41
9. "Add more CLI administrators (optional)" on page 32

Configuring DSM via Static IP Addressing

If you do not want to want to use DHCP, it can be turned off via the CLI and you can assign a static IP addresses to the DSM interfaces. The DHCP CLI commands are available in the Network category commands sub-menu and are described in detail in the CLI chapter of the *DSM Administrators Guide*.

To turn off DHCP do the following and then proceed with the procedures described below, "Configure appliance with static IP addressing enabled".

Log on to the CLI console with the CLI administrator credentials and enter the Network category of commands, and turn off DHCP on the `eth0` interface;

```
$ network
0001:network$ ip dhcp release <interface> version 4
Example:
```

```
$ network
0001:network$ ip dhcp release eth0 version 4
WARNING: Changing network ip address may disconnect your session and will
require the server software to be restarted.
Continue? (yes|no)[no]:yes
DHCP operations may take some time, please wait....
SUCCESS: Please restart server software to pick up the changes.
0002:network$
```

The following sections below describe how to configure the DSM appliance using static IP addressing:

Configure appliance with static IP addressing enabled

1. Assemble required information using the checklist (page 13)
2. "Specify host name resolution method" on page 15, if required
3. "Configure DSM ports" on page 16, if applicable
4. "Configure network settings" on page 20
5. "Configure a bonded NIC device" on page 22, if you choose to use this feature
6. "Configure NTP, time zone, date, time" on page 26
7. "Configure the hostname" on page 27
8. "Enable remote administration" on page 27
1. "Generate DSM Certificate Authority and create ACS" on page 28
2. "Configuring High Availability for V6100" on page 41
3. "Add more CLI administrators (optional)" on page 32

Assumptions

- Data center conditions meet the appliance racking, networking, and power requirements.
- The IP address, routing configuration and DNS addresses for the DSM allow connectivity to all servers where Vormetric Encryption Agents are installed.

DSM Installation Checklist

Use this table to collect the information you need for the installation.

Table 2: Installation Checklist

REQUIREMENT	VALUE
Hardware Requirements	

Table 2: Installation Checklist

Two power outlets with an independent, 120/240V, 47/63Hz, 12/6A power source.	
Serial console—this should be connected to the DSM appliance using the serial cable included with the appliance.	
Two network (Ethernet) cables, these are included with the DSM appliance.	
Trusted verification device (TVD) and set of smart cards (V6100 only)	
Laptop or PC to connect the TVD (V6100 only)	
1u rack space	
Network Information	
eth0—this interface is DHCP enabled by default. DHCP must be disabled to assign a static IP address	DHCP Server[a] If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
eth1—this interface comes configured with a default IP address; 192.168.10.1. We recommend that you retain this configuration in the event that you need a recovery option to access the appliance.	DHCP Server If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
bond0—this interface is used when the eth0 and eth1 interfaces are aggregated into a single logical interface for load balancing/fault tolerance. If configured, the `bond0` interface supersedes the eth0 and eth1 interfaces, and must be used to access the DSM appliance.	DHCP Server If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
IPMI NIC—this interface comes configured with a default IP address; 192.168.10.10 This interface supports DHCP, refer to the CLI chapter in the *DSM Administrators Guide* for details.	DHCP Server If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
Primary DSM Hostname: FQDN	
Failover DSM Hostname: FQDN	
Domain Name Server (DNS) addresses - up to 3 plus optional DNS search domain.	

Table 2: Installation Checklist

NTP server FQHN or IP address (if applicable)	
DSM V6100 appliance with DSM software	
Certificate Information	
DSM Hostname: FQDN	
Name of your organizational unit	
Name of your organization	
Name of your city or locality. Must be fully spelled out, no abbreviations, e.g., San Jose, *not* SJC.	
Name of your state or province. Must be fully spelled out, no abbreviations, e.g., California *not* CA	
Two-letter country code	

a. DSM DHCP support enables configuration of the appliance IP address, net mask, gateway, and search domain. It does not configure an appliance host name, or an NTP server

Pre-configuration tasks

Specify host name resolution method

You can map a host name to an IP address using a Domain Name Server (DNS). DNS is the preferred method of host name resolution. DNS names are case sensitive, make sure host names are correctly entered while configuring DNS and registering hosts.

You can also modify the `hosts` file on the DSM or identify a host using only the IP address.

- If you use DNS to resolve host names, use the FQDN for the host names.
- If you do NOT use a DNS server to resolve host names, do the following on all of the DSMs and the protected hosts:
  - Modify the *host* file on the DSM: To use names like serverx.domain.com, enter the host names and matching IP addresses in the */etc/host*s file on the DSM using the `host` command under the `network` menu. For example:

    ```
    0011:network$ host add <hostname> 192.168.1.1
    SUCCESS: add host
    0012:network$ host show
    name=localhost1.localdomain1 ip=::1
    name=<host name>.<domain name>.com ip=192.168.10.8
    name=<host name> ip=192.168.1.1
    SUCCESS: show host
    ```

    You must do this on *each* DSM, since entries in the host file are not replicated across DSMs.

- Modify the *host* file on the protected hosts: Enter the DSM host names and matching IP addresses in the */etc/hosts* file on the protected host. *You must do this on EACH protected host making sure to add an entry for all DSM nodes (if using HA).*

OR

- Use IP addresses: You may use IP addresses or the FQDN to identify the host simultaneously. In other words, they don't all have to use an IP address or FQDN.

Configure DSM ports

If a DSM is to communicate with a device behind a firewall, you must open various ports in the firewall as shown in the following figures.

Figure 5: Port to open between workstation and DSM

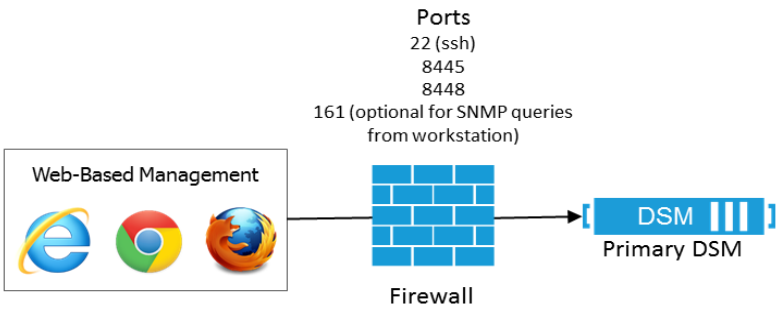


Figure 6: Ports to open between DSMs

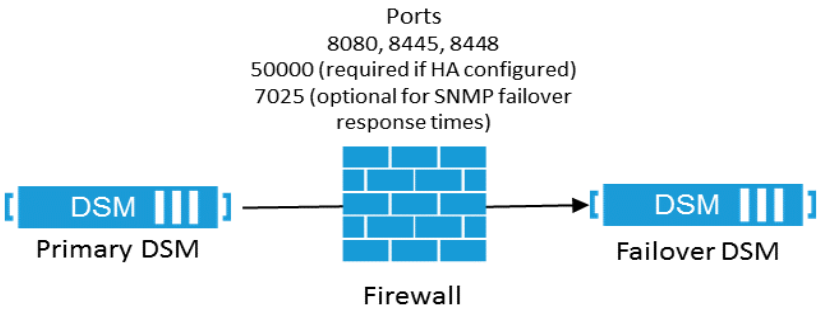
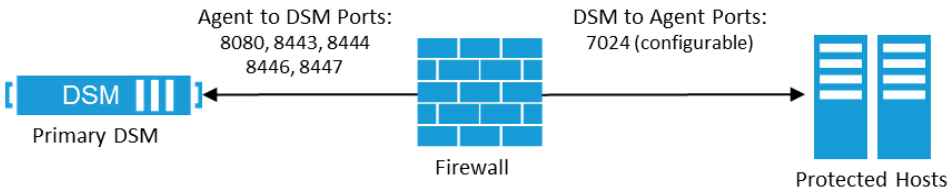


Figure 7: Ports to open between DSM and agent



The following table lists the communication direction and purpose of each port you must open.

Table 3: Ports to configure

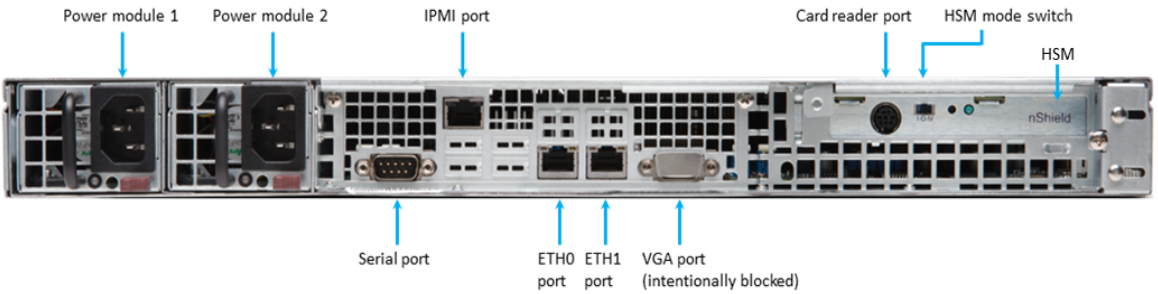
Port	Protocol	Communication Direction	Purpose
22	TCP	Management Console → DSM DSM → SSHD Server	CLI SSH Access Auto-backup via SCP
161	TCP/UDP	SNMP Manager → DSM	SNMP queries from an external manager
445	TCP	DSM → CIFS Server	Auto-backup via CIFS
5696	TCP	KMIP client → DSM	Allows communication between the KMIP client and primary DSM
7024	TCP	DSM → Agent	Policy/Configuration Exchange
7025	UDP	DSM ↔ DSM	Uses SNMP to get failover node response time.
8080	TCP	Agent → DSM DSM ↔ DSM	Default TCP/IP port for HTTP that is used to exchange certificates between the DSMs in an HA configuration. Also, used once to perform the initial certificate exchange between an agent host and DSM.
8443	TCP	Agent → DSM	TCP/IP port through which the agent communicates with the DSM. The agent establishes a secure connection to the DSM, via certificate exchange, using this port.
8444	TCP	Agent → DSM	Agent log messages uploaded to DSM
8445	TCP	Browser → DSM DSM ↔ DSM (fall back)	Management Console, VMSSC, and fall back for HA communication in case port 8448 is dropped.
8446	TCP	Agent → DSM	Configuration Exchange using Elliptic Curve Cryptography (Suite B)
8447	TCP	Agent → DSM	Agent uploads log messages to DSM using Elliptic Curve Cryptography (ECC)
8448	TCP	Browser → DSM DSM ↔ DSM	GUI Management during enhanced security using Elliptic Curve Cryptography (Suite B). Also for secure communication between DSMs in HA cluster.

Port	Protocol	Communication Direction	Purpose
50000	TCP	DSM (primary) → DSM (failover)	HA information exchange
9005	TCP	DSM ↔ trusted verification device	Used by Remote Administration Service process to accept connections from the Remote Administration Client.
If NTP server and Syslog server are used to synchronize DSM time and forward log messages, it will require opening up the following ports			
123	UDP	DSM → NTP Server	NTP Synchronization
514	UDP/TCP	DSM → Syslog Server	Logging to Syslog. Note that 514 is the default, but is configurable depending on the syslog server.

Configuration tasks

To configure the DSM you need to access the DSM CLI through a terminal connection in the back of the DSM hardware appliance. Figure 8 shows the various DSM appliance ports.

Figure 8: V6100 appliance ports



Connect to the V6100 appliance

Connect to the V6100 appliance through the console serial port with a DB-9 cable. Configure your console connection using the following parameters:

- Terminal Type: VT100
- Baud Rate: 9600
- Parity: None
- Data bits: 8
- Stop bits: 1

Optionally, you can connect a laptop to the DSM `eth1` using a standard network cable (cat-5). We recommended that you use the console serial interface to perform initial network

configuration because, if you are logged onto the appliance through the Ethernet interface, the connection will drop when you change the Ethernet interface IP address.

If configuring the appliance via IPMI, connect a standard network cable (cat-5) to the IPMI port with the default IP address 192.168.10.10. See "Configuring and Accessing IPMI on the DSM" on page 146 for more information about configuring the DSM via IPMI.

Access the DSM Command Line Interface (CLI)

1. Manually set the IP address for the laptop to 192.168.10.2 (or higher) with a default mask of 255.255.255.0
2. SSH to 192.168.10.1
3. Log in with the default login and password:

   `Login: cliadmin`

   `Password: cliadmin123`
4. The license agreement is displayed, type 'y' to accept and press **Enter**.
5. When prompted, type in a new password and press **Enter**. Reconfirm your password.

Warning! Do not lose this password.

After connecting your laptop to the DSM, use the DSM Command Line Interface (CLI) to configure the DSM (see the first few steps in "Configure network settings" on page 20). CLI commands are grouped into the following categories or *submenus*. Enter "?" on the CLI command line to lists the categories:

```
$ ?
network      Networking configuration
system       System configuration
hsm          HSM configuration
maintenance  System maintenance utilities
ha           HA configuration
ipmi         IPMI configuration
user         User configuration
exit         Exit
```

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

```
0037:vormetric$ maintenance
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
```

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}
0043:maintenance$ diag
usage: diag [log [ list | view LOG_FILE_NAME] | vmstat | diskusage |
hardware | osversion | uptime ]
0044:maintenance$
```

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

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

Configure network settings

1. Navigate to the `network` commands menu. Type:

   ```
   0001:vormetric$ network
   ```

2. Configure an IP address for the DSM.

NOTE: The `eth0` interface is DHCP enabled by default. See "Configuring DSM via DHCP"for more information, and for instructions on how to switch to static addressing if desired.

We recommend that you retain the default `eth1` IP address configuration in the event that you need a recovery option to access the DSM appliance.

Type:

```
ip address init <DSM IP address>/<subnet mask (e.g. 16 or 24)> dev eth1
```

Example:

```
0002:network$ ip address init 192.168.10.4/16 dev eth1
```

IPv6 example:

```
0002:network$ ip address init fa01::3:15:130/64 dev eth1
```

NOTE: If you are connected via ETH0, you will be disconnected at this step. Reconnect on the new IP address.

3. (Optional) If you have configured ETH0, you can also configure an IP address for ETH1 if you want to communicate with agents on a different subnet for example, or if you want to access the Management Console from a different subnet. To configure an IP address for ETH1, type:

   `ip address init <eth1 IP address>/<subnet mask (e.g., 16 or 24)> dev eth1`

   Example:

   ```
   0003:network$ ip address init 192.168.10.3/16 dev eth1
   ```

   IPv6 example:

   ```
   0003:network$ ip address init fa01::3:15:130/64 dev eth1
   ```

   The following warning is displayed:

   ```
   WARNING: Changing the network ip address requires server software to be
   restarted.
   Continue? (yes|no) [no]:
   ```

   Type 'yes' to continue with the IP address configuration.

4. Configure the IP address for the default gateway. Type:

   `ip route add default table main.table dev [eth0 or eth1] via <IP address for the default gateway>`

   Example:

   ```
   0004:network$ ip route add default table main.table dev eth0 via
   192.168.1.5
   ```

   IPv6 example:

   ```
   0004:network$ ip route default table main.table dev eth0 via
   fa01::3:15:120
   ```

5. Verify the interface settings. Type:

   ```
   0005:network$ ip address show
   ```

6. Verify the route settings. Type:

   ```
   0006:network$ ip route show
   ```

7. If you are using DNS, set the primary DNS server for the DSM. Type:

   ```
   0007:network$ dns dns1 <ip address for dns server 1>
   ```

8. If you have a second or third DNS server, set them for the DSM. Type:

   ```
   0008:network$ dns dns2 <ip address for dns server 2>
   ```

9. If you want to set the search domain, type:

   ```
   0009:network$ dns search <search_domain>
   ```

10. Show the DNS settings. Type:

    ```
    0010:network$ dns show
    ```

11. Return to the main menu. Type:

    ```
    0010:network$ up
    ```

Configure a bonded NIC device

This section describes how to aggregate the two NICs on the DSM into a single logical interface to provide load balancing and/or fault tolerance. The bonded NIC device is called `bond0`.

NOTE: In order to use the bonded NICs feature, you must ensure that your switch is configured to use Link Aggregation Control Protocol (LACP).

DSM physical appliances have two physical NICs called `eth0` and `eth1`. Only two NICs `eth0` and `eth1` are supported. Any additional physical/virtual NICs are ignored.

The NIC bonding setting is system specific. If it is to be used for all nodes in a cluster, it must be enabled on all nodes individually.

If configured, this interface supersedes the `eth0` and `eth1` interface configurations and must be used to access the appliance.

1. Access the DSM CLI and login with your credentials. If this is the first time you are logging in, then you will be required to accept the license agreement and change the default password, see "Configure network settings".

2. Navigate to the network commands menu;

   ```
   $ network
   0001:network$
   ```

3. Enable the bonded NIC;

   ```
   0001:network$ ip address init <ip_address>/<subnet_mask> dev bond0
   ```

Example: `ip address init 1.2.3.4/16 dev bond0`

In the event that a bonded NIC is being configured after the initial configuration, or after the DSM has been upgraded, if you want to reuse an IP address that was originally assigned to `eth0` or `eth1`, then you must delete that address from `eth0` or `eth1` first, and then reassign it to the bond0 device.

4. Add a default gateway for the `bond0` device;

   `0001: ip route add default table main.table dev bond0 via <gateway_ip_address>`

   Example: `ip route add default table main.table dev bond0 via 1.2.7.8`

If a `bond0` interface is configured after setting up the `eth0` and/or `eth1` interfaces, and it is configured with an IP address that is on the same subnet as a default gateway, that gateway configuration continues to apply. However, if you configure `bond0` with an IP address on a different subnet, you will have to reconfigure the default gateway.

5. You can change the bonding driver mode based on your requirements. There are seven modes available from 0-6. See "Bonding driver modes" for more information.

   When the mode option is specified the speed option cannot be specified (i.e. the options mode and speed are mutually exclusive). In other words, `bond0` does not take the speed option and both `eth0` and `eth1` don't take the mode option. However, the MTU and up/down options can still be used for the `bond0` device.

   To set or change the mode type:

   `0002:network$ ip link set bond0 mode <mode>`

   Example: `ip link set bond0 mode 0`

   To see what mode is currently in use type:

   `0002: network$ ip link show bond0`

   The output of this command displays the physical link settings on the system. You can use it to verify any changes to the physical link settings:

   Example:

```
Device  State   MTU     Mediatype       Speed
eth0    UP      1500    copper          auto
eth1    UP      1500    copper          auto

Device State   MTU     Mode
bond0   UP      1500    0

Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: load balancing (round-robin)
MII Status: down
```

```
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

SUCCESS: show ip link
```

6. To disable or break up a bonded NIC device, you can use either the `delete` or `flush` command. The `delete` command will only delete a specific IP address (multiple can be assigned) and `flush` will clear all assigned IP addresses.

   ```
   0003:network$ ip address delete <ip_address>/<subnet_mask> dev bond0
   ```

   or

   ```
   0003:network$ ip address flush bond0
   ```

   Routes that are associated with this bonded NIC device will also be deleted.

Bonding driver modes

The modes specify bonding policies. Some options for certain modes are configurable (the `transmit hash policy` for bonding modes 2 and 4, and the `updelay` for bonding mode 6), while the others take the default values for those modes, except for the `miimon` setting.

The transmit hash policy for bonding modes 2 and 4, is used for slave selection in these modes. To set the transmit hash policy for mode 2 or 4, use the `ip link set` command, for example;

```
0004:network$ ip link set bond0 mode 2 xmithashpolicy layer2+3
```

To view the changes, use the `ip link show` command;

```
Device  State   MTU     Mediatype       Speed
eth0    UP      1500    copper          auto
eth1    UP      1500    copper          auto

Device  State   MTU     Mode
bond0   UP      1500    2

Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: load balancing (xor)
Transmit Hash Policy: layer2+3 (0)
MII Status: down
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0
```

The `miimon` setting specifies the MII link monitoring frequency in milliseconds, which determines how often the link state of each slave is inspected for link failures. The `miimon` setting has a value of 100 instead of the default value of 0.

The following modes are supported:

Table 4: Bonding driver modes

Mode	Name	Description	Load-balancing	Fault tolerance
0	balance-rr	Round-robin policy. Transmit packets in sequential order from the first available through the last. This is the default mode for the bonded NICs.	Yes	Yes
1	active-backup	Active-backup policy: Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch.	No	Yes
2	balance-xor	XOR policy: Transmit based on the selected transmit hash policy. The default policy is a simple [(source MAC address XOR'd with destination MAC address) modulo slave count].	Yes	Yes
3	broadcast	Broadcast policy: transmits everything on all slave interfaces.	No	Yes
4	802.3ad	IEEE 802.3ad Dynamic link aggregation. Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.	Yes	Yes
5	balance-tlb	Adaptive transmit load balancing: channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.	Yes	Yes
6	balance-alb	Adaptive load balancing: includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware addresses for the server.	Yes	Yes

Enable DHCP on `bond0` interface:

To configure a `bond0` interface using DHCP, you need to enable DHCP on that interface. The `bond0` interface inherits the IP address that was dynamically assigned to the `eth0` interface when the DSM was initially deployed.

Log on to the CLI console and navigate to the Network category of commands and enable DHCP.

Example:

```
0004:network$ ip dhcp enable bond0 version 4

WARNING: Changing network ip address may disconnect your session
and will require the server software to be restarted.

Continue? (yes|no)[no]:yes

DHCP operations may take some time, please wait....

SUCCESS: Please restart server software to pick up the changes.

0005:network$
```

Configure NTP, time zone, date, time

You must have the correct time set on your DSM server(s) as this will affect system functions such as agent registration, log timestamps, high availability cluster synchronization, and certificate exchange. Although configuring an NTP server is not mandatory, it is strongly recommended.

1. Navigate to the *maintenance commands* menu. Type
   `0001:vormetric$ maintenance`

2. Show the current ntpdate settings. Type
   `0002:maintenance$ ntpdate show`

3. Add a new ntpdate server. Type
   `0002:maintenance$ ntpdate add <IP address/Hostname for the` *ntpdate server*`>`

   Repeat this step for each ntpdate server.

4. Activate the ntpdate server connection. Type
   `0003:maintenance$ ntpdate on`

5. Show the current timezone settings. Type
   `0004:maintenance$ gmttimezone show`

6. Set the country and city where the DSM resides. Type:

   0005:maintenance$ gmttimezone set <*country/city*>

7. Set the date. (If you used `ntpdate synch`, this step is not necessary.) Type:

   0006:maintenance$ date <*mm/dd/yyyy*>

8. Set the time. (If you used `ntpdate synch`, this step is not necessary.) Type:

   0007:maintenance$ time <*hh:mm:ss*>

   Where *hh* is 00 to 23.

9. Verify your settings. Type:

   0008:maintenance$ time
   0008:maintenance$ date

10. Return to the main menu. Type:

    0008:maintenance$ up

Configure the hostname

1 Navigate to the *system* menu. Type:

0001:vormetric$ system

2 Show the current setting. Type:

0002:system$ setinfo show

The default host name in the output is *your. name.here*.

3 Set the hostname. You must enter the fully qualified domain name for the DSM. Type:

0003:system$ setinfo hostname <*FQHN*>

Example:

0003:system& setinfo hostname dsm.company.com

Enable remote administration

Before you can use the TVD and smart cards to generate the certificate authority, you need to enable remote administration.

1. Navigate to the *hsm* menu and check the remote administration status. Type:

   $ hsm
   0001:hsm$ remoteadmin show

```
HSM remote administration is disabled.
SUCCESS: remoteadmin command ran successfully.
```

2. Turn remote administration on. Type:

```
0002:hsm$ remoteadmin on
HSM remote administration is enabled.
SUCCESS: remoteadmin command ran successfully.
```

3. Return to the main menu. Type:

```
0003:hsm$ up
```

Generate DSM Certificate Authority and create ACS

On completion of the preliminary configuration, you must now generate the DSM certificate authority which requires the ACS. Read "ACS Guidelines" on page 8 before going through the procedures in this section.

Prerequisites

Move the mode switch on the back panel of the appliance to the Operational (**O**) position.

Warning! The switch must remain in the Operational (**O**) position at all times when using either local or remote administration.

1. Install the client software on the laptop or PC. Instructions for how to install the TVD client software are available in the CD and guide that came with your TVD. The software must be installed on all laptops and PCs participating in the ACS creation. Refer to the TVD release notes for supported operating systems.
2. Connect the TVD to your laptop or PC.
3. Determine the total number of smart cards, *N*, you require for your Administrator Card Set (ACS).
4. Determine the quorum (K) i.e., the number of cards required to perform an administrative operation.
5. Document the ACS group for each card as well as the security officer to which a card belongs. You can also add the passphrase and any additional information you consider useful for your situation.

The following steps display the DSM CLI commands and output when you create the certificate authority and ACS.

Generating the CA and the ACS

1. From your laptop or PC, open a DSM CLI session and log in using the CLI Administrator credentials you set here, "Access the DSM Command Line Interface (CLI)".
2. Start the client software on the laptop or PC.
3. Generate a new certificate authority for the DSM and create the ACS. At the prompt, type:
   `0012:system$ security genca`
4. A warning message is displayed informing you that all agent and peer node certificates will need to be resigned after the new certificate authority is created and that the DSM software will be restarted, type 'yes' to generate the certificate.

   ```
   WARNING: All Agents and Peer node certificates will need to be re-signed
   after CA and server certificate regenerated, and the security server
   software will be restarted automatically!
   Continue? (yes|no)[no]:yes
   ```

5. The following message is displayed. Read it, enter the required information to generate the CA, and ensure the DSM host name is correct, press enter:

   ```
   This computer may have multiple IP addresses. All the agents will have to
   connect to Security Server using same IP.
   Enter the host name of this computer. This will be used by Agents to talk
   to this Security Server.
   This Security Server host name[<hostname>.com]:
   Please enter the following information for key and certificate
   generation.
   What is the name of your organizational unit? []:Engineering
   What is the name of your organization? []:Vormetric, Inc.
   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]:
   Regenerating the CA and server certificates now...
   ```

6. You will now create your ACS.

Caution: ***Do not*** set the number of cards to use in the ACS to more than the number of cards in your possession. See "ACS Guidelines" for details.

7. You will be prompted to enter the total number of cards to use in the ACS, (N), and the minimum number of cards required to perform an administrative task (K).

```
Enter the total number of cards (N) you would like to use in your
Administrator Card Set (ACS).
Note: To create a Security World that meets the requirements of Common
Criteria this value should be at least 3.
This value must be at least 2 and no higher than 64: 2

Enter the number of cards (K) required to authorize an action. This
number K is known as the quorum.
Note 1: The value for K must be less than N. Creating card sets in which
K is equal to N is not allowed because an error on one card would render
the whole card set unusable.
Note 2: To create a Security World that meets the requirements of Common
Criteria this value should be greater than half of N.
This value must be at least 1 and less than 2: 1
10:52:18 WARNING: Module #1: preemptively erasing module to see its
slots!
Create Security World:
 Module 1: 0 cards of 2 written
 Module 1 slot 0: empty
 Module 1 slot 0: unknown card
```

8. If a card is not inserted in the reader, you will be prompted to insert one. If a previously used (written) card is inserted, you will be prompted to overwrite it. A previously used card is referred to as an '*unknown*' card and a used card that has been erased is referred to as a '*blank*' card.

   You will be prompted to enter a passphrase, this is optional

Caution: You *must not* lose this passphrase or your cards will be unusable.

```
 Module 1 slot 0: Enter new passphrase:
 Module 1 slot 1:- no passphrase specified - overwriting card
 Module 1 slot #1: Processing . . .
 Module 1: 1 card of 2 written
 Module 1 slot 0: remove already-written card #1
 Module #1 Slot #0: Remove card.
 Module 1 slot 0: empty
 Module #1 Slot #0: Insert appropriate card.
Checking Modules and reading cards ...
Module 1 slot 0: unknown card
Module 1 slot 0: Overwrite card? (press Return).
Module 1 slot 0: Enter new passphrase: .
```

```
Module 1 slot 1:- no passphrase specified - overwriting card
Module #1 slot #1: Processing . . .
```

This process continues until you have created your N cards. The following message is displayed after the last card is written:

```
Card writing complete.
security world generated on module #0; hknso =
f7387fed7f52625bc06b79607bb4b0afdd93a6b1
```

The hash value above, is the same hash value that will be displayed when you create a failover DSM. You can compare the hash values to verify a successful failover creation.

Caution: Do NOT remove the card from the smart card reader until the server private key is generated.

9. You can now remove the smart card from the reader.

```
Creating and signing the server certificates...
done
CA and Server certificates have been generated successfully.
JBoss vault keystore password have been completed successfully.
You may now start the Security Server
Stopping Security Server
Stopping data store
Starting data store
Starting Security Server
SUCCESS: The CA and security certificates are re-generated and the
Security Server software is restarted.

Regenerating CA will make certificates at failover servers and agents
invalid. You may need to:
        - Re-sign certificates at each failover server
        - Cleanup and re-register each agent
0002:system$
```

Your primary DSM with HSM is now configured.

Verify Web Access

After configuring your appliance, you need to access the DSM Management Console from a browser, to administer the DSM.

Open a browser and confirm access over HTTPS to either the DSM hostname (if configured in DNS) or the IP address defined in “Configure network settings” on page 20. Example URL:

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

If this doesn't work because, for example, port 443 was blocked by a firewall, specify port 8445. Example:

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

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

- Does not have repeating characters
- Uses at least 1 upper and 1 lower case character
- Uses at least 1 special character

The DSM Management Console has a help icon (?) located on the right-hand side of the title bar, which is located under the menu bar, on each page of the Web UI. Click the icon for help with tasks on a specific page.

Upload a license file

The first time you log on to a DSM, the dashboard displays “License file not found,” and all you will see are the *Dashboard* and *System* tabs. You need to click **System** and select **License**, then **Upload the license file**. After uploading your license file, all the other tabs for which you have a license are visible.

1. Log on to your primary DSM as a DSM administrator of type System or All.
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. In the **License File** box, enter the full path of the license file or click **Browse** to locate and select the license file.
6. Click **Ok**.

Menu items available to you per your license will now be visible.

Add more CLI administrators (optional)

1. Navigate to the *users commands* menu. Type
   `user`
2. For each administrator you want to add, type
   `add <administrator name>`
3. When prompted, enter a password. The password criteria are:

- Does not have repeating characters
- Uses at least 1 upper- and 1 lower-case character
- Uses at least 1 special character

4. Return to the main menu. Type

   up

Full Disk Encryption

As of v6.0.2, the DSM root filesystem is automatically encrypted for enhanced security. This feature is only available on a fresh installation of the DSM v6.0.2 software. This feature is not available if you upgrade to v6.0.2.

NOTE: This feature is not supported on the V5800 appliances.

To maintain the security of the encrypted root file system, a DSM System administrator can set a passphrase that will be required at boot time to unlock the system. Setting a boot passphrase is not required. Users who prefer an unattended boot, can continue to use the DSM without a passphrase. However in the interest of better security, we recommend that you set a boot passphrase.

Set boot passphrase

Once a boot passphrase is set, it is required *each time* the system boots. The passphrase is set via the CLI and is available under the 'System' category of commands in the security sub-menu, refer to the CLI chapter of the *DSM Administrators Guide* for details about usage.

If you plan to create a high availability cluster, we recommend, that you set a passphrase on each node in the cluster, in order to maintain a consistent level of security.

To set a passphrase the following are required:

- An RSA key pair with a minimum length of 2048 bits. The public key of the pair is used to encrypt the passphrase. The private key is required to decrypt the passphrase for recovery, in the event that it is lost.
- Console access to the DSM appliance, either direct or remotely via IPMI. After setting the passphrase, the DSM will reboot and any network connections will no longer work. Upon reboot, a prompt will appear on the console, and the system will wait for the correct boot passphrase to be entered.

See "Configuring IPMI on the DSM" for how to set up the IPMI. If using a virtual appliance, you can connect to the DSM via the console available from the virtualization application in use.

1. Log on to the console, and enter the System category of commands and type `security boot-passphrase set` at the prompt;

```
$ system

0001:system$ security boot-passphrase set
```

2. You will be prompted for an RSA public key with a minimum length of 2048 bits. Copy and paste the contents of your public key file at the prompt, then press Enter again to end with an empty line;

```
An RSA public key with minimum length of 2048 bits is required
for boot passphrase recovery. Please enter one now, ending with
an empty line:

-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwYIf0Z04nzne9j78BY7m
Q9kMTgh8YErtklECnVVhxExob/UvAWOvSBcGDVgixpeMCywWVh8OgTIbj751PVfa
TI8/C+gP4Rd6cdtO7fGzsYsAZxN9OCssRQlCJfCe6y6fNep3dDOh1noTFyFNTqOy
c3WW0gAlJ9ILPwn6uxVRgtXPgLnFfP9zNieyWmHTLw6He8BZAAYkWbESMgnA5BoJ
mcxdpv/i/8ZODTMMo/6Ji4oYpQPa8i9Ex7qTZinl5hxjIjC8eIcUOMNdAhvslNzs
T6FZPJ2BEYBU6TAQpxDPLwPAQIEw1x/NzcYUUfgaP1pZIAdhWFJUZkx4FqmEA5od
MwIDAQAB

-----END PUBLIC KEY-----
```

3. Next, you will be prompted to enter a passphrase, which must conform to the configured password policy. After you enter the passphrase, a message is displayed, warning you that you will need access to the console, either directly or via IPMI, so that you can enter the boot passphrase when prompted. If the console is available, type 'yes' to continue.

