IBM® Guardium Data Encryption

Administrators Guide

Release v3.0.0.2

IBM Guardium Database Encryption 3.0.0.2 is the same product as Vormetric Data Security (VDS) Release 6.1.0. VDS Release 6.1.0 consists of Data Security Manager release and Vormetric Agents releases.

THALES

Vormetric Data Security Platform

Vormetric Data Security

Version 6.1.0

Administrators Guide

SEPTEMBER 06, 2018

DOCUMENTATION VERSION 1

Vormetric Data Security
DSM release 6
Version 6.1.0
Administrators Guide
September 06, 2018
PN: 50-1000170-09
Produced in the United States of America

NOTICES, LICENSES, AND USE RESTRICTIONS

Vormetric, Thales, and other Thales trademarks and logos are trademarks or registered trademark of Thales e-Security, Inc. in the United States and a trademark or registered trademark in other countries.

All other products described in this document are trademarks or registered trademarks of their respective holders in the United States and/or in other countries.

The software ("Software") and documentation contains confidential and proprietary information that is the property of Thales e-Security, Inc. The Software and documentation are furnished under license from Thales and may be used only in accordance with the terms of the license. No part of the Software and documentation may be reproduced, transmitted, translated, or reversed engineered, in any form or by any means, electronic, mechanical, manual, optical, or otherwise.

The license holder ("Licensee") shall comply with all applicable laws and regulations (including local laws of the country where the Software is being used) pertaining to the Software including, without limitation, restrictions on use of products containing encryption, import or export laws and regulations, and domestic and international laws and regulations pertaining to privacy and the protection of financial, medical, or personally identifiable information. Without limiting the generality of the foregoing, Licensee shall not export or re-export the Software, or allow access to the Software to any third party including, without limitation, any customer of Licensee, in violation of U.S. laws and regulations, including, without limitation, the Export Administration Act of 1979, as amended, and successor legislation, and the Export Administration Regulations issued by the Department of Commerce, or in violation of the export laws of any other country.

Any provision of any Software to the U.S. Government is with "Restricted Rights" as follows: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277.7013, and in subparagraphs (a) through (d) of the Commercial Computer-Restricted Rights clause at FAR 52.227-19, and in similar clauses in the NASA FAR Supplement, when applicable. The Software is a "commercial item" as that term is defined at 48 CFR 2.101, consisting of "commercial computer software" and "commercial computer software documentation", as such terms are used in 48 CFR 12.212 and is provided to the U.S. Government and all of its agencies only as a commercial end item. Consistent with 48 CFR

12.212 and DFARS 227.7202-1 through 227.7202-4, all U.S. Government end users acquire the Software with only those rights set forth herein. Any provision of Software to the U.S. Government is with Limited Rights. Thales is Thales eSecurity, Inc. at Suite 710, 900 South Pine Island Road, Plantation, FL 33324.

THALES PROVIDES THIS SOFTWARE AND DOCUMENTATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND ANY WARRANTIES ARISING OUT OF CONDUCT OR INDUSTRY PRACTICE. ACCORDINGLY, THALES DISCLAIMS ANY LIABILITY, AND SHALL HAVE NO RESPONSIBILITY, ARISING OUT OF ANY FAILURE OF THE SOFTWARE TO OPERATE IN ANY ENVIRONMENT OR IN CONNECTION WITH ANY HARDWARE OR TECHNOLOGY, INCLUDING, WITHOUT LIMITATION, ANY FAILURE OF DATA TO BE PROPERLY PROCESSED OR TRANSFERRED TO, IN OR THROUGH LICENSEE'S COMPUTER ENVIRONMENT OR ANY FAILURE OF ANY TRANSMISSION HARDWARE, TECHNOLOGY, OR SYSTEM USED BY LICENSEE OR ANY LICENSEE CUSTOMER. THALES SHALL HAVE NO LIABILITY FOR, AND LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD THALES HARMLESS FROM AND AGAINST, ANY SHORTFALL IN PERFORMANCE OF THE SOFTWARE, OTHER HARDWARE OR TECHNOLOGY, OR FOR ANY INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS, AS A RESULT OF THE USE OF THE SOFTWARE IN ANY ENVIRONMENT. LICENSEE SHALL DEFEND, INDEMNIFY, AND HOLD THALES HARMLESS FROM AND AGAINST ANY COSTS, CLAIMS, OR LIABILITIES ARISING OUT OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY. NO PROVISION OF ANY AGREEMENT BETWEEN LICENSEE AND ANY THIRD PARTY SHALL BE BINDING ON THALES.

Protected by U.S. patents:

6,678,828

6,931,530

7,143,288

7,283,538

7,334,124

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 *IBM Guardium Data Encryption (GDE)Administrators Guide*:

- Describes managing data security through the IBM GDE and the various tasks and responsibilities from the viewpoint of the administrators who must administer the GDE.
- Provides guidance for provisioning and day-to-day use of the GDE Appliance to secure sensitive data residing on their network and servers. The reader should be familiar with standard data center concepts, networking, and other aspects of IT security.

Documentation Version History

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

Table 1: Documentation History

Documentation Version	Date	Changes
GDE 3b	12/14/2017	GA release of GDE v3b. This patch release contains import security fixes.
GDE 3.0.0.1	06/22/2018	GA release of GDE 3.0.0.1. This release introduces support for nShield Connect Integration, Automatic registration of LDT/Docker hosts,and Bring Your Own Encryption Keys (BYOK).
GDE 3.0.0.2	09/06/2018	GA release of v3.0.0.2. This release introduces the following new features and enhancements: new encryption mode (CBC-CS1), Identity-Based Key Access (VAE), multiple communication slots, and REST API signature slots.

Scope

The Administrators Guide covers the GDE Appliance-specific administrator types that do the day-to-day GDE Appliance operations.

Audience

This Guide is for data center security teams tasked with securing the data residing on their network and servers. The reader should be familiar with standard data center concepts, IT security concepts, and networking.

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

GDE Appliance

1

The GDE Appliance creates, stores and manages the policies that protect data. It is available as a virtual appliance. This document describes the work flow needed to set up the GDE Appliance to protect your data. Refer to the corresponding version of the release notes for information about new features and updates.

This chapter contains the following sections:

GDE Appliance Overview

The GDE Appliance lets you create, store, and manage policies that protect data residing on host servers (referred to as ‘hosts’ from here on throughout the document, unless otherwise specified). The GDE Appliance is managed by GDE Appliance administrators who access the GDE Appliance through a browser-based user interface called the Management Console.

GDE Appliance administrators manage VTE and VAE Agents that reside on host servers and protect the data on those hosts. GDE Appliance administrators specify data access policies that are sent to these agents. Policies are created, stored and managed by GDE Appliance administrators. GDE Appliance administrators specify data access policies, create new administrators and administrative domains, generate usage reports, register new hosts, and access security logs.

For high availability (HA), GDE Appliances can be configured together in a cluster. One primary GDE Appliance in the cluster is used as a central point of management, and the contents of the primary are synchronized with the other members of the cluster—the failover GDE Appliances. The failover GDE Appliances are also used for load balancing the VTE agents.

The GDE Appliance generates log entries for all configuration changes, system events, access attempts, and file system agent communications. These log entries can be sent to standard Syslog servers in several formats.

Separation of Duties

Although the main focus of the GDE Appliance is the security of your data through encryption, segregation of data, and policy-based access enforcement, a key feature of the GDE Appliance incorporates the critical IT security concept of *separation of duties* with regard to administration of the GDE Appliance and the VTE agents and with the overall data center operation. It is this *separation of duties* that enhances compliance with regulatory requirements.

