

# GDE Appliance

## Installation and Configuration Guide

Release 4.0.0.4

Document Version 2

10/21/2020



# GDE Appliance

## Installation and Configuration Guide

### Release 4.0.0.4

Installation and Configuration Guide

4.0.0.4

Document Version 2

10/21/2020

All information herein is either public information or is the property of and owned solely by Thales DIS France S.A. and/or its subsidiaries or affiliates who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Thales DIS France S.A. and any of its subsidiaries and affiliates (collectively referred to herein after as "Thales") information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided "AS IS" without any warranty of any kind. Unless otherwise expressly agreed in writing, Thales makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Thales reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

**Thales hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Thales be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.**

**Thales does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Thales be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Thales products. Thales disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.**

Copyright 2009 - 2020 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales and/or its subsidiaries and affiliates and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the properties of their respective owners.

---

IBM® Guardium Data Encryption

Installation & Configuration Guide

Release 4.0.0.4

IBM Guardium Data Encryption 4.0.0.4 is the same product as Vormetric Data Security (VDS) Release 6.4.3. VDS Release 6 consists of Data Security Manager and Vormetric Agents.

# Contents

---

<b>Preface</b> .....	<b>v</b>
Documentation Version History .....	v
Assumptions .....	v
Document Conventions .....	v
Typographical Conventions .....	vi
Notes, tips, cautions, and warnings .....	vi
Hardware-Related Warnings .....	vii
Sales and Support .....	vii
<b>Chapter 1: Installing &amp; Configuring GDE</b> .....	<b>1</b>
Overview .....	1
Register on the Thales Support Site in order to download the OVA file .....	1
Extract the GDE appliance license .....	2
Installing the GDE Appliance .....	2
System Requirements .....	2
Hardware Requirements .....	3
Installation Plan .....	3
GDE Appliance Installation Checklist .....	3
Specify host name resolution method .....	4
Port configuration .....	5
Access the Command Line Interface (CLI) .....	5
Deploying the GDE Appliance .....	6
Configure the appliance .....	7
Configure network settings .....	7
Configure a bonded NIC device .....	8
Configure NTP, time zone, date, time .....	9
Configure the hostname .....	10
Generate the Certificate Authority .....	10
Add CLI administrators .....	11
Verify web access .....	11
Upload a license file .....	12
<b>Chapter 2: Upgrading GDE Appliance Software</b> .....	<b>13</b>
Upgrade Paths .....	13
Migrating to a GDE 3.0 Appliance .....	13
Backup the current configuration .....	14
Create or import a wrapper key .....	14
Create a backup .....	15

Install and configure a GDE appliance .....	15
Restore backup to new GDE appliance .....	16
Upload a license .....	16
Upgrade to the DSM patch 6.1.0.9229 .....	16
Upgrade to GDE 4.0.0.4 .....	17
<b>Chapter 3: HA for V6x00 and Virtual Appliances .....</b>	<b>18</b>
HA Overview .....	18
Supported HA Deployments .....	18
Configuring HA for Virtual Appliances .....	18
Prerequisites .....	18
Network Latency .....	19
Adding Nodes to an HA Cluster .....	19
Join a Node to an HA Cluster .....	20
Adding a Host to a new HA node .....	22
Upgrading an HA Cluster .....	22
Prerequisite .....	23
Remove Nodes from the HA cluster .....	23
Upgrade the Initial HA node .....	24
Optimize the Upgrading of Nodes in the HA Cluster .....	24
Deleting a Node from a Cluster .....	24
Deleting a Node from a Cluster with no Hosts assigned .....	24
Deleting a Node from a Cluster with Hosts assigned .....	25
Moving a Host to a different Node with the CLI .....	25
Moving a Host to a different Node with the UI .....	25
<b>Appendix A: Ports .....</b>	<b>27</b>
Ports to Configure .....	27
<b>Appendix B: Troubleshooting .....</b>	<b>29</b>
Loss of Connection .....	29
Is the Management Console accessible? .....	29
Check whether Agent communication ports are open from the UI .....	29

# Preface

---

The Installation and Configuration Guide describes how to install and configure the appliance. This document is intended for system administrators who install the GDE appliance and connect it to a network.

## Documentation Version History

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

Document Version	Date	Changes
GDE v3.0 v1	09/22/2017	The GDE 3.0a release is the same as DSM release v6.0.1. This release introduces the following new features: Bonded NICs, a new concise initialization method that reduces the load on the appliance and the network when the agents are re-initialized, and re-signing of host settings. Enhancements have been made to Availability.
GDE 3.0b v1	12/14/2017	GDE 3.0b release is the same as DSM release v6.0.2-patch. This release addresses several security issues.
GDE 3.0.0.2 v1	09/07/2018	GA release of GDE 3.0.0.2. The GDE 3.0.0.2 release is the same as DSM release v6.1.0. Virtual appliances can now be HMS-enabled by connecting them to an nShield Connect appliance.
GDE 4.0.0.0	4/11/2019	GA release; HA is now active/active, new CLI commands, new API calls . This guide contains new troubleshooting information. Added rules for hostnames.
GDE 4.0.0.1	09/13/19	Supports Efficient Storage with VTE 6.2.0, Excluding files from encryption, fixed security vulnerabilities.
GDE 4.0.0.2	12/19/2019	GDE Appliance now compatible with Smart cards, users can create GuardPoints for Cloud Object Storage devices, System admins can prevent domain admins from deleting other admins, LDAP limits raised.
GDE 4.0.0.3 v1	5/22/2020	GDE Appliance is now compatible with IDT GuardPoints, SecureStart now works with ESG devices.
GDE 4.0.0.4 v1	10/16/2020	Various GUI improvements. You can now integrate with multiple LDAP forests. Web Certificate supports using SAN.

## Assumptions

This documentation assumes that you have knowledge of your computer network as well as network configuration concepts.

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

## Document Conventions

The document conventions describe common typographical conventions and important notice and warning formats used in Thales technical publications.

## Typographical Conventions

This section lists the common typographical conventions for Thales technical publications.

**Table 4-1: Typographical Conventions**

Convention	Usage	Example
<b>bold regular font</b>	GUI labels and options.	Click the <b>System</b> tab and select <b>General</b> Preferences.
<i>bold italic monospaced font</i>	variables or text to be replaced	https://<Token Server name>/admin/ Enter password: <Password>
regular monospaced font	Command and code examples XML examples	Example: session start iptarget=192.168.253.102
<i>italic regular font</i>	GUI dialog box titles	The <i>General Preferences</i> window opens.
	File names, paths, and directories	<i>/usr/bin/</i>
	Emphasis	<i>Do not</i> resize the page.
	New terminology	<i>Key Management Interoperability Protocol (KMIP)</i>
	Document titles	See <i>Installation and Configuration Guide</i> for information about GDE Appliance.
quotes	File extensions Attribute values Terms used in special senses	“js”, “.ext” “true” “false”, “0” “1+1” hot standby failover

## Notes, tips, cautions, and warnings

Notes, tips, cautions, and warning statements may be used in this document.