```
Enter new boot passphrase:

Enter new boot passphrase again:


WARNING: After setting the new boot passphrase, the system will
be rebooted automatically and the new passphrase must be entered
on the console. If you do not have direct or IPMI access to the
console, then choose 'no' to cancel. DSM will not boot up until
a correct boot passphrase is entered.

Continue? (yes|no)[no]: yes
```

Caution: Save this encrypted passphrase as it is required each time the DSM reboots. In the event that you forget the passphrase and lose the encrypted passphrase and/or the RSA private key, your DSM will be unrecoverable.

4. You will be reminded to set a boot passphrase on each of the designated DSM failover nodes as well. A message confirming that a boot passphrase has been set is displayed and the system will reboot.

```
NOTE: run this command on every server node in the cluster to
keep them at a uniform security level.

SUCCESS: custom boot passphrase has been set.

DSM server is rebooting...
```

5. Open the IPMI Java console (or if using a virtual machine, the console from the virtualization application). During the reboot you will be prompted to enter the boot passphrase. The system will continue to reprint the prompt until the correct value is entered.

```
Please enter passphrase for disk <disk_name> (DSM_ROOT)!
```

6. Enter the passphrase, the system startup messages will continue to scroll until the system is ready and the log in prompt is displayed. Now you can log into your system as before.

```
Welcome to the Vormetric Data Security Manager on
<dsm_server_name>.com

<dsm_server_name> login: cliadmin

Password:
```

Recovering a lost passphrase

After you set a boot passphrase, we strongly recommend that you save a copy of the encrypted passphrase in a safe location, as well as the RSA key pair associated with that passphrase. As a best practice, we recommend that the encrypted passphrase be stored separately from the associated private key.

To recover a lost passphrase while the system is still booted, do the following:

1. Log on to the DSM CLI and navigate to the system category of commands. Type `security boot-passphrase recovery show` at the prompt;

```
$ system

0001:system$ security boot-passphrase recovery show

SUCCESS

The following passphrase recovery files are available:

0. 201710031407
```

2. Enter the number of the file to display contents, the encrypted passphrase and the public key used to encrypt it. An example of the command you can use to decrypt the passphrase is also displayed.

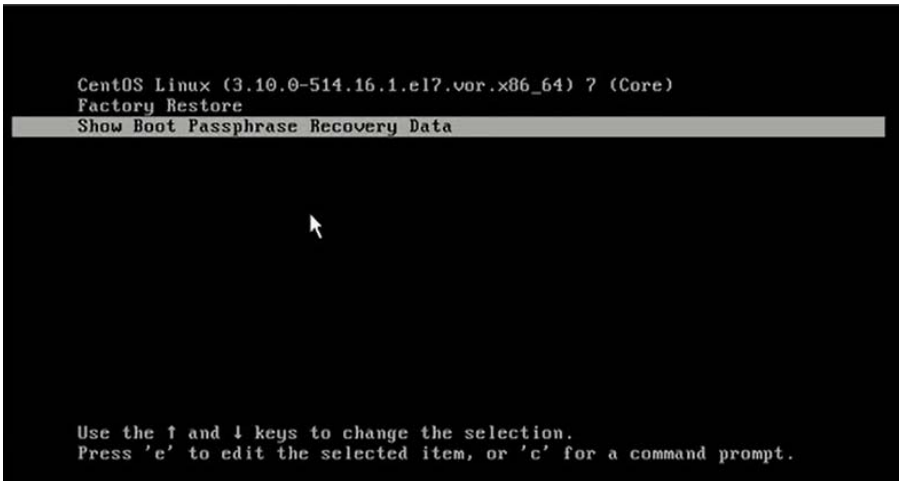
```
Type the number of a file to view the contents, or 'q' to quit: 0

Encrypted passphrase (base64 encoded):

fqWOGbKe4x6R3vmWtBMFvoAauaEpOnQ9OGLmFW9eZhFbv+w1+u0LPgIGYx9e5AT
5nPnPD2GAyMWM
H8GOvuJvht7UzBodMA07DHNMpyMnOEsy6Nz+ouWsMWhHen5JFNMXKWM9TYQ9/yr
1D2cFuBsppFLV
W/2McKIYuBqgeaOefzL2jr8vyyFudq6TGgTjRJe1edLDCqTJbcK100o036U0vyn
EsvMucps1sq0k
Lpes6Zp1ud5usWngn2J2X6PrlAugHp4nMMDIRLQBgzX95x7Fb7VLebcb/eIGn39
KJaPU9sxEiFwl
xh/f6azXhHpjahwjirzfpZl0300VFYT0P9o5xg==


Public key used for encryption:


 -----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwYIf0Z04nzne9j78BY7m
Q9kMTgh8YErtklECnVVhxExob/UvAWOvSBcGDVgixpeMCywWVh8OgTIbj751PVfa
TI8/C+gP4Rd6cdtO7fGzsYsAZxN9OCssRQlCJfCe6y6fNep3dDOh1noTFyFNTqOy
c3WW0gAlJ9ILPwn6uxVRgtXPgLnFfP9zNieyWmHTLw6He8BZAAYkWbESMgnA5BoJ
mcxdpv/i/8ZODTMMo/6Ji4oYpQPa8i9Ex7qTZinl5hxjIjC8eIcUOMNdAhvslNzs
T6FZPJ2BEYBU6TAQpxDPLwPAQIEw1x/NzcYUUfgaP1pZIAdhWFJUZkx4FqmEA5od
MwIDAQAB

 -----END PUBLIC KEY-----
```

   Save the encrypted passphrase in file (see recommendation in “Recovering a lost passphrase” above). Run the example command on a system with OpenSSL installed that can access the file with the encrypted passphrase, and the private key required to recover that passphrase.

If you have forgotten your password and the DSM has not booted up, you can also recover the password from the GRUB menu, available from the IPMI Java console.

1. As the DSM reboots, open a console (direct or via IPMI). When the GRUB menu is displayed, use the arrow keys to select the ‘Show Boot Passphrase Recovery Data’ option and press Enter, see Figure 9: “GRUB menu options” below.

Figure 9: GRUB menu options



After the system messages scroll past, a message is displayed:

```
The following passphrase recovery files are available:

0. 684734609723

Type the number of a file to view the contents, or ‘q’ to quit:
```

2. Type ‘0’ to view the contents of the recovery file;

```
Encrypted passphrase (base64 encoded):

fqWOGbKe4x6R3vmWtBMFvoAauaEpOnQ9OGLmFW9eZhFbv+w1+u0LPgIGYx9e5AT
5nPnPD2GAyMWM
H8GOvuJvht7UzBodMA07DHNMpyMnOEsy6Nz+ouWsMWhHen5JFNMXKWM9TYQ9/yr
1D2cFuBsppFLV
W/2McKIYuBqgeaOefzL2jr8vyyFudq6TGgTjRJe1edLDCqTJbcK100o036U0vyn
EsvMucps1sq0k
Lpes6Zp1ud5usWngn2J2X6PrlAugHp4nMMDIRLQBgzX95x7Fb7VLebcb/eIGn39
KJaPU9sxEiFwl
xh/f6azXhHpjahwjirzfpZl0300VFYT0P9o5xg==

Public key used for encryption:


 -----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwYIf0Z04nzne9j78BY7m
Q9kMTgh8YErtklECnVVhxExob/UvAWOvSBcGDVgixpeMCywWVh8OgTIbj751PVfa
TI8/C+gP4Rd6cdtO7fGzsYsAZxN9OCssRQlCJfCe6y6fNep3dDOh1noTFyFNTqOy
c3WW0gAlJ9ILPwn6uxVRgtXPgLnFfP9zNieyWmHTLw6He8BZAAYkWbESMgnA5BoJ
mcxdpv/i/8ZODTMMo/6Ji4oYpQPa8i9Ex7qTZinl5hxjIjC8eIcUOMNdAhvslNzs
T6FZPJ2BEYBU6TAQpxDPLwPAQIEw1x/NzcYUUfgaP1pZIAdhWFJUZkx4FqmEA5od
MwIDAQAB

 -----END PUBLIC KEY-----
```

Caution: Copy and paste functionality is *not* available from the IPMI Java console, you will have to manually copy the contents of the encrypted passphrase file and save it. That file needs to be accessible, along with the private key so that you can run the command to decrypt the passphrase.
We recommend you save the encrypted passphrase ahead of time from the CLI so you don't have to manually transcribe it from the boot menu. See "Full Disk Encryption" on page 33.

3. Enter the passphrase when prompted to do so on the IPMI Java console to unlock the system and boot up the DSM.

Configuring IPMI

The Intelligent Platform Management Interface (IPMI) is a computer interface specification for autonomous computer subsystems. IPMI provides remote DSM access to users from different locations. It allows a system administrator to monitor system health and manage computer events from a remote location. IPMI is not supported by the DSM virtual appliance.

The IPMI Java console is recommended when setting a boot passphrase for the DSM.

Although not necessary for DSM maintenance and operation, some administrators may find the IPMI features useful. See "IPMI" on page 145, for IPMI best practices in a DSM environment.

The DSM appliance has a dedicated IPMI Ethernet port that is pre-configured with the IP address, 192.168.10.10. The DSM IPMI Ethernet port is separate from the other two DSM Ethernet ports, see Figure 10: "IPMI Ethernet port" below.

Figure 10: IPMI Ethernet port

This section describes how to configure IPMI and access the IPMI management console.

IPMI Ports

The following ports can be configured for IPMI on the V6000/V6100 DSM hardware appliance

Table 5: IPMI Ports

Port	Protocol	Communication Direction	Purpose
80	TCP	Browser → IPMI	This port is disabled by default and should not be used.
443	TCP	Browser → IPMI	This port is enabled by default. It is used for the IPMI GUI. If you change the port through which you access IPMI through https through your browser ("Change the port through which you access IPMI" on page 149), then you should close port 443.
5900	TCP	Browser → DSM	This port is disabled by default. It is used for remote KVM (Keyboard Video Mouse) management. Enable if you want to use the remote console.
623	UDP	Browser → DSM	This port is disabled by default. Enable only if you want to attach virtual media.

Configuring IPMI on the DSM

Before you can use IPMI to configure your DSM V6000/V6100 appliance, you need to configure an IP address, and enable the KVM port for remote Java console support.

If you want to configure the IPMI Ethernet port IP address to use an IPv6 address, you must do this via the IPMI GUI—you cannot configure the IPMI Ethernet port IP address via the CLI.

NOTE: If the HTTP and HTTPS ports are both enabled for IPMI, IPv6 will not work for HTTPS. The workaround is to either disable HTTP or use IPv4 rather than IPv6.

Configure IPMI IP address:

7. Access the DSM CLI and log on to the CLI console.
8. Enter the `ipmi` submenu, type:

```
0011:vormetric$ ipmi
0012:ipmi$
```

9. Set the IPMI IP address using the command `ip set`. Type;

```
0012:ipmi$ ip set <ip address>
```

10. Set the IPMI net mask using the command `mask set <net mask>`, type;

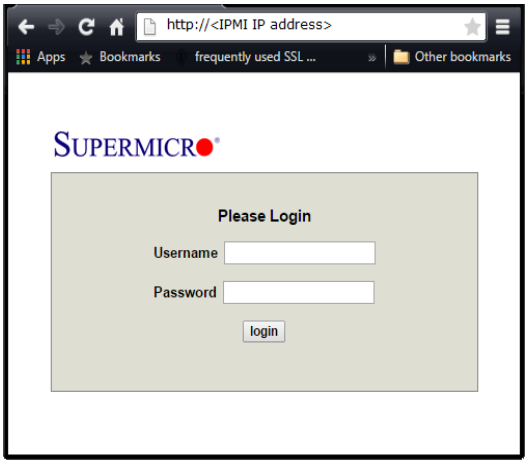
    `0013:ipmi$ mask set <net mask>`

11. Enable the KVM port using the command `port enable kvm`. The KVM port is required for remote Java console support. At the prompt, type;

    `0014:ipmi$ port enable kvm`

12. Open a browser session and point the browser to the URL that contains the IPMI IP address you just configured; https://<IPMI IP address>.
13. You will see the IPMI login screen, see Figure 11 below.

Figure 11: IPMI Login screen



The default login credentials are as follows; Username: ADMIN and password: ADMIN.

14. Navigate to **Remote Control > Console Redirection** and click **Launch Console**. Download and run the resulting `.jnlp` file to open a Java console for your DSM. This Java console provides access to the DSM CLI.
15. Log on to the CLI using the default CLI administrator credentials; Username; cliadmin, password: cliadmin123. You will be prompted to change the CLI administrator password. After that you will be prompted to change the IPMI GUI login password as well.
    The new password must be at least 8 characters long, must contain at least one upper case letter, one special character, and one number.
16. Configure the network settings, see “Configure network settings” on page 20 and then generate the CSR, see.“Generate DSM Certificate Authority and create ACS” on page 28.

Configuring High Availability for V6100

See "Configuring HA for a V6100 Hardware Appliance" on page 136 for the procedure to configure high availability.

3

DSM V6000 Hardware Appliance

This chapter describes how to set up a newly purchased or replacement Vormetric V6000 DSM hardware appliance. At the end of this process, your DSM hardware appliance will be connected to the network and ready to support protected hosts.

Figure 12: V6000 DSM hardware appliance

Front

Back

This chapter contains the following sections:

Overview

As of DSM v6.0.3, the V6000 and virtual appliances can be network HSM-enabled by connecting them to an nShield Connect HSMs. This feature enables the DSM appliance to utilize an nShield Connect HSM to create and protect the DSM master key. For more about this feature see, "nShield Connect Integration" below.

Configuring a V6000 Appliance

The following are the high-level steps for installing and configuring the DSM V6000 hardware appliance with DHCP enabled, or if you choose to turn it off, how to configure the appliance using static IP addressing.

Follow the procedure described in "Specifications, Racking, and Cabling for the V6000 and V6100", to install the physical appliance.

After installation and configuration, the DSM must have connectivity to all hosts that have Vormetric Transparent Encryption Agents installed.

Configuring the DSM via DHCP

The DSM appliance `eth0` interface is now DHCP-enabled by default. This section describes how to configure the DSM appliance with DHCP enabled. You must have a DHCP Server properly configured to ensure that the DSM appliance gets the correct IP address.

DHCP support is available for all the DSM interfaces; `eth0` (enabled by default), `eth1`, and `bond0`. The DSM DHCP implementation configures the interface IP address, subnet mask, router (default gateway), DNS server, and the search domain. It does not configure a host name, an NTP server, or Time Zone for the DSM appliance, these have to be manually configured via the CLI. You can choose to turn off dynamic IP addressing and use static IP addressing instead, see "Configuring the DSM via Static IP Addressing". DHCP is managed via the CLI, the DHCP CLI commands are available in the Network category of commands and are described in detail in the *DSM Administrators Guide*.

After accepting the license agreement and changing the CLI administrators password, you need to set the host name and configure an NTP server. The steps are as follows:

- Assemble configuration information using the "DSM Installation Checklist".
- "Specify host name resolution method", if required
- "Configure DSM ports", if applicable
- "Configure the hostname"

- "Configure NTP, time zone, date, time"
- "Enable DHCP on `bond0` interface" if you choose to use this feature
- "Generate the DSM Certificate Authority" after you configure the hostname and NTP server
- Open a browser, after generating the CA, to access the DSM Management Console see, "Verify web access"
- "Upload a license file"

Configuring the DSM via Static IP Addressing

If you do not want to want to use DHCP, it can be turned off via the CLI and you can assign a static IP addresses to the DSM interfaces. The DHCP CLI commands are available in the Network category commands sub-menu and are described in detail in the CLI chapter of the *DSM Administrators Guide*.

To turn off DHCP do the following and then proceed with the configuration as described in the sections below:

Log on to the CLI console with the CLI administrator credentials and enter the Network category of commands, and turn off DHCP on the `eth0` interface;

```
$ network
0001:network$ ip dhcp release <interface> version 4
Example:
$ network
0001:network$ ip dhcp release eth0 version 4
WARNING: Changing network ip address may disconnect your session and will
require the server software to be restarted.
Continue? (yes|no)[no]:yes
DHCP operations may take some time, please wait....
SUCCESS: Please restart server software to pick up the changes.
0002:network$
```

After you release DHCP on an interface, all network configuration information is lost, you need to configure the gateway, and DNS information again. Do the following to configure the appliance with static IP addressing:

- "Specify host name resolution method", if required
- "Configure DSM ports", if applicable
- "Configure network settings"
- "Configure a bonded NIC device", if you choose to use this feature
- "Configure NTP, time zone, date, time"
- "Configure the hostname"
- "Generate the DSM Certificate Authority"

- Open a browser, after generating the CA, to access the DSM Management Console see, "Verify web access"
- "Upload a license file"

Assumptions

- Data center conditions meet the appliance racking, networking, and power requirements.
- The IP address, routing configuration and DNS addresses for the DSM allow connectivity to all servers where Vormetric Encryption Agents are installed.
- The IP address, routing configuration and DNS addresses for the DSM allow connectivity to all servers where Vormetric Encryption Agents are installed.

DSM Installation Checklist

Use this table to collect the information you need for the installation.

Table 6: Installation Checklist

REQUIREMENT	VALUE
Software requirements	
Obtain the Vormetric DSM - Virtual Appliance 6.x.x.xxxx.zip file from Vormetric support, and unzip the file.	
Hardware requirements for Virtual Machine	
2 virtual sockets, 2 cores per socket	
4GB memory	
1 virtual NIC card	
100GB virtual disk	
Hardware Requirements	
Two power outlets with an independent, 120/240V, 47/63Hz, 12/6A power source.	
Serial console—this should be connected to the DSM appliance using the serial cable included with the appliance.	
Two network (Ethernet) cables, these are included with the DSM appliance.	
Trusted verification device (TVD) and set of smart cards (V6100 only)	
Laptop or PC to connect the TVD (V6100 only)	

1u rack space	
Network Information	
eth0—this interface is DHCP enabled by default. DHCP must be disabled to assign a static IP address	DHCP Server[a] If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
eth1—this interface comes configured with a default IP address; 192.168.10.1. Thales recommends that you retain this configuration in the event that you need a recovery option to access the appliance.	DHCP Server If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
bond0—this interface is used when the eth0 and eth1 interfaces are aggregated into a single logical interface for load balancing/fault tolerance. If configured, the `bond0` interface supersedes the eth0 and eth1 interfaces, and must be used to access the DSM appliance.	DHCP Server If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
IPMI NIC—this interface comes configured with a default IP address; 192.168.10.10 This interface supports DHCP, refer to the CLI chapter in the *DSM Administrators Guide* for details.	DHCP Server If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
Primary DSM Hostname: FQDN	
Failover DSM Hostname: FQDN	
Domain Name Server (DNS) addresses - up to 3 plus optional DNS search domain.	
NTP server FQHN or IP address (if applicable)	
DSM V6100 appliance with DSM software	
Certificate Information	
DSM Hostname: FQDN	
Name of your organizational unit	
Name of your organization	
Name of your city or locality. Must be fully spelled out, no abbreviations, e.g., San Jose, *not* SJC.	
Name of your state or province. Must be fully spelled out, no abbreviations, e.g., California *not* CA	

Two-letter country code	

a. DSM DHCP support enables configuration of the appliance IP address, net mask, gateway, and search domain. It does not configure an appliance host name, or an NTP server

Pre-configuration tasks

Specify host name resolution method

You can map a host name to an IP address using a Domain Name Server (DNS). DNS is the preferred method of host name resolution.

You can also modify the `hosts` file on the DSM or identify a host using only the IP address.

- If you use DNS to resolve host names, use the FQDN for the host names.
- If you do NOT use a DNS server to resolve host names, do the following on all of the DSMs and the protected hosts:
  - Modify the *host* file on the DSM: To use names like serverx.domain.com, enter the host names and matching IP addresses in the */etc/host*s file on the DSM using the `host` command under the `network` menu. For example:

    ```
    0011:network$ host add <hostname> 192.168.1.1
    SUCCESS: add host
    0012:network$ host show
    name=localhost1.localdomain1 ip=::1
    name=<host name>.<domain name>.com ip=192.168.10.8
    name=<host name> ip=192.168.1.1
    SUCCESS: show host
    ```

    You must do this on *each* DSM, since entries in the host file are not replicated across DSMs.
  - Modify the *host* file on the protected hosts: Enter the DSM host names and matching IP addresses in the */etc/host*s file on the protected host. *You must do this on EACH protected host making sure to add an entry for all DSM nodes (if using HA).*

OR

- Use IP addresses: You may use IP addresses or the FQDN to identify the host simultaneously. In other words, they don't all have to use an IP address or FQDN.

Configure DSM ports

If a DSM must communicate with a device behind a firewall, you must open various ports in the firewall as shown in the following figures.

Figure 13: Ports to open between workstation and DSM

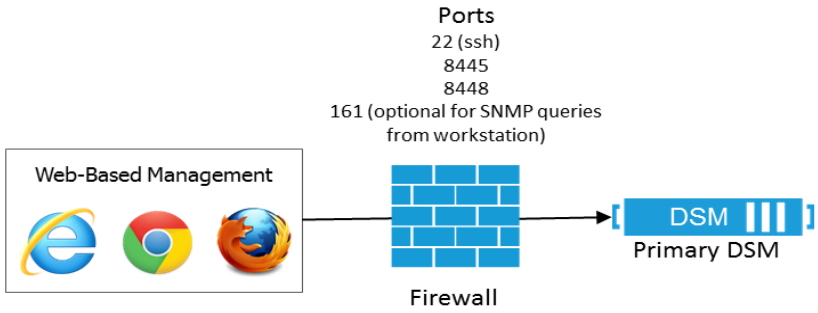


Figure 14: Ports to open between DSMs

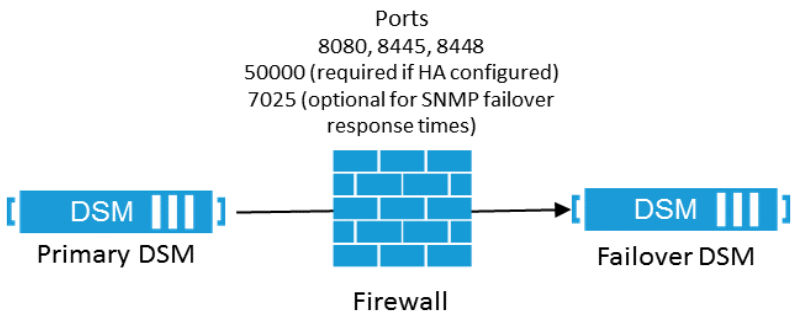
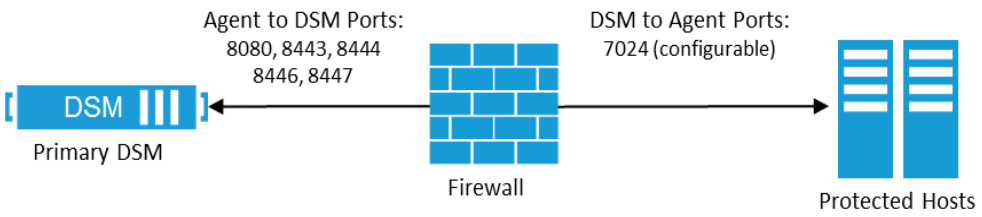


Figure 15: Ports to open between DSM and agent



The following table lists the communication direction and purpose of each port you must open.

Table 7: Ports to configure

Port	Protocol	Communication Direction	Purpose
22	TCP	Management Console → DSM DSM → SSHD Server	CLI SSH Access Auto-backup via SCP
161	TCP/UDP	SNMP Manager → DSM	SNMP queries from an external manager
445	TCP	DSM → CIFS Server	Auto-backup via CIFS
5696	TCP	KMIP client → DSM	Allows communication between the KMIP client and primary DSM
7024	TCP	DSM → Agent	Policy/Configuration Exchange
7025	UDP	DSM ↔ DSM	Uses SNMP to get failover node response time.
8080	TCP	Agent → DSM DSM ↔ DSM	Default TCP/IP port for HTTP that is used to exchange certificates between the DSMs in an HA configuration. Also, used once to perform the initial certificate exchange between an agent host and DSM.
8443	TCP	Agent → DSM	TCP/IP port through which the agent communicates with the DSM. The agent establishes a secure connection to the DSM, via certificate exchange, using this port.
8444	TCP	Agent → DSM	Agent log messages uploaded to DSM
8445	TCP	Browser → DSM DSM ↔ DSM (fallback)	Management Console, VMSSC, and fallback for HA communication in case port 8448 is dropped.
8446	TCP	Agent → DSM	Configuration Exchange using Elliptic Curve Cryptography (Suite B)
8447	TCP	Agent → DSM	Agent uploads log messages to DSM using Elliptic Curve Cryptography (ECC)
8448	TCP	Browser → DSM DSM ↔ DSM	GUI Management during enhanced security using Elliptic Curve Cryptography (Suite B). Also for secure communication between DSMs in HA cluster.
9004	TCP	DSM ↔ nShield Connect	DSM communication with nShield Connect and associated RFS
50000	TCP	DSM (primary) → DSM (failover)	HA information exchange
If NTP server and Syslog server are used to synchronize DSM time and forward log messages, it will require opening up following ports			
123	UDP	DSM → NTP Server	NTP Synchronization
514	UDP/TCP	DSM → Syslog Server	Logging to Syslog. Note that 514 is the default, but is configurable depending on the syslog server.

Configuration tasks

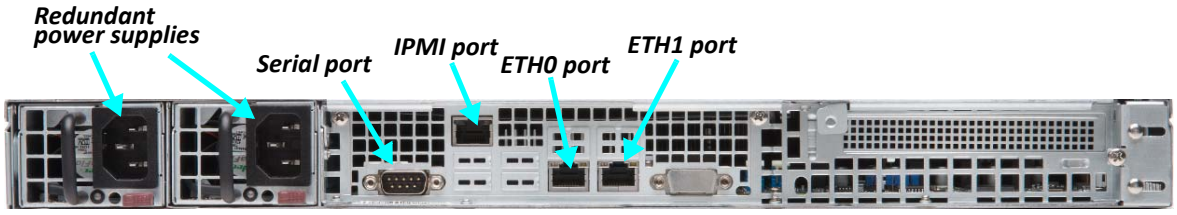
Connect to the V6000 appliance

To configure the DSM, you need to access the DSM Command Line Interface (CLI). To access the DSM CLI, you need connect through the console serial port with a DB-9 cable. Configure your console connection using the following parameters:

- Terminal Type: VT100
- Baud Rate: 9600
- Parity: None
- Data bits: 8
- Stop bits: 1

Optionally you can connect a laptop to the DSM ETH0 using a standard network cable (cat-5). We recommended that you use the console serial interface to perform initial network configuration because, if you are logged onto the appliance through the Ethernet interface, the connection will drop when you change the Ethernet interface IP address.

Figure 16: V6000 DSM ports



Access the DSM Command Line Interface (CLI)

The DSM CLI commands are used to configure the DSM. The commands are grouped into the following categories or *submenus*. Entering "?" on the CLI command line lists those categories:

```
$ ?
network      Networking configuration
system       System configuration
hsm          HSM configuration
maintenance  System maintenance utilities
ha           HA configuration
ipmi         IPMI configuration
user         User configuration
exit         Exit
```

To enter a submenu, enter a name or just the first few letters of the name. To display the commands for that submenu, enter a '?'. For example, the submenu `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
```

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}
0043:maintenance$ diag
usage: diag [log [ list | view LOG_FILE_NAME] | vmstat | diskusage |
hardware | osversion | uptime ]
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 enter system,
then enter reboot. To return to the main level when finished, enter up.
```

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

Configure network settings

1. Connect a laptop to the DSM ETH0 (left port) using a standard network cable (cat-5). Optionally, you can connect through the console serial port with a DB-9 cable. Or if configuring the appliance via IPMI, connect a standard network cable (cat-5) to the IPMI port with the default IP address 192.168.10.10. See "Configuring and Accessing IPMI on the DSM" on page 146 for more information about configuring the DSM via IPMI.
2. Manually set the IP address for the laptop to 192.168.10.2 (or higher) with a default mask of 255.255.255.0
3. SSH to 192.168.10.1
4. Log in with the default login and password:

Login: cliadmin

Password: cliadmin123

5. The Vormetric license agreement is displayed, type 'y' to accept and press **Enter**.
6. When prompted, type in a new password and press **Enter**. Reconfirm your password.

Warning! Do not lose this password.

7. Navigate to the network commands menu. Type:

   `network`

8. Configure an IP address for the DSM.

NOTE: The `eth0` interface DHCP enabled by default. See "Configuring the DSM via DHCP" for details, and for instructions to switch to static addressing if desired.
We recommend that you retain the default `eth1` IP address configuration in the event that you need a recovery option to access the DSM appliance.

Type:

```
ip address init <DSM IP address>/<subnet mask (e.g. 16 or 24)> dev
eth0/eth1
```

Example: `ip address init 192.168.10.2/16 dev eth1`

IPv6 example: `ip address init fa01::3:15:130/64 dev eth1`

NOTE: If you are connected via ETH0, you will be disconnected at this step. Reconnect on the new IP address.

9. (Optional) If you have configured ETH0, you can also configure an IP address for ETH1 if you want to communicate with agents on a different subnet for example, or if you want to access the Management Console from a different subnet. To configure an IP address for ETH1, type:

   `ip address init <eth1 IP address>/<subnet mask (e.g., 16 or 24)> dev eth1`

   Example: `ip address init 192.168.10.3/16 dev eth1`

   IPv6 example: `ip address init fa01::3:15:130/64 dev eth1`

   The following warning is displayed:

```
WARNING: Changing the network ip address requires server software to be
restarted.
Continue? (yes|no) [no]:
```

Type 'yes' to continue with the IP address configuration.

10. Add the IP address for the default gateway. Type:

    `ip route add default table main.table dev [eth0 or eth1] via <IP address for the default gateway>`

    Example: `ip route add default table main.table dev eth0 via 192.168.1.5`

    IPv6 example:
    `ip route default table main.table dev eth0 via fa01::3:15:120`

11. Verify the interface settings. Type:

    `ip address show`

12. Verify the route settings. Type:

    `ip route show`

13. If you are using DNS, set the primary DNS server for the DSM. Type:

    `dns dns1 <ip address for dns server 1>`

14. If you have a second or third DNS server, set them for the DSM. Type:

    `dns dns2 <ip address for dns server 2>`

15. If you want to set the search domain, type:

    `dns search <search_domain>`

16. Show the DNS settings. Type:

    `dns show`

17. Return to the main menu. Type:

    up

Configure a bonded NIC device

This section describes how to aggregate the two NICs on the DSM into a single logical interface to provide load balancing and/or fault tolerance. The bonded NIC device is called `bond0`.

NOTE: In order to use the bonded NICs feature, you must ensure that your switch is configured to use Link Aggregation Control Protocol (LACP).

The DSM physical appliances have two physical NICs called `eth0` and `eth1`. Only two NICs `eth0` and `eth1` are supported. Any additional physical/virtual NICs are ignored.

The NIC bonding setting is system specific. If it is to be used for all nodes in a cluster, it must be enabled in all nodes individually.

1. Access the DSM CLI and login with your login credentials. If this is the first time you are logging in, then you will be required to accept the license agreement and change the default password.

2. Navigate to the network commands menu;

   ```
   $ network
   0001:network$
   ```

3. Enable the bonded NIC;

   ```
   0001:network$ ip address init <ip_address>/<subnet_mask> dev bond0
   ```

   Example: `ip address init 1.2.3.4/16 dev bond0`

In the event that a bonded NIC is being configured after the initial configuration, or after the DSM has been upgraded, if you want to reuse an IP address that was originally assigned to `eth0` or `eth1`, then you must delete that address from `eth0` or `eth1` first, and then reassign it to the `bond0` device.

4. Add a default gateway for the `bond0` device;

   ```
   0001: ip route add default table main.table dev bond0 via
   <gateway_ip_address>
   ```

   Example: `ip route add default table main.table dev bond0 via 1.2.7.8`

If a `bond0` interface is configured after setting up the `eth0` and/or `eth1` interfaces, and it is configured with an IP address that is on the same subnet as a default gateway, that gateway configuration continues to apply. However, if you configure `bond0` with an IP address on a different subnet, you will have to reconfigure the default gateway.

1. You can change the bonding driver mode based on your requirements. There are seven modes available from 0-6. See "Bonding driver modes" for more information. Note however, that only the default options are available with each of the modes and these options cannot be changed.

   When the mode option is specified the speed option cannot be specified (i.e. the options mode and speed are mutually exclusive). In other words, bond0 does not take the speed option and both eth0 and eth1 don't take the mode option. However, the MTU and up/down options can still be used for the bond0 device.

   To set or change the mode type:

   ```
   0002:network$ ip link set bond0 mode <mode>
   ```

   Example: `ip link set bond0 mode 2`

   To see what mode is currently in use type:

   ```
   0002: network$ ip link show bond0
   ```

2. To disable or break up a bonded NIC type: you can use either the delete or flush command. Delete will only delete a specific IP address (multiple can be assigned) and flush will clear all assigned IP addresses.

   ```
   0003:network$ ip address delete <ip_address>/<subnet_mask> dev bond0
   ```

   or

   ```
   0003:network$ ip address flush bond0
   ```

   Routes that are associated with this bonded NIC device will also be deleted.

Bonding driver modes

The modes specify the bonding policies. The following modes are supported (see Table 8 below), but none of the options for the modes are configurable and take the default values for those modes, except for the `miimon` setting. The `miimon` setting specifies the MII link monitoring frequency in milliseconds, which determines how often the link state of each slave is inspected for link failures. The `miimon` setting has a value of 100 instead of the default value of 0.

Table 8: Bonding driver modes

Mode	Name	Description	Load-balancing	Fault tolerance
0	balance-rr	Round-robin policy. Transmit packets in sequential order from the first available through the last. This is the default mode for the bonded NICs.	Yes	Yes
1	active-backup	Active-backup policy: Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch.	No	Yes
2	balance-xor	XOR policy: Transmit based on the selected transmit hash policy. The default policy is a simple [(source MAC address XOR'd with destination MAC address) modulo slave count].	Yes	Yes
3	broadcast	Broadcast policy: transmits everything on all slave interfaces.	No	Yes
4	802.3ad	IEEE 802.3ad Dynamic link aggregation. Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.	Yes	Yes
5	balance-tlb	Adaptive transmit load balancing: channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.	Yes	Yes
6	balance-alb	Adaptive load balancing: includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware addresses for the server.	Yes	Yes

Enable DHCP on `bond0` interface

To configure a `bond0` interface using DHCP, you need to enable DHCP on that interface. The `bond0` interface inherits the IP address that was dynamically assigned to the `eth0` interface when the DSM was initially deployed.

Log on to the CLI console and navigate to the Network category of commands and enable DHCP.

Example:

```
0004:network$ ip dhcp enable bond0 version 4

WARNING: Changing network ip address may disconnect your session
and will require the server software to be restarted.