The GDE Appliance allows the creation of domains to separate administrators and the data they access from other administrators. A domain is a self-contained environment composed of keys, policies, hosts, administrators, and audit records. There are three primary types of administrators, each with specific roles and permissions. Segmenting administrative functions by type ensures that one administrator cannot control the entire data security process.

GDE Appliance Domains

A GDE Appliance administrative domain is a logical entity used to separate administrators, and the data they manage, from other administrators. Administrative tasks are done in each domain based upon each administrator’s assigned type. The benefits of administrative domains are:

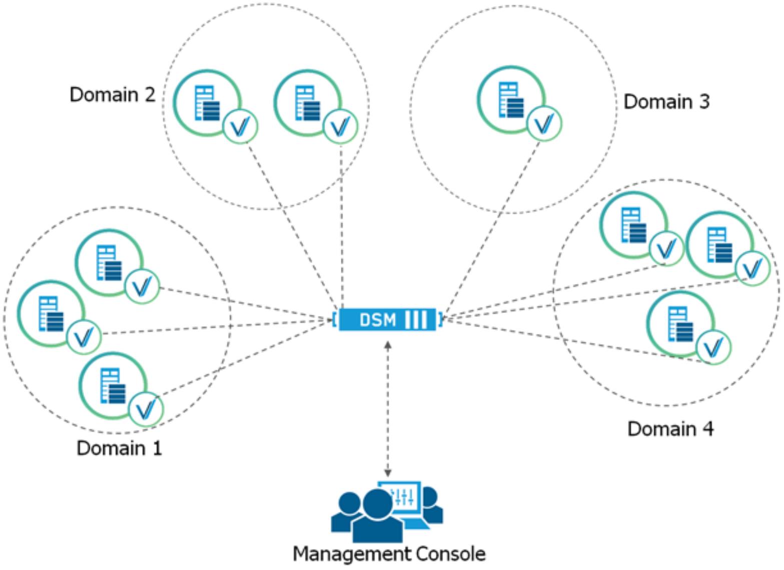
- Segregation of data for increased security
- Separation of responsibilities
- No single administrator has complete control over the GDE Appliance and the data it protects

Two types of domains can be created; global domains and restricted or local domains.

Global domains are created at the system level and can share GDE Appliance Domain Administrators and GDE Appliance Security Administrators. GDE Appliance global domains enable different business units, application teams, or geographical locations to share the GDE Appliance’s protection without having access to each other’s security configuration.

Restricted or local domains are domains in which administration is restricted to Domain Administrators and Security Administrators assigned to that domain and configuration data in one domain is invisible to administrators in other domains. GDE Appliance Domain administrators in restricted domains cannot be assigned to multiple domains. Once the first Domain Administrator is created and assigned to a restricted domain, that Domain Administrator creates additional Domain Administrators and Security Administrators as required. Domain Administrators created within a restricted domain are not visible outside of that domain, and can only be created and deleted by a Domain Administrator from that restricted domain.

Figure 1: GDE Appliance Domains



GDE Appliance Administrators

The GDE Appliance is administered by a GDE Appliance System Administrator. GDE Appliance System Administrators are different from regular data center system administrators—a GDE Appliance administrator's primary responsibility is to provide data access to those who need it and block data access to those who don't need it, including other GDE Appliance Administrators and data center system administrators.

To enforce separation of duties for strict adherence to good IT security practices and standards, we recommend creating customized administrator roles for individual users such that no one user has complete access to all data and encryption keys in all domains, see "Separation of Duties" for more information.

GDE Appliance administrators protect data by establishing data access policies, encrypting data, and auditing data access attempts.

GDE Appliance Administrator Types

There are three types of administrators, each with specific roles and permissions. Segmenting administrative functions by type ensures that one administrator cannot control the entire data security process. Each GDE Appliance administrative type is allowed to do specific administrative tasks. By default, a GDE Appliance administrator is assigned one administrator type and is allowed to do the tasks for only that one administrator type.

The GDE Appliance provides the following three primary types of administrators:

- GDE Appliance System Administrators. GDE Appliance System administrators create domains and administrators and assign a domain’s first administrator
- GDE Appliance Domain Administrators. A GDE Appliance Domain administrator, once assigned to a domain, can assign more domain administrators and security administrators to the domain or unassign them from the domain.
- GDE Appliance Security Administrators. A GDE Appliance Security administrator, once assigned to a domain (with appropriate roles), can manage hosts, keys and policies in the domain.

However, under a “relaxed security mode”, combined administrator type assignments can also be configured:

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

Additionally, any of these types of administrators can be created as read-only users. A read-only administrative user inherits all the privileges of the type of administrator being created, but without the ability to modify any settings. A read-only administrator can only view all the configuration information available to its administrator type.

System Administrator type

GDE Appliance System Administrators operate outside of domains. They create domains and assign administrators of type GDE Appliance Domain Administrator to the domains. The GDE Appliance System Administrator creates domains but does not operate within them. Administrators of types GDE Appliance Domain Administrator and GDE Appliance Security Administrator operate within those domains created by the GDE Appliance System Administrator. The default GDE Appliance Administrator, `admin`, has a GDE Appliance System Administrator type. In this type, the `admin` administrator creates additional GDE Appliance administrators and domains, and then assigns one or more administrators of type GDE Appliance Domain Administrator to each domain.

Domain Administrator type

GDE Appliance Domain Administrators operate within domains. They add additional GDE Appliance Domain Administrators and Security Administrators to each domain. There are two types of administrative domains; global domains and restricted domains. Domain Administrators assigned to a global domain are operate within their assigned domains, but can also be assigned to multiple global domains. GDE Appliance global Domain Administrators who are members of multiple global domains can switch between the domains. Global Domain Administrators who are members of multiple global domains must always know what domain they are in before performing any tasks. If you log in as a Domain Administrator or a Security Administrator, and you notice that the administrator, host, or log data is wrong, you are most likely in the wrong domain.

Domain Administrators assigned to a restricted domain are restricted to that particular domain—they *cannot* be assigned to multiple domains.

The GDE Appliance Domain Administrator also adds GDE Appliance Security Administrators to a domain and assigns them *roles* (i.e., *Audit*, *Key*, *Policy*, *Host*, *Challenge & Response,* and/or *Client Identity*) that are applied within that domain.

Security Administrator type

All tasks done by the GDE Appliance Security Administrator occur within domains. GDE Appliance Security Administrators assigned to a global domain are restricted to their assigned domains, but can be assigned to multiple domains. GDE Appliance Security Administrators that are assigned to multiple global domains have only the roles that were assigned when they were made a member of that domain. That is, the same administrator can have different roles in different domains.

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

Roles are assigned by GDE Appliance Domain Administrators when they assign a GDE Appliance Security Administrator to a domain. A brief description of the roles is described below.

- ***Audit***—Allows the GDE Appliance Security Administrator to view log data.
- ***Key***—Allows the GDE Appliance Security Administrator to create, edit, and delete local key-pairs, public keys only, and key groups. Can also view log data.
- ***Policy***—Allows the GDE Appliance Security Administrator to create, edit, and delete policies. (A *policy* is a set of rules that specify who can access which files with what executable during what times. Policies are described in more detail later.) Can also view log data.
- ***Host***—Allows the GDE Appliance Security Administrator to configure, modify, and delete hosts and host groups. Can also view log data. The *Challenge & Response* role is automatically selected when the *Host* role is selected.