A Note provides guidance or a recommendation, emphasizes important information, or provides a reference to related information. For example:

### Note

It is recommended to keep tokenization keys separate from the other encryption/decryption keys.

A tip is used to highlight information that helps you complete a task more efficiently, such as a best practice or an alternate method of performing the task.

### Tip

You can also use Ctrl+C to copy and Ctrl+P to paste.

Caution statements are used to alert you to important information that may help prevent unexpected results or data loss. For example:



### CAUTION

**Make a note of this passphrase. If you lose it, the card will be unusable.**

A warning statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data. For example:



**WARNING**

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

## Hardware-Related Warnings

The following warning statement is used to indicate the risk of electrostatic discharge of equipment:



**ELECTROSTATIC DISCHARGE**

**If this warning label is affixed to any part of the equipment, it indicates the risk of electrostatic damage to the module. To prevent equipment damage, follow suitable grounding techniques.**

The following warning statement is used to indicate the risk of hazardous voltages of equipment:



**HAZARDOUS VOLTAGES**

**The warnings in this section indicate voltages that could cause serious danger to personnel.**

## Sales and Support

If you encounter a problem while installing, registering, or operating this product, please refer to the documentation before contacting support. If you cannot resolve the issue, contact your supplier or Thales Customer Support.

Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

For support and troubleshooting issues:

- <https://supportportal.thalesgroup.com>
- (800) 545-6608

For Thales Sales:

- <https://enterprise-encryption.vormetric.com/contact-sales.html>
- [CPL\\_Sales\\_AMS\\_TG@thalesgroup.com](mailto:CPL_Sales_AMS_TG@thalesgroup.com)
- (888) 267-3732



# Chapter 1: Installing & Configuring GDE

---

This chapter describes how to install the IBM Guardium Data Encryption (GDE) virtual appliance as a standalone server or HA node. It contains the following sections:

Overview .....	1
Register on the Thales Support Site in order to download the OVA file .....	1
Extract the GDE appliance license .....	2
Installing the GDE Appliance .....	2
Configure the appliance .....	7

## Overview

The the IBM GDE virtual appliance helps you protect structured and unstructured data and meet compliance requirements. It provides centralized encryption key and policy management to simplify data security management.

In conjunction with the GDE appliance, VTE/VAE/VTs/VPTD agents enable data-at-rest encryption and the collection of security intelligence logs without re-engineering applications or infrastructure.

## Register on the Thales Support Site in order to download the OVA file

1. Go to the Thales Support portal: <https://supportportal.thalesgroup.com>.
2. Click **Register**.
3. Enter the User and Company Info requested.
4. For the Customer Identifier, enter the code 6-ACCT0121078.
5. Select the option to agree to the privacy terms.
6. Click **Submit**.

After submitting your registration form, you will receive a confirmation email with a temporary password. Once you have that, complete your registration.

1. Go to the Thales Support portal and click **Login**.
2. Enter your business email address with which you registered and click **Login**.
3. After a successful login, follow the prompts and change your password.
4. Click **Submit**.
5. In the search field under the Quick Links section, enter the current version and build (<version>.<build>) of the DSM file.
  - For GDE 4.0.0.4, search for 6.4.3.17026

**Note:** The entire naming format is: Vormetric-DSM-Virtual-Appliance-<version>.<build>.ova.

6. Click on the “**Vormetric Data Security Manager 6.4.3.17026 Downloads**” link to go to the Download page.

7. In the table, click on the OVA link in the **Virtual DSM - OVA** section.

**Note:** When you are performing an upgrade, download the file in the **Upgrade Package** field. See ["Upgrade to GDE 4.0.0.4" on page 17](#) for more information on upgrading to the latest version.

8. Once you are on the KB page, click the download link to the right of: **Click here to download file**.

## Extract the GDE appliance license

The GDE enabler contains the license for installation. You will need to upload the license once the GDE appliance is deployed and configured.

### Linux

- GDE\_4\_0\_0\_4.bin
- GDE\_README

### Windows

- GDE\_4\_0\_0\_4.exe
- GDE\_README

1. Download the GDE enabler from the IBM Passport website.
2. For Linux, run the enabler file (GDE\_4\_0\_0\_4.bin). The file must be run on a RedHat or CentOS 6/7 system. To run the file type the following at the prompt:  

```
./GDE_4_0_0_4.bin
```
3. For Windows, run the enabler file (GDE\_4\_0\_0\_4.exe) website by double-clicking it.
4. Select a language to display the instructions and the EULA, by entering a number that corresponds to that language.
5. Accept the default location to install the license, or follow the on-screen instructions to save it to another location. Press **ENTER** to continue.
6. Accept the license agreement.
7. The license is saved on your system in the default location or to the one you specified.

**Note:** Make sure you can access the system on which you have saved the license from the GDE appliance. You will need to upload this license file to start using the appliance.

8. Import the license to your GDE Appliance. You can do this by logging in to the GDE Web UI, navigating to **System > License**, and clicking **Upload License File**.

**Note:** This is also the license that you will use to enable CCKM (CipherTrust Cloud Key Manager)

## Installing the GDE Appliance

This section describes the steps to build a GDE appliance.

### System Requirements

- VMware ESXi v6.0 or later with v9 hardware or later
- VMware vSphere Client

- GDE virtual appliance OVA file

These instructions assume the IP address, routing configuration, and DNS addresses for the GDE, appliance allow connectivity to all hosts where the Vormetric Agents are installed.

## Hardware Requirements

The hardware hosting the virtual machine must meet the following requirements:

### Virtual machine hardware requirements

	Number of Agents			
	1 to 10	11 to 50		Over 250
Number of CPUs	2	4	4	6
RAM (in GB)	4	8	12	16
HD (in GB) (Use "thin" provision to minimize storage utilization.)	250	250	250	above 250

## Installation Plan

1. Assemble configuration information using the checklist, see ["GDE Appliance Installation Checklist" below](#)
2. Complete the pre-configuration tasks.
3. Deploy the GDE appliance as described here, see ["Deploying the GDE Appliance" on page 6.](#)
4. Setup initial and basic configurations as described here, ["Configure the appliance" on page 7](#)
5. Verify Web access as described here, ["Verify web access" on page 11.](#)

## GDE Appliance Installation Checklist

### Installation Checklist

REQUIREMENT	VALUE
Software requirements	
GDE - Virtual Machine file from Support.	
Hardware requirements for Virtual Machine	
1 virtual socket, 4 cores per socket	
4GB memory	
2 virtual NIC cards	
250GB virtual disk	
<b>Network Information</b>	
eth0—dhcp by default.	IP address netmask default gateway (optional)

eth1—this 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.	IP address netmask 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 GDE appliance.	IP address netmask default gateway (optional)
GDE appliance Initial HA node Hostname: FQDN (lowercase only)	
GDE appliance: HA node Hostname: FQDN (lowercase only)	
Domain Name Server (DNS) addresses - up to 3 plus optional DNS search domains.	
NTP server FQDN or IP address (if applicable)	
<b>Certificate Information</b>	
GDE appliance Hostname: FQDN (must be an exact match to the hostname)	
Name of your organizational unit	
Name of your organization	
Name of your city or locality. Must be fully spelled out, no abbreviations.	
Name of your state or province. Must be fully spelled out, no abbreviations, e.g., California <i>not</i> CA	
Two-letter country code	

## 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. A valid hostname must:

- Be an FQDN
- Be in all lowercase
- Match exactly with:
  - Name set in the CLI (system\$ set hostname)
  - Hostname used when running (system\$ security genca)
  - Hostname used when running (system\$ security gencert)

You can also modify the `/etc/hosts` file on the GDE Appliance or identify a host using only the IP address.