Continue? (yes|no)[no]:yes

DHCP operations may take some time, please wait....

SUCCESS: Please restart server software to pick up the changes.

0005:network$
```

Configure NTP, time zone, date, time

You must have the correct time set on your DSM server(s) as this will affect system functions such as agent registration, log timestamps, high availability cluster synchronization, and certificate exchange. Although configuring an NTP server is not mandatory, it is strongly recommended.

1. Navigate to the *maintenance commands* menu. Type:
   `maintenance`
2. Show the current ntpdate settings. Type:
   `ntpdate show`
3. Add a new ntpdate server. Type:
   `ntpdate add <IP address/Hostname for the` *ntpdate server>*

   Repeat this step for each ntpdate server.
4. Activate the ntpdate server connection. Type:
   `ntpdate on`
5. Show the current timezone settings. Type:
   `gmttimezone show`
6. Set the country and city where the DSM resides. Type:
   `gmttimezone set <country/city>`
7. Set the date. (If you used `ntpdate synch`, this step is not necessary.) Type:

```
date <mm/dd/yyyy>
```

8. Set the time. (If you used `ntpdate synch`, this step is not necessary.) Type:

```
time <hh:mm:ss>
```

   Where *hh* is 00 to 23.

9. Verify your settings. Type:

```
time
date
```

10. Return to the main menu. Type:

```
up
```

Configure the hostname

1. Navigate to the *system* menu. Type:

```
0001:vormetric$ system
```

2. Show the current setting. Type:

```
0002:system$ setinfo show
```

   The default host name in the output is *your. name.here*.

3. Set the hostname. You must enter the fully qualified domain name for the DSM. Type:

```
0003:system$ setinfo hostname <FQHN>
```

   Example:

```
0003:system& setinfo hostname dsm.company.com
```

Generate the DSM Certificate Authority

1. Generate a new certificate authority for the DSM. Type:

```
security genca
```

2. A warning is displayed, informing you that all agents and peer node certificates will need to be re-signed after the CA and server certificate have been regenerated, and the DSM server software will be restarted. Type ‘yes’ to continue, the default is ‘no’.
3. Enter the FQDN of this DSM, the name displayed in ‘This Security Server host name [FQDN of the DSM], should be correct, if you entered the host name information in the previous sections correctly. Press **Enter** to accept the name.
4. Next, enter the information required to generate the certificate. Answer the prompts:

   a. What is the name of your organizational unit? []:

   b. What is the name of your organization? []:

c. What is the name of your City or Locality? []:

d. What is the name of your State or Province? []:

e. What is your two-letter country code? [US]:

5. Once the certificate is signed, return to the main menu. Type:
   up

Add more CLI administrators (optional)

1. Navigate to the *users commands* menu. Type
   user
2. For each administrator you want to add, type
   add <*administrator name*>
3. When prompted, enter a password. The password criteria are:
   - Does not have repeating characters
   - Uses at least 1 upper- and 1 lower-case character
   - Uses at least 1 special character
4. Return to the main menu. Type
   up

Configuring IPMI for the V6000 (optional)

Although not necessary for DSM maintenance and operation, some administrators may find the IPMI features useful. See "IPMI" on page 145 for complete details.

Verify web access

Open a browser and confirm access over HTTPS to either the DSM hostname (if configured in DNS) or the IP address defined in "Configure network settings" on page 52. Example URL:

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

If this doesn't work because, for example, port 443 was blocked by a firewall, specify port 8445. Example:

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

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

- Does not have repeating characters
- Uses at least 1 upper and 1 lower case character
- Uses at least 1 special character

Upload a license file

The first time you log on to a DSM, the dashboard displays “License file not found" and all you will see are the *Dashboard* and *System* tabs. You need to click **System** and select **License**, then **Upload the license file**. After uploading your license file, all the other tabs for which you have a license will be visible. See “Upload a license file” on page 32 for instructions about uploading a license file.

The DSM Management Console has a help icon (?) located on the right-hand side of the title bar, which is located under the menu bar, on each page of the Web UI. Click the icon for help with tasks on a specific page.

Full Disk Encryption

As of v6.0.2, the DSM root file system is automatically encrypted for enhanced security. This feature is only available on: a fresh installation of the DSM v6.0.2 software on the V6x00 appliances and a fresh DSM v6.0.2 build on a virtual appliance. See “Full Disk Encryption” on page 33 for details and procedures for this feature.

This feature also requires use of the IPMI, see “Configuring IPMI” on page 38 for details and procedures for this feature.

nShield Connect Integration

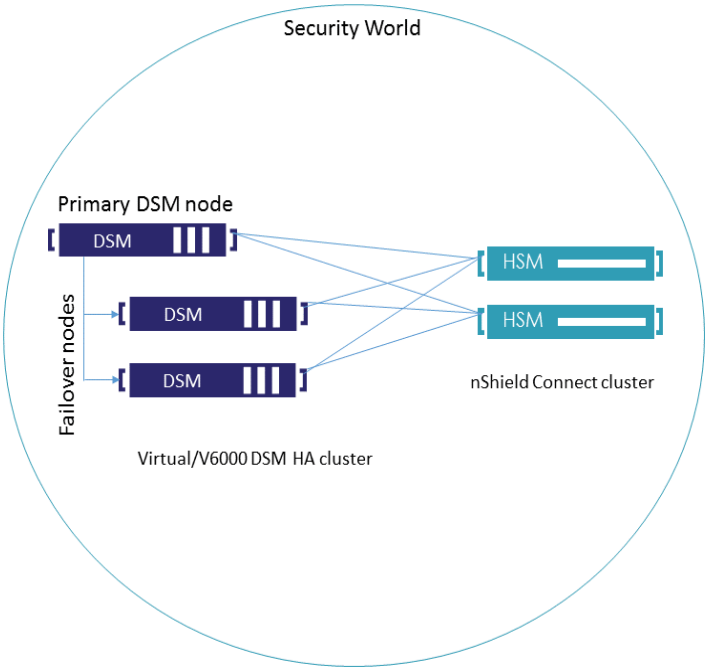
DSM appliances that do not have a built in hardware security module (HSM)—DSM V6000 hardware and virtual appliances—can now be configured to utilize an nShield Connect HSM to create and protect the DSM master key. The nShield Connect series includes nShield Connect + and nShield Connect XC, the DSM can be configured with either of these appliances.

NOTE: The V6100 appliance does not support this feature

Deployment

The figure below shows an example of a network HSM-enabled DSM HA cluster deployment. The DSM could be virtual appliances on-premise or in the cloud, or V6000 appliances on-premise. The nShield Connect HSMs are clustered for fault tolerance—if one of them fails, the Security World is still available to the DSMs via the failover Connect appliance.

Figure 17: Network HSM enabled V6000/virtual DSM HA cluster



The nShield Connect HSMs use the Security World paradigm to provide a secure environment for all HSM and key management operations. The nShield Connect HSM has its own Security World, and the DSM (or DSM high availability cluster) joins that Security World. For more about the Security World paradigm, see, "Security World" on page 7.

When a DSM appliance joins the nShield Connect HSM Security World, that DSM appliance is network HSM-enabled and functions similarly to a V6100 appliance—with important differences in how backups are restored, see "Backing up and Restoring network HSM-enabled DSM".

New CLI commands have been added to the HSM category of commands to enable and manage this feature. Refer to the CLI chapter of the *DSM Administrators Guide* for a detailed description of the new commands.

Warning! Once a DSM appliance is converted to an HSM enabled appliance, it cannot be rolled back to a non-HSM configuration unless you run the `config load default` command, which wipes all configuration and resets the DSM appliance to the state in which it was shipped.

High Availability

A DSM high availability (HA) cluster must consist of similar appliance types, for example, if you plan to create an HA cluster for a network HSM-enabled DSM, then all nodes in the cluster must be network HSM-enabled appliances. As this feature is supported on both V6000 and virtual DSMs, an HA cluster for a network HSM-enabled DSM may consist of both V6000 and virtual DSMs, as long as they are all network HSM-enabled.

Network HSM-enabled DSMs cannot be clustered with V6100 appliances—the V6100 creates its own Security World, whereas a network HSM-enabled DSM belongs to the nShield Connect Security World, and since all nodes in a cluster have to belong to the same Security World, the V6100 and network HSM-enabled DSM appliances cannot be combined.

When creating a cluster, Thales recommends that you configure at least two or more nShield Connect HSMs for fault tolerance. Refer to the nShield Connect HSM documentation for information about configuring additional nShield Connect HSMs.

Each DSM node in a network HSM-enabled DSM cluster can be configured with one or more nShield Connect HSMs for fault tolerance, provided they all belong to the same Security World. See "Configuring High Availability for network HSM-enabled DSM" for more about network HSM-enabled DSM high availability clusters.

System and Software Requirements

- DSM V6000 or virtual appliances with v6.0.3 of the DSM firmware. This feature is only supported on v6.0.3 of the DSM firmware, you must upgrade your system to this version to enable this feature. See the "Upgrade and Migration" on page 105 for details about upgrading your system.

NOTE: The V6100 appliance does not support network HSM.

- At least one nShield Connect HSM and its corresponding remote file system (RFS) deployed on the network. The nShield HSM must belong to a Security World. If there are more than one nShield Connect HSMs in the deployment, they must all belong to the same Security World for the DSM to connect to them. Thales recommends that you add another nShield Connect HSM to the Security World for fault tolerance.

NOTE: Client licenses are required for each nShield Connect HSM that is configured for the DSMs—the number of client licenses required per nShield Connect HSM is equal to the number of DSMs used.

- The nShield Connect HSM used to enable this feature can be either of the following; nShield Connect+, or nShield Connect XC.For more information about configuring the nShield Connect HSM and RFS, refer to the relevant nShield Connect HSM user documentation.
- Port 9004 must be opened on the network path between the DSMs and the nShield Connect HSM(s) to enable communication between the DSMs, the nShield Connect HSM(s) and its associated RFS.

Configuring nShield Connect HSM with DSM

The following is the overall sequence of procedures to enable this feature:

1. Deploy and configure an nShield Connect HSM and its associated RFS
2. Add the DSM as a client to the nShield Connect HSM
3. Add the nShield Connect HSM to the DSM

If you plan to setup a network HSM-enabled DSM HA cluster, you can do so after the primary node is configured, see "Configuring High Availability for network HSM-enabled DSM" for more information.

Configure nShield Connect appliance and associated RFS

Refer to the nShield Connect documentation to set up your nShield Connect appliance and the associated RFS.

Add DSM as an nShield Connect client

Before a DSM node (primary or failover) is configured to use an nShield Connect HSM, it must first be added as a client to the nShield Connect HSM. The DSM node must be enrolled as a privileged client that does not require nToken authentication.

Refer to the nShield Connect user documentation for detailed procedures about how to enroll a privileged client.

Add the nShield Connect HSM to the DSM

The next step is to add the nShield Connect HSM to the DSM. Open a CLI session on the DSM appliance that is a client of the nShield Connect HSM

NOTE: If the nShield Connect Security World is FIPS 140-2 level 3 compliant, only one card from the associated ACS is required for this step. The card is only required for the first HSM device to be added to the DSM, it is not required for any subsequent nShield Connect HSMs that are added.

1. Navigate to the HSM category of commands, type the following at the prompt:

   ```
   0000:dsm$ hsm

   0001:hsm$
   ```

2. Use the connect add command to add the nShield Connect HSM to the DSM. Type the following command at the prompt,

   ```
   0001:hsm$ connect add <nShield_Connect_IP_Address>
   <RFS_IP_Address>
   ```

   where,

   <*nShield_Connect_IP_Address*> is the IP address of the nShield Connect HSM and

   <*RFS_IP_Address*> is the IP address of the computer that has the RFS installed.

   For example,

   ```
   0001: hsm$ connect add 1.2.3.18 1.2.3.4
   ```

3. A warning displays, informing you that once this DSM is converted to a network HSM-enabled appliance, it cannot be rolled back. Type 'yes' to continue.

   The DSM is restarted if the operation is successful.

4. Follow the prompts to add the nShield Connect HSM to the DSM.

5. To view the nShield Connect HSM that has been added run the `connect show` command.

6. If there are more nShield HSMs in the same Security World you can add them now using the connect add command.

7. The *About* page of the DSM Web UI also displays the nShield Connect HSMs that have been configured.

Figure 18: Configured HSM devices on DSM Web UI *About* page

Configuring High Availability for network HSM-enabled DSM

When configuring high availability (HA) for network HSM-enabled DSMs, Thales recommends the following:

- Configure at least two nShield Connect HSMs in the Security World for fault tolerance. This means in the event one of the appliances is not reachable for some reason, the Security World is still available.

NOTE: Client licenses will be required for each nShield Connect appliance that is configured for the DSMs—the number of client licenses required per Connect appliance will be equal to the number of DSMs connected to the nShield appliance.

- Each network HSM-enabled DSM node in the HA cluster must be connected to at least two of the nShield Connect HSMs in the Security World. This ensures that if one of the nShield Connect is not reachable for some reason, the DSM nodes can still access the Security World of via the second nShield Connect.

A network HSM-enabled DSM HA cluster can be configured in one of two ways:

The first way is to configure DSMs as standalone nodes and enable network HSMs for each of them in the same Security World. That is, all the DSMs must be configured with nShield Connect HSM(s) that are part of the same Security World. You can now create a network HSM-enabled DSM cluster in the same way as for any other DSM cluster

The high-level steps for to configure a network HSM-enabled DSM HA cluster in this way are:

1. Configure two nShield Connect HSMs and the associated RFS.
2. Configure the DSMs that are to be part of the HA cluster.
3. Add the DSMs individually to the nShield Connect Security World to make each DSM network HSM-enabled. This means you must run the connect add command on each of the DSMs to add them to that Security World.
4. Add both nShield Connect HSMs to each of the DSMs.

   Steps 1 to 4 are described here “Configuring nShield Connect HSM with DSM”, do this for each DSM server that is to be part of the HA cluster.
5. Configure HA per the standard procedure described here, “Configuring HA for V6000 and Virtual Appliances” on page 144.

The second way to create a network HSM-enabled HA cluster is to configure a standalone network HSM-enabled DSM, as the primary node. Add non network HSM-enabled DSM appliances as failover nodes on the primary node. An additional step is required when the convert2failover command on the failover node completes—the system displays the nShield Connect HSMs that are configured on the primary node, and prompts you to add the first nShield Connect HSM in the list. If there are more than one nShield Connect HSMs configured, it will prompt you to connect the failover node to those devices as well.

If there are additional nShield Connects in that same Security World but they have not bee configured on the DSM primary node, you can connect to those devices instead. As long as they

are part of the same Security World, the failover node(s) can be connected to separate nShield Connect appliances.

The steps to add non network HSM-enabled DSMs as failover nodes to a network HSM-enabled primary node are:

1. Configure two nShield Connect HSMs in the same Security World and the associated RFS.
2. Configure a DSM and add it to the Security World you just created.
3. Add both nShield Connect HSMs to the DSM.

   These steps are described here "Configuring nShield Connect HSM with DSM".

   Now you can add the failover nodes as follows:
4. Log on to the DSM Web UI and click High Availability to navigate to the High Availability Servers page.
5. Click **Add** to add a failover node, enter the failover node's FQDN and click **Ok**, that server will now be listed in the table on the *High Availability Servers* page with the role of 'failover'.
6. Log on to the CLI of the failover node and type ha to enter the High Availability category of commands, then run `convert2failover` command,

   ```
   0001:dsm$ ha
   0002:ha$ convert2failover
   ```

   A warning is displayed, type `yes` to continue.
1. Enter information about the primary DSM at the prompt;

   ```
   Primary Security Server host name:primary.hostname.com
   Primary Security Server system administrator name:admin
   Primary Security Server system administrator password:xxxxxxx
   ```
2. Enter the failover DSM information at the prompts to generate the server certificate. You will be asked to recheck and confirm the information you just entered, confirm that it is all correct.
3. Type `yes` to continue, the DSM server software, is stopped while the conversion to failover is done and the security certificate is signed.
4. A message is displayed informing you that the primary server has nShield Connect HSMs configured with the IP addresses displayed, you will be prompted to add the first nShield Connect HSM in the list, type `yes`. The `connect add` command is run automatically when you choose to add the nShield Connect appliance.
5. You will be prompted to add the second nShield Connect, type `yes`.

   If you have more than two nShield HSMs in that same Security World, you could choose not to add either or both of the appliances listed on the console prompt, and instead add one of the other nShield Connect HSMs available in the same Security World. To ensure business continuity, Thales recommends that you connect each node to at least two nShield appliances.
6. Repeat these steps for each failover node.

Once a DSM is network HSM-enabled, it must be connected to at least one nShield Connect HSM. If you remove an nShield Connect from a Security World, you must make sure that any DSM appliances that were connected to it, are now connected to another nShield HSM belonging to that same Security World.

In this case, if more than one nShield Connect HSM is available in the Security World, a DSM Administrator could choose to use any of them after the DSM has been converted to a failover node.

Managing network HSM-enabled DSM

To switch to another nShield Connect HSM in the Security World:

1. Open a CLI session on the network HSM-enabled DSM appliance to be moved to using another nShield Connect.
2. First add the nShield Connect appliance that you want the DSM node to use. Type the following at the prompt:

   ```
   0000:dsm$ hsm
   0001:hsm$
   0001:hdm$ connect add
   ```

3. To view the available nShield Connect appliances, type the following at the prompt:
4. 0002:hsm$ connect show
5. If you want to remove the existing nShield Connect, type the following at the prompt:

   ```
   0003:hsm$ connect delete
   ```

Backing up and Restoring network HSM-enabled DSM

A network HSM-enabled DSM is backed up in the same way as any other DSM appliance. You should also take a backup of the RFS when you backup the DSM and keep the two backup files together. The RFS backup is done separately as part of the nShield Connect administration, refer to the nShield Connect user documentation for details and procedures.

If the backup is to be restored to the same DSM appliance, then the nShield RFS backup is not required.

If the backup is to be restored on a another network HSM-enabled DSM in another Security World, you will need to restore the RFS first and then the DSM backup. The associated ACS will also be required.

The high-level steps to backup a network HSM-enabled DSM and restore the backup to another DSM in another Security World are as follows:

1. Backup the network HSM-enabled DSM. The backup procedure for a network HSM-enabled DSM or cluster is the same as for any other DSM deployment. Refer to the DSM Administrators Guide chapter, “Backing Up and Restoring the DSM”.
2. Backup the nShield Connect RFS. Refer to the nShield user documentation for the procedure.
3. Restore the Security World data on the nShield Connect device connected to the new network HSM-enabled DSM that belongs to another Security World.
4. Run the `connect secworldupdate` command on the DSM to update the Security World.
5. Restore the network HSM-enabled DSM backup. The restore procedure for a network HSM-enabled DSM or cluster is the same as for any other DSM deployment. Refer to the DSM Administrators Guide chapter, “Backing Up and Restoring the DSM”.

A backup of a network HSM-enabled DSM can be restored as follows:

- on the same DSM appliance
- on another DSM appliance in the same Security World
- on a DSM V6100 appliance—to restore a network HSM-enabled DSM backup to a V6100appliance, ACS of the nShield Connect device that was configured with the network HSM-enabled DSM is required. Refer to the DSM Administrators Guide chapter, “Backing Up and Restoring the DSM” for a detailed description of the procedure.

Additionally, you can restore the following types of backups to a network HSM-enabled DSM:

- a backup of a non-HSM DSM (V6000 or virtual DSM)

Domain level backups can be restored as follows:

- a domain backup from a network HSM-enabled DSM to a domain on a non network HSM-enabled DSM (V6000 or virtual appliance) and vice versa
- a domain backup from a network HSM-enabled DSM to a domain on a V6100 appliance and vice versa

Updating a network HSM-enabled DSM Security World

In the event that the nShield Connect Security World changes, the network HSM-enabled DSM’s Security World must be synchronized with the new one. A Security World change may be triggered for various reasons, for example the ACS has been replaced.

To update the Security World on the network HSM-enabled DSM:

1. Open a CLI session on the DSM, if this is a high availability cluster, do this on all the nodes in the cluster.
2. Navigate to the HSM submenu:

```
0000:dsm$ hsm
0001:hsm$
```

3. Type the following at the prompt:

```
0001:hsm$ secworldupdate
SUCCESS: Security World data on this DSM node updated
0002:hsm$
```

You can view the DSM audit logs, accessed via *Log >Logs* from the DSM Web UI, to see the Security World update event.

High Availability (HA) Configuration for V6000 hardware appliance

See "Configuring HA for V6000 and Virtual Appliances" on page 140 for procedures to configure high availability.

4 Installing and Configuring a DSM

The DSM virtual appliance is available as an OVA file, Azure VHD, AWS AMI, and KVM image. The OVA is available as a standard image, and a fastboot image with Open VM Tools (OVT) bundled in for Cloud Service Providers. OVT is the open source implementation of VMware Tools, and consists of a suite of virtualization utilities that improves the functionality, administration, and management of virtual machines within a VMware environment.

This section describes how to deploy the various virtual images.

This chapter contains the following sections:

Overview

DSM supports full disk encryption for enhanced security, and dynamic IP addressing via DHCP. The full disk encryption feature is only available on a fresh installation of v6.0.2 or later.

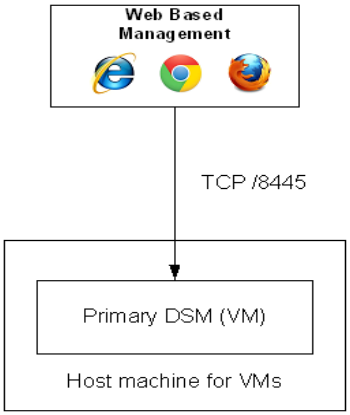
DHCP is enabled by default on the `eth0` interface on a fresh v6.0.2 and above installation but, must be enabled manually, if a DSM appliance is upgraded to v6.0.2 and later versions. See "Upgrading the DSM" on page 107 for details about upgrading the DSM appliance.

As of this release, DSM v6.1, the V6000 and virtual appliances can be HSM-enabled by connecting them to an nShield Connect appliance. The Network HSM support feature enables DSMs that do not have a built-in hardware security module (HSM) —DSM V6000 hardware appliance and the virtual appliance—to utilize an nShield Connect HSM appliance to store the

DSM master key. See “nShield Connect Integration” on page 60 in Chapter 3, for details about this feature. The appliance can be HSM-enabled after it has been configured.

After enabling the HSM, you will have the DSM virtual appliance setup as shown in Figure 19.

Figure 19: Virtual DSM Architecture



Assumptions

- VMware vSphere Client installed.
- DSM virtual appliance software. Obtain the Data Security Manager - Virtual Machine file—OVA file depending on your requirement—from Thales support.
- The IP address, routing configuration, and DNS addresses for the DSM to allow connectivity to all servers where VTE/VAE Agents are installed.

Virtual machine hardware requirements

The virtual machine must meet the following requirements:

Table 9: Hardware requirements for Virtual Machine

	Number of Agents			
	1 to 10	**11 to 50**	**51 to 250**	**Over 250**
Number of CPUs	2	4	4	6
RAM (in GB)	8	8	12	16
HD (in GB)[a] for VM instance	250	250	250	above 250

Table 9: Hardware requirements for Virtual Machine

Cloud instance	120	160	200	250

a. The disk size change was introduced in v5.3.1, however you can still use “thin” provision to minimize storage utilization.

Configuring a Virtual Appliance

The following are the high-level steps for installing and configuring the DSM virtual appliance using DHCP, or if you choose to turn it off, how to configure the appliance using static IP addressing.

Configuring DSM using DHCP

The DSM appliance `eth0` interface is now DHCP-enabled by default. This section describes how to configure the DSM appliance with DHCP enabled. You must have a DHCP Server properly configured to ensure that the DSM appliance gets the correct IP address.

DHCP support is available for all the DSM interfaces; `eth0` (enabled by default), `eth1`, and `bond0`. The DSM DHCP implementation configures the interface IP address, subnet mask, router (default gateway), DNS server, and the search domain. It does not configure a host name, an NTP server, or Time Zone for the DSM appliance, these have to be manually configured via the CLI. You can choose to turn off dynamic IP addressing and use static IP addressing instead, see “Configuring DSM using Static IP Addressing”. DHCP is managed via the CLI, the DHCP CLI commands are available in the Network category of commands and are described in detail in the *DSM Administrators Guide*.

After accepting the license agreement and changing the CLI administrators password, you need to set the host name and configure an NTP server. The steps are as follows:

1. Assemble configuration information using the “Virtual DSM Installation Checklist”.
2. Set up the virtual appliance, see “Virtual Appliance Setup”
3. “Specify host name resolution method”
4. “Configure Ports”, if applicable
5. “Configure NTP, time zone, date, time”
6. “Configure the hostname”
7. “Enable DHCP on `bond0` interface” if you choose to use these features
8. “Generate the Certificate Authority”
9. “Add DSM CLI console administrators (optional)”

10. "Verify web access"

Configuring DSM using Static IP Addressing

If you do not want to want to use DHCP, it can be turned off via the CLI and you can assign a static IP addresses to the DSM interfaces. The DHCP CLI commands are available in the Network category commands sub-menu and are described in detail in the CLI chapter of the *DSM Administrators Guide*.

To turn off DHCP do the following and then proceed with the configuration as described in the sections below:

Log on to the CLI console with the CLI administrator credentials and enter the Network category of commands, and turn off DHCP on the `eth0` interface;

```
$ network
0001:network$ ip dhcp release <interface> version 4
Example:
$ network
0001:network$ ip dhcp release eth0 version 4
WARNING: Changing network ip address may disconnect your session and will
require the server software to be restarted.
Continue? (yes|no)[no]:yes
DHCP operations may take some time, please wait....
SUCCESS: Please restart server software to pick up the changes.
0002:network$
```

After you release DHCP on an interface, all network configuration information is lost, you need to configure the gateway, and DNS information again. Do the following to configure the appliance with static IP addressing:

1. Assemble configuration information using the "Virtual DSM Installation Checklist".
2. Setup the virtual appliance, see "Virtual Appliance Setup"
3. "Specify host name resolution method"
4. "Configure Ports", if applicable
5. "Configure network settings"
6. "Configure a bonded NIC device", if you choose to use this feature
7. "Configure NTP, time zone, date, time"
8. "Configure the hostname"
9. "Generate the Certificate Authority"
10. "Add DSM CLI console administrators (optional)"
11. "Verify web access"

Virtual DSM Installation Checklist

Use this table to collect the information you need for the installation.

Table 10: Installation Checklist

REQUIREMENT	VALUE
Software Requirements	
Refer to "Assumptions" for details	OVA, ISO, KVM image depending on requirement Virtualization software
Hardware Requirements for Virtual machine	
Refer to "Virtual machine hardware requirements" for details	CPU: RAM: HD:
Network Information	
eth0—this interface is DHCP enabled by default. DHCP must be disabled to assign a static IP address	DHCP Server[a] If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
eth1—this interface comes configured with a default IP address; 192.168.10.1. We recommend that you retain this configuration in the event that you need a recovery option to access the appliance.	DHCP Server If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
bond0—this interface is used when the eth0 and eth1 interfaces are aggregated into a single logical interface for load balancing/fault tolerance. If configured, the bond0 interface supersedes the eth0 and eth1 interfaces, and must be used to access the DSM appliance.	DHCP Server If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
IPMI NIC—this interface comes configured with a default IP address; 192.168.10.10 This interface supports DHCP, refer to the CLI chapter in the *DSM Administrators Guide* for details.	DHCP Server If you choose to use static IP addressing, you need the following: IP address: net mask: default gateway (optional):
Primary DSM Hostname: FQDN	
Failover DSM Hostname: FQDN	

Domain Name Server (DNS) addresses - up to 3 plus optional DNS search domain.	
NTP server FQDN or IP address (if applicable)	
Certificate Information	
DSM Hostname: FQDN	
Name of your organizational unit	
Name of your organization	
Name of your city or locality. Must be fully spelled out, no abbreviations, e.g., San Jose, *not* SJC.	
Name of your state or province. Must be fully spelled out, no abbreviations, e.g., California *not* CA	
Two-letter country code	

a. DSM DHCP support enables configuration of the appliance IP address, net mask, gateway, and search domain. It does not configure an appliance host name, or an NTP server

Pre-Configuration tasks

This section details the installation and pre-configuration tasks required for DSM. It consists of the following tasks:

- "Specify host name resolution method" on page 76
- "Configure Ports" on page 77
- "Access the Command Line Interface (CLI)" on page 79

Specify host name resolution method

You can map a host name to an IP address using a Domain Name Server (DNS). DNS is the preferred method of host name resolution.

You can also modify the `hosts` file on the DSM or identify a host using only the IP address.

- If you use DNS to resolve host names, use the FQDN for the host names.
- If you do NOT use a DNS server to resolve host names, do the following on all of the DSMs and all of the protected hosts:
  - Modify the *host* file on the DSM: To use names like serverx.domain.com, enter the host names and matching IP addresses in the */etc/hosts* file using the `host` command under the `network` menu. For example:

```
0011:network$ host add <hostname> 192.168.1.1
SUCCESS: add host
0012:network$ host show
name=localhost1.localdomain1 ip=::1
```

```
name=<host name>.<domain name>.com ip=192.168.10.8
name=<host name> ip=192.168.1.1
SUCCESS: show host
```

You must do this on *each* DSM, since entries in the host file are not replicated across DSMs.

- Modify the *host* file on the protected hosts: Enter the DSM host names and matching IP addresses in the */etc/hosts* file on the protected host. *You must do this on EACH protected host making sure to add an entry for all DSM nodes (if using HA).*

OR

- Use IP addresses: You may use IP addresses or the FQDN to identify the host simultaneously. In other words, they don't all have to use an IP address or FQDN.

Configure Ports

If a DSM must communicate with a device behind a firewall, you must open various ports in the firewall as shown in the following figures.

Figure 20: Ports to open between workstation and DSM

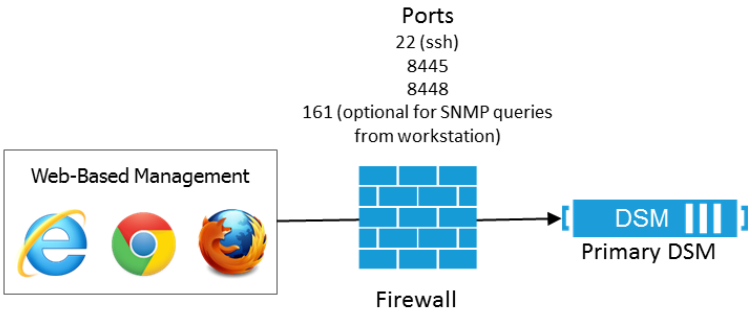


Figure 21: Ports to open between DSMs

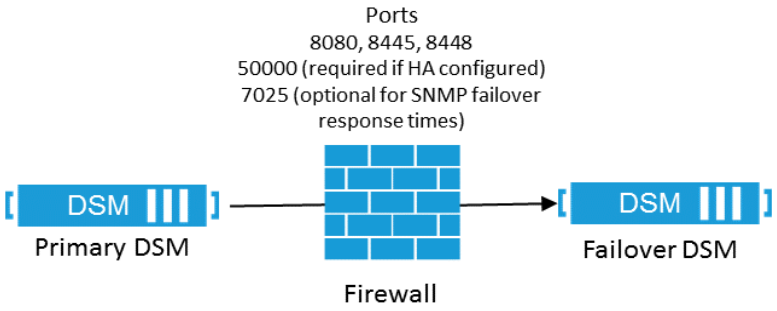
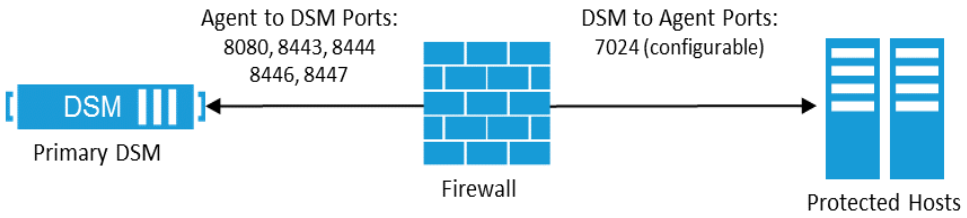


Figure 22: Ports to open between DSM and agent



The following table lists the communication direction and purpose of each port you must open.

Table 11: Ports to configure

Port	Protocol	Communication Direction	Purpose
22	TCP	Management Console → DSM DSM → SSHD Server	CLI SSH Access Auto-backup via SCP
161	TCP/UDP	SNMP Manager → DSM	SNMP queries from an external manager
445	TCP	DSM → CIFS Server	Auto-backup via CIFS
5696	TCP	KMIP client → DSM	Allows communication between the KMIP client and primary DSM
7024	TCP	DSM → Agent	Policy/Configuration Exchange
7025	UDP	DSM ↔ DSM	Uses SNMP to get failover node response time.
8080	TCP	Agent → DSM DSM ↔ DSM	Default TCP/IP port for HTTP that is used to exchange certificates between the DSMs in an HA configuration. Also, used once to perform the initial certificate exchange between an agent host and DSM.
8443	TCP	Agent → DSM	TCP/IP port through which the agent communicates with the DSM. The agent establishes a secure connection to the DSM, via certificate exchange, using this port.
8444	TCP	Agent → DSM	Agent log messages uploaded to DSM
8445	TCP	Browser → DSM DSM ↔ DSM (fallback)	Management Console, VMSSC, and fallback for HA communication in case port 8448 is dropped.
8446	TCP	Agent → DSM	Configuration Exchange using Elliptic Curve Cryptography (Suite B)
8447	TCP	Agent → DSM	Agent uploads log messages to DSM using Elliptic Curve Cryptography (ECC)

8448	TCP	Browser → DSM DSM ↔ DSM	GUI Management during enhanced security using Elliptic Curve Cryptography (Suite B). Also for secure communication between DSMs in an HA cluster.
9004	TCP	DSM ↔ nShield Connect/RFS	DSM communication with nShield Connect and its associated RFS
50000	TCP	DSM (primary) → DSM (failover)	HA information exchange
If NTP server and Syslog server are used to synchronize DSM time and forward log messages, it will require opening up following ports			
123	UDP	DSM → NTP Server	NTP Synchronization
514	UDP/TCP	DSM → Syslog Server	Logging to Syslog. Note that 514 is the default, but is configurable depending on the syslog server.

Access the Command Line Interface (CLI)

The CLI commands are used to configure the DSM. The commands are grouped into the following categories or *submenus*. Entering ? on the CLI command line lists those categories:

```
$ ?
network      Networking configuration
system       System configuration
hsm          HSM configuration
maintenance  System maintenance utilities
ha           HA configuration
ipmi         IPMI configuration
user         User configuration
exit         Exit
```

To enter a submenu, enter a name or just the first few letters of the name. To display the commands for that submenu, enter a ?. For example, the submenu `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
```

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}
0043:maintenance$ diag
usage: diag [log [ list | view LOG_FILE_NAME] | vmstat | diskusage |
hardware | osversion | uptime ]
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 enter system, then enter reboot. To return to the main level when finished, enter up.