- ***Challenge & Response***—Allows a GDE Appliance Security Administrator to generate a temporary passphrase to give to a host administrator to decrypt data on the host when there is no connection to the GDE Appliance.
- ***Identity-Based Key Access***—Allows a Security Administrator to create a client identity profile. A client identity is used to restrict access to encryption keys for VAE/VKM host users. See “Identity-Based Key Access” in the chapter on “Managing Keys” on page 203 for details about this feature.
- Combination GDE Appliance administrative types

GDE Appliance administrator of type All

Administrators of type All can operate inside and outside of domains. To operate inside a domain, GDE Appliance administrators of type All must be assigned to that domain first. When an administrator of type All enters a domain, that administrator can do GDE Appliance Domain Administrator and GDE Appliance Security Administrator tasks. When an administrator of type All exits the domain, the administrator can do GDE Appliance System Administrator tasks.

GDE Appliance administrator of type Domain and Security

The GDE Appliance Domain and Security Administrator can do every task that is allowed an administrator from inside a domain. For example, the GDE Appliance Domain and Security Administrator can add administrators to the domains of which they are a member, but they cannot create new administrators.

The administrator types are outlined in Table 1.

Table 1: Administrator Types

Type	Permissions
GDE ApplianceSystem Administrators. This administrator cannot do any security procedures in any domain.	Configure High Availability (HA) Upgrade GDE Appliance software Backup and restore GDE Appliance Add and delete all administrators Reset passwords for all administrators Add and delete all domains Assign one Domain Administrator to each domain Configure syslog server for system-level messages Install license file Configure GDE Appliance preferences View logs

Type	Permissions
GDE ApplianceDomain Administrators. This administrator cannot remove domains and cannot do any of the domain security roles.	Add and remove administrators (Domain, Security, All) to and from domains Backup and restore GDE Appliance Configure Security Administrator roles (Audit, Key, Policy, Host, Challenge & Response, Client Identity) Configure Syslog server for application-level messages View GDE Appliance preferences View logs
GDE ApplianceSecurity Administrators. Do the data protection work specified by their roles. Different roles allow them to create policies, configure hosts, audit data usage patterns, apply GuardPoints, and do other duties.	Configure signature sets Configure keys and key groups Configure online and offline policies Configure hosts and host groups Assign host passwords (manually or generated) Apply GuardPoints Share a host with another domain Export the GDE Appliance public key Import symmetric keys View GDE Appliance preferences View logs
GDE ApplianceDomain and Security Administrators.	Domain Administrator and Security Administrators capabilities combined. Administrators of this type are deleted from the GDE Appliance database upon switching from relaxed to strict domain mode.
All.	System, Domain, and Security Administrators capabilities combined. Administrators of type All are deleted from the GDE Appliance database upon switching from relaxed to strict domain mode.

NOTE: The person who does the initial GDE Appliance setup and configuration using the GDE Appliance CLI can also be thought of as another type of administrator. They are system users or data center system administrators with UNIX login accounts. Although they access the GDE Appliance through the CLI, for strict security practices, they should not have access to the Management Console. Conversely, the GDE Appliance administrators listed above can access the Management Console, but should not have access to the CLI.

Read-Only Administrators

In addition to the types of GDE Appliance administrators and the associated roles, a GDE Appliance administrator can be created as a ‘read-only’ user. A GDE Appliance System Administrator can create other administrator types as read-only users—except for Domain administrators that are restricted to a domain. The first administrator of a domain must have privileges to create and administer other users within that domain, therefore a restricted

Domain administrator cannot be created as read-only by a GDE Appliance administrator of type *System*, or *All*.

A read-only user inherits all the privileges of the type of administrator and the associated roles being created however, can only view all the information available to that user. A read-only administrator does not have the ability to modify any settings. For example, the GDE Appliance administrator creates an administrator of type All as a read-only user. This read-only administrator of type All can view all the configuration information on the GDE Appliance , but cannot modify that information. Read-only administrators can only change their passwords.

CLI Administrators

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

2

Multitenancy

Multitenancy enables the creation of multiple *restricted* or *local domains* within a single GDE Appliance. A restricted or local domain is a GDE Appliance domain in which GDE Appliance administration is restricted to Domain Administrators or Security Administrators assigned to that domain. Multitenancy is particularly useful for Cloud Service Providers.

This chapter contains the following sections:

- "Overview"
- "Implementing Multitenancy"

Overview

With multitenancy, the GDE Appliance platform supports the creation of restricted domains. Restricted or local domains are different from global domains in that Domain Administrators not assigned to that local domain, cannot modify or administer that domain in any way. Unlike global domains, local domain administrator accounts cannot be assigned to any other domains. GDE Appliance administration tasks are restricted to local Domain Administrators or local Security Administrators within that domain.

The GDE Appliance System administrator creates the first Domain administrator for a restricted domain, all subsequent administrators are created by the Domain administrator of that restricted domain. All other administrative tasks within a restricted domain are done by the local Domain administrator of that domain.

Table 2 on page 10 lists some differences between the two types of domains/administrators.

Table 2: Differences between global and local domains.

Global Domains and Administrators	Local Domains and Administrators
• Administrator names must be unique within all global domains. • Domain and Security Administrators can be assigned to multiple global domains • GDE Appliance System Administrators can: o Create and assign the first global Domain Administrator to a global domain. That same global administrator can be assigned to other global domains as well. After that the GDE Appliance System Administrators do no tasks within global domains. o Change the password of any global administrator o Delete any global administrator. o Add or delete a global domain. o Disable all administrators in a global domain.	• Administrator names must be unique within a local domain, *but* can be identical if they are in different local domains. • Local Domain and Security Administrators can only function within their local domain. • GDE Appliance System Administrators: o Create the first local Domain Administrator for a restricted or local domain. After that the GDE Appliance System Administrators do no tasks within local domains. o Cannot change the password of a local administrator o Cannot delete local administrators o Cannot access log files in a local domain. o Can add or delete local domains. o Can disable all administrators in a local domain.

Implementing Multitenancy

To create a local domain, the GDE Appliance System Administrator creates a single Domain Administrator for a domain. After that, complete control of the domain is maintained by that domain's Domain Administrator and any Domain or Security Administrators created by that Domain Administrator.

Administrators in a local domain do GDE Appliance duties in **exactly** the same way as in global domains. The only differences are as follows:

- They are restricted to doing GDE Appliance work only in their own local domain
- Administrators not in their local domain (including GDE Appliance System Administrators) cannot do any domain-related work.

NOTE: While GDE Appliance System Administrators cannot view the administrators in the local domain, GDE Appliance System Administrators can disable all administrators in a local domain.

The Domain Administrator of a local domain can also create 'read-only' administrators. A read-only user inherits all the privileges of the administrator type (and the associated roles in the case of Security administrators), being created. See "Read-Only Administrators" on page 7 for more information about Read-Only administrators.

Creating Local Domain Administrators

This section describes how to create a local domain and its local Domain Administrator.

1. Log on to the Management Console as a GDE Appliance System Administrator.
2. Create a domain:

   a. Exit the current domain if necessary.

   b. Go to **Domains > Manage Domains > Add**. Enter domain name (example: **`Domain-2`**) and click **Ok**.
3. Create a Domain Administrator for this domain.