- If you use DNS to resolve host names, use the FQDN for the host names.

- Both forward and reverse address resolution is required for nodes in a cluster.
- FQDN name must be lowercase
- If you do NOT use a DNS server to resolve host names, do the following on all of the GDE Appliances and the protected hosts:
  - Modify the *host* file on the GDE Appliance: To use names like serverx.domain.com, enter the host names and matching IP addresses in the `/etc/hosts` file on the GDE Appliance 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 one of the following on *each* GDE Appliance, since entries in the host file are not replicated across GDE Appliances.
  - Modify the *host* file on the protected hosts: Enter the GDE Appliance host names and matching IP addresses in the `/etc/hosts` file on the protected host.

**Note**

*You must do this on EACH protected host making sure to add an entry for all GDE Appliance nodes (if using HA).*

- 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.

## Port configuration

If a GDE appliance must communicate with a device behind a firewall, you must open various ports in the firewall.

The port table lists the communication direction and purpose of each port you must open. See "[Ports to Configure](#)" on page 27.

## Access the Command Line Interface (CLI)

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

```
0000:dsm$ ?
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:dsm$ 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 CLI commands can be found in the *Administrators Guide*.

## Deploying the GDE Appliance

This section describes how to deploy the OVA file to create the appliance. The GDE appliance uses static IP addresses and cannot be assigned an address by DHCP.

1. Open 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. Click **Next**. The **Name and Location** page opens.
5. Type in a name for the Virtual Appliance and then click **Next**. The **Storage** page opens.
6. Select a destination for the Virtual Appliance and then click **Next**. The **Disk Format** page opens.
7. 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 Thick Provisioned Lazy Zeroed.
8. Select **Thick Provisioned Lazy Zeroed** and click **Next**. The *Ready to Complete* window opens.
9. Click **Finish** to deploy the Virtual Appliance. This takes a few minutes.

10. At the message **Completed Successfully**, click **Close**. The main screen of the vSphere Client appears.
11. In the left pane, select the Virtual Appliance you just created and then click the power on icon in the tool bar. It takes about a half hour to provision the VM and build the appliance.
12. To watch the output as the installation progresses, click the Console tab and click inside the console window. When the installation is finished, continue to the next section.

## Configure the appliance

This section describes how to configure network settings, NTP, Time Zone and Date/Time, and the hostname. It describes how to configure a bonded NIC device type should you choose to use this feature. It also describes how to generate a certificate authority (CA), add console administrators, and verify Web access.

If you are setting up the GDE appliance in a high availability (HA) deployment, configure each node as a standalone appliance, which is the same procedure as described here. Then add each node to the initial node and join the HA network.

## Configure network settings

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

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

2. The Thales EULA is displayed, type 'y' to accept and press Enter.
3. When prompted, type in a new password and press **Enter**. Reconfirm your password.
4. Do not lose this password.
5. Navigate to the *network commands* menu. Type:

```
0000:dsm$ network
```

6. Add an IP address for the GDE appliance. Type:

### Note

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

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

```
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 and you choose to configure eth0 with a new IP address, you will be disconnected at this step. Reconnect on the new IP address.

7. (Optional) You may choose to configure the eth0 interface instead of retaining the default IP address 192.168.10.1, if for example, you want the GDE appliance to communicate with agents on a different subnet, or access the Management Console from a different subnet. To configure an IP address for eth0, type:

```
0001:network$ ip address init <eth0 IP address>/<subnet mask (e.g., 16 or 24)> dev eth0
ip address init 192.168.10.3/16 dev eth0
```

```
IPv 6 Example: ip address init fa01::3:15:130/64 dev eth0
```

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.

8. 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>
```

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

IPv 6 Example:

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

9. Verify interface settings. Type:

```
ip address show
```

10. Verify route settings. Type:

```
ip route show
```

11. If you are using DNS, set the initial DNS server for the GDE appliance. Type:

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

12. If you have a second or third DNS server, set them for the GDE appliance. Type:

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

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

```
dns search <search_domain>
```

14. Show the DNS settings. Type:

```
dns show
```

15. Return to the main menu. Type:

```
up
```

## Configure a bonded NIC device

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

On the 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 appliances 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 on all nodes individually.



1. Access the GDE appliance 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;

```
0000:dsm$ network
0001:network$
```

3. Enable the bonded NIC;

```
0001:network$ ip address init <ip_address>/<subnet_mask> dev bond0
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 GDE appliance 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` interface.

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

```
0001: ip route add default table main.table dev bond0 via <gateway_ip_address>
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 Appendix 1: "Bonding Driver Modes" on page 1 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
0003:network$ ip address flush bond0
```

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

## Configure NTP, time zone, date, time

You must have the correct time set on your GDE appliance(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:

```
0000:dsm$ maintenance
```

2. Show the current ntpdate settings. Type:

```
0001:maintenance$ ntpdate show
```

3. Add a new ntpdate server. Type:

```
0002:maintenance$ ntpdate add <IP address/Hostname for the ntpdate server>
```

4. Repeat this step for each ntpdate server.

5. Activate the ntpdate server connection. Type:

```
0003:maintenance$ ntpdate on
```

6. Show the current timezone settings. Type:

```
0004:maintenance$ gmtimezone show
```

7. Set the country and city where the GDE appliance resides. Type:

```
0005:maintenance$ gmtimezone set <country/city>
```

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

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

9. 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.