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

Virtual Appliance Setup

This section describes how to deploy the DSM OVA file.

NOTE: The DSM virtual appliance OVA file hardware version has been upgraded to version 9. The version 9 hardware is supported on ESXi version 5.5 or later.

The installation procedure for the fastboot DSM virtual appliance and the fastboot DSM virtual appliance for CSPs, is the same as the standard DSM virtual appliance. See "Disk Re-encryption for DSM Fastboot Image" for a description of further configuration requirements for the fastboot image.

Warning! All systems created from a fastboot OVA template utilize the *same* master key for their encrypted disks. This is a security issue, as anyone with access to the OVA could potentially decrypt the disk for any system created from that OVA template. You will be prompted to re-encrypt the disk when the virtual DSM comes up after deployment, we recommend that you continue with this procedure in the interests of security. See "Disk Re-encryption for DSM Fastboot Image" for details.

1. Launch the VMware vSphere Client.

2. Click **File > Deploy OVF template**.
3. Click **Browse** and locate the OVA file. Select the file and click **Next**. The *OVF Template Details* page appears.

   The file name format for the OVA file is *Vormetric DSM - Virtual Appliance<version>.OVA*
4. Verify the details on the OVF Template page, then click **Next**. The *Name and Location* page opens.
5. Type in a name for the Virtual Appliance, then click **Next**. The *Storage* page opens.
6. Select a destination for the Virtual Appliance, then click **Next**. The *Disk Format* page opens.

   Select the type of provisioning based on the storage characteristics for your system. The options are:
   - Thick Provisioned Lazy Zeroed–creates the VM and allocates all the blocks for the VM but doesn't zero them.
   - Thick Provisioned Eager Zeroed–creates the VM, allocates and zeros all the blocks.
   - Thin Provision–creates the VM with just the header information, but it does not allocate or zero blocks.

   In the following example, we use Thin Provision.
7. Select **Thin Provision** and click **Next**. The *Ready to Complete* page displays. Select the **Power on after deployment** check box, to power on the virtual DSM after deploying the template.
8. Click **Finish** to deploy the Virtual Appliance. This takes a few minutes.
9. At the message **Completed Successfully**, click **Close**. The main screen of the vSphere Client appears.
10. If you haven't chosen to power on the virtual DSM (see step 7 above) after deploying the template, then in the left pane, select the Virtual Appliance you just created, and click the green Power On icon in the tool bar, or right-click the VM and select **Power > Power On**.

    It takes about a half hour to provision the VM and build the DSM.
11. To watch the output as the installation progresses, click the **Console** tab and click inside the console window.

    The DSM `eth0` interface is DHCP enabled by default. For DHCP to work properly you must have a DHCP Server configured to ensure that the DSM gets the correct IP address and other configuration information. However, you will still need to configure the hostname and an NTP server or time zone for the virtual appliance see the following sections; "Configure the hostname" and "Configure NTP, time zone, date, time" for a detailed description of the procedures.

    If you want to use static IP addressing for the virtual DSM appliance, see "Configuring DSM using Static IP Addressing".

Disk Re-encryption for DSM Fastboot Image

1. Once the virtual DSM has been created from the fastboot OVA template, you will be prompted to log into the virtual appliance. As this is the first log in, use the default log in credentials:

   Login: cliadmin
   Password: cliadmin123

2. You will be prompted to re-encrypt the root disk container.

   ```
   This is a fast-boot image suitable for quick evaluation of DSM.
   It is recommended to re-encrypt the disk for production systems.
   The disk re-encryption will take approximately 15 to 25 minutes.
   Do NOT power off or shut down the session manually during this
   process. If you choose to skip this step now, you can run
   'maintenance config load default' later to re-encrypt the root
   disk. Note, however, that "config load default" will destroy all
   data so you will need to take a backup first if you wish to keep
   it.
   Do you want to reencrypt now? (yes|no)
   ```

   Type yes to continue with this step. Should you choose to re-encrypt the disk later, follow the procedure described here, "Disk Re-encryption after initial setup" .

3. After the re-encryption completes and the DSM restarts, you will need to log in with the default credentials again.
4. The license agreement is displayed, type 'y' to accept and press 'Enter'.
5. When prompted, type in a new password and press 'Enter'.

The DSM root filesystem is encrypted for enhanced security. A DSM System administrator can set a passphrase at boot time to unlock the system.

NOTE: Setting a boot passphrase is not required. Users who prefer an unattended boot, can continue to use the DSM without a passphrase. However in the interest of better security, we recommend that you set a boot passphrase. See "Set boot passphrase" on page 33 for details.

Disk Re-encryption after initial setup

If you choose to re-encrypt the disk and create a new master key later after the initial setup, you need to do the following:

- If your system is part of an HA deployment, you need to break up the cluster, this procedure is described here, "Break up HA cluster:" on page 109.
- If you have any configuration information or data created after the initial setup of your DSM, backup your DSM, this procedure is described here, "Backup current DSM configuration" on page 107.

- Restore the system to factory defaults.
  - Open a CLI session and login with the CLI Administrator credentials.
  - At the prompt, type in maintenance > config load default,

    ```
    $ maintenance

    0001:maintenance$ config load default

    Loading manufacture default will wipe out all the configuration
    data and system upgrade and set the machine to the manufacture
    default. System will reboot automatically.

    Continue? (yes|no):
    ```

    Type yes to continue.
- Complete the initial configuration steps, see "Virtual Appliance Configuration" for details.
- Restore the backup, this procedure is described here, "Restore backup" on page 111.
- If applicable, recreate the cluster, this procedure is described here, "Upgrade primary node and reconfigure cluster:" on page 109.

  In the interests of security, we recommend that you set a boot passphrase, see "Set boot passphrase".

Virtual Appliance Configuration

Configure network settings

1. Access the DSM CLI and log in with the default login and password:

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

2. The license agreement is displayed, type 'y' to accept and press **Enter**.
3. When prompted, type in a new password and press **Enter**. Reconfirm your password.

Warning! Do not lose this password.

4. Navigate to the *network commands* menu. Type:

   ```
   $ network
   ```

5. Add an IP address for the DSM.

NOTE: The `eth0` interface is DHCP enabled by default. See "Configuring DSM using DHCP" for more information, and for instructions on how to switch to static addressing if desired.
We recommend that you retain the default `eth1` IP address configuration in the event that you need a recovery option to access the DSM appliance.

Type:

```
0001:network$ ip address init <DSM IP address>/<subnet mask (e.g. 16 or
24)> dev eth0/eth1
```

Example: `ip address init 192.168.10.2/16 dev eth1`

IPv6 example: `ip address init fa01::3:15:130/64 dev eth1`

NOTE: If you are connected via `eth0`, you will be disconnected at this step. Reconnect on the new IP address.

6. (Optional) If you have configured `eth0`, you can also configure an IP address for `eth1` if you want to communicate with agents on a different subnet for example, or if you want to access the Management Console from a different subnet. To configure an IP address for `eth1`, type:

   ```
   0001:network$ ip address init <eth1 IP address>/<subnet mask (e.g., 16 or
   24)> dev eth1
   ```

   Example: `ip address init 192.168.10.3/16 dev eth1`

   IPv6 example: `ip address init fa01::3:15:130/64 dev eth1`

   The following warning is displayed:

   ```
   WARNING: Changing the network ip address requires server software to be
   restarted.
   Continue? (yes|no) [no]:
   ```

   Type 'yes' to continue with the IP address configuration.

7. Add the IP address for the default gateway. Type:

   ```
   0001:network$ ip route add default table main.table dev [eth0 or eth1]
   via <IP address for the default gateway>
   ```

   Example: `ip route add default table main.table dev eth0 via 192.168.1.5`

   IPv6 Example: `ip route default table main.table dev eth0 via fa01::3:15:120`

8. Verify interface settings. Type:

   `ip address show`

9. Verify route settings. Type:
   `ip route show`

10. If you are using DNS, set the primary DNS server for the DSM. Type:
    `dns dns1 <ip address for dns server 1>`

11. If you have a second or third DNS server, set them for the DSM. Type:
    `dns dns2 <ip address for dns server 2>`

12. If you want to set the search domain, type:
    `dns search <search_domain>`

13. Show the DNS settings. Type:
    `dns show`

14. Return to the main menu. Type:
    `up`

Configure a bonded NIC device

This section describes how to aggregate the two NICs on the DSM into a single logical interface to provide load balancing and/or fault tolerance. The bonded NIC device is called `bond0`.

NOTE: In order to use the bonded NICs feature, you must ensure that your switch is configured to use Link Aggregation Control Protocol (LACP).

The DSM physical appliances have two physical NICs called `eth0` and `eth1`. Only two NICs `eth0` and `eth1` are supported. If using a virtual appliance, you must configure at least two NICs and define them as `eth0` and `eth1` in order to enable the bond0 device type. Any additional physical/virtual NICs are ignored. For virtual DSMs where only one network connector is configured for a virtual machine, the `bond0` interface cannot be enabled—the network interface itself can be up but, no IP address can be assigned to it.

The NIC bonding setting is system specific. If it is to be used for all nodes in a cluster, it must be enabled in all nodes individually.

1. Access the DSM CLI and login with your login credentials. If this is the first time you are logging in, then you will be required to accept the license agreement and change the default password.
2. Navigate to the network commands menu;
   ```
   $ network
   0001:network$
   ```
3. Enable the bonded NIC;

```
0001:network$ ip address init <ip_address>/<subnet_mask> dev bond0
```

Example: `ip address init 1.2.3.4/16 dev bond0`

In the event that a bonded NIC is being configured after the initial configuration, or after the DSM has been upgraded, if you want to reuse an IP address that was originally assigned to `eth0` or `eth1`, then you must delete that address from `eth0` or `eth1` first, and then reassign it to the `bond0` device.

4. Add a default gateway for the `bond0` device;

```
0001: ip route add default table main.table dev bond0 via
<gateway_ip_address>
```

Example: `ip route add default table main.table dev bond0 via 1.2.7.8`

If a `bond0` interface is configured after setting up the `eth0` and/or `eth1` interfaces, and it is configured with an IP address that is on the same subnet as a default gateway, that gateway configuration continues to apply. However, if you configure `bond0` with an IP address on a different subnet, you will have to reconfigure the default gateway.

5. You can change the bonding driver mode based on your requirements. There are seven modes available from 0-6. See "Bonding driver modes" for more information. Note however, that only the default options are available with each of the modes and these options cannot be changed.

   When the mode option is specified the speed option cannot be specified (i.e. the options mode and speed are mutually exclusive). In other words, `bond0` does not take the speed option and both `eth0` and `eth1` don't take the mode option. However, the MTU and up/down options can still be used for the `bond0` device.

   To set or change the mode type:

```
0002:network$ ip link set bond0 mode <mode>
```

   Example: `ip link set bond0 mode 2`

   To see what mode is currently in use type:

```
0002: network$ ip link show bond0
```

6. To disable or break up a bonded NIC type, you can use either the delete or flush command. Delete will only delete a specific IP address (multiple can be assigned) and flush will clear all assigned IP addresses.

```
0003:network$ ip address delete <ip_address>/<subnet_mask> dev bond0
```

   or

```
0003:network$ ip address flush bond0
```

   Routes that are associated with this bonded NIC device will also be deleted.

Bonding driver modes

The modes specify the bonding policies. The following modes are supported (see Table 12 below), but none of the options for the modes are configurable and take the default values for those modes, except for the `miimon` setting. The `miimon` setting specifies the MII link monitoring frequency in milliseconds, which determines how often the link state of each slave

is inspected for link failures. The `miimon` setting has a value of 100 instead of the default value of 0.

Table 12: Bonding driver modes

Mode	Name	Description	Load-balancing	Fault tolerance
0	balance-rr	Round-robin policy. Transmit packets in sequential order from the first available through the last. This is the default mode for the bonded NICs.	Yes	Yes
1	active-backup	Active-backup policy: Only one slave in the bond is active. A different slave becomes active if, and only if, the active slave fails. The bond's MAC address is externally visible on only one port (network adapter) to avoid confusing the switch.	No	Yes
2	balance-xor	XOR policy: Transmit based on the selected transmit hash policy. The default policy is a simple [(source MAC address XOR'd with destination MAC address) modulo slave count].	Yes	Yes
3	broadcast	Broadcast policy: transmits everything on all slave interfaces.	No	Yes
4	802.3ad	IEEE 802.3ad Dynamic link aggregation. Creates aggregation groups that share the same speed and duplex settings. Utilizes all slaves in the active aggregator according to the 802.3ad specification.	Yes	Yes
5	balance-tlb	Adaptive transmit load balancing: channel bonding that does not require any special switch support. The outgoing traffic is distributed according to the current load (computed relative to the speed) on each slave. Incoming traffic is received by the current slave. If the receiving slave fails, another slave takes over the MAC address of the failed receiving slave.	Yes	Yes
6	balance-alb	Adaptive load balancing: includes balance-tlb plus receive load balancing (rlb) for IPV4 traffic, and does not require any special switch support. The receive load balancing is achieved by ARP negotiation. The bonding driver intercepts the ARP Replies sent by the local system on their way out and overwrites the source hardware address with the unique hardware address of one of the slaves in the bond such that different peers use different hardware addresses for the server.	Yes	Yes

Enable DHCP on `bond0` interface

To configure a `bond0` interface using DHCP, you need to enable DHCP on that interface. The `bond0` interface inherits the IP address that was dynamically assigned to the `eth0` interface when the DSM was initially deployed.

Log on to the CLI console and navigate to the Network category of commands and enable DHCP.

Example:

```
0004:network$ ip dhcp enable bond0 version 4

WARNING: Changing network ip address may disconnect your session
and will require the server software to be restarted.

Continue? (yes|no)[no]:yes

DHCP operations may take some time, please wait....

SUCCESS: Please restart server software to pick up the changes.

0005:network$
```

Configure NTP, time zone, date, time

You must have the correct time set on your DSM server(s) as this will affect system functions such as agent registration, log timestamps, high availability cluster synchronization, and certificate exchange. Although configuring an NTP server is not mandatory, it is strongly recommended.

1. Navigate to the *maintenance commands* menu. Type
   `maintenance`
2. Show the current ntpdate settings. Type
   `ntpdate show`
3. Add a new ntpdate server. Type
   `ntpdate add <IP address/Hostname for the` *ntpdate server*`>`

   Repeat this step for each ntpdate server.
4. Activate the ntpdate server connection. Type
   `ntpdate on`
5. Show the current timezone settings. Type
   `gmttimezone show`
6. Set the country and city where the DSM resides. Type
   `gmttimezone set <country/city>`
7. Set the date. (If you used `ntpdate synch`, this step is not necessary.) Type
   `date <mm/dd/yyyy>`
8. Set the time. (If you used `ntpdate synch`, this step is not necessary.) Type
   `time <hh:mm:ss>`

   Where *hh* is 00 to 23.

9. Verify your settings. Type

```
time
date
```

10. Return to the main menu. Type

```
up
```

Configure the hostname

1 Navigate to the *system* menu. Type:

```
0001:vormetric$ system
```

2 Show the current setting. Type:

```
0002:system$ setinfo show
```

The default host name in the output is *your. name.here*.

3 Set the hostname. You must enter the fully qualified domain name for the DSM. Type:

```
0003:system$ setinfo hostname <FQHN>
```

Example:

```
0003:system& setinfo hostname dsm.company.com
```

Generate the Certificate Authority

1. Generate a new certificate authority for the DSM. Type

```
security genca
```

2. A warning is displayed, informing you that all agents and peer node certificates will need to be re-signed after the CA and server certificate have been regenerated, and the DSM server software will be restarted. Type 'yes' to continue, the default is 'no'.
3. Enter the FQDN of this DSM, the name displayed in 'This Security Server host name [FQDN of the DSM]', should be correct if you entered the host name information in the previous sections correctly. Press **Enter** to accept the name.
4. Next, enter the information required to generate the certificate. Answer the prompts:

a. What is the name of your organizational unit? []:

b. What is the name of your organization? []:

c. What is the name of your City or Locality? []:

d. What is the name of your State or Province? []:

e. What is your two-letter country code? [US]:

5. Once the certificate is signed, return to the main menu. Type

   up

Add DSM CLI console administrators (optional)

With separation of duties for good security practices, CLI administrators can only log into the CLI and administer the DSM. Management Console administrators can only log on to the Management Console to administer the DSM.

1. Navigate to the *users commands* menu. Type

   user

2. Add an administrator. Type

   add *<administrator name>*

3. When prompted, enter a password. The password criteria are:
   - Does not have repeating characters
   - Uses at least 1 upper and 1 lower case character
   - Uses at least 1 special character
4. Return to the main menu. Type up

Verify web access

The Management Console is a Web-based GUI used for day-to-day security and administration tasks. Open a browser and confirm access over HTTPS to either the DSM hostname (if configured in DNS) or the IP address defined in “Configure network settings” on page 83. Example URL:

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

If this doesn't work because, for example, port 443 was blocked by a firewall, specify port 8445. Example:

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

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

- Does not have repeating characters
- Uses at least 1 upper and 1 lower case character
- Uses at least 1 special character

Upload a license file

The first time you log on to a DSM, the dashboard displays "License file not found," and all you will see are the *Dashboard* and *System* tabs. You need to click **System**, select **License**, and then **Upload the license file**. After uploading your license file, all the other tabs for which you have licenses are available. See "Upload a license file" on page 32 for instructions about uploading a license file.

The DSM Management Console has a help icon (?) located on the right-hand side of the title bar, which is located under the menu bar, on each page of the Web UI. Click the icon for help with tasks on a specific page.

Full Disk Encryption

The DSM root filesystem is automatically encrypted for enhanced security. This feature is only available on: a fresh installation of the DSM software on the V6x00 appliances and a fresh DSM build on a virtual appliance. See "Full Disk Encryption" on page 33 for details and procedures for this feature.

This feature also requires use of the IPMI, see "Configuring IPMI" on page 38 for details and procedures for this feature.

nShield Connect Integration

DSM appliances that do not have a built in hardware security module (HSM)—DSM V6000 hardware appliance and the virtual appliance—can now be enabled to utilize an nShield Connect HSM appliance to create and protect the DSM master key. The DSM can be configured any of the following nShield appliance types; nShield Connect, nShield Connect Plus, or nShield Connect XC. See "nShield Connect Integration" on page 60 for details about this feature.

DSM Installation on bare metal using IBM SoftLayer

To install the DSM virtual appliance on a bare metal system using IBM SoftLayer, you need to have a SoftLayer account and your bare metal system in place before you begin.

Upload the DSM ISO image to the SoftLayer NAS storage

This process assumes that you have a SoftLayer account with SoftLayer NAS storage, and have set up your bare metal system.

1. Enable SoftLayer VPN access using SSL.

   Open a local secure shell session (SSH) and connect to your bare metal system using the public IP address and root password. The public IP address is available under the Configuration tab for your device. The root user password is available under the Password tab. Use the secure copy (scp) command to copy the DSM ISO image to your bare metal system.
2. Open an SSH, log into your bare metal system as root and follow the instructions to mount NAS in SoftLayer.
3. Copy the DSM ISO image to the mounted NAS directory.
4. Log into the SoftLayer portal and enable VPN access and set your VPN password.
5. Next, file a ticket with SoftLayer requesting the following:

   a: Permission to "mount" virtual media in KVM.

   b: Support to change the BIOS boot order.

   - If you are using dual-processors with multi-core, e.g., E5 CPU, then request to boot the hard disk first and CDROM second. SoftLayer locks BIOS access with a password, which is why you need to request a change in the boot order.
   - If you are using single-processor with multi-core, e.g., E3 CPU, then request to boot the IPMI CDROM first and then the hard disk. The E3 motherboard does not offer an F11 to change the boot order during boot up so we need to boot IPMI CDROM first.

   Once SoftLayer has configured your changes, you can mount the DSM ISO through virtual media using KVM.
6. Log into the SoftLayer portal and click **Devices > Device List** and select your bare metal device.
7. Click on **Remote Management** tab and click show and copy the KVM password.
8. On the **Remote Management** tab, click http://vpn.softlayer.com link to connect to the VPN.
9. When you've successfully logged into the SoftLayer VPN, you can connect to the IPMI interface. Select your device from the **Devices > Device List**.
10. Click **Actions** and select **KVM Console**.
11. Next, another browser popup will redirect you the IPMI login screen. Log in as *root* user and the associated password, from the **Remote Management** tab.
12. After you have logged into IPMI, click **Virtual Media > CDROM image**.
13. You need to fill in the following information: Share host, path to image, user name, and password. This is the same information for mounting SoftLayer NAS. You can reuse the

information from **Storage > File Storage**. Use the NAS IP address instead of the DNS name for the Share host field. Ping the NAS hostname to get the IP address.

14. Click **Mount** and **Refresh Status**. Device 1 should show as mounted. Make sure that you've requested mount permission from SoftLayer support first. Otherwise, you cannot mount the virtual CDROM.
15. Click **Save** to save the information.
16. Navigate to **Remote Control > Console Redirection** and click **Launch Console**.
17. Download and run the resulting `.jnlp` file to open a Java console for your DSM.
18. From the power control menu in the Java Console, power cycle the DSM.
19. Wait for the DSM to boot up. It will try to boot from network first, time out, and then boot from the ISO image.
20. Click **Enter** when you see the "Thales" banner to begin the installation.

    If you receive a message saying “cannot find kickstart file”, type cdrom1 at the boot prompt when you see the Thales banner. The installation will proceed as normal.

Configure Virtual DSM in SoftLayer

As of v6.0.2 the DSM `eth0` interface has DHCP enabled by default. If you have a DHCP server configured, your virtual appliance will obtain an IP address from that server. See “Configuring DSM using DHCP”, for more information about DHCP for DSM. If you want to assign a static IP address to your virtual DSM device, see “Configuring DSM using Static IP Addressing”, for how to disable DHCP. Follow the procedure below to assign a static IP address for your virtual DSM device.

1. Gather the required system information from the Device menu option. You need the following information for network port 0 (private network) and port 1 (public network):
   - Hostname
   - IP address
   - Subnet mask
   - Gateway address

   Once you have this information, you need to log into the DSM CLI to configure the virtual device.
2. Open an SSH and log into the CLI via the public IP address of your bare metal system using cliadmin as the user name. For example: ssh cliadmin@<public IP address>

   The default cliadmin user password is cliadmin123. You will be prompted to change the default password.

   Type network at the prompt to enter the network category command menu and follow the steps below. Note that the IP addresses are used as *examples*:

- Delete the default IP Address, type:

```
0001:vormetric$ network
0002:network$ ip address delete 192.168.10.1/16 dev eth0
```

- Add private IP Address, type:

```
0002:network$ ip address add 10.114.160.214/26 dev eth0
```

- Add public IP Address, type:

```
0002:network$ ip address add 169.53.182.122/28 dev eth1
```

- Add default public gateway, type:

```
0002:network$ ip route add default table main.table via 169.53.182.113
```

- Add default private gateway, type:

```
0002:network$ ip route add 10.0.0.0/8 table main.table via
10.114.160.193
```

- Clear DNS, type:

```
0002:network$ dns clear
```

- Add DNS1, type:

```
0002:network$ dns dns1 10.0.80.11
```

- Add DNS2, type:

```
0002:network$ dns dns2 10.0.80.12
```

- Change hostname. Go up one CLI level by typing ‘up’ at the prompt. Type:

```
0002:network$ up
0003:vormetric$ system
0004:system$ setinfo hostname dsm523.softlayer.com
```

- Verify the IP address, at the prompt type:

```
0001:vormetric$ network
0002:network$ ip address show
```

- To verify route settings, type:

```
0001:vormetric$ network
0002:network$ ip route show
```

- To verify DNS settings, type:

```
0001:vormetric$ network
0002:network$ dns show
```

- To verify hostname, type:

```
0001:vormetric$ system
0002:system$ setinfo show
```

NOTE: SoftLayer does not allow reverse lookup of hostname in Softlayer unless you have your domain name. If you want to use DNS for name resolution in Softlayer, you can either register your own domain or setup a DNS server within Softlayer.

See"Generate the Certificate Authority" on page 89, to complete the DSM configuration.

DSM Installation on Hyper-V

This process assumes that you have Hyper-V installed and running with at least one virtual switch for the DSM virtual appliance to use to connect to the network.

1. Open Hyper-V Manager. Click **Start**, point to **Administrative Tools**, and then click *Hyper-V Manager*.
2. From the **Action** pane, click **New**, and then click **Virtual Machine**.
3. In the **New Virtual Machine** Wizard, click **Next**.
4. On the **Specify Name and Location** page, specify the name of the virtual machine and where you want to store it.
5. On the **Generation for the Machine** page, select "Generation 1" for the virtual machine.

NOTE: Generation 2 does not support CentOS 5.x

6. On the **Memory** page, specify a minimum of 4GB memory to run the guest operating system for the virtual machine.

   We recommend that you disable the **Use Dynamic Memory for this virtual machine** option, which is enabled by default. This is to prevent memory over commits.
7. On the **Networking** page, connect the network adapter to an existing virtual switch to establish network connectivity at this point. A second (optional) switch can be added later if desired.

   If you want to use a remote image server to install an operating system on your test virtual machine, select the external network.
8. On the **Connect Virtual Hard Disk** page, select **Create a virtual hard disk**. Specify a size for the virtual hard disk based on the number of agents you plan to install.

   Refer to Table 9, "Hardware requirements for Virtual Machine," on page 72, for the virtual machine hardware requirements.
9. On the **Installation Options** page, select the following option to install the operating system:

Install an operating system from a boot CD/DVD-ROM. Click **Browse** to navigate to the DSM ISO file location and select the file. Click **Next**.

10. Review your selections and click **Finish**.
11. Connect to the virtual machine console, and power on the machine to build the DSM.

NOTE: Make sure the hard drive is set as first in the boot order, *before* you power on your virtual machine.

12. Once the DSM has been built, see "Configuring a Virtual Appliance" for details about how to configure the DSM.

Deploying a DSM Azure Image

This section describes how to install the DSM Azure image. The image is available on the Azure marketplace: `https://azuremarketplace.microsoft.com/en-ca/marketplace/`.

Requirements

- A Microsoft Azure account
- Knowledge of the following:
  - Creating Azure instances
  - Networking and storage configuration basics

Deployment Procedure

To ensure the proper deployment of a DSM Azure image, Thales recommends the configuration parameters described below:

1. Log on to the Azure portal with your credentials.
2. From the Dashboard, click **Create a Resource** on the upper left corner of the Azure portal.
3. In the search field, type: Thales.
4. Select the latest version of Vormetric Data Security Manager from Thales eSecurity.
5. After reading the online material, click **Create**.
6. Enter the following details for the virtual machine:
   - Virtual machine name.
   - Select **HDD** as the VM disk type.
   - In the User name field, type **cliadmin**. This is the default user available on the DSM during initial start up.
   - For Authentication Type, select **Password**. You cannot use this password when the DSM initially launches. You will need to use the default user credentials to log on for the first time, see“Virtual Appliance Configuration” for more information.
   - For Subscription, Pay-As-You-Go is the default option.
   - If you plan to create a new resource group, select **Create New** and enter a name for the group.

     If you have an existing resource group that fits your requirements, select **Use Existing** and select that group from the drop-down list. Refer to the Azure documentation for more information about resource groups.
   - Choose a location to host the virtual machine.

7. Click **OK**.
8. Select a size for the virtual machine. If you plan to use the DSM in a production environment, refer to "Virtual machine hardware requirements" and select a size for your VM.
   - Minimum requirements: 2 virtual CPUs, 8GB RAM and 250GB hard disk size
   - Recommended size: 4 CPU/14GB RAM
9. In the Settings section, enter the following details:
   - For **High Availablility**, set to **None**.
   - For **Storage**, click **Yes** for Use managed disks.
   - For **Network**, if you selected an existing resource group, then the virtual network will be selected by default from that resource group.

     To create a new virtual network, click the arrow, enter a name and accept the default settings.
   - Accept the default settings for **Subnet**.
   - For **Public IP address**, select Assignment: **Static**.
   - For **Network security group**, accept the default settings and enter a name for the group. You can select an existing group if you know that it applies to your requirements.
   - For **Auto-shutdown,** select **Off**.
   - For **Monitoring**, in **Boot diagnostics** and **Guest OS diagnostics,** accept the default settings.
   - For **Diagnostics storage account**, you can choose to create an account or select an existing account if it fits your requirements.
   - For managed Service identity, click **Yes** to control access to the storage account.
10. Click **OK**. Review the **Summary** and click **Create** to start the virtual machine deployment.