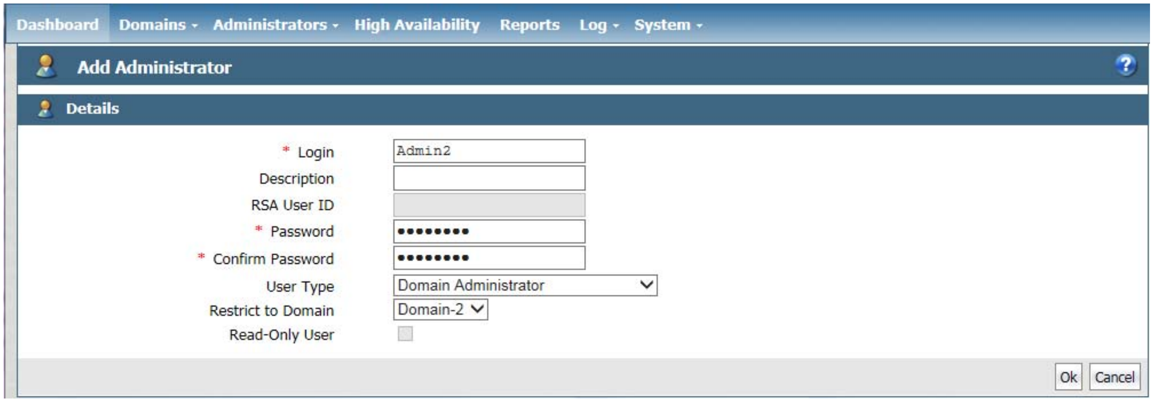
   a. Go to **Administrators > All > Add**.

   b. Enter **Login** and **Password**.

   c. For **User Type** select **Domain Administrator**.

   d. **Restrict to Domain** field displays. Select the domain to restrict in the pull-down. Click **Ok**.

Figure 2: Create a restricted domain administrator



* Login	Admin2
Description	
RSA User ID	
* Password	••••••••
* Confirm Password	••••••••
User Type	Domain Administrator
Restrict to Domain	Domain-2
Read-Only User	□

You have now created a local domain (Domain-2) and a local Administrator (Admin2). When you return to the Administrators window, you will not see the administrator's name listed in the table. The new administrator is in a local domain, and does not appear in the list of global administrators.

Logging in to a local domain

1. Go to the log in screen of the Management Console.
2. Enter the login and password of the local Domain or Security Administrator.
3. Check the **I am a local domain administrator** checkbox and enter the domain name.

4. Click **Ok**. The Dashboard displays the administrator and the current domain on the top right of the console.

Creating a local Security Administrator

Like a global Domain Administrator, the local Domain Administrator cannot do any of the standard security roles (Audit, Key, Policy, Host, Challenge & Response, and/or Client Identity) unless the administrator has been created as a Domain and Security Administrator, see "Combination GDE Appliance administrative types" on page 6, for more information about this administrator type. If the Domain administrator is a separate role, the local Domain Administrator must create local Security Administrators to do tasks associated with the different security roles.

NOTE: GDE Appliance System Administrators *cannot* create GDE Appliance Security Administrators for a restricted domain.

1. Go to the log in screen of the Management Console and log in as a local Domain Administrator.
2. Click **Administrators > Manage Administrators > New**.
3. In the **Add Administrator** window, enter a login and password. Select *User Type* as **Security Administrator**.
4. Select the **Roles** for this administrator account and click **Ok**.
5. A new local Security Administrator is created.

Creating a local Domain or Security Administrator as Read-Only

1. Go to the log in screen of the Management Console and log in as a local Domain Administrator.
2. Click **Administrators > Manage Administrators > New**.
3. In the **Add Administrator** window, enter a login and password.
4. Select a **User Type** from the drop down list.
5. Select the **Read-Only User** check box to create an administrator with read-only privileges. An administrator with read-only access will not be able to add, delete, or modify any settings in the domain. Read-only administrators will only be able to change their passwords and view the different settings per their type and the roles assigned to them.

Creating, Adding, and Deleting Administrators

3

A default GDE Appliance Administrator of type System called `admin` already exists on the GDE Appliance. . The first time you log on to the GDE Appliance, you do so using the default GDE Applianceadministrator credentials. Additional administrators must be created to do tasks that `admin` as an administrator of type System, cannot.

This chapter contains the following sections:

- "Creating Administrators"
- "Importing Administrators"
- "Deleting Administrators"
- "Resetting Administrator Passwords"

Creating Administrators

We recommend that you create backup administrators for each administrator type as a precaution. This way, if a particular administrator is compromised, that administrator can be deleted and their administrative tasks can be assumed by a different administrator of the same type.

1. Log on to the Management Console as a GDE Appliance Administrator of type *System* or type *All*.

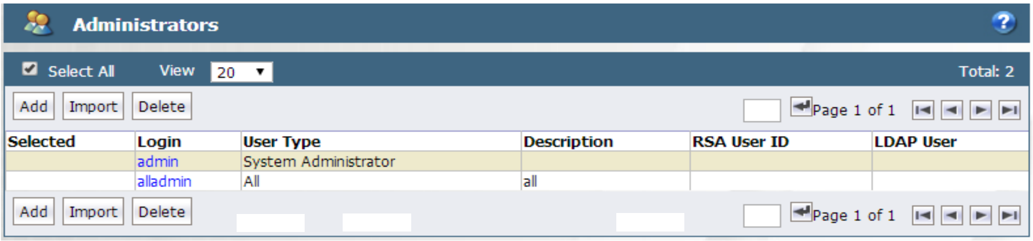
   If this is the first time you are logging in, you must log in with the credentials of the default administrator *admin*; with the default password `admin123`, you will be redirected to the reset password page, you must reset the password. This is true for any GDE Appliance administrator logging ion for the first time.

   NOTE: The default administrator *admin* cannot be deleted.

2. After resetting your password, the Management Console Dashboard displays. Click **Administrators** on the main menu bar.

   The ***Administrators*** window opens listing all the administrators for this GDE Appliance.

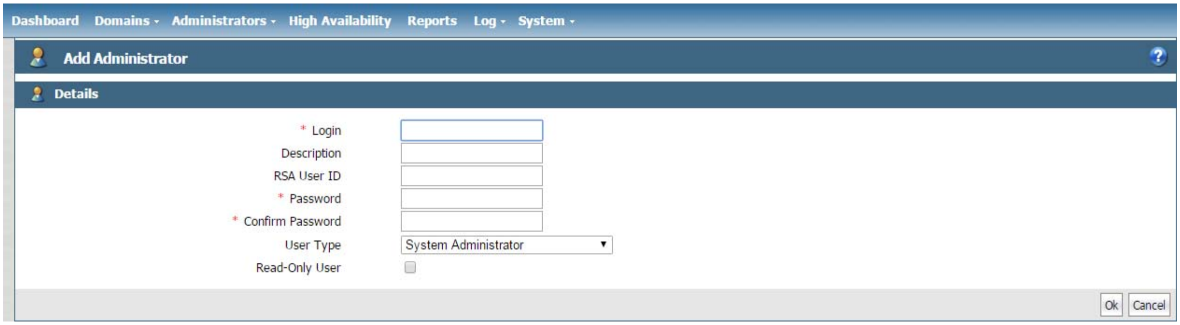
Figure 3: Administrators page



Selected	Login	User Type	Description	RSA User ID	LDAP User
	admin	System Administrator			
	alladmin	All	all		

3. Click **Add**. The *Add Administrator* window displays.

Figure 4: Add Administrators window



* Login	
Description	
RSA User ID	
* Password	
* Confirm Password	
User Type	System Administrator
Read-Only User	□

4. In the *Add Administrator* window, enter the following information:

- **Login**—Type a name. Only one instance of an administrator name is allowed.
- **Description**—(Optional) Enter a phrase or string that helps you to identify the administrator. The maximum number of characters is 256.
- **RSA User ID**—(Optional) Enter the RSA user name in the RSA User Name field. An RSA Authentication Manager software application deployment and an RSA SecurID device are required. The RSA SecurID device and RSA user name are bound together in the RSA Authentication Manager software application by a responsible security administrator. Enter the RSA user name that was configured by the responsible security administrator in the RSA User Name text-entry box. The value entered in this text-entry box is displayed in the RSA User Name column of the *Administrator* window.
- **Password**—Enter a password. The password must conform to the attributes defined in the password preferences. The maximum password length is 256 characters.