10. Verify your settings. Type:

```
0008:maintenance$ time
```

```
0009:maintenance$ date
```

11. Return to the main menu. Type:

```
0010:maintenance$ up
```

## Configure the hostname

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

```
0001:dsm$ system
```

2. Show the current setting. Type:

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

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

4. Set the hostname. You must enter the fully qualified domain name for the GDE appliance. Type:

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

5. Example:

```
0003:system$ setinfo hostname securityserver.company.com
```

## Generate the Certificate Authority

1. Generate a new certificate authority for the GDE appliance. Type:

```
0004:system$ 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 GDE appliance server software will be restarted. Type 'yes' to continue, the default is 'no'.

3. Enter the FQDN of this appliance, the name displayed in 'This Security Server host name [FQDN of the GDE appliance]', 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]:
  - f. What is the validity period of the generated certificate (from 2 to 10 years)? [10]:
5. Once the certificate is signed, return to the main menu. Type:

## Add CLI administrators

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

1. Navigate to the *user commands* menu. Type:  

```
0001:dsm$ user
```
2. Add an administrator. Type:  

```
0002:user$ 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:  

```
0003:user$ 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 GDE appliance hostname (if configured in DNS) or the IP address.

Example URL:

```
https://securityserver.vormetric.com
```

If the URL doesn't work because, for example, port 443 is blocked by a firewall, specify port 8448 or 8445.

### Example:

```
https://securityserver.vormetric.com:8448
```

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

If the link still does not work, make sure all the necessary ports are open, see "IPMI Ports" on page 1

The first time you connect to the appliance via a web browser, a self-signed certificate is used by default. Your browser will display a warning about the SSL certificate, follow the instructions on your browser to continue with the default self-signed certificate. You can configure the GDE appliance to use third party signed certificates after you have logged in for the first time. Refer to the *GDE Administrators Guide*, chapter 6 for procedures to do this.

The default user name and password to log on to the GDE appliance 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 the GDE appliance, 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**.

Upload the license file that you extracted from the enabler package.

After uploading your license file, all the other tabs for which you have licenses are displayed.

# Chapter 2: Upgrading GDE Appliance Software

This chapter contains instructions for upgrading and migrating data to GDE 4.0.0.4

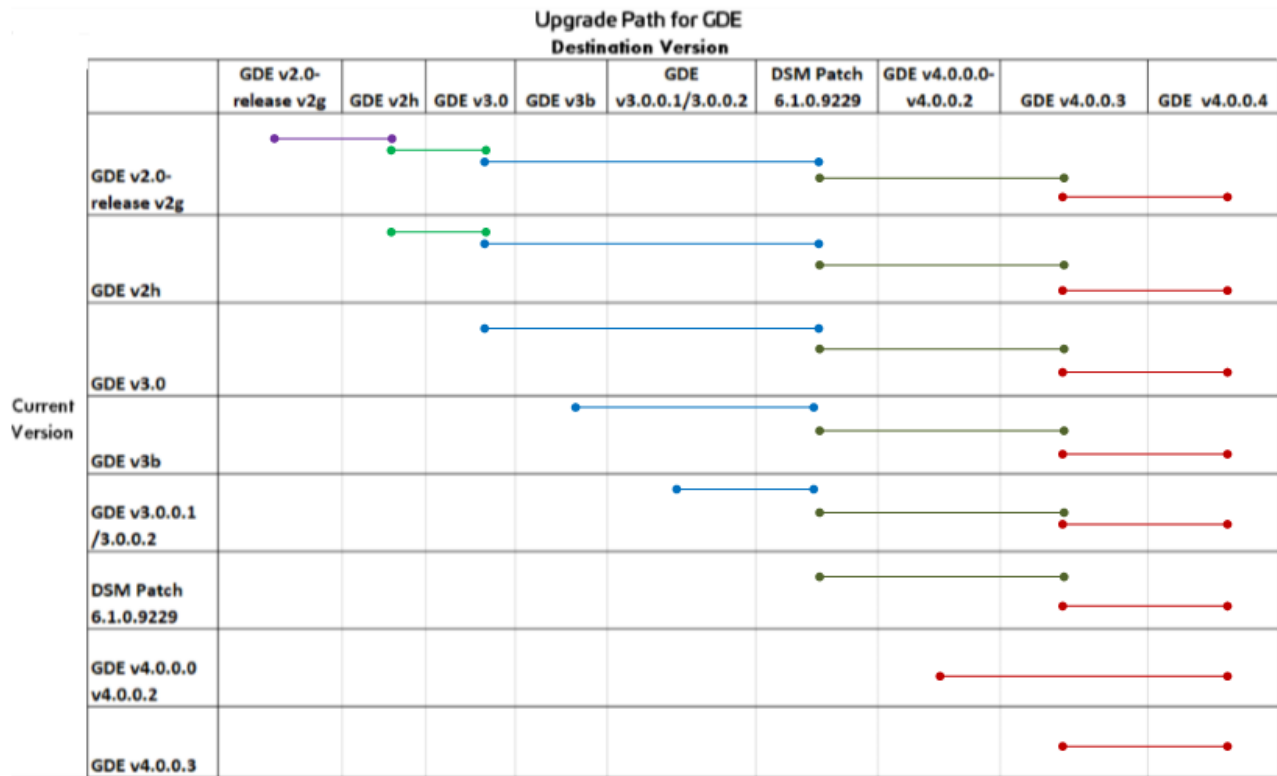
It contains the following sections:

- [Upgrade Paths](#) ..... 13
- [Migrating to a GDE 3.0 Appliance](#) ..... 13
- [Upgrade to the DSM patch 6.1.0.9229](#) ..... 16
- [Upgrade to GDE 4.0.0.4](#) ..... 17

## Upgrade Paths

The following table describes the GDE upgrade path based on your current version:

**Figure 2-1: Upgrade Path for GDE**



- The change from DSM patch 6.1.0.9229 to GDE v4.0.0.3 involves a database migration. That migration is built into 6.1.0.9229, which is why all users must upgrade to 6.1.0.9229 first, and then upgrade from 6.1.0.9229 to GDE v4.0.0.3.
- The change from v4.0.0.3 to v4.0.0.4 involves a BDR upgrade. This requires all users to upgrade to GDE v4.0.0.3 first, and from there, upgrade to GDE v4.0.0.4

## Migrating to a GDE 3.0 Appliance

As illustrated in the upgrade path illustration, you must first upgrade your GDE appliance to GDE 3.0. To complete this task, you must:

1. Backup the current configuration
2. Install and configure a GDE appliance
3. Restore backup to new GDE appliance

#### Note

If you are upgrading from a version higher than GDE 3.0, you can upgrade directly to the DSM patch 6.1.0.9229. Prior to upgrading, follow the steps below to backup your current configuration, in case the upgrade fails to upgrade your system properly.

## Backup the current configuration

A backup is a snapshot of a GDE appliance configuration. When a backup is restored, the GDE appliance Management Console will contain and display the same information captured at the time the backup was originally made.

## Create or import a wrapper key

GDE appliance backup files are encrypted with a wrapper key to keep them secure. This wrapper key must be created, or imported from a previous create operation, before creating a backup. The same wrapper key used to encrypt a backup is also required to restore that backup. For additional security, wrapper keys can be broken up into key shares—pieces of a wrapper key. These key shares can then be divided amongst two or more custodians, such that each custodian must contribute their key share in order to assemble a complete wrapper key. This is also referred to as split key knowledge or M of N configuration.

For example, you can break up the wrapper key amongst a total of five custodians and set the minimum number of required custodians at two. When the wrapper key is required, at least two of the custodians must contribute their key share in order to assemble a complete wrapper key. The wrapper key must be created by a System administrator or an All Admin.

1. Log on to the Management Console as a System administrator or an All Admin.
2. Select **System > Wrapper Keys** from the menu bar.
3. In the Wrapper Keys window, select **Operation > Create**, then click **Apply** to create the wrapper key.
4. Select **System > Backup and Restore > Manual Backup and Restore** from the menu bar.  
A confirmation message also displays on this tab, stating that the wrapper key exists. You can now proceed with creating a backup.
5. Click **Backup** tab and select **Ok**.

#### Note

Some Browsers will automatically save and download the file. Some will display a Save as dialog.

6. Click **Save** in the File Download dialog box, if your browser displays one.
7. 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\_<gde server name>\_yyyy\_mm\_dd\_hhmm.tar (.zip for Windows). Where <gde\_server name> is the FQDN of the GDE appliance that is being backed up.
8. Return to the **System > Wrapper Keys** menu option and select **Operation > Export** to export key shares.
9. 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.

10. Select the GDE appliance administrators who will serve as custodians for the wrapper key shares.  
Administrators of type System Administrator and All are listed. You can select any of these administrators, with the exception of the default initial log on administrator admin, as a custodian.
11. Click **Apply** on the bottom right hand corner.  
If you have selected more than one custodian, each of them is given a share of the wrapper key. The wrapper key share is displayed on their Dashboard page, beneath the fingerprint for the CA, when they log into the Management Console. The generated wrapper key, or key shares, are exported and are visible on the Dashboard, beneath the fingerprint for the CA. The Wrapper Key Share displayed on the Dashboard is a toggle. Click **Show** to display the wrapper key share value. Each administrator must see a unique wrapper key share displayed on the dashboard beneath the fingerprint for the CA.
12. On the Dashboard, click **Wrapper Key Share** string to hide the value and display 'Show'.
13. Ensure the administrator(s) or wrapper key custodian(s) securely store a copy of this key or key share. This is required, as part of their role in a GDE appliance restore operation.

**Note**

Do NOT lose the wrapper key used to create the backup. You cannot restore the backup without the wrapper key that was used to create it.

14. Create a backup of the GDE appliance configuration after the wrapper key has been created.

## Create a backup

1. Log on to the Management Console as a System/All Administrator.
2. Select the **System > Backup and Restore** menu option. The Manual Backup and Restore page opens.
3. Click **Backup** tab and then click **Ok**.
4. 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_<gde server name>_yyyy_mm_dd_hhmm.tar (.zip)`  
Where <gde server name> is the FQDN of the GDE appliance that is being backed up.
5. Save the backup to a secure location. Access to the backup should be limited to only a few employees and should be audited.

## Install and configure a GDE appliance

In order to ensure the continuity of your GDE deployment, you must configure the GDE 3.0 appliance with the same hostname as the GDE appliance that is being migrated. You can assign a new IP address to the appliance, however you must ensure that the hostname resolution method in use is correspondingly updated.

**Note**

If you are using a third party SSL certificate, then a change in the GDE appliance hostname will cause a conflict when you restore the backup.

You will have to upload a new third party certificate with the new GDE appliance hostname.

After you configure the new GDE 3.0 appliance with the same hostname and IP address, you must take the old appliance off of the network, otherwise any registered agents will try and communicate with both the old and the new GDE appliance and cause conflicts in your system.

If you configure a GDE 3.0 appliance and give it a new hostname, then when you reach your destination version of the GDE software, VTE agents that were registered with the earlier GDE appliance backup will have to re-register with the new GDE appliance. Refer to the VTE Agent Installation and Configuration Guide for detailed procedures to re-register agents.

For procedures to install and configure a GDE appliance, see ["Installing the GDE Appliance" on page 2](#).

## Restore backup to new GDE appliance

The GDE appliance backup is restored via the Management Console.

1. Locate the backup that is to be restored.
2. Log on to the Management Console as a System/All administrator.

### Note

If you already have the Wrapper Key imported, skip to Step 8.

3. Import wrapper keys. Select **System > Wrapper Keys** from the menu bar.
4. Select **Import from the Operation** dropdown menu. Click **Add**.
5. If key shares have created from the wrapper key, paste a Key Share value from one previously stored with a custodian into the Key Share text field and click Ok.
6. Repeat steps 5 and 6 for each administrator selected as a key custodian if you have chosen to have more than one custodian for the wrapper key. 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.
7. Click **Apply** to finish importing the wrapper key.
8. Restore the backup file. Select **System > Backup and Restore** from the menu bar.
9. Select the **Restore** tab.
10. Click **Browse**. Locate and select the backup file to restore.
11. Click **Ok**. The restored file uploads and the GDE appliance disconnects from the Management Console. The restore operation takes up to 30 minutes to complete.  
If the browser has not refreshed automatically after the restore operation, you must manually refresh the browser to log back on to the Management Console.  
If you were using a third party SSL certificate, this certificate will now also be restored as part of this operation. See ["Verify web access" on page 11](#) for more details.
12. Log back on to the Management Console as an administrator of type System or All. Verify that the configuration is restored correctly

## Upload a license

As part of the process of configuring a new GDE 3.0 appliance, you will have already uploaded the GDE 3.0 license. However, once you restore a backup of the earlier GDE version, you will need to upload the license once again. Click **System > License > Upload the license file**.

## Upgrade to the DSM patch 6.1.0.9229

After upgrading to GDE 3.0 or higher, you must upgrade to the DSM patch 6.1.0.9229:

1. Click **System > Software upgrade**.



2. Delete the idle version if it exists.
3. Select the 6.1.0.9229 upgrade tar file.
4. Click **Upgrade**.

## Upgrade to GDE 4.0.0.4

After upgrading to 6.1.0.9229, you can upgrade to GDE 4.0.0.3.

1. Click **System > Software upgrade**.
2. Delete the idle version if it exists.
3. Select the GDE 4.0.0.3 upgrade tar file, which is 6.4.2.16023.
4. Click **Upgrade**.

After upgrading to 4.0.0.3, you can upgrade to GDE 4.0.0.4.

1. Click **System > Software upgrade**.
2. Delete the idle version if it exists.
3. Select the GDE 4.0.0.4 upgrade tar file, which is 6.4.3.17026.
4. Click **Upgrade**.

# Chapter 3: HA for V6x00 and Virtual Appliances

---

HA Overview .....	18
Supported HA Deployments .....	18
Configuring HA for Virtual Appliances .....	18
Adding a Host to a new HA node .....	22
Upgrading an HA Cluster .....	22
Deleting a Node from a Cluster .....	24

This chapter describes how to set up High Availability (HA) for V6x00 hardware and virtual appliances. Refer to the High Availability chapter in the *Administrators Guide* for details about managing an HA deployment.

## HA Overview

To configure High Availability (HA) for GDE Appliances, you need to be a System/All administrator and have GDE Appliances CLI privileges. A GDE Appliances HA configuration consists of two or more GDE Appliances HA nodes.

As of GDE Appliances v6.2.0, HA is now configured as Active-Active. This means that there is no longer a primary or a failover node. All nodes are peers. When one node fails, the other nodes continue operating normally. When the failed node is working properly again, it synchronizes with the other HA nodes. that if you are migrating from 6.1.x or an earlier version, then you can't upgrade or migrate. You have to create a new cluster.

### Note

If you are migrating from an HA cluster that is GDE Appliances v6.1.x or an earlier version, then you cannot upgrade or migrate your cluster to 6.2.x or 6.3.x. You must create a new cluster. See "[Migrating from DSM v6.1.0.9229 to DSM 4.0.0.4](#)" on page 1 for more information.

## Supported HA Deployments

You must have at least two GDE Appliance HA nodes installed on the same network to create an HA cluster. The maximum number of nodes allowed in an HA cluster is eight.

To ensure reliable operation, the appliances in an HA cluster must run the same version of the GDE Appliances software and have the same hardware configurations.

## Configuring HA for Virtual Appliances

This section describes how to configure an HA cluster for a virtual appliance in an HA cluster.

### Prerequisites

Before you set up your HA cluster, do the following:

1. Specify a hostname 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 modify the `hosts` file on the HA node:

- a. Log in to the CLI menu.
- b. Type: **network**
- c. Type: **host add <hostname> <IP address>**

You can also identify a host using only the IP address.

- If you use DNS to resolve host names, use the FQDN for the host names.
  - Both forward and reverse address resolution is required for nodes in a cluster.
  - FQDN name can be lower or uppercase, however, the GDE Appliances converts and displays all node names as lowercase.

2. Open all required ports. To see the ports to configure, see "IPMI Ports" on page 1

#### Note

For upgrades and fresh installations of GDE Appliances 6.2.0, if you are using HA, you must open port 5432 in your firewall to allow communication between GDE Appliances HA nodes. For Azure and AWS platforms, you will need to add this port to your security groups. You can now close port 50000 as it is no longer used.

3. Perform a 'ping' operation on all of the GDE Appliances to ensure that network communication is working between the GDE Appliances HA nodes.

## Network Latency

If the network latency between the HA nodes 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 in network latency is the Policy Version History setting (System > General Preferences > System > Policy (Maximum Number of Saved Policy History)). Each time changes are made to a policy, a new version of that policy is created. This setting determines how many previous versions of the policy to keep. The more versions that are kept, the longer the delay because it increases the time required to replicate policy data to the cluster nodes. We recommend changing this value to 0 or 5 from the default of 10 if you experience network latency.

## Adding Nodes to an HA Cluster

Only add one HA host to the cluster at a time. Adding multiple hosts at the same time does not work.

1. Install and configure your GDE Appliances as described in previous chapters of this guide.

#### Note

The license must be installed on the GDE Appliance designated as HA node 1 before you can configure the other HA nodes.

2. On HA node 1 (the Initial Server), log on to the Management Console as an administrator of type System, or All.
3. Click **High Availability** in the menu bar. The *High Availability Servers* window opens.
4. Click **Add**. The **Add High Availability Server** window opens.
5. In the **Server Name** field, enter the host name or FQDN of a GDE Appliance node.
6. Click **Ok**. The GDE Appliance node is listed in the High Availability Servers window. It is designated as 'Not Configured'.

Figure 3-1: Node added but not configured/joined to the cluster

Selected	Name	Response Time (ms)	Configured	Synchronization Status
<input type="checkbox"/>	dsnc5090.i.vorwetric.com		<input checked="" type="checkbox"/>	<span style="color: green;">●</span>
<input type="checkbox"/>	dsnc5096.i.vorwetric.com	SNMP Disabled	<input checked="" type="checkbox"/>	<span style="color: green;">●</span>
<input type="checkbox"/>	dsnc5100.i.vorwetric.com	SNMP Disabled	<input checked="" type="checkbox"/>	<span style="color: green;">●</span>
<input type="checkbox"/>	dsnc5103.i.vorwetric.com	SNMP Disabled	<input type="checkbox"/>	<span style="color: orange;">▲</span> Not Configured

**Note**

You can also add nodes in the CLI. See the High Availability Category section in the CLI chapter in the GDE Appliance Admin guide.

### Join a Node to an HA Cluster

Joins the current node to the HA cluster. If you are joining an HA cluster after an upgrade, and the node previously had a host assigned to it, after it successfully joins the cluster, the GDE Appliances asks if you want the host restored to the node. Only join one HA host to the cluster at a time. Joining multiple hosts at the same time does not work.

To join an HA node to the HA cluster:

1. In the CLI, log on to HA Node 2 on the Cluster.

2. Switch to the HA menu, type:

```
0000:dsm$ ha
```

3. Join the node to the cluster. Type:

```
0000:dsm$ join
```

**System Response:**

```
WARNING: This server node is about to join an HA cluster.
```

```
Please make sure the HA cluster is running and has this server node in its HA node list.  
This may take several minutes.
```

**Note**

Sometimes, when GDE Appliances nodes are spread far apart geographically, or are in a cloud environment, the Join function takes so long that the ssh session times out and terminates automatically before the Join can finish. If the Join function fails, type: **join longwait** to make the join command proceed in a 'longwait mode' (as opposed to the 'normalwait' mode). The difference between the two modes is the duration that it waits for the node replication status state to be set to 'ready.' Longwait waits for approximately twice as long as the normalwait mode.

4. Follow the prompts:

- a. Type **yes** to continue.
- b. For **HA Initial Server host name**, type the hostname of HA Node 1.
- c. For **Initial Security Server system administrator name**, type the UI admin name for the **Current** node.
- d. For **Initial Security Server system administrator password**, type the UI admin password for the **Current** node.

**System Response:**

This node may have multiple IP addresses. All the agents will have to connect to the Security Server using the same IP.

Enter the host name of this node. This will be used by Agents to talk to this Security Server.

This Security Server host name[dsml5100.i.vormetric.com]:

Please enter the following information for key and certificate generation.

5. The HA cluster will issue the certificate using the information you provide in the following steps:

- e. What is the name of your organization? []:
- f. What is the name of your City or Locality? []:
- a. What is the name of your organizational unit? []:
- b. What is the name of your State or Province? []:
- c. What is your two-letter country code? [US]:
- d. What is your email address? []:
- e. What is the validity period of the generated certificate (from 2 to 10 years)? [10]:

**System Response:**

WARNING: The following information you entered will be used to join this server to the HA cluster, please make sure the information is correct

Initial Security Server host name:HaNode1.i.vormetric.com

Initial Security Server system administrator name:voradmin

Initial Security Server system administrator password:xxxxxxx

This Security Server host name[dsml5100.i.vormetric.com]:HaNode2.i.vormetric.com

The name of your organizational unit: TP

The name of your organization: Thales

The name of your City or Locality: SJ

The name of your State or Province: CA

Your two-letter country code[US]: US

What is your email address: groot@thales.com

Restore original host assignment back to this node (yes/no)[yes]:

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

6. Type **yes** to continue.

7. The installation utility creates certificates, completes the installation process, and then starts the HA node. This may take a few minutes.

The CA certificate fingerprint is displayed.

8. On HA node 1 on the Management Console, click the **Dashboard** tab.

9. Match the fingerprint from the output on HA node 2 with the **RSA CA fingerprint** on the HA node 1 **Dashboard**.

**Sample output:**