Configure the Hostname

After launching the virtual DSM, you must configure a hostname.

1. Navigate to the Dashboard on the Azure portal and search for the newly configured DSM.
2. Click the name of the virtual DSM. A summary of the instance is displayed in the top panel.
3. Under DSN name , click **Configure**.
4. Enter a name for the host in the **DNS name label** field.

NOTE: Although this field is tagged optional, it is required for the virtual DSM to complete the configuration.

5. Click **Save**.

Return to the **Dashboard > Overview** page. Under **DNS name**, you now see the FQDN for this instance—the hostname and the complete domain hierarchy.

6. Copy the FQDN to a location that you can access from the DSM CLI.
7. SSH to the DSM CLI. The first time you log on to the DSM CLI, you must log in with the default user name and password:

   Login: cliadmin

   Password: cliadmin123
8. A message asks "Do you want to re-encrypt the disk now? (yes|no)[no]:". Click **yes** if you plan to use this disk for anything other than a quick evaluation.
9. Accept the license agreement and then type in a new password when prompted.
10. Navigate to the System menu, type:

    ```
    0001:vormetric$ system
    ```
11. Enter the FQDN that you copied to the clipboard to set the hostname, type:

    ```
    0002:system$ setinfo hostname <FQDN>
    ```

    Example:

    ```
    0002:system$ setinfo hostname mycompany.vdsm.westus.cloudapp.azure.com
    ```

Generating the CA

After configuring a hostname, you must generate the DSM certificate authority.

1. Generate a certificate authority for the virtual DSM instance, type:

   ```
   0003:system$ security genca
   ```

   A warning displays, informing you that all agents and peer node certificates will need to be re-signed after the CA and server certificate have been regenerated, and the DSM server software will be restarted. Type 'yes' to continue, the default is 'no'.
2. Enter the FQDN of this DSM. The name displayed in 'This Security Server host name [FQDN of the DSM]', should be correct. Press **Enter** to accept the name, or enter the FQDN that you copied to the clipboard.
3. Enter the information required to generate the certificate. Answer the prompts:
   - What is the name of your organizational unit? []:
   - What is the name of your organization? []:
   - What is the name of your City or Locality? []:
   - What is the name of your State or Province? []:
   - What is your two-letter country code? [US]:

4. Once the certificate is signed, you can access the virtual DSM through the web-based GUI. Open a browser and confirm access over HTTPS to the DSM hostname. Example URL: `https://dsm.vormetric.com`

   If this does not work because, for example, port 443 was blocked by a firewall, specify port 8445. Example URL: `https://dsm.vormetric.com:8445`.

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

Configuring a Failover node

1. Add the failover node to the primary node:

   a. On the primary node, log on to the Management Console.

   b. Click **High Availability** in the menu bar. The *High Availability Servers* window opens.

NOTE: The license must be installed on the primary DSM before HA can be configured.

   c. Click **Add**. The *Add Server* window opens.

   d. In **Server Name**, enter the host name or FQDN of the failover node.

   e. Click **Ok**. The failover node is listed in the **High Availability Servers** table with the role of Failover.

2. Register the failover node with the primary node, see "Registering DSM2 as a failover with DSM1" on page 141.
3. Configure replication, see "Configuring replication" on page 143.

Deploying a DSM AWS image

This section describes how to install the DSM AMI on Amazon Virtual Private Cloud (VPC). Refer to Amazon's documentation for more information about VPC. Contact Thales Support to obtain the image.

Requirements

- An Amazon Web Services (AWS) account, with a VPC and subnet
- The DSM AMI template
- Knowledge of the following:
  - creating AWS instances

- command line interface of your host operating system
- how to open TCP and ICMP port connections on your protected hosts
- network and storage configuration basics

Installing DSM

The DSM AMI is visible on the EC2 Dashboard under Images > AMIs.

1. Select the DSM AMI and click **Launch** at the top of the page or right-click the AMI file and select **Launch** from the pull-down menu.
2. Select the instance type. If you plan to use the DSM in a production environment, the minimum requirements are: 2 virtual CPUs, 8GB RAM and 250GB hard disk size, refer to "Virtual machine hardware requirements" for details. The t2.large image has the minimum required configuration; 2 vCPUs and 8G RAM. Click **Next**.
3. Select the number of DSM instances to create, this is set to 1 by default. To set up a high availability (HA) configuration, enter the total number of nodes (up to a maximum of eight including the primary node) to launch them simultaneously, if you plan to have the HA cluster nodes in the same region. If you want to use different regions you will need to change your region and repeat these steps.

   Refer to the HA chapter in *DSM Administrators Guide* for more information about configuring and managing a DSM HA cluster.

   Configure the instance details by selecting the following network requirements:

   - **Network**—select an existing VPC or if you need to, create a new one, refer to the Amazon documentation for any help you require.
   - **Subnet**—select an existing subnet, or if you need to create a new one, refer to the Amazon documentation for any help you require.
   - **Auto-assign Public IP**—change the setting **Use subnet setting** to **Disable**, which means no IP address is assigned. You can set the IP address later by clicking **Elastic IPs** and allocating an IP address for the DSM instance.
   - **Termination protection**—we recommend that you enable this setting to avoid accidentally terminating a DSM instance.

   Click **Next**.
4. The **Add Storage** page displays, accept the default size of 250GB, or increase it per your requirements and click **Next**.
5. Click **Add Tags** page, in the Key field type "Name" and enter a name for the DSM instance in the "Value" field, click **Next**.

6: If you already have an existing correctly configured DSM security group, select that security group. Or, on the **Configure Security Group** page, configure the following ports:

Table 13: Port Configuration

Protocol	Port (service)	Source
ICPMPl	All—used to run Ping	0.0.0.0/0
TCP	22 (SSH)	0.0.0.0/0
TCP	443 (HTTPS)—redirected to 8443 unless the DSM is in suite b mode, in which case it is redirected to 8448	0.0.0.0/0
TCP	5696—for KMIP	0.0.0.0/0
TCP	8080 (HTTP)—agent registration	0.0.0.0/0
TCP	8443(HTTPS)—agent communication with the DSM	0.0.0.0/0
TCP	8444—to upload agent logs to the DSM	0.0.0.0/0
TCP	8445—DSM web UI	0.0.0.0/0
TCP	8446—certificate exchange in suite b mode	0.0.0.0/0
TCP	8447—to upload agent logs to DSM in suite b mode	0.0.0.0/0
TCP	8448—DSM wen UI in suite b mode	0.0.0.0/0
TCP	50000—HA information exchange	0.0.0.0/0
UDP	161—SNMP queries from external manager	0.0.0.0/0
UDP	7025—SNMP	0.0.0.0/0
UDP	123—NTP synchronization, if an NTP server is being used	0.0.0.0/0
UDP/TCP	514—logging to Syslog server, if one is being used.	0.0.0.0/0

Click **Review and Launch**.

7: Review the summary of the settings you selected and then click **Launch**. You will be prompted to select an existing key pair, or create a new one. The private key is required to use SSH to connect to the DSM instance.

After you've launched the DSM instance you need to allocate an Elastic IP address and associate it with the DSM instance.

- Click **Allocate New Address**, select **EIP used in VPC** and **Yes, Allocate**. You can also associate and existing IP address that is not being used elsewhere.

- Select this new address, click **Associate Address** and select the host instance on which to associate the EIP.
- Use this EIP address to set up your SSH session.

NOTE: Deploying the DSM AMI may take some time to complete and the some of the status checks on the dashboard may display as failed, this is no cause for concern, the status will change to passed once the deployment is complete.

Configuring HA

To set up an HA cluster in multiple regions, copy the DSM AMI to the regions where you want to locate the other nodes. To do this, go to **Images > AMIs**, and either select or right-click the AMI and then choose **Copy AMI**. A dialog box displays with the following options

- Destination region
- Name
- Description

Select the region to copy the AMI to. The name is pre-populated but, you can change it as per your requirements. The description is also pre-populated, again you can change it as per your requirements. To initiate the copy, click **Copy AMI**.

KVM Deployment

This section describes how to deploy a KVM image using the virt-manager desktop interface and using the virtsh command line tool. If you choose to deploy the KVM image using virtsh, you must also download the XML file that is provided.

virt-manager

1. Launch the virt-manager software, click **File > New Virtual Machine**.
2. Select **Import existing disk image** and click **Forward**.
3. Browse to your `.qcow2` file and select it.

   Choose Linux/CentOS 7.0 for the **OS type/Version** and click **Forward**.
4. Set RAM to 4096 MB minimum, CPUs to 4 minimum, and click **Forward**.
5. Name your virtual machine and select your network adapter. For a bridge, select **Specify shared device name** and enter the name for your bridge device, for example "br0".

6: Check **Customize configuration before install**.

7: Click **Finish**.

8: You can now add or modify your hardware selections. Add another NIC now if desired.

9: Set the CPU topology, the recommended configuration is:

- 1 Socket
- 4 Cores
- 1 Thread

  Set this and click **Apply**.

10: Click **Begin Installation** to start the virtual machine.

virsh

1. Edit the XML file and change the virtual machine name and description to your requirements. The name of the XML file and the virtual machine *must* be the same. Rename the XML file as necessary.
2. In the XML file, change the path to the location where you saved the `.qcow2` file. You must change it to the absolute path.
3. Change name of the bridge devices (there are two NICs) to match existing bridge(s) or create a bridge "br0" to match.
4. Change the UUID for the virtual machine, as well as the MAC addresses for the two NICs as necessary.
5. To start the virtual machine, type the following command at the prompt;

   `virsh create <xml_filename>`
6. Connect to the VM using a VNC viewer from the local host.

   Example: vncviewer localhost:0.

High Availability (HA) Configuration for Virtual Appliances

See "Configuring HA for V6000 and Virtual Appliances" on page 140 for procedures to configure high availability.

5 Upgrade and Migration

This chapter describes how to upgrade your DSM software version to the latest DSM v6.0.3 version. It describes how to migrate from older (V5800) hardware appliances to the new V6x00 hardware appliances. It also describes how to enable Remote HSM Management for the V6100 appliance.

Warning! Thales strongly recommends that you backup your DSM configuration *before* upgrading or migrating to a new version. An upgrade *cannot* be rolled back. The only way to go back to a previous version is to restore a backup of the DSM configuration that was made before the upgrade, to the version of the software in use before the upgrade.

This chapter contains the following sections:

Overview

The software on a DSM appliance can always be upgraded to the next immediate release version. In some cases upgrades to higher version while skipping intermediate releases is also possible.

In a scenario that involves a platform change, it is called a migration. A migration is when you upgrade the DSM hardware appliance (currently the V5800 appliances), to the new V6x00 appliances.

Both upgrades and migrations are described in the sections below, including upgrades and migrations when using DSM with KMIP.

Supported Upgrade Paths

In order to upgrade to DSM v6.0.3, you must be at v6.0, v6.0.1, or v6.0.2. To upgrade from release 5 versions of the DSM software, you need to upgrade to v6.0 before you can proceed with upgrading to the latest version, refer to the release notes or contact Thales Support for more information.

The procedures to upgrade a standalone DSM are described in “Upgrading a Single Node Deployment”, and to upgrade an HA deployment, follow the procedure described here, “Upgrading an HA Deployment”.

NOTE: If you are upgrading from an earlier version of DSM v5.3 or v5.3.1 with KMIP data, contact Thales e-Security Support.

The following appliance upgrade paths are supported:

Table 1: DSM hardware appliance upgrade paths

Minimum supported version	Upgrade to version 6.0
V6x00 appliance with DSM version 6.0 installed.	Yes
V5 hardware appliance (no HSM) with DSM version 6.0 installed.	Yes
Virtual DSM appliance with DSM version 6.0 installed.	Yes
V5 hardware appliance (with HSM) with DSM version 6.0 installed[a]	No

a. However you can migrate from a V5800 with HSM appliance to a V6100 appliance, see “Migrating from V5 appliances to V6x00 appliances”

Upgrading the DSM

This section describes how to upgrade the software on a DSM appliance. Before you upgrade your DSM, make sure you are at the minimum required version of the software that supports the upgrade path you want to follow.

NOTE: As of release v6.0.3 the DSM supports nShield Connect integration to make the DSM V6000 or virtual DSM a network HSM-enabled DSM. See, "nShield Connect Integration" on page 60 for details.

Upgrading a Single Node Deployment

This section describes upgrading a standalone DSM appliance.

Backup current DSM configuration

1. A wrapper key is required to create a system level backup of the DSM. If you have not created a wrapper key, do the following, else skip to step 11.
2. Log on to the Management Console as an administrator of type System Administrator or All.
3. Select **System > Wrapper Keys** from the menu bar.
4. On the *Wrapper Keys* page, select **Create** from the **Operation** menu, then click **Apply** to create the wrapper key.
5. You will see a confirmation message stating that the key exists. The same confirmation message is also displayed on the *Manual Backup and Restore* page with a message saying you can proceed with creating a backup.
6. You must export this wrapper key in order to use it, select **Export** from the **Operation** menu to export key shares.
7. Set a number for both the **Minimum Custodians Needed** and the **Total Number of Custodians**. This setting splits the wrapper key value among multiple custodians. If only a single administrator is to control the wrapper key, enter a value of 1 in both fields.
8. Select the check box next to the DSM administrators who will serve as custodians for the wrapper key shares. Administrators of type System Administrator and All are listed. Any of these administrators, with the exception of the default initial log-on administrator *admin*, can be selected as a custodian.

   If more than one custodian has been selected, each of them is given a share of the wrapper key. The wrapper key share is displayed on their *Dashboard* page when they log into the Management Console. Each administrator must see a unique wrapper key share displayed on the dashboard beneath the fingerprint for the CA.

9. Click **Apply** on the bottom right hand corner. The generated wrapper key or key shares are exported and is visible on the *Dashboard*, beneath the fingerprint for the CA. The **Wrapper Key Share** displayed in the *Dashboard* window is a toggle. Click **Show** to display the wrapper key share value. Click **Wrapper Key Share** value to display the string **Show**.
10. Each administrator must securely store a copy of this key share. They must provide this as part of their role in a DSM restore operation.
11. Log on to the Management Console as an administrator of type System Administrator or All.
12. Select the **System > Backup and Restore** menu option. The *Manual Backup and Restore* page opens.
13. Click the **Backup** tab and select **Ok**.
14. Click **Save** in the **File Download** dialog box. Save the file to a secure location that you are sure will still be accessible if the server fails. By default, the file name will be in the format:

    backup_config_<dsm server name>_yyyy_mm_dd_hhmm.tar

    Where <*dsm server name*> is the FQDN of the DSM that is being backed up.
15. Save the backup to a secure location.

Upgrade Server Software:

1. Select **System > Software Upgrade**. The *Upgrade Software* window opens.
2. If two software images are present, click **Delete Idle Version** to delete the version not in use.
3. Click **Browse** and select the upgrade file that was provided to you by Thales Support.
4. Click **Open**, and then click **Upgrade** to start the upgrade. Follow the directions on the screen.
5. Refresh your browser to view the log in screen after the upgrade completes.

Enable DHCP

You can now choose to enable DHCP on the appliance:

Log on to the CLI console and navigate to the Network category of commands and enable DHCP.

Example:

```
0004:network$ ip dhcp enable bond0 version 4

WARNING: Changing network ip address may disconnect your session
and will require the server software to be restarted.

Continue? (yes|no)[no]:yes

DHCP operations may take some time, please wait....

SUCCESS: Please restart server software to pick up the changes.

0005:network$
```

To configure a `bond0` interface using DHCP, enable DHCP on that interface. The `bond0` interface inherits the IP address that was dynamically assigned to the `eth0` interface when the DSM was initially deployed.

Upgrading an HA Deployment

If you are upgrading an HA deployment, the procedure is as follows:

1. Backup your current DSM configuration, as described above, "Backup current DSM configuration".

   If synchronization is in progress anywhere in the cluster, wait until it completes before upgrading each of the nodes in the cluster.

Break up HA cluster:

1. On the primary node, log on to the Management Console as an administrator of type System Administrator or All.
2. Navigate to the *High Availability* page, select a failover server and click **Cleanup Replication**, and then click **OK** when prompted to proceed with cleanup.
3. Repeat step 2 for each failover server.
4. When all failover servers are independent of the primary server, no more updates are pushed to the failover servers. The agents continue to be serviced by the failover servers while the primary is upgraded.

Upgrade primary node and reconfigure cluster:

1. Select **System > Software Upgrade**. The *Upgrade Software* window opens.
2. If two software images are present, click **Delete Idle Version** to delete the one which is not being used.
3. Click **Browse** and select the upgrade file that was provided to you.
4. Click **Open**, and then click **Upgrade** to start the upgrade. Follow the directions on the screen.
5. Refresh your browser to view the log in screen after the upgrade completes
6. Upgrade each of the failover nodes per step 4.
7. Once the software on each of the nodes is complete, reconfigure the HA cluster:

   a. Log on to the CLI of the failover server.

   b. Type ha to access the HA category of commands.

   c. Type `convert2failover`.

   d. Follow the instructions to enter necessary data.

e. Wait until the conversion process is complete. This could take several minutes.

f. Log on to the Management Console on the primary DSM as a user of type System Administrator or All.

g. Select the failover server in the *High Availability Servers* window and click **Config Replication**.

h. Repeat steps **a** through **g** on each failover node, one at a time. Wait until synchronization is complete.

The upgrade is complete.

NOTE: If you plan to enable nShield Connect integration on a DSM V6000 or virtual DSM appliance cluster see, "Configuring High Availability for network HSM-enabled DSM" on page 64.

Migrating from V5 appliances to V6x00 appliances

The V5800 with HSM appliances do not support DSM v6.0 or later. If you want to start using DSM v6.0 or later, on a DSM with HSM appliance, you must purchase the V6100 appliance. This platform change is called a migration. A V5800 appliance without HSM can be upgraded to DSM v6.0 or later, follow the procedure described here, "Upgrading the DSM".

The high-level steps to migrate from a V5800 hardware appliances to V6x00 hardware appliances are described here:

1. Backup your DSM configuration to ensure you have a copy of the latest configuration before starting the migration. You will need a wrapper key to create the backup, create one if you have not already done so. Make sure you export the wrapper key or wrapper key shares used to create the backup. The wrapper key is required to restore the backup. See "Backup current DSM configuration" for detailed procedures.
2. Turn off the old hardware appliance and take it off the network. You must turn off the old DSM hardware appliance and remove it from the network, before you restore the DSM to the new hardware appliance, otherwise any registered agents will try and communicate with both the old DSM and the new DSM and cause conflicts in your system.
3. Configure the V6x00 appliance as described in the *DSM Installation and Configuration Guide*.
4. Assign the new V6x00 appliance with the same IP address and the FQDN of the primary V5 appliance from which you are migrating.
5. Run the `security genca` CLI command on the new appliance.
6. Import the wrapper key shares to the new V6x00 appliance.
7. Restore the backed up DSM configuration to the new V6x00 appliance.

Restore backup

1. Log on to the Management Console as an administrator of type System Administrator or All.
   a. Import the wrapper keys used to create the backup. Select **System > Wrapper Keys** from the menu bar.
   b. Select **Import** from the Operation pull-down menu and click **Add**.
   c. If you have created key shares from the wrapper key, get the key shares from the custodians and paste a key share value into the **Key Share** text field and click **Ok**. Repeat this for each administrator selected as a key custodian, if you have chosen to have more than one custodian for the wrapper key shares. A key share must be imported for at least as many as were specified by the **Minimum Number of Custodians** value when the wrapper key was exported.

      Click **Apply** to finish importing the wrapper key.

d. Restore the backup file. Select **System > Backup and Restore** from the menu bar. Select the **Restore** tab.

e. Click **Browse** to locate and select the backup file to restore. Click **Ok**. The restored file uploads and the DSM disconnects from the Management Console.

f. Log back in to the Management Console as an administrator of type Security or All. Verify that the configuration is restored correctly.

Once restore procedure is complete, log in to the DSM and verify that the KMIP keys and secret data are available.

Migrating from V5 appliances to V6x00 appliance (KMIP)

If you use KMIP with your DSM V5800 (with or without HSM), and you want to continue using KMIP with the new V6x00 appliances, contact Thales Support before you migrate to the new appliances.

NOTE: The V5800 with HSM appliance ***does not*** support the v6 release of the DSM software.

The procedure to migrate to the new V6x00 appliances is the same as described above.

Enabling Remote Administration for Upgraded V6100 Appliances

This section describes how to enable remote HSM administration after upgrading the DSM software version on the V6100 appliance. For more information about supported upgrade paths see “Supported Upgrade Paths”.

The remote administration feature is turned off by default and must be enabled.

If you choose to switch to using remote administration, you will need to plan maintenance windows for the following tasks;

- Upgrading DSM software; if this is part of a cluster, each node will have to be upgraded
- Enabling remote administration; requires installing a KLF2 warrant from Thales Support, which takes up to 24 hours to obtain.
- Replacing the ACS; if this is part of a cluster, you need to enable remote administration on each of the nodes and this requires obtaining a warrant for each node

The warrant, which is similar to a digital certificate, is a security requirement for remote administration. You will need to apply to Thales Support to obtain the warrant. The steps to obtain a warrant are outlined below.

Requirements for Remote HSM Administration

If you choose to use the remote administration feature, after upgrading to DSM software v6.0, the following are required:

- Trusted verification device (TVD) and card set. Contact your Thales Sales representative for more information.
- Obtain a KLF2 warrant.
- Replace the old card set with the new card set, see below for detailed procedure. Should you choose to, you can continue to use the existing card reader along with the remote administration TVD and card set.

Obtain a warrant

Once you have received your TVD and card set, obtain a warrant from Thales Support.

1. Move the mode switch on the back panel of the appliance to the Operational (**O**) position.

IMPORTANT: The switch must remain in the Operational (**O**) position at all times after upgrading to version 6.0.1 of the software.

2. At the prompt type;

   ```
   0001:vormetric$ hsm
   ```

   to enter the **hsm** sub-menu.

3. The `remoteadmin show` command will display the status of this feature, type

   ```
   0001:hsm$ remoteadmin show
   ```

   If the feature is not turned on, you will see the following output on the CLI;

   ```
   HSM warrant needs to be upgraded to KLF2 for remote administration
   HSM remote administration is disabled
   SUCCESS: remoteadmin command ran successfully
   0001:hsm$
   ```

4. Next you need to enable remote administration, type;

   ```
   0001:hsm$ remoteadmin on
   HSM warrant needs to be upgraded to KLF2 for remote administration
   The warrant in this HSM needs to be upgraded for remote administration
   to work.
   If you've already received the signed warrant from Vormetric support,
   enter the content of the warrant file (copy and paste) and end with a
   blank line. If not, please send an email to Vormetric support
   (support@vormetric.com) with the following information to request a
   warrant upgrade:
   ```

```
ESN: B0FF-8213-3E55
Content of the CSR file /opt/nfast/kmdata/warrants/csr_B0EG-8218-3F55:
0a00000014000000210e59ed694e5d0fe1aa8e31a654b795dfe60d5414000000f135b1
e84d5269b30ca5c1328bc7a2505c03bf09dc0000000400000000900000020020000200
00000f000000423045462d383231382d33453535000000d0000002249d39dc0294ac1ec
58b1c9a2f336c8159bcc3c2e0000000600000000000000440000000507b04338782583
2949dce4295499615903b32b9acbe88c8a9535762c9b6d0debced6e381149b6ab4a84a
1d42a0d24f7eec6b6d1a9bc1802c6bc6e1b4c4e03dac01000044000000ebff58428d7e
25a5c5992fe5d5d04b1a8ca2eed62116b8c516c715e7036fd28364592587c66c36551a
25da1df37073f4001d6325d5f6877ab4ebc2f805ffd54ebf000000bb000000
Enter the contents of the warrant file (copy and paste) followed by a
blank line or just press Enter to abort.
```

Copy and paste the contents, including the ESN and the content of the CSR file and email it to Support (support@vormetric.com). You will receive the signed warrant within 24 hours.

5. Copy the contents of the warrant file you received at the prompt;

```
KLF2 Warrant for B0FF-8213-3E55
6E4369706865722D6865782D4B4C463257617272616E74000000039E93374B57
41524E2D31B2375061796C6F6164C5EFB33B44656C65676174654B6579435 45
43445341365075626C6963384E4953545035323192F4C542014450694D476864
B5B6D5EB57ABC19CDE258232029F59988B5DF7A5326D1FD780344F9ED8E2AF34
AAB987F18163B5A1205C68D2563B2602AB01633E90BB51CB1E05F4C54201D46C
0D3D17BDEC2584930DC77011E3A734098018681A5886BDEAFA952894B5E08F2D
8E625F2C3BAF1088008F1FD20A4F3A17F0B905400A1000376DA3C124AFC7D137
5369674D656368923545434453419235454D534131365348413531 32C4165761
7272616E744365727469666696361746554797065 3A44656C65676174696F6E39
5369676E6174757265C5840021CDF6DEE1FBEB059B7A09C22FFCA50D6BD26AC4
8B1AFB7CB37A9022165589EBB1F3579C80BEDACCBC0930521EA7BD6566C8B2C8
92944533EAE39AE15F4614B28A00E7B0093E043FDF38776159DA1ABD5C5602EE
799DA9D3951022F8D4289E7D8F0A7D55D58BDF01649AD0CA20F6477DBE9B5A78
69BCFE4E665F8EA9F0536A99A016D7B2375061796C6F6164D5016FB6C416456C
656374726F6E696353657269616C4E756D6265722E423045462D383231382D33
453535C41450687973696361 6C53657269616C4E756D6265722933362D4A3332
38383939417070726F76616C7391943746495053313430020 3C4114D756C7469
43686970456D626564646564C41657617272616E744365727469666963617465
54797065C41D4669656C645570677261646 54D6F64756C65496E666F726D6174
696F6E374B4C463270756294354543445341365075626C6963384E4953545035
323192F4C54201AC3DE0C4B4E1C66B2C80C19B1A6D6BEC7E4FD2A0421D4AA8B4
6A9B1481E3D6CEEB0D6D9B2C7635958A8CE8CB9A2BB3035961995429E4DC4929
8325783843B00705F4C541BF4ED5FF05F8C2EBB47A87F6D525631D00F47370F3
1DDA251A55366CC68725596483D26F03E715C716C5B81621D6EEA28C1A4BD0D5
E52F99C5A5257E8D4258FEEB384B4C46326D6563689235454343453419235454D
534131365348413531323953696 76E6174757265C584001A5B42B33DA5444F63
6ED39EF37FF086CCC7DE9512F676C30A469B8167E1534EB08F86913ADE3EBEAC
BF4A34E79B6BAF6BB1D1EE16413D37BDFF58CE6F7B122EE2003A92CFF4548B77
```

```
4AF280F0354A96F2668CBD1A0217322D40C239E5F39FEC142E25952594626338
99D8890E95A0FB23BA94DA8AA44118AA8ED804770D236F299C26C4387975F3A3
CDB62276BA301BC4DC112E246A4F000000000000000000000000000000000000

Warrant for module B0FF-8213-3E55 installed
HSM remote administration is enabled
SUCCESS: remoteadmin command ran successfully
```

On entering the contents of the warrant file, remote administration is enabled.

Replacing the ACS

After enabling remote administration, you need to replace the old card set with the new card set. Replacing the ACS does not recreate a copy of the old ACS, but creates a completely new ACS to access the security world (the primary and failover DSMs) that replaces the old ACS.

NOTE: You may also want to run a replace ACS procedure if you lose a card from the smart card set, or if a card is compromised, or corrupted.

If you have a DSM backup created using the old card set, you should retain that old card set in case you want to restore the backup, in which case, *do not* erase the old card set when prompted during the `replaceacs` procedure.

ACS replacement guidelines

- Obtain a set of blank cards equal to N.
- You cannot change K or N when you replace the ACS.
- As a precaution, make a backup of your encrypted data before replacing the ACS. Note that this backup of the encrypted data will require the current ACS (the ACS about to be replaced) in order to be restored. The new ACS will not be able to restore this backup data, so you will want to keep the old ACS set until you are sure you no longer need this backup.
- You will be prompted to optionally erase your old ACS cards after you create the replacement set. This will prevent the old ACS from being reused again. However, keep the old ACS if you want to restore any backup data protected by the old ACS.
- If you use pass phrases, make sure you do not forget them or the card will be inoperable.

IMPORTANT: You can only replace the old ACS, you cannot change K or N during this procedure.

1. Start an SSH client session from the laptop or PC to the V6100 appliance, and log in using your CLI administrator credentials.

2. To replace your ACS, insert one card from the quorum of the old card set into the old card reader, and at the prompt type `replaceacs` and follow the instructions;

```
0002:vormetric$ hsm
0002:hsm$ hsm replaceacs
Before you start to replace ACS, you must ensure that you have enough
blank cards to create a complete new AC.
If you start the procedure without enough cards, you will have to
cancel the procedure part way through.
Have a quorum of cards from the current ACS ready. Please wait...
Insert ACS to authorize ACS replacement:
Module 1: 0 of 1 card read
Module 1 slot 0: empty
Module 1 slot 2: empty
.
.
.
Module 1 slot 17: empty
Module 1 completed.

Writing new ACS:
Module 1: 0 of 2 written
Module 1 slot 0: Admin Card #1
Module 1 slot 2: empty
.
.
.
Module 1 slot 17: empty
Module 1 slot 0: empty
Insert/change card in module 1 (or change module mode)
```

3. Start the remote Administration Client software on your laptop or PC. On the first screen enter the V6100 appliance IP address and click **Connect**.
4. Select the Electronic Serial Number (ESN) of the HSM from the Choose HSM screen, click **Next**.
5. The Remote Administration Client displays if you have inserted a card into the reader (TVD) or not.
6. Insert a card into the TVD, the Card Inserted column displays Yes, click **Next**.
7. Click the green OK button on the TVD to confirm the HSM ESN. If you take more than a minute to do this step, an orange light will blink asking you to abort this step.
8. On the CLI, you will be prompted to overwrite the inserted card, press Enter to overwrite the card.

9. Next you will be prompted to enter a passphrase for the card. Enter a passphrase if using one and press enter.

Caution: Make a note of this passphrase, if you lose it the card will be unusable.

10. Remove the written card and insert the next card that is part of the quorum.
11. Enter a passphrase if using one and make a note of it.
12. Once you've completed writing the cards, you will be prompted to erase the old cards. If you plan on keeping the old set, do not erase them.

The new cards can be used with the old card reader, however, the old cards cannot be read with the new TVD.

Enabling remote administration for an HA configuration

If you have an HA deployment, follow this task sequence:

1. break up the cluster, see "Break up HA cluster:".
2. upgrade the primary, "Upgrade Server Software:"
3. enable remote administration on the primary DSM and obtain a warrant, see "Obtain a warrant"
4. replace the ACS, see "Replacing the ACS"
5. upgrade the failover nodes, same as step 2 above.
6. enable remote administration on the failover nodes same as step 3 above
7. recreate the cluster, convert to failover from the TVD on the primary node, see "Upgrade primary node and reconfigure cluster:".

NOTE: Remote administration is also available for DSM V6000 or virtual appliances that nShield Connect integration enabled, however this needs to be configured on the nShield Connect device. Refer to the nShield Connect documentation for more information about enabling remote administration.

Specifications, Racking, and Cabling for the V6000 and V6100

A

This chapter provides the V6000/V6100 hardware appliance specifications and installation instructions. It contains the following sections:

Hardware Appliance Diagrams

Figure 1: Front view of DSM hardware appliance with bezel :

Warning! The DSM appliance is covered with three FIPS tamper evident stickers. Removing or damaging the stickers voids FIPS compliance and the equipment warranty.

Figure 2: Vormetric DSM hardware appliance with FIPS tamper evident stickers

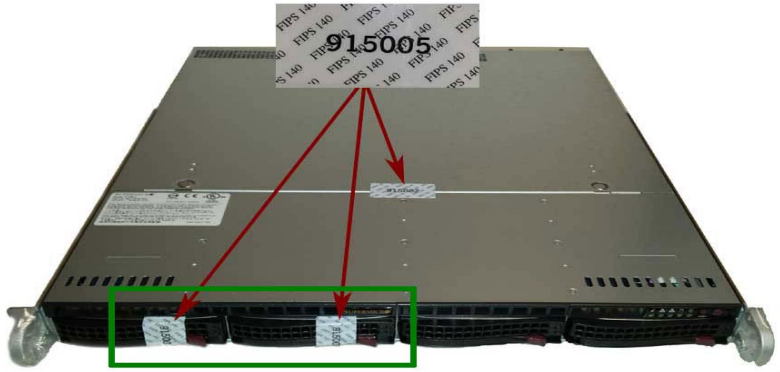
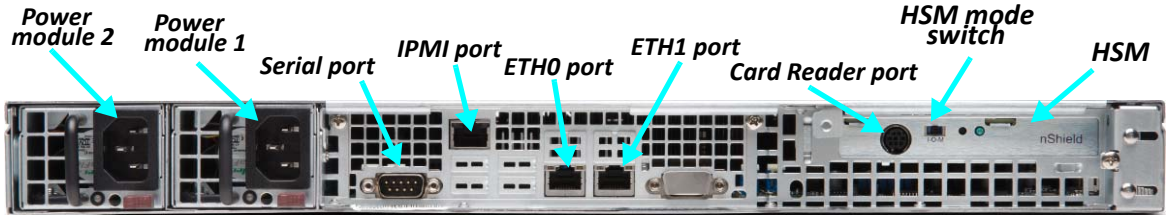


Figure 3: Rear view of V6100 DSM with HSM (V6000 has no HSM)



Control Panel LEDs

The control panel located on the front of the SC813M chassis has five LEDs. These LEDs provide you with critical information related to different parts of the system. This section explains what each LED indicates when illuminated and any corrective action you may need to take.