If you have enabled and configured multi-factor authentication, an administrator can have two passwords to log on to the Management Console: one for a GDE Appliance administrator and one for an RSA user. The GDE Appliance Administrator Password is used to log on to the Management Console, if multi-factor authentication is disabled or the administrator is not configured for multi-factor authentication. When multi-factor authentication is enabled and the administrator is configured for multi-factor authentication, the GDE Appliance administrator logs into the Management Console with the RSA SecurID password and the Token Code displayed on the RSA SecurID device.

- **Confirm Password**—Retype the password.
- **User Type**—Select **System Administrator**, **Domain Administrator**, **Security Administrator**, **Domain and Security Administrator**, or **All** from the drop-down menu. The **Domain and Security Administrator** and **All** options are only available when the **Enable Separation of Duties** checkbox is not selected in the **System > General Preferences > System** tab.

NOTE: The first time an administrator logs on to the Management Console with a newly created GDE Appliance Administrator account, they are prompted to change the password. Administrators cannot reuse the same password to create the account.

- **Read-Only User**—Select this check box to create an administrator with read-only privileges. You can assign read-only privileges to any type of administrator—except for Local Domain administrators that are the first administrators to be assigned to a domain. If the first administrator added to a local domain is read-only, that administrator will not be able to create any more administrators for that domain.
  An administrator with read-only access will not be able to add, delete, or modify any settings on the GDE Appliance. Read-only administrators will only be able to change their passwords and view the different settings per their type and the roles assigned to them.

5. Click **Ok**. A new GDE Appliance Administrator is created. The *Administrators* page displays a table with the name and type of the new administrator.

Importing Administrators

The **Import** function imports data from an LDAP server such as Active Directory (AD). Once an LDAP server has been identified and configured, the administrator can import the desired values. See “LDAP Configuration” on page 121 for more about configuring an LDAP server.

You need the LDAP login ID and password to import values from an LDAP directory.

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

4. Search options:

   a. Use the LDAP Query field to filter searches using the LDAP query language. Results depend on how the LDAP service is set up. See RFC2307 for full details on syntax.

   b. Select a Group from the **Group** drop down list.

   c. Enter a User name in the **User** field.

   d. The **Maximum number of entries to return** field lets you limit the maximum number of records to import or display. The default value is 300. The minimum value is one. A high integer value may result in a delay depending on the database size.

5. Click **Go**.

Selecting LDAP administrators

The Management Console provides a GUI interface to the mapped LDAP directory values such as Login and User Description. As an Administrator logged into the LDAP directory, you can provide input to the following fields in order to select and manage LDAP users. See "LDAP Configuration" for more information about adding LDAP users.

- **Group Object Class**: Select a value from the drop down menu to filter by group type
- **User Object Class**: Enter a value or partial value to filter on specific users. Entering a partial value acts as a "wild-card" returning all values matching what was entered.
- **Go:** Click to refresh the screen
- **Select All**: Click to select all values on this page.
- **View**: Select a value from this drop down box to control how many values appear on any page.
- **Selected**: Click to select individual values.
- **User Type**: Select a value from this drop down box to define the type of Administrator or role of the values you import.
- **Add/Cancel**: Select to add or cancel your selections.

Deleting Administrators

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

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

To remove an administrator from a domain:

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

To delete an administrator

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

Resetting Administrator Passwords

GDE Appliance administrator passwords cannot be viewed. If a GDE Appliance administrator forgets their password, the GDE Appliance System Administrator can assign a new temporary password. The GDE Appliance System Administrator informs the administrator about their new temporary password. The next time the administrator logs on, they are directed to enter a new password.

If a GDE Appliance administrator is currently running an active Management Console session when the GDE Appliance System Administrator changes their password, the Management Console session is immediately terminated and the administrator must log on again.

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

The Domain Administrator, Security Administrator, or All account must be enabled in every domain of which they are a member at the time the password is changed. Enabling an administrator in one domain does not enable them for all the domains of which they are a member.

To change another administrator's password:

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

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

   If you are changing the password of a Domain Administrator or Security Administrator, have a Domain Administrator switch to each domain in which the administrator is a member and check the GDE Appliance log of each domain.
3. Select **Administrators > All**. The *Administrators* window opens.
4. Select an administrator in the **Login** column. The *Edit Administrator* window opens.
5. Enter the password and then click **Ok**.

   The password is applied to the administrator. If the administrator is currently logged on to a Management Console session, the login becomes inactive and the administrator must log back into the Management Console to resume operation. The maximum password length is 256 characters.
6. For administrators of type Domain Administrator, Security Administrator, or All, have a different administrator of type Domain Administrator, Domain and Security Administrator, or All re-enable that administrator's domains.

Domain Management

4

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

This chapter contains the following sections:

- "Adding Domains"
- "Deleting Domains"
- "Assigning Domains to Domain Administrators"

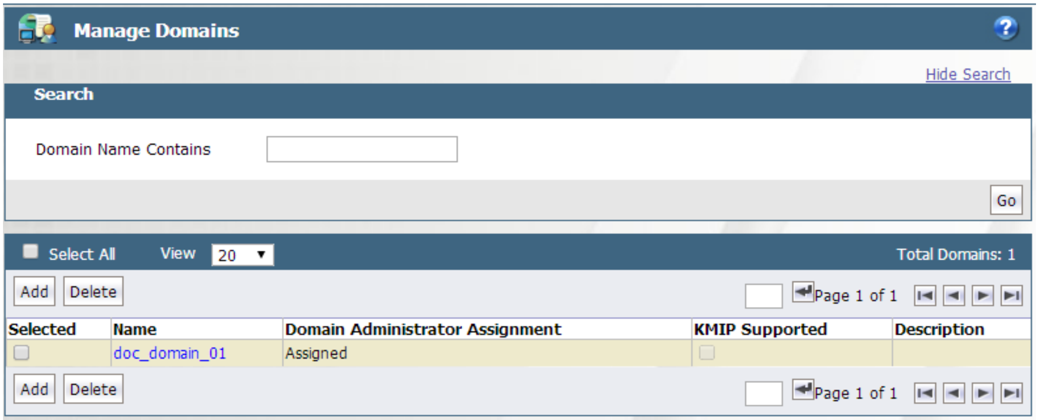
Adding Domains

To add a domain:

1. If you are already logged into the Management Console, log out and log in again as the GDE Appliance System Administrator `admin`. Otherwise, just log on as `admin`.
2. Click **Domains > Manage Domains** to bring up the *Manage Domains* window.

   If you are in a domain click **Exit Domain** to exit the domain and then click **Manage Domains**.

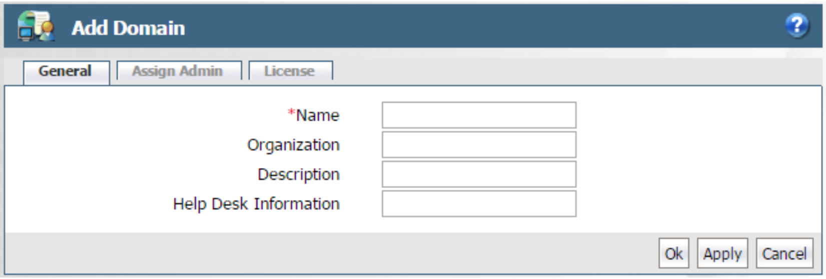
Figure 5: Manage Domains window



Selected	Name	Domain Administrator Assignment	KMIP Supported	Description
□	doc_domain_01	Assigned	□	

3. Click **Add**. The *Add Domain* window opens.

Figure 6: Add Domain window



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

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

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

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

   d. **Help Desk Information**: (Optional) Enter the phone number to call to get the response string for challenge-response authentication. If you leave this box empty, the default message is “`Please contact a Security Server administrator for a response.`” (Note: The term “Security Server” refers to the GDE Appliance.)