```
Initial_Server=HaNode1.i.vormetric.com CAs_  
Fingerprint=8F:104:BE:78:0E:BB:28:4F:64:4D:54:5A:B1
```

Ensure the fingerprint listed above matches the one on the Security Server web console dashboard.

Self test in progress: passed

Starting data store

Starting Security Server

Security Server started in compatible mode

SUCCESS: joined to the HA cluster. The server is started. Please verify the fingerprint.

0009:ha\$

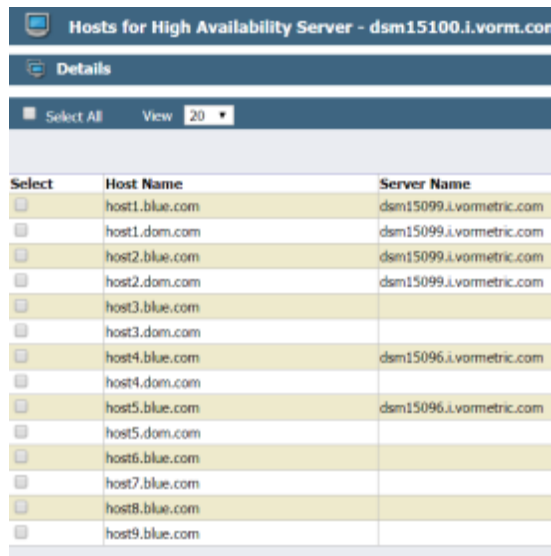
10. In the GUI, click the **High Availability** tab. In the row for the HA node 2, the **Synchronization status** should contain a green circle and the Configured column should contain a check.

## Adding a Host to a new HA node

If an HA node fails, when the HA node is running again, it will synchronize with the other HA nodes. However, if a host requires a connection to an HA node in the cluster and cannot wait for that node to restart, you can manually move the host to another node. To move the hosts:

1. On the GDE Appliance, click **High Availability**.
2. Click on the Name of the node to which you want to move the Agent(s).
3. Click **Host Assignment**.
4. Click **Add**. The Details page opens and displays all of the Agents connected to the HA cluster.

**Figure 3-2: Host Assignments for HA Server**



The screenshot shows a web interface titled "Hosts for High Availability Server - dsm15100.i.vormetric.com". Below the title is a "Details" section with a "Select All" button and a "View" dropdown set to "20". The main content is a table with three columns: "Select", "Host Name", and "Server Name". The table lists 14 hosts, each with a checkbox in the "Select" column. The "Host Name" column contains entries like "host1.blue.com", "host1.dom.com", "host2.blue.com", "host2.dom.com", "host3.blue.com", "host3.dom.com", "host4.blue.com", "host4.dom.com", "host5.blue.com", "host5.dom.com", "host6.blue.com", "host7.blue.com", "host8.blue.com", and "host9.blue.com". The "Server Name" column contains "dsm15099.i.vormetric.com" for hosts 1-5, "dsm15096.i.vormetric.com" for hosts 4-5, and is empty for hosts 6-9.

Select	Host Name	Server Name
<input type="checkbox"/>	host1.blue.com	dsm15099.i.vormetric.com
<input type="checkbox"/>	host1.dom.com	dsm15099.i.vormetric.com
<input type="checkbox"/>	host2.blue.com	dsm15099.i.vormetric.com
<input type="checkbox"/>	host2.dom.com	dsm15099.i.vormetric.com
<input type="checkbox"/>	host3.blue.com	
<input type="checkbox"/>	host3.dom.com	
<input type="checkbox"/>	host4.blue.com	dsm15096.i.vormetric.com
<input type="checkbox"/>	host4.dom.com	
<input type="checkbox"/>	host5.blue.com	dsm15096.i.vormetric.com
<input type="checkbox"/>	host5.dom.com	
<input type="checkbox"/>	host6.blue.com	
<input type="checkbox"/>	host7.blue.com	
<input type="checkbox"/>	host8.blue.com	
<input type="checkbox"/>	host9.blue.com	

5. Select and click **OK** for nodes that you want to move to your current node. The GDE Appliance moves the selected Agent host from the previous HA node to the current HA node.

### Note

You can assign both unassigned hosts and hosts currently assigned to other nodes. GDE Appliances will move those nodes from the previous node to the current node.

6. Once the original HA node is up and running, you can reassign the VTE Agent(s) back to the original node, if desired.

## Upgrading an HA Cluster

When upgrading the nodes in an HA cluster, you must break the cluster by removing a node from the cluster, running the HA cleanup function and then upgrading that node independently.

### Note

If you are migrating from an HA cluster that is DSM v6.1.x or an earlier version, then you cannot upgrade or migrate your cluster to 6.2.x or 6.3.x. You must create a new cluster.

After upgrading all of the HA nodes:

1. Add them back into the HA cluster.
2. Join them to the HA cluster.
3. Assign new VTE Agents to their nodes.

**Note**

Do not reassign hosts in the HA cluster that are already registered to a node. The host assignment is preserved. When a node is removed from the cluster and then joined back into it, the host(s) are reassigned to the same node.

## Prerequisite

- Backup your current GDE Appliances configuration, as described above, "[Backup current DSM configuration](#)" on [page 1](#).

**Note**

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

## Remove Nodes from the HA cluster

Breaking up the HA cluster involves removing the nodes from the HA cluster. On HA node 1, the initial node, log in to the CLI menu as CLI Admin.

1. Switch to the HA menu, type:

```
0001:dsm$ ha
```

2. Remove the node from the HA menu, type:

```
0002:ha$ remove <FQDN/HA_node_IP>
```

**Example**

```
0002:dsm$ remove HAnode3.i.vormetric.com
```

**System Response:**

```
WARNING: This command is going to remove one server node from the HA cluster.  
This may take several minutes.  
Continue? (yes|no)[no]: yes  
SUCCESS: Removed server node HAnode3.i.vormetric.com from the HA cluster.
```

3. Repeat the previous step for all of the nodes in the HA cluster.
4. After removing the nodes, log on to one of the other nodes, (not the initial one) as CLI Admin and switch to the HA menu.

```
0001:dsm$ ha
```

5. Cleanup the HA configuration data on the node, type:

```
0002:ha$ cleanup
```

**System Response:**

```
WARNING: This command cleans up HA configuration data of, and restarts, this server.  
This may take several minutes.  
Continue? (yes|no)[no]:
```

6. Type **yes** to continue.