Figure 4: Front view of DSM hardware appliance with bezel removed

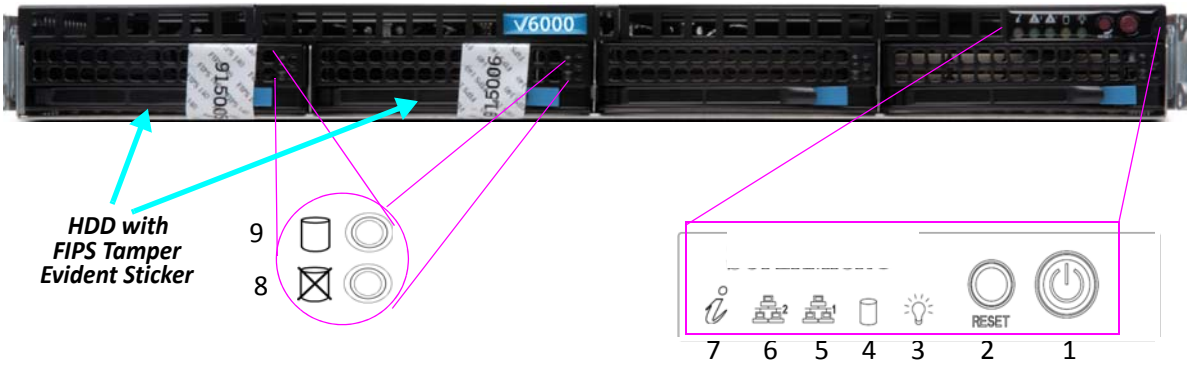


Table 1: DSM Appliance features

Number	Description
1	**Power Button**: Used to apply or remove power from the power supply to the server system. Turning off system power with this button removes the main power but keeps standby power supplied to the system. Therefore, you must unplug system before servicing.
2	**Reset**: The reset button is used to reboot the system.
3	**Power LED**: Indicates power is being supplied to the system's power supply units. This LED should normally be illuminated when the system is operating.
4	**HDD**: Indicates IDE channel activity. SAS/SATA drive and/or DVD-ROM drive activity when flashing.
5	**NIC1**: Indicates network activity on Gigabit LAN1 when flashing.
6	**NIC2**: Indicates network activity on Gigabit LAN2 when flashing.
7	Information LED. See Table 2 on page 122.
8	Hard drive fail.
9	Hard drive fail signal.

Table 2: Informational LEDs

Status	Description
Solid red	An overheat condition has occurred. (This may be caused by cable congestion).
Blinking red (1Hz)	Fan failure, check for an inoperative fan.
Blinking red (0.25Hz)	Power failure, check for a non-operational power supply.
Solid blue	Local UID has been activated. Use this function to locate the server in a rack mount environment.
Blinking blue (300 msec)	Remote UID is on. Use this function to identify the server from a remote location.

DSM Hardware Appliance Specifications

Table 3: V6000/V6100 Specifications

Specification	Description
Chassis	1U rack mountable; 17’ wide x 20 1/2” long x 1.75” high
Weight	V6000: 21.5 lbs (9.8 kg) V6100: 22 lbs (10 kg)
Memory	16GB
Hard Drive	Seagate Savvio 600GB mirrored
Serial Ports	1
Ethernet	2 x 1GB
IPMI	1 x 100Mb
Power Supplies	2 removable 80+ certified (100VAC-240VAC/50-60Hz) 400W
Chassis Intrusion Detection	Yes
Maximum BTU	410 BUTU max
Operating Temperature	10° to 35° C (50° to 95° F)
Non-operating Temperature	-40° to 70° C (-40° to 158° F)

Specification	Description
Operating Relative Humidity	8% to 90% (non-condensing)
Non-operating Relative Humidity	5% to 90% (non-condensing)
Safety Agency Approval	FCC, UL, and BIS certifications
FIPS 140-2 level 3 HSM	V6100 only

Space, Network, and Power Requirements

Physical dimensions

- 1u, rack-mountable chassis
- dimensions: 17”×20-1/2”×1.75”

External connectors

- two 10/100/1000baseT network connectors
- one IPMI connector
- one DB-9 RS-232 serial console connector

Power requirements

The Vormetric hardware appliance includes two auto-switching, field-replaceable, AC power modules. The power modules are shipped pre-installed in the Data Security Manager Appliance chassis.

Each power module requires an independent, 100-240V, 47-63Hz, 12V 6A power source.

Peak power consumption on the appliance is 190W.

Power switch and power reset buttons are on the front panel. Power connectors are on the back panel.

Data center environmental requirements

The table below lists the required environmental conditions for the DSM.

Table 4: Environmental conditions for the DSM

Condition	Range
Maximum BTU	410 BTU max
Operating temperature	10° to 35° C (50° to 95° F
Non-operating temperature	-40° to 70° C (-40° to 158° F)
Operating relative humidity	8% to 90% (non-condensing)
Non-operating relative humidity	5% to 90% (non-condensing)

Appliance Rack Mount Safety Instructions

The only serviceable parts in the Vormetric Data Security Manager Appliance are the power supplies. This unit must be returned to the manufacturer for replacement of lithium batteries and all other parts.

The following safety conditions must be considered when rack mounting the DSM Appliance:

- Elevated operating temperature: If the DSM Appliance is installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than the room ambient temperature. Install the equipment in an environment within the range specified in Table 4.
- Reduced air flow: Installation of the DSM Appliance in a rack should be such that the amount of airflow required for safe operation is not compromised.
- Mechanical loading: Mounting the DSM Appliance in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit overloading: Consideration should be given to the connection of the DSM Appliance to the supply circuit and the effect that overloading of the circuits might have on over-current protection and supply wiring. Equipment nameplate ratings should be used when addressing this concern.
- Reliable grounding: The rack-mounted equipment should have a reliable ground. Particular attention should be given to supply connections other than direct connections to the branch circuit (example: power strips).

Rack Mounting the Appliance

This section provides a quick setup checklist to get your chassis installed.

Unpacking the system

Inspect the box the chassis was shipped in and note any damage. If the chassis itself shows damage, file a damage claim with the carrier.

Decide on a suitable location for the rack unit that will hold your chassis. Choose a clean, dust-free, well ventilated area. Avoid areas where heat, electrical noise and electromagnetic fields are generated. Placed near a grounded power outlet.

Preparing for setup

The box your chassis was shipped in includes two sets of rail assemblies, two rail mounting brackets, and the mounting screws needed to install the system into the rack. Read this section before beginning the installation procedure.

Choosing a setup location

- Leave enough clearance in front of the rack to open the front door completely (~25 inches).
- Leave ~30 inches of clearance in the back of the rack for sufficient airflow and ease in servicing.
- This product is for installation only in a Restricted Access Location (dedicated equipment rooms, service closets and the like).

Rack precautions

- Ensure that the leveling jacks on the bottom of the rack are fully extended to the floor with the full weight of the rack resting on them.
- In single rack installation, stabilizers should be attached to the rack.
- In multiple rack installations, the racks should be coupled together.
- Always make sure the rack is stable before extending a component from the rack.
- You should extend only one component at a time - extending two or more simultaneously may cause instability.

General server precautions

- Review the electrical and general safety precautions that came with the components you are adding to your chassis.

- Determine the placement of each component in the rack before you install the rails.
- Install the heaviest server components on the bottom of the rack first, and then work up.
- Use a regulating uninterruptible power supply (UPS) to protect the server from power surges, voltage spikes and to keep your system operating in case of a power failure.
- Allow the hot plug hard drives and power supply modules to cool before touching them.
- Always keep the rack's front door and all panels and components on the servers closed when not servicing to maintain proper cooling.

Rack mounting considerations

Ambient Operating Temperature. If installed in a closed or multi-unit rack assembly, the ambient operating temperature of the rack environment may be greater than the ambient temperature of the room. Therefore, consideration should be given to installing the equipment in an environment compatible with the manufacturer’s maximum rated ambient temperature (Tmra).

Reduced Airflow. Equipment should be mounted into a rack so that the amount of airflow required for safe operation is not compromised.

Mechanical Loading. Equipment should be mounted into a rack so that a hazardous condition does not arise due to uneven mechanical loading.

Circuit Overloading. Consideration should be given to the connection of the equipment to the power supply circuitry and the effect that any possible overloading of circuits might have on over current protection and power supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Ground. A reliable ground must be maintained at all times. To ensure this, the rack itself should be grounded. Particular attention should be given to power supply connections other than the direct connections to the branch circuit (that is, the use of power strips and so on).

Caution: To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:

- This unit should be mounted at the bottom of the rack if it is the only unit in the rack.
- When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.

- If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.

Rack Mounting Instructions

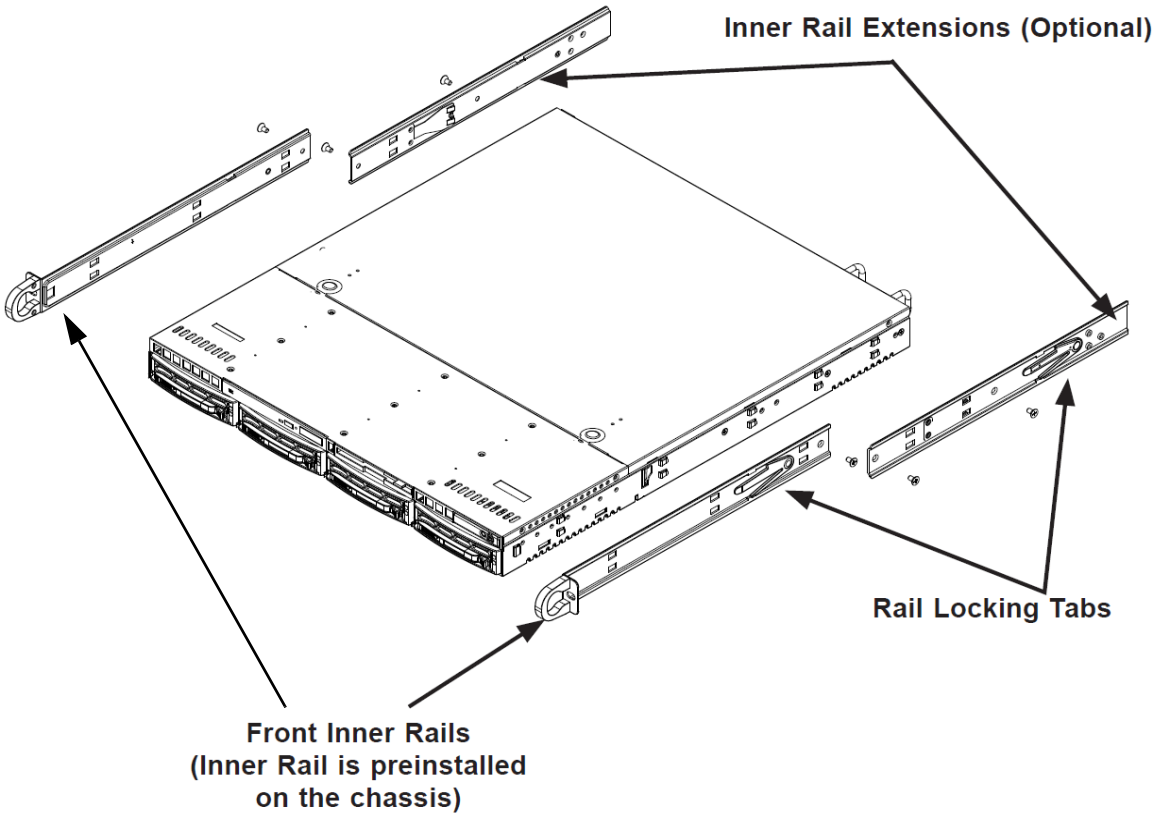
This section provides information on installing the V6000/V6100 chassis into a rack unit with the rails provided. There are a variety of rack units on the market, which may mean the assembly procedure will differ slightly. You should also refer to the installation instructions that came with the rack unit you are using.

NOTE: This rail will fit a rack between 26" and 33.5" deep.

Identifying the sections of the rack rails

The chassis package includes two rack rail assemblies in the rack mounting kit. Each assembly consists of two sections: an inner fixed chassis rail that secures directly to the server chassis and an outer fixed rack rail that secures directly to the rack itself.

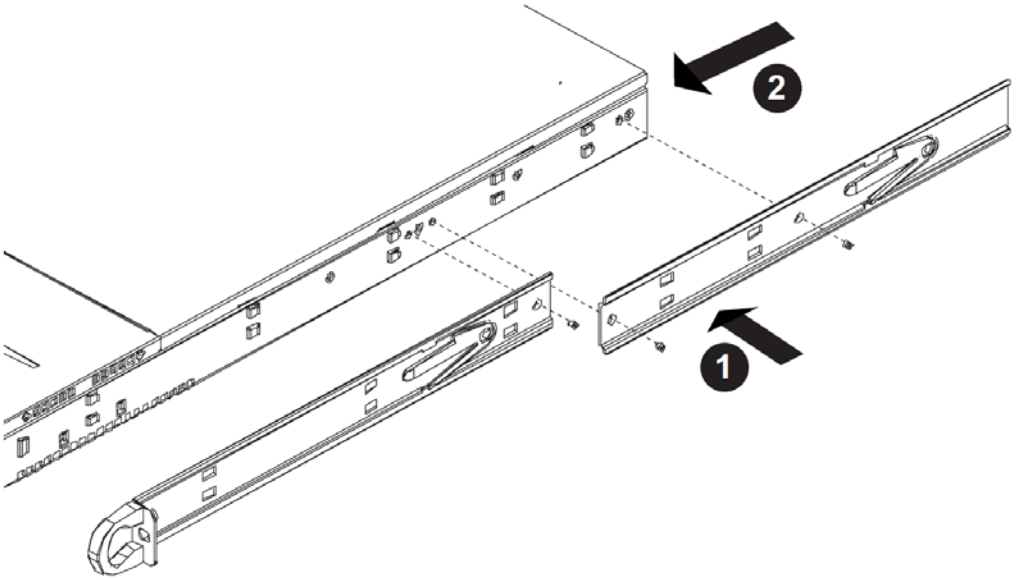
Figure 5: Identifying the Sections of the Rack Rails



Locking tabs

Both chassis rails have a locking tab. The tabs lock the server into place when installed and pushed fully into the rack. These tabs also lock the server in place when fully extended from the rack. This prevents the server from coming completely out of the rack when you pull it out for servicing.

Figure 6: Identifying the Sections of the Rack Rails (right side rail shown)



The Inner Rail Extension (Optional)

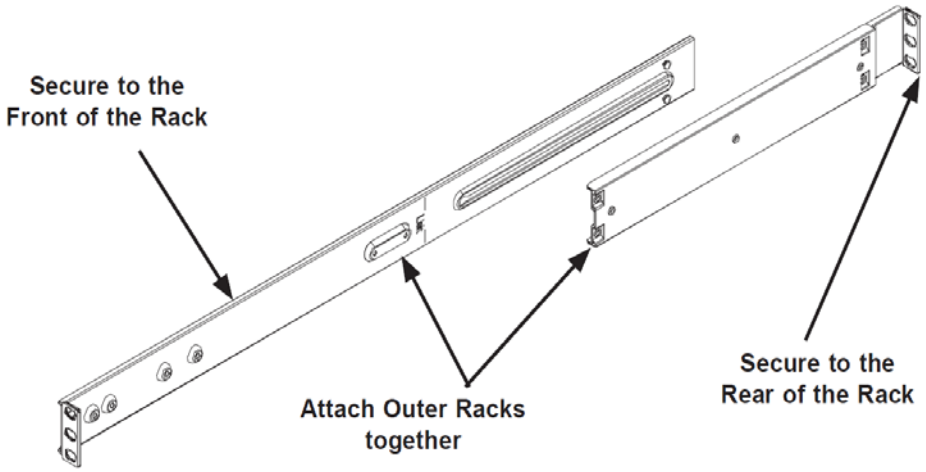
The inner rails are pre-attached and do not interfere with normal use of the chassis if you decide not to use a server rack. Attach the inner rail extension to stabilize the chassis within the rack. If you are not using a rack, you do not have to install the inner rail extensions.

Installing the inner rails

1. Place the inner rack extensions on the side of the chassis aligning the hooks of the chassis with the rail extension holes. Make sure the extension faces "outward" just like the pre-attached inner rail.
2. Slide the extension toward the front of the chassis.
3. Secure the chassis with two screws as illustrated. Repeat steps for the other inner rail extension.

Warning! Do not pick up the server by the front handles. They are designed to pull the system from a rack only.

Figure 7: Assembling the Outer Rails



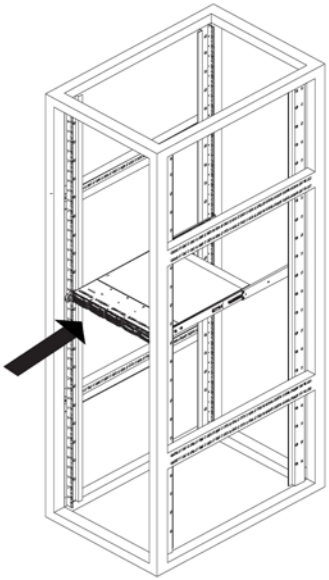
Outer rack rails

Outer rails attach to the server rack and hold the server in place. The outer rails for the V6000/V6100 chassis extend between 30 inches and 33 inches.

Installing the outer rails to the rack

1. Attach the short bracket to the outside of the long bracket. You must align the pins with the slides. Also, both bracket ends must face the same direction.
2. Adjust both the short and long brackets to the proper distance so that the rail fits snugly into the rack.
3. Secure the long bracket to the front side of the outer rail with two M5 screws and the short bracket to the rear side of the outer rail with three M5 screws.
4. Repeat steps 1-3 for the left outer rail.

Figure 8: Installing into a rack



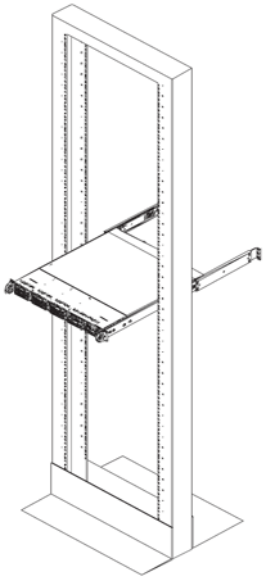
NOTE: Figures are for illustrative purposes only. Always install servers into racks from the bottom up.

Installing the chassis into a rack

1. Confirm that chassis includes the inner rails and rail extensions. Also, confirm that the outer rails are installed on the rack.
2. Line chassis rails with the front of the rack rails.
3. Slide the chassis rails into the rack rails, keeping the pressure even on both sides (It may be necessary to depress the locking tabs when inserting). When the server has been pushed completely into the rack, the locking tabs will "click" into the locked position.
4. (Optional) Insert and tightening the thumbscrews that hold the front of the server to the rack.

Caution: The rack stabilizing mechanism must be in place, or the rack must be bolted to the floor before you slide the unit out for servicing. Failure to stabilize the rack can cause the rack to tip over.

Figure 9: Installing into a rack



NOTE: Figures are for illustrative purposes only. Always install servers into racks from the bottom up.

Installing the chassis into a mid-mount position (telco) rack

1. Use the two L-shaped brackets on either side of the chassis (four total).
2. Determine how far the chassis will extend out the front of the rack. Larger chassis should be positioned to balance the weight between front and back. If a bezel is included on your server, remove it.
3. Attach the two front brackets to each side of the chassis, then the two rear brackets positioned with just enough space to accommodate the width of the telco rack.
4. Finish by sliding the chassis into the rack and tightening the brackets to the rack.

Installing and Connecting Cables

Applying power

Connect each power module to an independent, 100-240V, 47-63Hz, 12V 6A power source.

Always shut down the system before removing power to ensure that all files and processes are properly closed. The DSM appliance is started and shut down through the Vormetric Command Line Interface (CLI) with the `shutdown` command.

Connecting the serial console

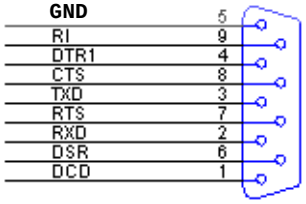
The serial console is connected to the system through the serial port in the back of the DSM Appliance. This is a DB-9 RS-232 connector. (See Figure 8 on page 18.)

The serial console port provides a direct connection to the DSM hardware appliance. By default, the serial console interface is always accessible and it can always be relied on to communicate with the DSM. Communication with the appliance is done through the DSM CLI after making a terminal connection. The serial console is used to configure the appliance Ethernet interfaces during initial setup. After the network is configured, a CLI administrator can log on to the appliance using an SSH connection, and complete the configuration process.

To log on using the CLI:

1. Configure your console connection using the following parameters:
    - Terminal Type: VT100
    - Baud Rate: 9600
    - Parity: None
    - Data bits: 8
    - Stop bits: 1
2. Connect the system serial console port and the DSM Appliance serial console port.
3. The pin-out of the DSM Appliance serial console port is:

Figure 10: Appliance serial console port pin-out



Pin #	Definition	Pin #	Definition
1	DCD	6	DSR
2	RXD	7	RTS
3	TXD	8	CTS
4	DTR1	9	RI
5	Gnd		

4. Open a console window, like Windows HyperTerminal, on your system.
5. The console window should display the DSM CLI login prompt. If it does not, press the <Enter> key.

Connecting to the network

Two RJ-45 10/100/1000 Mb Ethernet connections, `eth0` and `eth1`, are provided on the rear panel of the V6000/V6100 DSM hardware appliance (see Figure 8 on page 18). The `eth0` interface comes pre-configured from the factory. The `eth1` interface is not configured and is disabled by default.

You can access the DSM appliance immediately after bootup via a Secure Shell Protocol (SSH) connection. The default IP address of the `eth0` network interface is:

```
eth0: 192.168.10.1
```

If you want to connect to the DSM via Ethernet, manually set the IP address for the laptop to 192.168.10.2 (or higher) with a default mask of 255.255.255.0. Otherwise, use the serial console interface to configure the DSM network. We recommended that you use the serial console interface to perform initial network configuration because, if you are logged onto the appliance through the Ethernet interface, the connection will drop when you change the Ethernet interface IP address.

HA for V6x00 and Virtual Appliances

B

This chapter describes how to set up High Availability (HA) for V6x00 hardware and virtual appliances. Refer to the High Availability chapter in the *DSM Administrators Guide* for details about managing an HA deployment.

This appendix contains the following sections:

HA Overview

To configure High Availability (HA) for DSMs, you need administrators of type DSM *System Administrator* or type *All* as well as someone with DSM CLI privileges. A DSM HA configuration consists of two or more DSMs.

Supported HA Deployments

To ensure reliable operation, the appliances or systems in a HA configuration must run homogeneous configurations. That is, if the primary DSM uses an HSM, the failover DSMs must all use an HSM. If the primary DSM is a virtual appliance DSM, the failover DSMs should also be virtual appliances.

Table 5: Supported DSM HA Deployment Scenarios

HA Setup	Support
DSM version 5 appliance (without HSM) and V6000	Yes. All appliances in the cluster must have DSM software version installed.
DSM version 5 appliance (with HSM) and V6000	No. This option is not supported.
DSM version 5 appliance (without HSM) and V6100	No. This option is not supported.
DSM version 5 appliance (with HSM) and V6100	No. This option is not supported.

NOTE: All configuration settings, including changes to administrators, hosts, keys, and policies, must be made on the primary DSM only. Configuration changes and updates on the primary DSM are pushed to the failover DSMs at set intervals.

Configuring HA for a V6100 Hardware Appliance

This section describes how to configure a failover V6100 appliance. A thorough technical discussion of a DSM HA configuration is described in "HA Overview".

Refer to Table 5, "Supported DSM HA Deployment Scenarios," on page 135 for supported HA deployment scenarios for V6100. For more information on HA tasks and procedures refer to the *DSM Administrators Guide*.

Prerequisites

You must have two DSMs installed on the same network to create an HA system—a primary node and a failover node. The maximum number of nodes allowed in a DSM cluster is 8, including the primary node. Refer to "Configure network settings", for how to configure a DSM V6100 appliance.

All DSM appliances are configured as primary servers by default. You must reconfigure an appliance as a failover server *before* it can be added to a HA cluster as a failover server.

Before you set up your HA cluster, do the following:

1. Specify a hostname resolution method, see "Specify host name resolution method".
2. Open all required ports, see "Configure DSM ports".
3. Ensure that network communication between the designated primary and failover DSMs is working, perform a 'ping' operation on all the DSMs.

To configure HA for the V6100 hardware appliance you need the following:

- Two V6100 appliance installed and configured, with one appliance designated as the primary DSM, and the other appliance designated as the failover DSM. You cannot use a DSM without an HSM or a virtual DSM as a failover server.
- A TVD connected to a laptop or PC that is connected to the V6100 appliance..
- A quorum of activated smart cards--number of cards required to perform an administrative action and their pass phrases. See "Administrator Card Set (ACS)" for more about the ACS.

Add the failover DSM to the primary DSM

In this example, the primary DSM is referred to as *DSM1* and the failover as *DSM2*.

1. On DSM1 (primary), log on to the Management Console.
2. Click **High Availability** in the menu bar. The *High Availability Servers* window opens.
3. Click **Add**. The **Add Server** window opens.
4. In **Server Name**, enter the host name or FQDN of DSM2 (failover).
5. Click **Ok**. DSM2 is listed in the **High Availability Servers** with the role of **Failover**.

NOTE: Steps 6 through 9 are done on DSM2 (failover)

6. Connect to the DSM CLI to create and configure the failover DSM (DSM2) with the command `convert2failover` from the CLI. The following printout shows the actions and output when this command is run.
7. At the prompt, type ha to enter the ha commands menu:

   ```
   0016:dsm$ ha
   ```

8. To configure the DSM as a failover node, type `convert2failover` at the prompt,

   ```
   0017:ha$ convert2failover
   ```

9. Answer the prompts to continue the conversion to a failover node and have your ACS quorum ready to insert into the card reader when prompted.

   ```
   WARNING: We will now convert this server to failover server.
   Please make sure the primary server is running and has this server on its
   failover server list.
   This may take several minutes. After HA setup please make sure all the
   cluster server nodes are in the same suiteb mode.
   Continue? (yes|no)[no]:yes
   ```

   Type yes to continue.

10. Enter information about the primary DSM at the prompt;

    ```
    Primary Security Server host name:primary.hostname.com
    Primary Security Server system administrator name:admin
    Primary Security Server system administrator password:xxxxxxx
    ```

11. Enter the failover DSM information at the prompts to generate the server certificate. You will be asked to recheck and confirm the information you just entered, confirm that it is all correct;

    ```
    This computer may have multiple IP addresses. All the agents will have to
    connect to Security Server using same IP.
    Enter the host name of this computer. This will be used by Agents to talk
    to this Security Server.
    This Security Server host name[failover.hostname.com]:
    Please enter the following information for key and certificate
    ```

```
generation.
What is the name of your organizational unit? []:Engineering
What is the name of your organization? []:Company, Inc.
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]:

WARNING: The following information you entered will be used to convert
this server to failover server, please make sure the information is
correct

Primary Security Server host name:primary.hostname.com.com
Primary Security Server system administrator name:admin
Primary Security Server system administrator password:xxxxxxxx

This Security Server host name[failover.hostname.com]:failover.com
The name of your organizational unit: Engineering
The name of your organization: Company, Inc.
The name of your City or Locality: San Jose
The name of your State or Province: California
Your two-letter country code[US]:

Continue? (yes|no)[no]:yes
```

12. Type yes to continue. The DSM server software will be stopped, you will be prompted to enter your ACS quorum to generate the certificate. Once the failover DSM restarts, compare the certificate fingerprint to the certificate fingerprint on the Primary DSM dashboard, they must match.

```
Stopping Security Server
Stopping data store
Converting server role to failover...done.
Generating certificate signing request
Signing certificates
```

At this point you must have the quorum of cards from the ACS of the primary ready.

```
Have a quorum of cards from the ACS of the primary server Security World
ready.
13:46:59 WARNING: Module #1: preemptively erasing module to see its
slots!
Indoctrinating Module:
 Module 1: 0 cards of 1 read
 Module 1 slot 0: empty
Card reading complete.

security world loaded on 1 module; hknso =
f7387fed7f52625bc06b79607bb4b0afdd93a6b1

Failover Security Server certificates have been generated successfully.
```

```
JBoss vault keystore password have been completed successfully.
Starting data store
Starting Security Server
Primary_Server=ss190.i.vormetric.com
CAs_Fingerprint=40:BE:EA:44:AD:3D:35:C4:0A:64:57:9E:FA:CD:FA:4D:10:88:44
:36
Ensure the fingerprint listed above matches the one on the primary
Security Server web console dashboard.
SUCCESS: convert server to failover server. The server is started. Please
verify the fingerprint
```

13. The failover DSM is now configured.

Configuring DSM replication

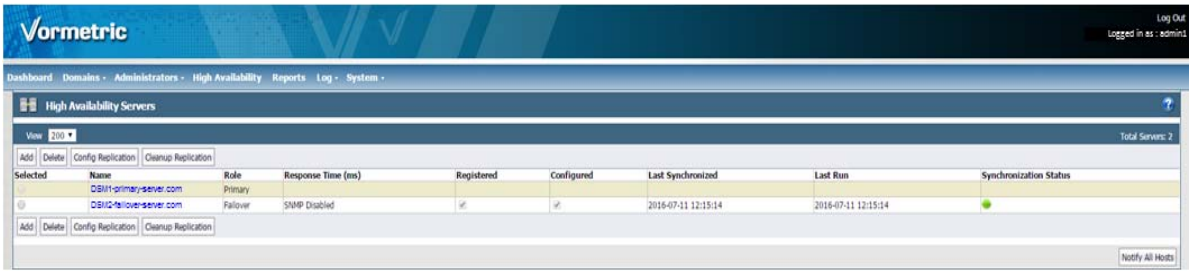
After the failover DSM is configured, you need to configure the primary DSM to replicate its information to the new failover.

1. Log on to the primary DSM Management Console and go to **High Availability**. In the **Selected** column, select the failover DSM.
2. Click **Config Replication**. A dialog box opens, prompting you to continue.
3. Click **OK**. The **Configured** check box for the failover DSM should be enabled after configuration completes.

Caution: Please be patient. There is a transition period after **Configure Replication** is completed. During the transition period, the **Last Synchronized** time and **Last Run** time may not reflect the real HA status until the **Synchronization Status** turns green.

4. Verify that the failover DSM configuration completed successfully. Check the *High Availability Servers* window on the primary DSM. Figure 11 shows vmSSA10, a fully configured and operational failover DSM that has been synchronized with the primary DSM.

Figure 11: Configured and synchronized failover DSM



See the *DSM Administrators Guide* for more information about managing your HA deployment.

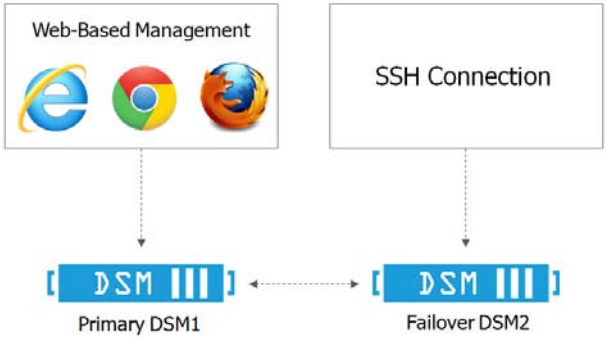
Configuring HA for V6000 and Virtual Appliances

You must have at least two DSMs installed on the same network to create an HA system—a primary DSM and a failover DSM. The maximum number of nodes allowed in a DSM cluster is 8, including the primary node.

NOTE: If you have configured nShield Connect integration on a DSM V6000 or virtual appliance, see "Configuring High Availability for network HSM-enabled DSM" on page 64, first for more information.

The following steps describe how to set up a two-node HA cluster. In this scenario, the DSM that remains the primary is referred to as **DSM1**. The DSM that becomes the failover is referred to as **DSM2** as shown in Figure 12.