5. Click **Apply** to save the domain information.

6. Click the **Assign Admin** tab to assign an administrator. If you do not assign an administrator when you add the domain, you can edit the domain later to add an administrator. However, you cannot switch to the domain until you assign an administrator.

7. (Optional) Click the **License** tab to allocate licenses or license hours per agent on this domain.
8. Click **Ok**. The **Domains** window opens with the name and description of the new domain.

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

Deleting Domains

NOTE: Back up security objects such as keys, policies, and logs, before you delete them. Without the keys, you cannot restore or access encrypted data. When you delete a domain, all the log data for that domain is also removed from the GDE Appliance database.

To delete a domain:

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

   You can delete all but one Domain Administrator; which is the administrator that you are currently logged in as.
8. Log out.
9. Log in as an administrator of type System Administrator or All.
10. Select **Domains > Manage Domains**.

    The Domains windows is displayed.
11. Enable the **Selected** check boxes for the domains to be deleted.
12. Click **Delete**.

    You are prompted to verify that you want to proceed with this operation.
13. Click **Ok**.

    The deleted domain(s) will no longer appear in the domains table in the *Domains* window

Assigning Domains to Domain Administrators

A GDE Appliance System Administrator creates other GDE Appliance administrators but can assign only one administrator of type Domain Administrator or Domain and Security Administrator to a domain. After the first administrator to a domain has been assigned, all subsequent administrators must be assigned or added (depending on the type of domain), from within the domain. The GDE Appliance Domain administrators that first are assigned to a domain can log into the domain from the Management Console and add additional Domain Administrators or Domain and Security Administrators to the domain. A global Domain Administrator can add only existing Domain Administrators, Security Administrators, and Domain and Security Administrators to the domain, listed in the global administrators table on the Administrators page to the domain. Restricted Domain administrators can create administrators within their domains and these administrators are not visible outside of the domain and cannot be shared. See "Assigning Domain Administrators or Security Administrators to Domains" on page 139

5

Configuring Preferences and Viewing Logs

As a GDE Appliance System Administrator (or type All), you can set the following preferences in the Management Console.

- General preferences—the number of GDE Appliance objects displayed based on the object type. For example, you can set a preference that displays all configured policies on one Web page, rather than just 20 per page.
  - System preferences—enable Syslog messaging, enable super administrators, and shorten the update interval when pushing changes to the same policy to hosts on different servers.
  - Password preferences—how long a password must be, the types of characters that a password must contain, and password duration. Password preferences can also configure the GDE Appliance response to repeated failed login attempts.
- Log preferences—log maintenance parameters on the GDE Appliance. For example, you can set the interval to wait before moving agent log entries from temporary buffers on the GDE Appliance to the GDE Appliance log database, and consequently to the log viewer.
  - Agent log preferences—how the GDE Appliance maintains agent-specific log data. For example, you can set the interval at which the agent uploads log data to the GDE Appliance.

This chapter contains the following sections:

- “Configuring Preferences”
- “Log Preferences”
- “Network Diagnostics”

Configuring Preferences

The General Preferences tab lets you specify display settings, system settings, password settings, and lets you configure the login banner message on the log in screen.

Setting display preferences

Display preferences are administrator-configurable parameters that control the number of objects to display and set the Management Console expiration time.

To set GDE Appliancedisplay preferences:

1. Log on to the Management Console as an administrator of type System Administrator or type All.
2. Select **System > General Preferences** in the menu bar.

   The *General Preference* window opens to the *Display* tab.
3. Change the values displayed in the attribute text-entry boxes or scroll-list.

   The following table lists and describes attributes and their values.

Table 3: General Preferences Display tab attributes and their values

Category	Parameter	Description
Domain Page Settings	Number of Domains Per Page	Sets the maximum number of administrators in the *Domains* window to display on one page. Navigation buttons are displayed in the *Domains* window to move between the pages. The default is 20.
Administrator Page Settings	Number of Administrators Per Page	Sets the maximum number of administrators in the *Administrators* window to display on one page. Navigation buttons are displayed in the *Administrators* window to move between the pages. The default is 20.
Host Page Settings	Number of Hosts Per Page	Sets the maximum number of hosts in the *Hosts* window to display on one page. Navigation buttons are displayed in the *Hosts* window to move between the pages. The default is 20.
	Number of Host Groups Per Page	Sets the maximum number of host groups in the *Host Groups* window to display on one page. Navigation buttons are displayed in the *Host Groups* window to move between the pages. The default is 20.
Policy Page Settings	Number of Policies Per Page	Sets the maximum number of policies in the *Policies* window to display on one page. Navigation buttons are displayed in the *Policies* window to move between the pages. The default is 20.
Key/Certificate Page Settings	Number of Keys Per Page	Sets the maximum number of keys in the *Keys* window to display on one page. Navigation buttons are displayed in the *Keys* window to move between the pages. The default is 20.
	Number of Key Groups Per Page	Sets the maximum number of key groups in the *Key Groups* window to display on one page. Navigation buttons are displayed in the *Key Groups* window to move between the pages. The default is 200.
Signature Page Settings	Number of Signature Sets Per Page	Sets the maximum number of signature sets to display on one page. Navigation buttons are displayed in the *Signature Sets* window to move between the pages. The default is 20.
Log Page Settings	Number of Log Messages Per Page	Sets the maximum number of log entries to display on one page. Navigation buttons are displayed in the *Logs* window to move between the pages. The default is 20.

Category	Parameter	Description
Management Console Timeout	Management Console Timeout	Sets the interval of inactivity allowed before automatically logging administrators out of the Management Console Web session. Unsaved changes are discarded. Choices are 5 minutes, 20 minutes, 1 hour, 2 hours, and 8 hours. The default is 1 hour.

4. Click **Apply** to set the changes.

Setting system preferences

You can configure attributes that:

- Enable or disable all GDE Appliance Administrator accounts of type Domain and Security and type All. By enabling the **Separation of Duties** option, all GDE Appliance Administrator accounts of type All and type Domain and Security Administrator are deleted from the GDE Appliance database, and only GDE Appliance Administrator accounts of type System Administrator, Domain Administrator, and Security Administrator remain and can be used.
- Speed up GDE Appliance updates when policy changes are pushed to VTE Agents that are administered by failover GDE Appliances. By enabling **Without Replication Confirmation**, the primary GDE Appliance no longer waits for failover GDE Appliances to synchronize before it begins pushing changes to its own agent hosts.
- Enable syslog logging. Once enabled and configured, a Syslog server can transmit/receive logging data.

To set system preferences:

1. Log on to the Management Console as an administrator of type System Administrator or All.
2. Select **System > General Preferences** in the menu bar.

   The *General Preference* window opens to the *Display* tab.
3. Click the *System* tab.
4. Change the values displayed in the attribute check boxes.

   The following table lists and describes the attributes and their values:

Table 4: General Preferences System tab attribute values and use

Category	Parameter	Description
Organization	Name	Enter the name of the organization (company, department, or function) responsible for or managed by this GDE Appliance. This is useful for reporting and auditing purposes.