```
SUCCESS: cleanup
```

7. Repeat the cleanup process for every node that you removed from the HA cluster.

## Upgrade the Initial HA node

In the GUI, upgrade the initial node to the latest version of the 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 one which is not in use.
3. Click **Browse/Choose File** 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 login screen after the upgrade completes.
6. Repeat these steps to upgrade each of the other nodes in the HA cluster.

## Optimize the Upgrading of Nodes in the HA Cluster

The initial node is the only node that needs to be upgraded. This ensures that all of the content of the node: policies, admins, domains, keys, reports, logs, etc. will be saved. However, an upgrade is unnecessary for the other nodes in the cluster, because all of the content of the initial node will be copied over from the initial node when all of the nodes in the HA cluster synchronize. Therefore, to optimize upgrading the virtual GDE Appliance for the additional nodes in the HA cluster:

1. Upgrade the initial node to GDE v4.0.0.4.
2. On each additional node, perform a fresh installation of GDE v4.0.0.4. In other words, use the OVA file for the installation, not the upgrade tar file.
3. Once the software upgrade/installation on each of the nodes is complete, add the nodes to the cluster and join the HA cluster. See ["Adding Nodes to an HA Cluster" on page 19](#) and ["Join a Node to an HA Cluster" on page 20](#) for more information.

## Deleting a Node from a Cluster

Deleting a node from a cluster with no host assigned to it is straightforward. When deleting nodes with hosts, you must reassign the hosts to other nodes.

### Deleting a Node from a Cluster with no Hosts assigned

Log into the Management Console on the Initial Server as a System/All Administrator.

1. Select **High Availability** in the menu bar.
2. Check the box next to the node to be deleted.
3. Click **Delete** to remove the node from the cluster.
4. Log in to the CLI of the HA node that you are removing from the cluster.
5. Switch to the HA menu, type:  

```
0001:dsm$ ha
```
6. To disable the communication between the nodes and stop synchronizations to the node, in the HA menu, type:  

```
0001:ha$ cleanup
```



## Deleting a Node from a Cluster with Hosts assigned

When deleting a node from an HA cluster, you must reassign the hosts in the CLI or in the UI. You can:

- Re-assign hosts from their designated HA node to another HA node.
- Use the `rr` (round robin) option and have the GDE Appliances evenly distribute the hosts to balance the load in the HA cluster.

## Moving a Host to a different Node with the CLI

To move the hosts to a specific HA node, type:

```
0001:ha$ remove <node1> reassignhost <node2>
```

### Example

```
0001:ha$ remove dsm15099.i.vormetric.com reassignhost dsm15100.i.vormetric.com
```

To make the GDE Appliances move the hosts to HA nodes and evenly distribute the load, type:

```
0001:ha$ remove <node1> reassignhost rr
```

### Example

```
0001:ha$ remove dsm15099.i.vormetric.com reassignhost rr
```

### System Response

WARNING: This command removes the given server node from the HA cluster. After deletion, running the "ha cleanup" command from its CLI will be required.

This may take several minutes.

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

SUCCESS: Removed server node from the HA cluster.



### WARNING

Remember to **ALWAYS** run `cleanup` on the node that was removed from the HA cluster.

## Moving a Host to a different Node with the UI

When you delete a node in the UI that has hosts assigned to it, a dialog opens providing options for host reassignment. You can cancel the delete and manually reassign the hosts yourself, or the GDE Appliances can perform the reassignment.

1. On the GDE Appliance, click **High Availability**.
2. Select the node to which you want to move the Agent(s).
3. Click **Delete**.

The Delete HA node dialog opens if the node has hosts attached. The options are:

- Manually assign the hosts to other nodes before deleting `<node>`. Click **Cancel**.  
See ["Adding a Host to a new HA node" on page 22](#).
- Leave hosts unassigned after deletion of `<node>`. Click **Delete**.  
See ["Deleting a Node from a Cluster with Hosts assigned" above](#)
- Let GDE Appliances assign hosts to available nodes in the cluster before deleting `<node>`. Click **Delete**.  
The GDE Appliances evenly distributes the hosts to balance the load in the HA cluster.

- Assign hosts to a specific node before deleting *<node>*. Click **Delete**.
4. When you select this last option, the “Node to assign to” menu opens. Select a node from the dropdown menu.
  5. Click Delete.

**Note**

After deletion, make sure that you log on to the deleted node through the CLI menu and run **HA > Cleanup**.

# Appendix A: Ports

Ports to Configure .....27

This section describes all of the ports that you must configure for your appliance.

## Ports to Configure

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

**Table A-1: Ports to Configure**

Port	Protocol	Communication Direction	Purpose
	ICMP	All ICMP	Used for Ping
22	TCP	Management Console → GDE Appliance	CLI SSH Access
161	TCP/UDP	SNMP Manager → GDE Appliance	SNMP queries from an external manager
443	TCP	Browser → GDE Appliance GDE Appliance ↔ GDE Appliance Agent → GDE Appliance	Redirects to either port 8445 or 8448 depending on the security mode. (8445 is used in compatible & RSA modes; 8448 is used in Suite B mode, for secure communication between GDE Appliances in an HA cluster and for LDT registration.)
5432	TCP	GDE Appliance (HA node 1) ↔ GDE Appliance (HA node n)	HA information exchange.
5696	TCP	KMIP client → GDE Appliance	Allows communication between the KMIP client and GDE Appliances
7024	TCP	DSM → Agent	Policy/Configuration Exchange
7025	TCP/UDP	GDE Appliance ↔ GDE Appliance	Uses SNMP to get HA node response time.
8080	TCP	Agent → GDE Appliance GDE Appliance ↔ GDE Appliance	Port 8080 is no longer used for registration, but you can manually close/open this legacy port for new deployment, for backward compatibility if you use previous versions of the agent and need to register to 8080. Default is on (open). Syntax 0001:system\$ security legacyregistration [ on   off   show ]

**Table A-1: Ports to Configure (continued)**

Port	Protocol	Communication Direction	Purpose
8443	TCP	Agent → GDE Appliance	RSA TCP/IP port through which the agent communicates with the GDE Appliance, in case 8446 is blocked. The agent establishes a secure connection to the GDE Appliance, through certificate exchange, using this port.
8444	TCP	Agent → GDE Appliance	RSA port via which the Agent log messages are uploaded to GDE Appliance, in case 8447 is blocked.
8445	TCP	Browser → GDE Appliance GDE Appliance ↔ GDE Appliance (fall back)	Management Console, VMSSC, and fall back for HA communication in case port 8448 is dropped.
8446	TCP	Agent → GDE Appliance	Configuration Exchange using Elliptic Curve Cryptography (Suite B)
8447	TCP	Agent → GDE Appliance	Agent uploads log messages to GDE Appliance using Elliptic Curve Cryptography (ECC) and RSA
8448	TCP	Browse → GDE Appliance GDE Appliance ↔ GDE Appliance Agent → GDE Appliance	GUI Management during enhanced security using Elliptic Curve Cryptography (Suite B). Also for secure communication between GDE Appliances in an HA cluster. Also used for communication between host with LDT host and GDE Appliance during Agent registration.
8449	TCP	Smart Card → GDE Appliance	Smart card used with RSA mode
8450	TCP	Smart Card → GDE Appliance	Smart card used with ECC/compatible mode
9005	TCP	GDE Appliance ↔ remote admin	Used by Remote Administration Service process to accept connections from the Remote Administration Client.

# Appendix B: Troubleshooting

---

Loss of Connection ..... 29

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](https://192.168.10.11:8448) for Suite B mode).
2. Check if the appliance is a trusted site in your web browser's Security Options.
3. Netcat or Telnet to the appliance and see if it's listening on port 8445. (8448 for Suite B mode.)

### 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 "[Ports to Configure](#)" on [page 27](#) for information about ports that need to be configured.