Figure 12: High Availability Configuration



Before you begin

Before you set up your HA cluster, do the following:

1. Specify a hostname resolution method, see "Specify host name resolution method".
2. Open all required ports, see "Configure DSM ports".
3. Ensure that network communication between the designated primary and failover DSMs is working, perform a 'ping' operation on all the DSMs.

NOTE: If the network latency between the primary DSM and the failover DSM exceeds 100ms, you may experience delays in HA replication, especially if you have many policies, or you have large policies that contain many resource sets, user sets, etc. Another factor to consider is the **Policy Version History** setting. Each time changes are made to a policy a new version of that policy is created. The **Policy Version History** setting determines how many previous versions of

the policy will be kept, which increases the time required to replicate policy data to the cluster nodes. Refer to Chapter 5 in the *DSM Administrators Guide*, or the DSM online help, for more information about this setting. We recommend changing this value to 0 or 5 from the default of 10.

Adding DSM2 to DSM1 database

1. Install and configure two DSMs as described in the relevant chapters in this guide. The license must be installed on the designated primary DSM before HA can be configured.
2. On DSM1 (primary), log on to the Management Console.
3. Click **High Availability** in the menu bar. The *High Availability Servers* window opens.

NOTE: The license must be installed on the primary DSM before HA can be configured.

4. Click **Add**. The **Add Server** window opens.
5. In **Server Name**, enter the host name or FQDN of DSM2 (failover).
6. Click **Ok**. DSM2 is listed in the **High Availability Servers** with the role of **Failover**.

Registering DSM2 as a failover with DSM1

1. On DSM2, log on to the DSM CLI. Type:

   `ha`
2. Type

   `convert2failover`

   Sample output:

```
0002:ha$ convert2failover
WARNING: We will now convert this server to failover server.
Please make sure the primary server is running and has this server on its
failover server list.
This may take several minutes. After HA setup please make sure all the cluster
server nodes are in the same suiteb mode.
Continue? (yes|no)[no]:
```

3. Follow the prompts:
   a. Type `yes` to continue.
   b. Type the host name or FQDN of DSM1, the primary server.
   c. Type the name of an administrator of type System Administrator or All that is configured on DSM1.

d. Type the same administrator's password.

e. Press **Enter** to use the default name for the local host. Do not change this name.

4. The primary DSM will issue the certificate using the information you provide in the following steps:

   a. What is the name of your organizational unit? []: Engineering

   b. What is the name of your organization? []: Vormetric, Inc.

   c. What is the name of your City or Locality? []: San Jose

   d. What is the name of your State or Province? []:CA

   e. What is your two-letter country code? [US]:

5. Type `yes` to continue. The installation utility creates certificates, completes the installation process, and then starts the DSM. This may take a few minutes.

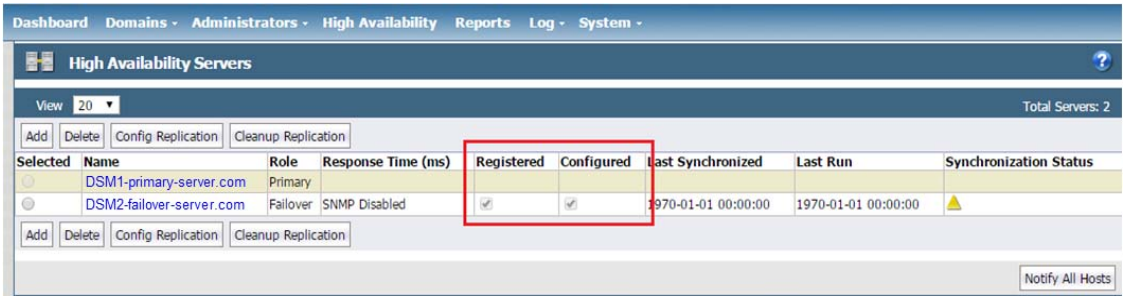
   The CA certificate fingerprint is displayed.

   Sample output:

```
Primary_Server=sys1.mycompany.com
CAs_Fingerprint=53:8C:62:A7:B2:7A:3E:0A:A4:BE:F8:31:A7:27:48:7D:FD:20:EE:63

Ensure the fingerprint listed above matches the one on the primary Security
Server web console dashboard.

SUCCESS: convert server to failover server. The server is started. Please
verify the fingerprint

0003:ha$
```

6. On DSM1 on the Management Console, click the **Dashboard** tab.
7. Match the fingerprint from the output on DSM2 with the **RSA CA fingerprint** on the **Dashboard**.
8. Click the **High Availability** tab. In the row for the failover DSM, the **Registered** check box should be selected.

Figure 13: Registered failover DSM on the Management Console

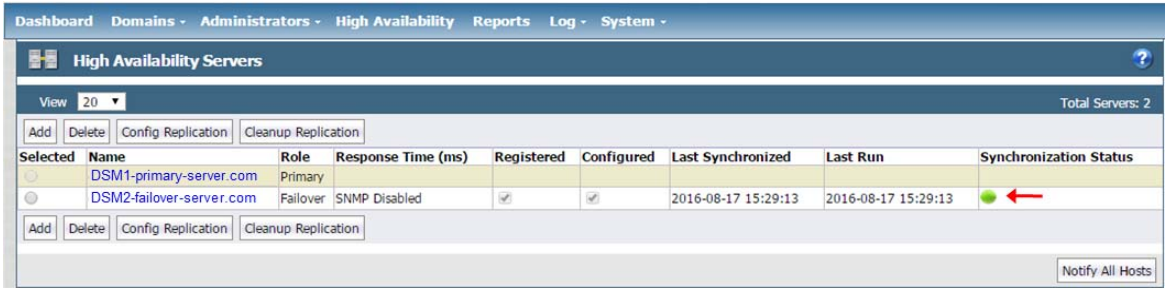


Configuring replication

After failover is configured, you need to configure the primary to replicate its information to the new failover.

1. In the **Selected** column, select the failover DSM.
2. Click **Config Replication**. A dialog box opens, prompting you to continue.
3. Click **OK**. The **Configured** check box for the failover DSM should be enabled after configuration completes.
4. Verify that the failover DSM configuration completed successfully. The Synchronization Status column should contain a green circle indicating that the failover has been synchronized with the primary. Check the *High Availability Servers* window on the primary DSM. Figure 14 shows a fully configured and operational failover DSM that has been synchronized with the primary DSM.

Figure 14: Configured and synchronized failover DSM



Other HA Functions

See the *VDS Administrators Guide* for instructions on other HA functions such as:

- Converting a Failover DSM to a Primary DSM
- Assigning Hosts to the DSM in an HA cluster
- Pushing Configuration Changes to Hosts
- Reassigning Hosts to Another DSM in the HA Cluster
- Displaying the High Availability Configuration

IPMI

C

The Intelligent Platform Management Interface (IPMI) provides browser-based remote access to the V6000 and V6100 hardware appliances. It allows administrators to remotely monitor appliance health (temperature, power consumption, physical drive status, chassis intrusion, and others), perform cold boots (power-off and power-on), and access the DSM CLI. IPMI is not supported by the DSM virtual appliance or hardware appliances earlier than V6000/V6100.

This chapter contains the following sections:

IPMI Overview

IPMI offers useful features, but it also introduces some security issues. Following these recommended best practices will reduce the probability of these security issues occurring.

- IPMI requires a browser with Java 7 or higher. Enable Java Network Launch Protocol (JNLP) and Java content in the browser to use the keyboard-video-mouse (KVM) for the remote console.
- Disable IPMI services if not needed. Disconnect the IPMI port at the back of the DSM hardware appliance from the network, or execute the DSM CLI command `ipmi disable`.
- Deploy IPMI in a secure private network behind a firewall, restricting inbound and outbound traffic to/from IPMI.
- Do not share the IPMI port with the other two DSM Ethernet ports. The Vormetric factory default sets the IPMI LAN interface to **Dedicated** (you can check the status in the IPMI GUI under **Network Link Status**).

Configuring and Accessing IPMI on the DSM

The DSM appliance has a dedicated IPMI Ethernet port that is pre-configured with the IP address, 192.168.10.10. The DSM IPMI Ethernet port is separate from the other two DSM Ethernet ports, see Figure 15: "IPMI Ethernet port" below.

Figure 15: IPMI Ethernet port

This section describes how to configure IPMI and access the IPMI management console.

Configuring IPMI

IPMI Ports

The following ports can be configured for IPMI on the V6000/V6100 DSM hardware appliance

Table 6: IPMI Ports

Port	Protocol	Communication Direction	Purpose
80	TCP	Browser → IPMI	This port is disabled by default and should not be used.
443	TCP	Browser → IPMI	This port is enabled by default. It is used for the IPMI GUI. If you change the port through which you access IPMI through https through your browser ("Change the port through which you access IPMI" on page 149), then you should close port 443.
5900	TCP	Browser → DSM	This port is disabled by default. It is used for remote KVM (Keyboard Video Mouse) management. Enable if you want to use the remote console.
623	UDP	Browser → DSM	This port is disabled by default. Enable only if you want to attach virtual media.

Configuring IPMI on the DSM

Before you can use IPMI to configure your DSM V6000/V6100 appliance, you need to configure an IP address, and enable the KVM port for remote Java console support.

If you want to configure the IPMI Ethernet port IP address to use an IPv6 address, you must do this via the IPMI GUI—you cannot configure the IPMI Ethernet port IP address via the CLI.

NOTE: If the HTTP and HTTPS ports are both enabled for IPMI, IPv6 will not work for HTTPS. The workaround is to either disable HTTP or use IPv4 rather than IPv6.

Configure IPMI IP address:

1. Access the DSM CLI and log on to the CLI console.
2. Enter the `ipmi` submenu, type:

   ```
   0011:vormetric$ ipmi
   0012:ipmi$
   ```

3. Set the IPMI IP address using the command `ip set`. Type;

   ```
   0012:ipmi$ ip set <ip address>
   ```

4. Set the IPMI net mask using the command `mask set <net mask>`, type;

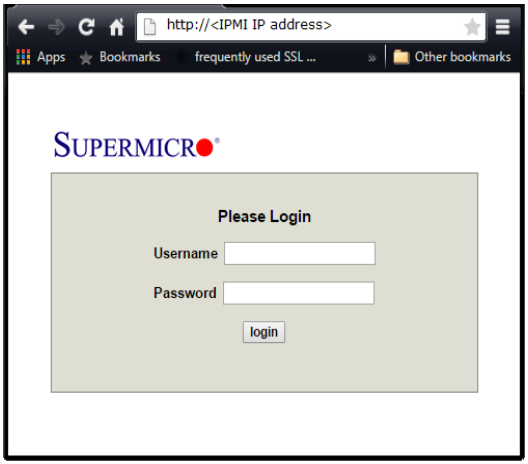
   ```
   0013:ipmi$ mask set <net mask>
   ```

5. Enable the KVM port using the command `port enable kvm`. The KVM port is required for remote Java console support. At the prompt, type;

   ```
   0014:ipmi$ port enable kvm
   ```

6. Open a browser session and point the browser to the URL that contains the IPMI IP address you just configured; https://<IPMI IP address>.
7. You will see the IPMI login screen, see Figure 16: “IPMI Login screen” below.

Figure 16: IPMI Login screen



The default login credentials are as follows; Username: ADMIN and password: ADMIN.

8. Navigate to **Remote Control > Console Redirection** and click **Launch Console**. Download and run the resulting `.jnlp` file to open a Java console for your DSM. This Java console provides access to the DSM CLI.
9. Log on to the CLI using the default CLI administrator credentials; Username; cliadmin, password: cliadmin123. You will be prompted to change the CLI administrator password. After that you will be prompted to change the IPMI GUI login password as well.
   The new password must be at least 8 characters long, must contain at least one upper case letter, one special character, and one number.
10. Configure the network settings, see "Configure network settings" on page 20 and then generate the CSR, see."Generate DSM Certificate Authority and create ACS" on page 28.

Best Practices after IPMI is Configured

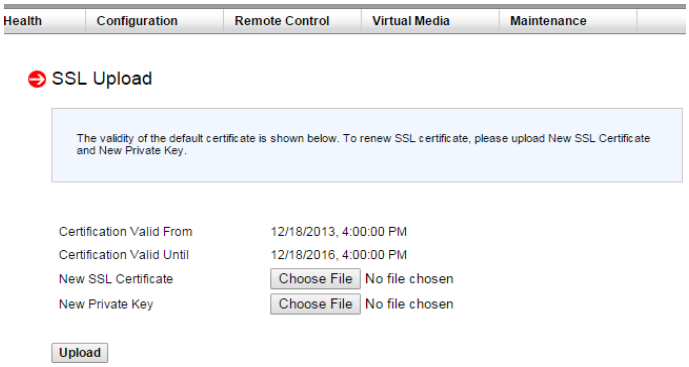
This section describes the best practices after IPMI is configured. Many of these best practices involve changing the IPMI configuration. These can be changed through both the IPMI management console, or through the DSM CLI (see "DSM IPMI CLI Commands" on page 155.

Replace the default self-signed IPMI certificate

Replace the default IPMI certificate to make your system more secure. To replace the certificate you need to upload an RSA2048 private key and the associated SHA256 certificate using the IPMI GUI.

1. Obtain an RSA-2048 private key.
2. In the IPMI GUI, click **Configuration > SSL Certification**:

Figure 17: SSL Upload

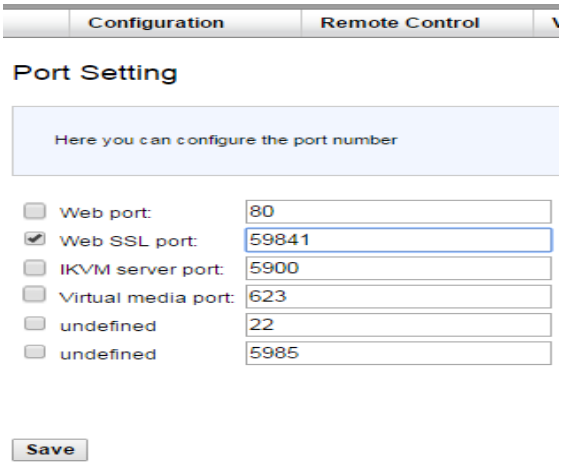


3. Select the new signed SHA256 certificate file and the RSA2048 private key file and click **Upload**.
4. The new certificate and key are now installed.

Change the port through which you access IPMI

By default you can only access the IPMI management console through HTTPS. The default port for HTTPS is 443. Changing the default port from 443, will present an obstacle to potential hackers. If you change the https port, for example to 59841, you will have to add it to the IPMI URL. For example, instead of accessing IPMI using `https://10.3.45.45` you will have to use `https://10.3.45.45:59841`

1. In the IPMI management console, click **Configuration > Port**.



2. Change the Web SSL port from 443 and click **Save**. You will lose connectivity to the IPMI console when you change the port number. Enter the URL to log in again with the new port number as; `https://<IP address or host name>:<Port number>`

   Example: `https://1.2.3.4:59841`
3. Navigate to Remote Control > Console Redirection and click Launch Console. Download the resulting .jnlp file. You need to edit the web port information in this .jnlp file. The first line in the file that contains the URL, needs to be edited to change the default port from 443 to the new port number, which, per our example, is 59841.
4. Save the file and then double-click the .jnlp file to launch the remote Java console.

Change the IPMI password

Use a complex password for IPMI. The new password must be at least 8 characters long, must contain at least one upper case letter, one special character, and one number.To change IPMI user passwords:

1. In the IPMI management console, click **Users** in the left column.
2. Highlight the user whose password will change, and click **Modify User.**
3. Click **Change Password**, enter **Password** and **Confirm Password**, then click **Modify**.

Creating IPMI users

You can create IPMI users by using the IPMI GUI or by using the DSM CLI `ipmi user add` command. We recommend using the DSM CLI `ipmi user add` command.

To create an IPMI user:

1. Log on to the DSM CLI and run the `ipmi user show` command to see what User IDs are available:

```
0003:ipmi$ user show
User ID | User Name | Privilege Level   | Enable
------- | ---------- | --------------- | ------
2       | ADMIN      | Administrator   | Yes
SUCCESS: user show
```

   `User ID` - IPMI user ID.
   `User Name` - IPMI user name up to 15 characters.
   `Privilege Level` - Administrator, Operator or User.

   In this example there is only on administrator, the default. The IPMI user ID is *2*, and the IPMI user name is *ADMIN*, and the privilege level is *Administrator*. Using the DSM CLI you can use any of the unused user IDs from 3 to 8. In this example, we'll use User ID *3*.

2. Choose a user name and privilege level for the administrator you are about to create. This can be of type *Administrator*, *Operator* or *User*. Each type has varying levels of privilege (see table below). The Administrator has full view and change control of all IPMI features. The Operator has change control of most IPMI features and viewing privileges of the rest. The User has the fewest privileges. Don't give Administrator privileges to all IPMI users. Create user types appropriate for each user.

Function	User	Operator	Administrator
System Information	Full Access	Full Access	Full Access
Chassis Locator Control	View Only	Full Access	Full Access
FRU Reading	Full Access	Full Access	Full Access
Sensor Reading	Full Access	Full Access	Full Access
Event Log	View Only	Full Access	Full Access
Alert	No	View Only	Full Access
LDAP	No	View Only	Full Access
Mouse Mode	No	Full Access	Full Access
Network	No	View Only	Full Access
Remote Session	No	View Only	Full Access
SMTP	No	View Only	Full Access

Function	User	Operator	Administrator
SSL	No	View Only	Full Access
Users	No	View Only	Full Access
Event Action	No	View Only	Full Access
Power Control	View Only	Full Access	Full Access
KVM	View Only	Full Access	Full Access
F/W Update	View Only	View Only	Full Access
SDR Update3	View Only	View Only	Full Access
Logout	Full Access	Full Access	Full Access

3. Run the `user add` command to create the user. `user add` has the following syntax:

   ```
   user add <userID Username privilege_level>
   ```

   In this example `userID` is 3, `Username` is `user1`, and `privilege_level` is `operator`:

   ```
   0017:ipmi$ user add 3 user1 3
   Enter new password:
   Enter password again:
   SUCCESS: ipmi user modified
   ```

   The new password must be at least 8 characters long, must contain at least one upper case letter, one special character, and one number.

   where ((4=administrator, 3=operator 2=user 1=callback)

Configuring Alerts

You can configure IPMI to send alert notifications about hardware events on the DSM appliance. To receive email alerts you will need to configure your SMTP server in the IPMI GUI. You can also configure SNMP trap alerts, to be sent to an SNMP manager.

Configure SMTP (optional - for e-mail alerts)

To receive e-mail alerts, first configure your SMTP server in the IPMI GUI as follows:

1. Log on to the IPMI GUI.
2. Click Configuration > SMTP.
3. Enter details for your SMTP mail server and click Save.

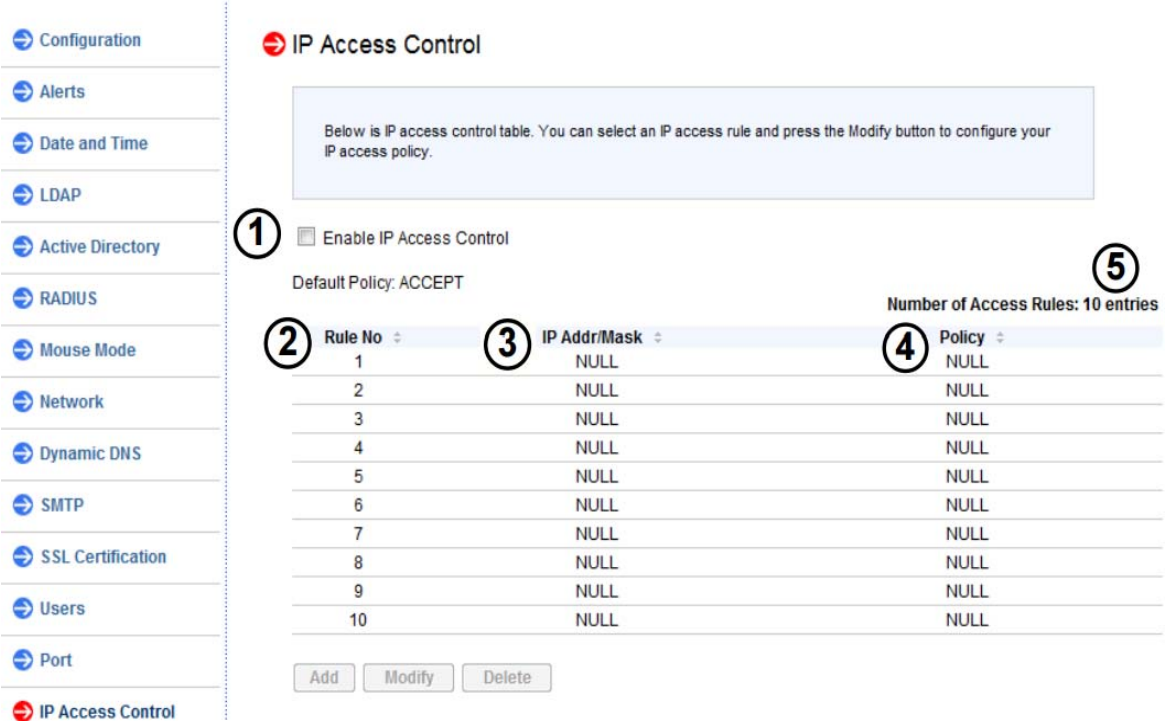
Configure an IPMI Alert (for SMTP and/or IPMI alerts)

1. In the IPMI GUI, navigate to **Configuration > Alerts**.
2. Select an alert from the numbered list that you want to configure and click **Modify**.
3. Set the severity level, the destination IP address to where you want to send the trap alert notification, and/or an email address to which to send the notification (see "Configure an IPMI Alert (for SMTP and/or IPMI alerts)" above for how to configure an SMTP server), a subject, and message if desired.
4. Click **Save** to save the updated settings.

To test your configuration setting, Click **Send Test Alert**. You should receive an alert notification if your settings are correct.

Restrict inbound traffic to IPMI through IP Access control

You can specify exactly which IP address can or cannot access IPMI. In the IPMI management console, click **Configuration > IP Access Control** to display:



1. Check this box to enable IP Access Control. When prompted, "Do you want to enable IP access control," click **OK**.

2. Rule Number: This column lists the number of IP Access Control rules.
3. IP Address/Mask: This column displays IP Address/Mask settings.
4. Policy: This column displays the status of an IP Access policy.
5. Number of Access Rules: This displays the maximum number of IP Access rules you can set for the system.

Adding or Modifying IP Access Rules

Click **Add** to add an IP access rule, or select a rule and click **Modify** to modify an existing rule. For each rule, enter an IP address and mask, then select **Accept** or **Drop** to allow or block the IP address from accessing IPMI. This item allows you to grant access to a specific IP address or a range of IP addresses.

For example, if you wanted to specify a range of IP addresses from 192.168.0.1 to 192.168.0.126, you would enter 192.168.0.1/25. Then select a policy. Select **Accept** to allow access for the IP address(es) entered above. Select **Drop** to deny access.

NOTE: If the IP access control is set incorrectly you may accidentally lock yourself out of IPMI. If this happens, use the DSM CLI IPMI command; `reset factorydefault`.

Reset your IPMI configuration to factory defaults

If you want to reset your IPMI configuration to the factory defaults (say you forgot your IPMI password or you locked yourself out of IPMI or you want to clear out the current IPMI configuration setup and start anew), use the DSM CLI command `ipmi reset factorydefault`. DO NOT use the IPMI management console to reset IPMI to factory settings. The command `ipmi reset factorydefault` is optimized for security, and the IPMI management console factory reset is not. The command `ipmi reset factorydefault` is more secure because it:

- Only allows access to the IPMI IP address through https.
- Disables the Dynamic Host Configuration Protocol (DHCP) so you can set the IPMI to use a static IP address. A static IP allows administrators to create firewall rules and monitor usage of this system.
- Sets IPMI LAN interface to **Dedicated** so that the IPMI must run in a dedicated IPMI-only LAN.
- Resets the IP address to the default 192.168.10.10. Username is reset to default (UserID: ADMIN Password: ADMIN).

DSM IPMI CLI Commands

The Intelligent Platform Management Interface (IPMI) provides remote access to the V6000 and V6100 hardware appliances. It allows administrators to remotely monitor appliance health (example: temperature, power consumption, physical drive status, chassis intrusion), perform cold boots (power-off and power-on), and access the DSM CLI. IPMI is not supported by the DSM virtual appliance or hardware appliances earlier than V6000/V6100.

Table 7: DSM CLI IPMI category commands

`ip`	Set, delete, or show ip address of machine using IPMI.
`mask`	Set, delete, or show subnet mask of machine using IPMI.
`gateway`	Set, delete, or show gateway of machine
`disable`	Disable IPMI network
`user`	Add, show, or delete user. Also change password and privilege level.
`clearint`	Clear chassis intrusion. If chassis cover is open, a chassis intrusion toggle is set that shows up in the IMPI GUI sensor reading, CLI maintenance diagnostic, and DSM log. This command resets the toggle.
`reset`	Reset IPMI configuration to factory default.
`reset bmc`	Reset IPMI BMC controller.
`selftest`	Triggers a test called the IPMI Baseboard Management Controller (BMC) self-test. Use this if you suspect the IPMI controller is not working. The BMC chip runs even when the rest of the system is down.
`version`	Show IPMI version.
`psinfo`	Show power supply information.
`dhcp`	Configure DHCP for the IPMI NIC
`port`	Configure IPMI ports.

ip

The `ip` command configures the IPMI network IP address.

The `ip` command includes the following elements:

Table 8: DSM CLI `ipmi` category `ip` command elements

`set`	Sets the IPMI IP address.
`delete`	Deletes the IP address.

show	Shows the IP address.

ip set

Set the IPMI IP address. Setting the IP address automatically sets the mask to 16-bit mask.

Syntax

```
ip set ip_address
```

Example

The following example sets the IPMI network interface IP address.

```
0001:vormetric$ ipmi
0002:ipmi$ ip set 10.3.99.77
IP=10.3.99.77
SUCCESS: ip set
```

ip delete

Delete the IPMI IP address. This sets the IP to 0.0.0.0.

Syntax

```
ip delete
```

Example

The following example deletes the IPMI network interface IP address.

```
0002:ipmi$ ip delete
IP=0.0.0.0
SUCCESS: ip delete
```

ip show

Show the IPMI IP address.

Syntax

```
ip show
```

Example

The following example shows the IPMI network interface IP address.

```
0002:ipmi$ ip show
IP=0.0.0.0
MAC=00:25:90:F7:12:52
SUCCESS: ip show
```

mask

The mask command sets, deletes or shows the subnet mask for the IP address. The mask command includes the following elements:

Table 9: DSM CLI IPMI category mask command elements

set	Sets the subnet mask for the IP address.
delete	Sets the IP subnet mask 0.0.0.0.
show	Shows the subnet mask for the IP address.

mask set

Set the subnet mask for the IP address.

Syntax

```
mask set subnet_mask
```

Example

```
0001:vormetric$ ipmi
0002:ipmi$ mask set 255.255.0.0
Subnet Mask=255.255.0.0
SUCCESS: subnet mask set
```

mask delete

Set the subnet mask for the IP address to 0.0.0.0..

Syntax

```
mask delete
```

Example

```
0002:ipmi$ mask delete
Subnet Mask=0.0.0.0
SUCCESS: subnet mask delete
```

mask show

Show the subnet mask for the IPMI IP address.

Syntax

```
mask show
```

Example

```
0002:ipmi$ mask show
Subnet Mask=255.255.0.0
SUCCESS: subnet mask show
```

gateway

The gateway command sets the IPMI gateway. The gateway command includes the following elements:

Table 10: DSM CLI IPMI category gateway command elements

set	Sets the IPMI gateway.
delete	Deletes the IPMI gateway.
show	Shows the IPMI gateway.

gateway set

Use the gateway set command to set the IPMI IPMI gateway.

Syntax

```
gateway set ip_address
```

Example

```
0001:vormetric$ ipmi
0002:ipmi$ gateway set 10.10.79.254
Gateway=10.10.79.254
SUCCESS: gateway set
```

gateway delete

Use the gateway delete command to delete the IPMI gateway.

Syntax

```
gateway delete
```

Example

```
0002:ipmi$ gateway delete
Gateway=0.0.0.0
SUCCESS: gateway delete
```

gateway show

Use the gateway show command to show the IPMI gateway.

Syntax

```
gateway show
```

Example

```
0003:ipmi$ gateway show
Gateway=0.0.0.0
SUCCESS: gateway show
```

disable

The `disable` command disables the IP, and mask, setting them both to 0.0.0.0.

Syntax

```
disable
```

Example

```
0001:vormetric$ ipmi
0002:ipmi$ disable
Do you want to disable IPMI network? Access to IPMI will not be
available afterwards. (yes|no)[no]:yes
SUCCESS: Disable IPMI network
```

user

The `user` command adds, shows, or deletes users. Also changes user password and privilege level. See "Creating IPMI users" on page 150 for more details. The `user` command includes the following elements:

Table 11: DSM CLI IPMI category `user` command elements

`add`	Add an IPMI user.
`delete`	Delete an IPMI user.
`show`	Show the IPMI users.
`password`	Change the IPMI user password.
`level`	Set the IPMI user privilege level.

user add

Add an IPMI user. After using this command, you will have created a user with no password. Use the user password command to add a password.

Syntax

```
user add userID User_name privilege_level
```

Where,

`userID` - IPMI user ID

`User_name` - IPMI user name up to 15 characters

`privilege_level` - Administrator, Operator or User. See "Creating IPMI users" on page 150 for details.

Example

```
0001:vormetric$ ipmi
0002:ipmi$ user add 3 user1 3
Enter new password:
Enter password again:
SUCCESS: ipmi user modified
```

user password

Change or add IPMI user's password. The password constraints are as follows; 8 characters minimum, 20 characters maximum. At least one capital letter, one number, and one special character are also required.

Syntax

```
user password userID
```

Example

```
0002:ipmi$ user password 3
Enter new password:
Enter password again:
SUCCESS: user password modified
```

user delete

Delete user.

Syntax

```
user delete userID
```

Example

```
0002:ipmi$ user show
0003:ipmi$ user delete <userid>
```

user show

Use `user show` to show the IPMI users.

Syntax

```
user show
```

Example

```
0003:ipmi$ user
User ID | User Name | Privilege Level   | Enable
------- | ---------- | --------------- | ------
2       | ADMIN      | Administrator   | Yes
SUCCESS: user show
```

user level

Change IPMI user's privilege. Don't assign administrative privileges to all users. Assign operator or user privilege instead.

Syntax

```
user level userID privilege_level
```

Example

```
user level 3 3
```

clearint

Clear chassis intrusion. When someone opens the chassis cover of the DSM, chassis intrusion will get flagged. When the cover is put back, run `clearint` to clear it.

Syntax

```
clearint
```

Example

```
clearint
```

reset

The reset command resets the IPMI configuration or resets the IPMI BMC controller. The reset command includes the following elements:

Table 12: IPMI category `reset` command elements

`factorydefault`	Reset IPMI configuration to factory default.
`bmc`	Reset IPMI BMC controller.

factorydefault

Wipe out IPMI configuration and return to IPMI factory default: ip=192.168.10.10, mask=255.255.0.0, gateway=0.0.0.0. ADMIN will be the only user left with default password ADMIN. All others users are deleted. Also disables DHCP and sets the IPMI to a dedicated non-share port.

Syntax

```
reset factorydefault
```

Example

```
reset factorydefault
```

reset bmc

Reset IPMI controller. When you want to do a reboot on the IPMI BMC controller chip because the IPMI is failing to respond, or a self-test failed, use this command to reset IPMI chip.

Syntax

```
reset bmc
```

Example

```
reset bmc
```

selftest

Test that the BMC chip is working.

Syntax

```
selftest
```

Example

```
selftest
Selftest: Passed.

SUCCESS: ipmi selftest
```

version

Show IPMI version.

Syntax

```
version
```

Example

```
version
Firmware Version: 03.40
SUCCESS: ipmi show version
```

psinfo

Show power supply information. If only one power module is plugged in, the output will display only one module.