Category	Parameter	Description
Separation of Duties	Enforce separation of duties	Check box to operate in relaxed domain mode or strict domain mode. When enabled, strict domain mode is applied. Administrators are assigned a single administrative type that can do a specific set of tasks. This means that at least three administrators must be configured, each with a specific type, in order to do all GDE tasks. When disabled, the domain mode rules are relaxed, and two additional compound administrative types (Domain and Security, and All) can be configured. When switching from strict to relaxed domain mode, all currently configured administrators are left intact. When switching from relaxed to strict domain mode, all the primary administrator types are left intact and all the compound administrators of type Domain and Security Administrator and type All are deleted immediately. The checkbox is disabled by default, indicating relaxed domain mode.
Push Host Configuration	Without replication confirmation	Enable this check box if you want the primary GDE Appliance to immediately update the locally administered hosts that are affected by a policy change, even if the same policy is also used for GuardPoints on remotely administered hosts. Disable the check box if you want the primary to delay pushing policy changes to locally administered hosts until after it successfully synchronizes with the failover GDE Appliances that apply the same policy. If the checkbox is disabled, the primary GDE can wait up to 15 minutes for all the failover GDE Appliances to synchronize before it pushes the policy changes to locally administered hosts. The checkbox is enabled by default.
Agent Keys	Key refreshing period (in minutes)	Defines the refresh period for Agent keys stored on the host. The refresh period value ranges from 1 to 44640 minutes (31 days). The default value is 10080 minutes (7 days). When set outside of a domain under General Preferences, the refresh period is applied globally, for all new keys. The refresh period is not reset for existing keys.
Key Template	Enforce Using Key Template to Define Key	When enabled, administrators creating keys must select a key template to define the key attributes.
Policy	Maximum Number of Policy History Show Validation Warnings	Sets the maximum number of policy history versions stored in the database. The default value is 10. User selectable values are 0, 5, 10, 50, 100. Changing this value does not delete any older versions until the next time a policy is changed and saved. When saved, the XML data of the older version is deleted and cannot be recovered (unless restored from a prior backup). Policy metadata such as who and when is not deleted. If you want to see validation warnings, enable the **Show Validation Warnings** check box. This is disabled by default.
Syslog Setting	Syslog Enabled	When enabled, properly configured syslog servers can receive logging data. Administrators of type System, Domain, Domain and Security, and All can configure syslog servers. Syslog messaging is domain-specific. Only the events that occur in the local domain are sent to the syslog server. If the administrator is not in a domain when configuring a syslog server, local GDE and appliance system messages are sent to the syslog server. This checkbox can be enabled and disabled by administrators of type System Administrator and All. The checkbox is disabled by default.

Category	Parameter	Description
Automatic Backup Settings	Automatic Backup Enabled	When enabled, allows administrators of type All or System, or from within a domain, administrators of type Domain or Domain and Security, to schedule automatic backups of the GDE or GDE domain configuration. This setting must be disabled to comply with Common Criteria standards. This setting is enabled by default.
Connection Timeout	Max Agent Connection Timeout	Distance and unreliable networks can cause configuration pushes and pulls between GDE Appliances and hosts to timeout. If, because of a slow connection, policy updates are not being pushed to a host, or a host is unable to pull the latest configuration changes, increase the timeout interval. Preference changes are not automatically pushed to hosts. To push a new timeout value to a host, change something in the host configuration, such as Host Settings, and the GDE will push the change, including the new timeout interval, to the host. You can also pull the new timeout onto the host. To pull the change onto a host, log onto the host, either via SSH or a Remote Desktop Connection, and kill the `vmd` process. Wait a moment and the `vmd` process will automatically restart. As `vmd` restarts, it queries the GDE for updates, including policy changes and the connection timeout value. The allowed range is `1` to `600` seconds. The default is `20` seconds.
Multi-Factor Authentication	Multi-factor authentication Configured	If selected, indicates that multi-factor authentication has been enabled on the primary GDE and all failover GDE Appliances. This checkbox is a display indicator only. Multi-factor authentication is enabled via the CLI, not the Management Console.
Backup Requests Management	Number of Processes to Handle Backup Requests	The GDE may contain several local domains that domain administrators want to backup. If multiple backup requests are made at the same time, this could cause the GDE Appliance to hang. Therefore the number of processes set aside to handle backup request is set to 10 by default. This means, if there are more than 10 backup requests, they will remain in the queue until a process is free to perform a backup. Select the number of processes from the drop down list.
HDFS Browse Connections	HDFS connection Time Out (not less than 15 seconds)	Set a time in seconds for connection timeout when browsing HDFS directories from the GDE. When the timeout limit is reached, the GDE aborts the attempt and tries to reconnect.

5. Click **Apply** to set the changes.

Setting password preferences

Administrator passwords are a vital part of a good security system. A Management Console administrator password can contain standard ASCII alphabet characters (`a-z, A-Z`), integers (`0-9`), and a limited set of special characters (`!@#$%^&*(){}[]`). The individual elements in this combination of characters cannot occur in sequential order. That is, a password cannot contain two instances of the same element if they are next to each other. For example, `mississippi` will not be accepted, but `misSisSipPi` will.

Additional restraints can be applied that require all new passwords to contain at least one uppercase alphabet character, at least one special character, and the minimum number of characters that must be used.

Password preferences are applied to both administrator passwords and host system passwords.

To set GDE Appliance password preferences:

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions or type All.
2. Select **System > General Preferences**.

   The *General Preferences* window opens.
3. Select the *Password* tab.
4. Change the values displayed in the attribute text-entry boxes or scroll-list.

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

Password Characteristics

- **Password Duration**: Passwords expire after the number of days set by an administrator. The password expiration interval is applied globally to each administrator account. If the administrator does not change the password prior to the expiration, the administrator must reset the password immediately the next time the administrator logs in. The expiration interval is an integer between 6 and 365. The default is 90. 'Password Duration' must be set to a value greater than 'Password Expiration Notification'.
- **Password History**: The GDE Appliance maintains a password history. You cannot use the same password more than once per the set limit. The default is 4, and the maximum value that can be set is 12. You can set this value to '0' to permit reuse of the current password.
- **Minimum Password Length**: Sets the minimum number of characters, including blank spaces that must be in a password. The minimum password length is an integer between 8 and the limit of the operating system. The default is 8.
- **Minimum Number of Character Changes**: Sets the minimum number of characters, including blank spaces, that constitute a password change.
- **Disallow Password Change Within (Days)**: Sets the number of days you must wait before you can change the password again.
- **Password Expiration Notification (Days)**: Sets the number of days prior to the password expiration at which to begin telling the administrator that their password is about to expire. Administrators are notified of the impending expiration at Management Console Login. The notification interval is an integer between 6 and 31. The default is 6.

Password Complexity

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

Account Lockout

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

The Account Lockout settings also apply to the registration shared secret, that is, if you set the maximum number of unsuccessful login attempts to 4 and the lockout time to 1 hour, then you have 4 attempts to use the registration password before you are locked out for an hour. You can attempt to register an agent again with the correct registration secret after the hour has elapsed.

Log Preferences

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

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

Log entries are displayed in the Management Console based on the current administrator type and the domain in which the administrator is working. However, all this log information combined is available in the server.log file on the GDE Appliance.

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

Additionally, you can view log files from the GDE Appliance CLI. See, “diag” on page 394 in the chapter, “Network Category Commands”.

Setting Log Preferences

The *Log Preferences* page lets you set logging preferences for the GDE Appliance and the encryption agents. Navigate to **System > Log Preferences** on the main menu bar to access the page.