Syntax

```
psinfo
```

Example

```
0001:ipmi$ psinfo

[SlaveAddress = 78h] [Module 1]

Item                            |                Value
```

```
----                            |                -----

Status                          |     [STATUS OK](00h)
AC Input Voltage                |              116.5 V
AC Input Current                |               0.34 A
DC 12V Output Voltage           |              12.00 V
DC 12V Output Current           |               2.25 A
Temperature 1                   |              27C/81F
Temperature 2                   |              34C/93F
Fan 1                           |             5472 RPM
Fan 2                           |                0 RPM
DC 12V Output Power             |                26 W
AC Input Power                  |                36 W
PMBus Revision                  |              0x8B22
PWS Serial Number               |      P406PCE24AT1144
PWS Module Number               |          PWS-406P-1R
PWS Revision                    |              REV1.1


[SlaveAddress = 7Ah] [Module 2]

Item                            |                Value

----                            |                -----

Status                          |     [STATUS OK](00h)
AC Input Voltage                |              117.0 V
AC Input Current                |               0.37 A
DC 12V Output Voltage           |              12.00 V
DC 12V Output Current           |               2.87 A
Temperature 1                   |              35C/95F
Temperature 2                   |             40C/104F
Fan 1                           |             6560 RPM
Fan 2                           |                0 RPM
DC 12V Output Power             |                36 W
AC Input Power                  |                43 W
PMBus Revision                  |              0x8D22
PWS Serial Number               |      P406PCE24AT1150
PWS Module Number               |          PWS-406P-1R
PWS Revision                    |              REV1.1

SUCCESS: Show power supply information
```

dhcp

Enable or disable Dynamic Host Configuration Protocol (DHCP). Forces the IPMI IP address to be static. By default it's off.

Syntax

```
dhcp [enable, disable]
```

Example

```
dhcp [enable, disable]
```

port

Enable, disable, or check the status of the IPMI port. The default ports are https=443, keyboard/video/mouse (kvm)=5900, vmedia=623, web=80. IPMI users can change the port numbers but the service will still get enabled or disabled with the same command.

Table 13: DSM CLI IPMI category `port` command elements

`enable`	Enable IPMI port.
`disable`	Disable IPMI port.
`status`	Show IPMI port status.

enable

Enable IPMI port.

Syntax

```
port enable [https | kvm | vmedia |web]
```

Example

```
0001:vormetric$ ipmi
0002:ipmi$ port enable https
```

disable

Disable IPMI port.

Syntax

```
port disable [https | kvm | vmedia |web]
```

Example

```
0002:ipmi$ port disable https
```

status

Check the status or IPMI ports.

Syntax

```
port status [https | kvm | vmedia |web]
```

Example

```
0003:ipmi$ port status https
IPMI https web port is enabled
```

Troubleshooting

D

This section describes some troubleshooting procedures for your appliance.

Loss of Connection

If you have created GuardPoints and for some reason the appliance cannot be reached, the GuardPoints will continue to function with no issues. However, if the system is rebooted, the agent cannot access its configuration from the appliance and the GuardPoints cannot use the encryption key to encrypt or decrypt data unless you are using a cached-on-host key. Challenge and response and manual passwords are good way to provide business continuity in these situations.

Is the Management Console accessible?

1. Try to open a web browser with the correct address to the appliance (example: https://192.168.10.11:8445 or 8448 for Suite B mode).
2. Check if the appliance is a trusted site in your web browser's Security Options.

Check whether Agent communication ports are open from the UI

1. Use the Network Diagnostic checkport tool in the Management Console (or CLI) to check those ports.
2. Refer to Table 1 on page 10 for information about ports that need to be configured.

Reset DSM Appliance and Remove All Data

The `config reset` command removes all configuration data added after the current DSM software is installed. This command is available on both appliance-based and software-only DSM installations.

The command preserves the currently installed DSM software but, removes all data except network configuration, and in the case of the V6100 appliance, the original security world

created using the ACS is also preserved. When you reconfigure the V6100 appliance you can then recover that security world with the ACS quorum used to create it. Alternatively, you can choose to destroy the old security world and create a new one with new cards.

Caution: If you choose to create a new Security World, we strongly recommend that you use a ***new*** set of cards (ACS) to create the new Security World. If you reuse the original ACS to create the new Security World, the cards will be overwritten. Any backups created with that original ACS will be ***unrecoverable***.

Reset Original Security World with Original ACS Quorum

To reset the current DSM installation to its initial unconfigured state—network configuration remains intact—and retrieve the original security world, do the following;

1. Log on to the DSM CLI console using the CLI Administrator credentials and at the prompt type `maintenance` to enter the maintenance category of commands, then type `config reset`;

   ```
   $ maintenance

   0001:maintenance$ config reset

   Reset configuration will wipe out all the configuration data and
   set the configuration data to the manufacture default. System
   will reboot automatically.

   Continue? (yes|no)[no]:yes

   config reset SUCCESS. You can reboot the Security Server now or
   it will reboot automatically in 60 seconds.

   0002:maintenance$
   ```

2. You will need to generate the DSM certificate authority (CA) again. This will require a quorum from the original ACS used to create the Security World. Wait until the system has rebooted and the `vormetric$` prompt is displayed, then run the `security genca` command.

   Type `up` at the prompt to return to the main menu and then type `system` to access the System category sub-menu;

   ```
   0002:maintenance$ up

   0003:vormetric$ system
   ```

   At the prompt, type `security genca` to generate the CA. A warning message is displayed informing you that all agent and peer node certificates will need to be resigned after the new certificate authority is created and that the DSM software will be restarted, type ‘yes’ to generate the certificate;

   ```
   0004:system$ security genca
   ```

```
WARNING: All Agents and Peer node certificates will need to be
re-signed after CA and server certificate regenerated, and the
security server software will be restarted automatically!

Continue? (yes|no)[no]:yes
```

3. The following message is displayed. Read it, enter the required information to generate the CA, and ensure the DSM host name is correct, press enter:

```
This computer may have multiple IP addresses. All the agents
will have to connect to Security Server using same IP.

Enter the host name of this computer. This will be used by Agents
to talk to this Security Server.

This Security Server host name[mycompany.com]:

Please enter the following information for key and certificate
generation.

What is the name of your organizational unit? []:

What is the name of your organization? []:

What is the name of your City or Locality? []:

What is the name of your State or Province? []:

What is your two-letter country code? [US]:

Regenerating the CA and server certificates now...
```

4. A message is displayed informing you that a Security World exists and provides you the option to reuse it. This is the Security World in place when the `config reset` command was run. Type yes to reuse the existing Security World. Keep the quorum of cards from the ACS used to create this original Security World available as these will be required for the next few steps. Follow the instructions on the screen;

```
There is an existing Security World.

Would you like to reuse it? (yes|no)[no]: yes

Please provide a quorum of cards from the ACS of the existing
Security World.

15:47:02 WARNING: Module #1: preemptively erasing module to see
its slots!


Indoctrinating Module:
 Module 1: 0 cards of 1 read
 Module 1 slot 0: empty
 Module 1 slot 2: empty
 Module 1 slot 3: empty
```

```
Card reading complete.

security world loaded on 1 module; hknso =
3546197a6456c5e3bfb28d7facd063072b7a8f52

Do NOT remove the smart card from the reader yet.

Creating CA keys and signer certificates...
done.

Generating server private key...
done.

You may now remove the smart card from the reader.

Creating and signing the server certificates...
done.

CA and Server certificates have been generated successfully.
JBoss vault keystore password have been completed successfully.
Self test in progress: passed
SUCCESS: The CA and security certificates are re-generated and
the Security Server software is restarted.

Regenerating CA will make certificates at failover servers and
agents invalid. You may need to:
        - Re-sign certificates at each failover server
        - Cleanup and re-register each agent
0005:system$
```

The DSM appliance is now ready to use with the original Security World. For procedures to restore a backup of your previous configuration, refer to the *DSM Administrators Guide*.

Create New Security World with New ACS

To reset the current DSM installation to its initial unconfigured state—network configuration remains intact—and create a new Security World, do the following;

1. Log on to the DSM CLI console using the CLI Administrator credentials and at the prompt type `maintenance` to enter the maintenance category of commands, then type `config reset`;

   ```
   $ maintenance

   0001:maintenance$ config reset

   Reset configuration will wipe out all the configuration data and
   set the configuration data to the manufacture default. System
   will reboot automatically.

   Continue? (yes|no)[no]:yes

   config reset SUCCESS. You can reboot the Security Server now or
   it will reboot automatically in 60 seconds.

   0002:maintenance$
   ```

2. You will need to generate the DSM certificate authority (CA) again. This will require a quorum from the original ACS used to create the Security World. Wait until the system has rebooted and the `vormetric$` prompt is displayed, then run the `security genca` command.

   Type up at the prompt to return to the main menu and then type `system` to access the System category sub-menu;

   ```
   0002:maintenance$ up

   0003:vormetric$ system
   ```

   At the prompt, type `security genca` to generate the CA. A warning message is displayed informing you that all agent and peer node certificates will need to be resigned after the new certificate authority is created and that the DSM software will be restarted, type 'yes' to generate the certificate;

   ```
   0004:system$ security genca

   WARNING: All Agents and Peer node certificates will need to be
   re-signed after CA and server certificate regenerated, and the
   security server software will be restarted automatically!

   Continue? (yes|no)[no]:yes
   ```

3. The following message is displayed. Read it, enter the required information to generate the CA, and ensure the DSM host name is correct, press enter:

   ```
   This computer may have multiple IP addresses. All the agents
   will have to connect to Security Server using same IP.

   Enter the host name of this computer. This will be used by Agents
   to talk to this Security Server.

   This Security Server host name[mycompany.com]:
   ```

```
Please enter the following information for key and certificate
generation.

What is the name of your organizational unit? []:

What is the name of your organization? []:

What is the name of your City or Locality? []:

What is the name of your State or Province? []:

What is your two-letter country code? [US]:

Regenerating the CA and server certificates now...
```

4. A message is displayed informing you that a Security World exists and provides you the option to reuse it. This is the Security World in place at the when the `config reset` command was run. Type no to destroy the old Security World and create a new Security World. Have the new set of cards available for this step. For information about the ACS and best practices, refer to the Administrative Card Set section in chapter 1 of the *DSM Installation and Configuration Guide*. Follow the instructions on the screen;

```
There is an existing Security World.

Would you like to reuse it? (yes|no)[no]: no

Enter the total number of cards (N) you would like to use in your
Administrator Card Set (ACS).

Note: The system can handle at most 64 cards but you should not
enter more than the number of available cards in your possession
currently.

This value must be at least 2 and no higher than 64: 2


Enter the number of cards (K) required to authorize an action.
This number K is known as the quorum.

Note: The value for K must be less than N. Creating card sets in
which K is equal to N is not allowed because an error on one card
would render the whole card set unusable.

This value must be at least 1 and less than 2: 1

17:10:29 WARNING: Module #1: preemptively erasing module to see
its slots!


Create Security World:
 Module 1: 0 cards of 2 written
 Module 1 slot 0: empty
 Module 1 slot 2: empty
```

```
 Module 1 slot 3: empty
 Module 1 slot 4: empty
 Module 1 slot 5: empty
.
.
.
Module 1 slot 2:- no passphrase specified - overwriting card
 Module 1: 1 card of 2 written
 Module 1 slot 2: remove already-written card #1
 Module 1 slot 2: empty
 Module 1 slot 2: unknown card
 Module 1 slot 2:- no passphrase specified - overwriting card
Card writing complete.

security world generated on module #0; hknso =
781eb7d9ae3abad631bfc4c7487279eadbcef4a8

Do NOT remove the smart card from the reader yet.

Creating CA keys and signer certificates...
done.

Generating server private key...
done.

You may now remove the smart card from the reader.

Creating and signing the server certificates...
done.

CA and Server certificates have been generated successfully.
JBoss vault keystore password have been completed successfully.
Self test in progress: passed
```

```
SUCCESS: The CA and security certificates are re-generated and
the Security Server software is restarted.


Regenerating CA will make certificates at failover servers and
agents invalid. You may need to:

        - Re-sign certificates at each failover server

        - Cleanup and re-register each agent

00053:system$
```

The DSM appliance is now ready to use with the new Security World. For procedures to restore a backup of your previous configuration, refer to the *DSM Administrators Guide*.

Caution: Restoring a backup of the previous configuration will restore the old Security World and the new one just created will be destroyed.

Glossary

access control

The ability of Vormetric Transparent Encryption (VTE) to control access to data on protected hosts. Access can be limited by user, process (executable), action (for example read, write, rename, and so on), and time period. Access limitations can be applied to files, directories, or entire disks.

admin administrator
The default DSM administrator created when you install the DSM. `admin` has DSM System Administrator privileges and cannot be deleted.

Administrative Domain
(domains). A protected host or group of protected hosts on which an DSM administrator can perform security tasks such as setting policies. Only DSM administrators assigned to a domain can perform security tasks on the protected hosts in that domain. The type of VTE tasks that can be performed depends on the type of administrator. See also "**local domain**".

administrator
See "**DSM Administrator and types**".

Agent utilities
A set of utilities installed with the VTE agents and run on protected hosts. These utilities provide a variety of useful functions such as gathering protected host and agent configuration data, registering agents on the DSM, and encrypting data on the protected host.

All Administrator, **Administrator of type All**
The DSM Administrator with the privileges of all three administrator types: *System*, *Domain* and *Security*.

appliance
The DSM server. Often referred to as a *DSM hardware appliance*, which is a hardened DSM server provided by Vormetric, or as a *DSM virtual appliance*, which is the software version of the DSM to be deployed by the customers as a virtual machine.

asymmetric key cryptography
See *public key cryptographic algorithm.*

asymmetric key pair
A public key and its corresponding private key used with a public key algorithm. Also called a key pair.

authentication
A process that establishes the origin of information, or determines the legitimacy of an entity's identity.

authorization
Access privileges granted to an entity that convey an "official" sanction to perform a security function or activity.

block devices
Devices that move data in and out by buffering in the form of blocks for each input/output operation.

catch-all rule
The last policy rule that applies to any GuardPoint access attempt that did not fit any of the other rules in the policy.

certification authority or CA
A trusted third party that issues digital certificates that allow a person, computer, or organization to exchange information over the Internet using the public key infrastructure. A digital certificate provides identifying information, cannot be forged, and can be verified because it was issued by an official trusted agency. The certificate contains the name of the certificate holder, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures) and the digital signature of the certificate-issuing authority (CA) so that a recipient can verify that the certificate is real. This allows others to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. The CA must be trusted by both the owner of the certificate and the party relying upon the certificate.

challenge-response
When a protected host is disconnected from the DSM, the GuardPoint data is not accessible to users. Challenge-response is a password-based procedure that allows users to gain access to their GuardPoint data during disconnection. Users run a utility, `vmsec challenge`, a seemingly random string (the challenge) is displayed. The user calls this in to their DSM Security administrator. The administrator returns a counter-string (the response) that the host user must enter to decrypt guarded data.

Character device
See ***"raw device."***

ciphertext
Data in its encrypted form. Ciphertext is the result of encryption performed on plaintext using an algorithm, called a cipher.

cleartext or plaintext
Data in its unencrypted form.

cryptographic algorithm
A computational procedure that takes variable inputs, including a cryptographic key, and produces ciphertext output. Also called a cipher. Examples of cryptographic algorithms include AES, ARIA, and DES.

cryptographic key
See "**encryption key**."

cryptographic signature
See "**signing files**."

Database Encryption Key (DEK)
A key generated by Microsoft SQL when TDE is enabled.

Data Security Manager (DSM)
Sometimes called the *Security Server* or *appliance*. A Vormetric server that acts as the central repository and manager of encryption keys and security policies. Receives instructions and configuration from administrators through a GUI-based interface called the *Management Console*. Passes and receives information to and from VTE Agents. Available as a complete hardened hardware system (*DSM Appliance*) or as software solution installed on a UNIX box (*software-only DSM*).

dataxform
A utility to encrypt data in a directory. Short for "data transform."

DB2
A relational model database server developed by IBM.

Decryption
The process of changing ciphertext into plaintext using a cryptographic algorithm and key.

Digital signature
A cryptographic transformation of data that provides the services of origin authentication, data integrity, and signer non-repudiation.

domains
See *administrative domains*.

Domain Administrator
The second-level DSM administrator created by a DSM *System Administrator*. The DSM *Domain Administrator* creates and assigns DSM *Security Administrators* to domains and assigns them their security "**roles**". See "**DSM Administrator and types**".

Domain and Security Administrator
A hybrid DSM administrator who is has the privileges of a DSM Domain Administrator and Security Administrator.

DSM
See ***"Data Security Manager (DSM)."***

DSM Administrator and types
Specialized system security administrators who can access the Vormetric DSM Management Console. There are five types of DSM administrators:

DSM System Administrator - Creates/removes other DSM administrators of any type, changes their passwords, creates/removes, domains, assigns a Domain Administrator to each domain. Cannot do any security procedures in any domain.

Domain Administrator - Adds/removes DSM Security Administrators to domains, and assign roles to each one. Cannot remove domains and cannot do any of the domain security roles.

Security Administrator - Performs the data protection work specified by their roles. Different roles enable them to create policies, configure hosts, audit data usage patterns, apply GuardPoints, and so on.

Domain and Security Administrator - Can do the tasks of DSM Domain and Security Administrators.

All - Can do the tasks of all three of the DSM administrative types

DSM Automation Utilities
Also called VMSSC. A set of command line utilities that is downloaded and installed separately on the protected host or any networked machine. These utilities can be used by advanced users to automate DSM processes that would normally be done with the Management Console. See the *DSM Automation Reference* for complete details.

DSM CLI
A command line interface executed on the DSM to configure the DSM network and perform other system-level tasks. See the *DSM Command Line Interface* documentation

DSM CLI Administrator
A user who can access the DSM CLI. DSM CLI Administrators are actual system users with real UNIX login accounts. They perform tasks to setup and operate the DSM installation. They do not have access to the Management Console.

DSM database
A database associated with the DMS containing the names of protected hosts, policies, GuardPoints, settings, and so on.

DSM System Administrator
The highest level of DSM administrator. This administrator creates/removes other DSM administrators of any type, creates/removes domains, and assigns a Domain Administrator to each domain. The DSM System Administrator cannot perform any security procedures in any domain or system. This administrator is not related to computer or network system administrators.

EKM
See "**Extensible Key Management (EKM)**."

Encryption
The process of changing plaintext into ciphertext using a cryptographic algorithm and key.

encryption agent
See *Vormetric Transparent Encryption agent*.

encryption key
A piece of information used in conjunction with a cryptographic algorithm that transforms plaintext into ciphertext, or vice versa during decryption. Can also be used to encrypt digital signatures or encryption keys themselves. An entity with knowledge of the key can reproduce or reverse the operation, while an entity without knowledge of the key cannot. Any VDS policy that encrypts GuardPoint data requires an encryption key.

Extensible Key Management (EKM)
An API library specification provided by Microsoft that defines a software framework that allows hardware security module (HSM) providers to integrate their product with the Microsoft SQL Server.

failover DSM
A secondary DSM that assumes the policy and key management load when a protected host cannot connect to the primary DSM or when a protected host is specifically assigned to the failover DSM. A failover DSM is almost identical to the primary DSM, having the same keys, policies, protected hosts, and so on.

FF1
See “Format Preserving Encryption (FPE)”.

FF3
See “Format Preserving Encryption (FPE)”.

file signing
See *signing files*.

File Key Encryption Key (FKEK)
The key used to encrypt the file encryption key that is used to encrypt on-disk data, also known as a wrapper key.

FKEK
See “File Key Encryption Key (FKEK)”

File System Agent
A Vormetric software agent that resides on a host machine and allows administrators to control encryption of, and access to, the files, directories and executables on that host system. For example, administrators can restrict access to specific files and directories to specific users at specific times using specific executables. Files and directories can be fully encrypted, while the file metadata (for example, the file names) remain in cleartext. Also called the “**VTE Agent**”.

Format Preserving Encryption (FPE)
An encryption algorithm that preserves both the formatting and length of the data being encrypted. Examples of such algorithms used by Vormetric include FF1 and FF3, both of which are approved by NIST. Vormetric’s **FPE tokenization format** uses the FF3 algorithm.

FQDN
Fully qualified domain name. A domain name that specifies its exact location in the tree hierarchy of the Domain Name Server (DNS). For example: `example.vormetric.com`.

GPFS
General Parallel File System is a high-performance shared-disk clustered file system developed by IBM.

GuardPoint
A location in the file system hierarchy, usually a directory, where everything underneath has a Vormetric data protection policy applied to it. The File System Agent intercepts any attempt to access anything in the GuardPoint and uses policies obtained from the DSM to grant or deny the access attempt. Usually, depending on the policies, data copied into a GuardPoint is encrypted, and only authorized users can decrypt and use that GuardPoint data.

Hardware Security Module or HSM
A tamper-resistant hardware device that stores keys and provides stringent access control. It also provides a random number generator to generate keys. The DSM Appliance can come with an embedded Hardware Security Module.

host locks
Two Management Console options, **FS Agent Locked** and **System Locked,** that are used to protect the File System Agent and certain system files. File System Agent protection includes preventing some changes to the File System Agent installation directory and preventing the unauthorized termination of File System Agent processes.

host password
This is not a regular login or user password. This is the password entered by a host system user to unlock a GuardPoint when there is no DSM connection. This password decrypts cached keys when the DSM is not accessible. The host must also be configured with **Cached on Host** keys. See "**challenge-response**".

initial test policy
A first data security policy applied to a GuardPoint that is used to gather directory access information so DSM Security Administrators can create a permanent operational policy. The initial test policy encrypts all data written into the GuardPoint; decrypts GuardPoint data for any user who access it; audits and creates log messages for every GuardPoint access; reduces log message "noise" so you can analyze the messages that are important to you for tuning this policy; is run in the "**Learn Mode**" which does not actually deny user access, but allows you to record GuardPoint accesses.

After enough data is collected, the DSM Security Administrator can modify the initial test policy into an operational policy.

Key Agent
A Vormetric agent that provides an API library supporting a subset of the PKCS#11 standard for key management and cryptographic operations. It is required for the following products: Vormetric Key Management (VKM), Vormetric Tokenization, Vormetric Application Encryption (VAE), Vormetric Cloud Encryption Gateway (VCEG). Sometimes called the *VAE Agent*.

key group
A key group is a collection of asymmetric keys that are applied as a single unit to a policy.

key management
The management of cryptographic keys and other related security objects (for example, passwords) during their entire life cycle, including their generation, storage, establishment, entry and output, and destruction.

key template
A template that lets you quickly add agent keys or third-party vault keys by specifying a template with predefined attributes. You can define specific attributes in a template, then you can call up the template to add a key with those attributes.

key shares
When data is backed up or exported from VTE (for example, symmetric keys or DSM database backups), they can be encrypted in a wrapper key needed to restore the exported data on the new machine. Wrapper keys can be split and distributed to multiple individuals. Each split piece of the wrapper key is called a *key share*. Decrypting the data requires that some specified number of the individuals that received key shares contribute their key share to decrypt the data.

key wrapping
A class of symmetric encryption algorithms designed to encapsulate (encrypt) cryptographic key material. The key wrap algorithms are intended for applications such as protecting keys while in untrusted storage or transmitting keys over untrusted communications networks. Wrapper keys can be broken up into *key shares*, which are pieces of a wrapper key. Key shares are divided amongst two or more *custodians* such that each custodian must contribute their key share in order to assemble a complete wrapper key.

Key Vault
A Vormetric product that provides passive key vaulting. It securely stores symmetric and asymmetric encryption keys from any application and tracks key expiration dates.

KMIP
Key Management Interoperability Protocol. A protocol for communication between enterprise key management systems and encryption systems. A KMIP-enabled device or client software can communicate with the DSM to manage encrypted keys.

Learn Mode
A DSM operational mode in which all actions that would have been denied are instead permitted. This permits a policy to be tested without actually denying access to resources. In the Learn Mode, all GuardPoint access attempts that would have been denied are instead permitted. These GuardPoint accesses are logged to assist in tuning and troubleshooting policies.

Live Data Transformation (LDT)
A separately licensed feature of Vormetric Transparent Encryption (VTE) that allows you to transform (encrypt or decrypt) or rekey GuardPoint data without blocking use or application access to that data.

local domain
A DSM domain in which DSM administration is restricted to Domain Administrators or Security Administrators assigned to that domain. To access a local domain in the Management Console, a DSM administrator must specify their local domain upon login.

Management Console
The graphical user interface (GUI) to the DSM.

Master encryption key (MEK)
The encryption key for Oracle Database used to encrypt secondary data encryption keys used for column encryption and tablespace encryption. Master encryption keys are part of the Oracle Advanced Security Transparent Data Encryption (TDE) two-tier key architecture.

MEK
See *Master encryption key.*

Microsoft SQL Server
A relational database server, developed by Microsoft.

Microsoft SQL Transparent Data Encryption (MS-SQL TDE)
Microsoft SQL Server native encryption for columns and tables.

multi-factor authentication
An authentication algorithm that requires at least two of the three following authentication factors: 1) something the user knows (for example, password); 2) something the user has (example: RSA SecurID); and 3) something the user is (example: fingerprint). VTE implements an optional form of multi-factor authentication for Management Console users by requiring DSM administrators to enter the token code displayed on an RSA SecurID, along with the administrator name each time the administrator logs on to the Management Console.

multitenancy
A VTE feature that enables the creation of multiple local domains within a single DSM. A local domain is a DSM domain in which DSM administration is restricted to Domain Administrators or Security Administrators assigned to that domain. This allows Cloud Service Providers to provide their customers with VTE administrative domains over which the customer has total control of data security. No other administrators, including CSP administrators, have access to VTE security in a local domain.

offline policy
Policies for Database Backup Agents. *Online policies* are for the File System Agent.

one-way communication
A VTE feature for an environment where the DSM cannot establish a connection to the agent, but the agent can establish a connection to the DSM. For example, the protected host is behind a NAT so protected host ports are not directly visible from the DSM, or the protected host is behind a firewall that prohibits incoming connections, or the protected host does not have a fixed IP address as in the cloud. When an agent is registered with one-way communication, changes made for that protected host on the DSM are not pushed to the protected host, rather as the protected host polls the DSM it will retrieve the change.

online policies
Policies for the File System Agent. *Offline policies* are for Database Backup Agents.

policy
A set of security access and encryption rules that specify who can access which files with what executable during what times, and whether or not those files are encrypted. Policies are created by DSM Security Administrators, stored in the DSM, and implemented on protected hosts by a File system Agent. See "**rule (for policies)**".

policy tuning
The process of creating a simple Learn Mode policy that allows any protected host user to access a GuardPoint; to examine who accesses the GuardPoint, what executables they use, and what actions they require; and to modify the policy such that it allows the right people, using the right executable, performing the right action to do their job, and prevent anyone else from inappropriate access.

process set
A list of processes that can be used by the users in a user set associated with a policy rule.

protected host
A host on which a VTE Agent is installed to protect that host's data.

public key cryptographic algorithm, public key infrastructure
A cryptographic system requiring two keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the ciphertext. Neither key can do both functions. One key is published (*public key*) and the other is kept private (*private key*). If the lock/encryption key is the one published, the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published, then the system serves as a signature verifier of documents locked by the owner of the private key. Also called asymmetric key cryptography.

raw device
A type of block device that performs input/output operations without caching or buffering. This results in more direct access.

register host
The process of enabling communication between a protected host and the DSM. Registration happens during agent installation. Before registration can happen, the host must be added to the DSM database.

rekeying
The process of changing the encryption keys used to encrypt data. Changing keys enhances data security and is a requirement to maintain compliance with some data security guidelines and regulations. Also called *key rotation*.

roles
A set of Management Console permissions assigned to DSM Security Administrators by DSM Domain Administrators. There are five roles: *Audit* (can generate and view logging data for file accesses), *key* (can create, edit, and delete keys), *Policy* (can create, edit, and delete policies), *Host* (can configure, modify, and delete protected hosts and protected host groups), and *Challenge & Response* (can generate a temporary password to give to a protected host user to decrypt cached encryption keys when connection to the DSM is broken).

RSA SecurID
A hardware authentication token that is assigned to a computer user and that generates an authentication code at fixed intervals (usually 60 seconds). In addition to entering a static password, Management Console administrators can be required to input an 8-digit number that is provided by an external electronic device or software.

rule (for policies)
Every time a user or application tries to access a GuardPoint file, the access attempt passes through each rule of the policy until it finds a rule where all the criteria are met. When a rule matches, the *effect* associated with that rule is enforced. A rule consists of five access criteria and an effect. The criteria are Resource (the file/directories accessed), User (the user or groups attempting access), Process (the executable used to access the data), When (the time range when access is attempted) and Action (the type of action attempted on the data, for example read. write, rename and so on). *Effect* can be permit or deny access, decrypt data access, and audit access attempt. See *policy*.

secfs
1) The File System Agent initialization script. 2) An acronym for Vormetric Secure File System agent. It generally refers to the kernel module that handles policies (locks, protected host settings, logging preferences) and keys, and enforces data security protection.

secvm
A proprietary device driver that supports GuardPoint protection to raw devices. `secvm` is inserted in between the device driver and the device itself.

Security Administrator
The third-level DSM administrator who does most of data protection work like creating policies, configuring protected hosts, auditing data usage patterns, applying GuardPoints and other duties. The privileges of each Security Administrator is specified by the roles assigned to them by the Domain Administrator. See *roles*. See "**DSM Administrator and types**".

Security Server
See "**DSM**".

separation of duties
A method of increasing data security by creating customized DSM administrator roles for individual DSM administrators such that no one administrator has complete access to all encryption keys in all domains of all files.

signing files
File signing is a method that VTE uses to check the integrity of executables and applications before they are allowed to access GuardPoint data. If file signing is initiated in the Management Console, the File System Agent calculates the cryptographic signatures of the executables that are eligible to access GuardPoint data. A tampered executable, such as a Trojan application, malicious code, or rogue process, with a missing or mismatched signature, is denied access. Also called *cryptographic signatures*.

Suite B mode
A set of publicly available cryptographic algorithms approved by the United States National Security Agency (NSA). These algorithms enhance security by adding up to 384-bit encryption to the communication between the Web browser and the DSM, the DSM and Agent, and between DSMs in HA environments.

Symmetric-key algorithm
Cryptographic algorithms that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys, in practice, represent a shared secret between two or more parties that can be used to maintain a private information link. This requirement that both parties have access to the secret key is one of the main drawbacks of symmetric key encryption, in comparison to public-key encryption.

System Administrator (DSM)
See "**DSM Administrator and types**".

Transparent Data Encryption (TDE)
A technology used by both Microsoft and Oracle to encrypt database content. TDE offers encryption at a column, table, and tablespace level. TDE solves the problem of protecting data at rest, encrypting databases both on the hard drive and consequently on backup media.

user set
A named list of users on which a policy rule applies.

VAE Agent
See "**Key Agent**".

VDE Agent
Vormetric agent installed on a protected host to implement disk encryption. See *Vormetric Disk Encryption (VDE)*.

vmd
Acronym for Vormetric Daemon, vmd is a process that supports communication between the DSM and kernel module.

VMSSC or Vormetric Security Server Command Line Interface
See *DSM Automation Utilities*.

Vormetric Application Encryption (VAE)
A product that enables data encryption at the application level as opposed to the file level as is done with VTE. Where VTE encrypts a file or directory, VAE can encrypt a column in a database or a field in an application. VAE is essentially an API library for key management and cryptographic operations based on PKCS#11. See the *Vormetric Application Encryption Installation and API Reference Guide*.

Vormetric Cloud Encryption Gateway (VCEG)
Vormetric product that safeguards files in cloud storage environments, including Amazon Simple Storage Service (Amazon S3) and Box. The cloud security gateway solution encrypts sensitive data before it is saved to the cloud storage environment, then decrypts data for approved users when it is removed from the cloud.

Vormetric Data Security Platform or VDS Platform
The technology platform upon which all other Vormetric products—Vormetric Transparent Encryption (VTE), Vormetric Application Encryption (VAE), Vormetric Key Management (VKM), Vormetric Cloud Encryption Gateway (VCEG), Vormetric Tokenization Server (VTS), Vormetric Key Management (VKM), and Vormetric Protection for Teradata Database—are based.

Vormetric Encryption Expert or VEE
Earlier name of the Vormetric Transparent Encryption (VTE) product. It may sometimes appear in the product GUI or installation scripts.

Vormetric Key Management (VKM)
Vormetric product that provides a standards-based platform for storing and managing encryption keys and certificates from disparate sources across the enterprise. This includes Vormetric encryption keys, 3rd-party software keys, KMIP device keys and so on.

Vormetric Protection for Teradata Database
Vormetric product that secures sensitive data in the Teradata environment.

Vormetric Security Intelligence
Vormetric product that provides support for Security Information and Event Management (SIEM) products such as ArcSight, Splunk and QRadar. Provides solutions that monitor real-time events and analyze long-term data to find anomalous usage patterns, qualify possible threats to reduce false positives, and alert organizations when needed. Documented in the VDS Platform Security Intelligence User Guide.

Vormetric Tokenization Server (VTS)
Vormetric product that replaces sensitive data in your database (up to 512 bytes) with unique identification symbols called tokens. Tokens retain the format of the original data while protecting it from theft or compromise.

Vormetric Transparent Encryption or VTE
Vormetric product that protects data-at-rest. Secures any database, file, or volume without changing the applications, infrastructure or user experience.

Vormetric Vault
A virtual vault to store 3rd-party encryption keys, certificates and other security objects.

VTE Agent
Vormetric agents that are installed on protected hosts to implement data protection. See “**File System Agent**”.

wrapper keys
See “**key wrapping**”.

WSDL
Web Services Description Language.