Server Log Preferences

The *Server* tab displays information about the current GDE Appliance logging and communication configuration. You can configure the following attributes:

- **Logging Settings**
  - **Logging Level**: Sets the severity level at which entries are sent to cgss.log. This information is displayed in the 'Logs' window. The choices are DEBUG, INFO, WARN, ERROR, and FATAL. Each level includes the levels below it. For example, FATAL logs only fatal errors, whereas WARN logs warnings, ERROR and FATAL conditions. The default is INFO.
  - **Log Upload DB Retry (secs)**: The interval before resuming the transfer of agent log data that had been uploaded, and is stored in system files, into the log viewer database after a failure, such as after losing the connection to the database. The default is 30 seconds.
  - **Log Buffer Size (messages)**: The maximum number of entries to place in the GDE Appliance log. When this limit is reached, or when Log Buffer Flush Time has elapsed, the entries are moved to the log viewer database. The default is 100 entries.
  - **Log Buffer Flush Time (secs)**: The interval to wait before moving log entries in the server log buffers to the log viewer database. The default is 15 seconds.
  - **Audit Log File Queue Size (files)**: The maximum number of audit log files queued for processing by the GDE Appliance. This is the number of files that can be queued while the GDE Appliance processes files to move them from temporary buffers on the GDE Appliance to the GDE Appliance log database or remote Syslog servers, or to email depending on the settings. If the queued log files exceed this number, they will be rejected until the GDE Appliance can process the ones in the queue. The default is 100. Use this setting with caution as you do not want this number to become so large that it slows the GDE Appliance performance.
- **Communication Settings**
  - **Update Host Frequency**: The interval between scans of the queue to see if any changes have been made to the host configuration on the GDE Appliance. Any changes are pushed to the host. The default interval between scans is 30 seconds.

- **Default Host Communication Port**: The port number on the GDE Appliance and on the file agent through which they communicate. When you change this port number, it is applied to all new hosts that are added after the configuration change is made. Existing file agent hosts are unaffected. The change is visible in the Communication Port field in the General tab of each new host. If you change the Communication Port number for an existing host, you must restart the file agent process that runs on that host.

Agent Log Preferences

Depending on the type of agent licenses that you have installed on your GDE Appliance, you will see an *FS Agent Log* tab and a *Key Agent Log* tab. You can configure logging preferences for the VTE (FS) and Key Agents from the respective tabs.

You can configure the file agent process information that is entered in the Management Console log. You can configure the process information globally, in which all the file system processes running on hosts systems are added after the configuration change inherit the log attributes, but all current file system configurations remain intact. Or, you can configure log attributes for individual file system installations. This section describes global file agent log configuration:

1. **Message Type**

   - Management Service: Logs messages that are related to the agent and VMD process server interaction in the agent logs. Log to File and Upload to Server are enabled by default. The default log message level is INFO.
   - Policy Evaluation: Logs messages that are related to policy evaluation in the agent log. Set the log message level to desired setting. The default log message level is ERROR.
   - System Administration: Logs messages that are related to system level events. The default log message level is ERROR.
   - Security Administration: Logs messages that are related to security related events. The default log message level is INFO.

2. **Message Destination**

   Log Messages can be stored in several locations.

   - **Log to File**: Send log messages to the /var/log/vormetric/vorvmd_root.log file of a UNIX host, or a Windows equivalent, such as \Documents and Settings\All Users.WINDOWS\Application\Data\Vormetric\DataSecurityExpert\agent\log\vorvmd.log.
   - **Log to Syslog**: Send log messages to the syslog server for a UNIX host. If a syslog server is not configured, it is sent to the host 'messages' file, such as /var/adm/messages. On a Windows host, the messages are sent to the Event Viewer (Application events).
   - **Upload to Server**: Upload to the GDE Appliance and display in the Management Console *Logs* window.

Level: Sets the level of error messages to be sent.

Duplicates: Allow or suppress duplicate messages:

- **Allow**: All duplicate messages of the corresponding Message Type are captured and displayed in the log.
- **Suppress**: Messages of the corresponding Message Type will follow the configured Threshold as to how many times duplicate messages are sent to the GDE Appliance during the given Interval.

3. **File Logging Settings**
   - **Maximum File Size (bytes)**: The agent starts a new, empty log file when the specified limit is exceeded. The default is 1000000 bytes.
   - **Delete Old Log Files**: Select this check box to delete old FS agent logs. This check box works in conjunction with the Number of Old Log Files to Keep text-entry box. For example, Select this check box and enter 3 as the Number of Old Log Files to Keep value. After 3 logs are generated, the first log, log1, is deleted and a new log, log4, is created. If you do not Select this check box, log files will continue to accumulate in the server database and you will have to remove them manually.
   - **Number of Old Log Files to Keep**: Appears only when you select Delete Old Log Files. Specifies the maximum number of agent log files to leave in the server database. This text-entry box is only displayed when the Delete Old Log Files check box is enabled. The default is 5.
4. **Syslog Settings**
   - Local: Send syslog messages to the local machine.
   - Server (1, 2, 3, 4): Enter the hostname of the syslog server
   - Protocol: UDP or TCP
   - Message Format: Specifies the format of the message; Plain Message, CEF, or RFC5424.
5. **Upload Logging Settings**
   - **Maximum Number of Messages to Upload At Once**: Limits the number of messages sent to the GDE Appliance at one time. When the specified number of log entries is reached, those entries are uploaded to the GDE Appliance. The default is 1000.
   - **Upload Messages At Least Every (seconds)**: The maximum interval to wait before the agent is to upload messages to the GDE Appliance. Use this attribute to update the log viewer even when the Maximum Number of Messages to Upload At Once has not been reached. You can lower the interval if there is little agent activity. The default is 10 seconds.
   - **Upload Messages At Most Every (seconds)**: The minimum interval to wait before the agent is to upload messages to the GDE Appliance. You can increase the interval if there is considerable agent activity, so the agents do not flood the network with log messages. The default is 1.

- **Normal Time Out (seconds)**: The maximum interval of time the agent is to wait for the GDE Appliance to acknowledge a backup or restore request and upload related message data. If the agent cannot connect to the GDE Appliance within the specified interval, the agent will try again after the interval configured by the Upload Messages At Least Every attribute. The default is 2 seconds.
- **Shutdown Time Out (seconds)**: The maximum interval of time the agent is to wait for the GDE Appliance to acknowledge job completion and upload related message data. If the agent is unable to upload the log messages within the specified interval, they are left on the agent system. The agent will resend the messages at the beginning of the next job. The default is 30 seconds.
- **Drop If Busy**: Select to slow log message generation and drop log files during periods of extreme logging.

6. **Duplicate Message Suppression Settings**

- **Enable Concise Logging**: When enabled, the number of audit log messages are reduced. This option is disabled by default. Instead of logging messages for each file system operation, only the following types of audit messages are logged:
  - only one audit message for each read or write activity is logged at the start of that activity.
  - audit messages for reading file status information and setting file attributes (and extended attributes) are not logged.
  - audit messages for directory open, close and read attributes are not logged.

  When this setting is enabled at the system level, it applies to all hosts that are added to the GDE Appliance, but will not apply to any existing hosts. Hosts added to the GDE Appliance after this setting is enabled will inherit this setting. These settings can be customized on each host and the host setting will override the system level settings. Note that this feature is not available for VTE versions prior to v6.0.
- **Threshold**: Used when the Duplicates value is set to Suppress. Specifies the maximum number of duplicate messages the agent is to send to the GDE Appliance within the amount of time specified by the Interval parameter. The default is 5 messages. The maximum is 100.
- **Interval**: Used when the Duplicates value is set to Suppress. Specifies the time period in which the number of duplicate messages, specified by Threshold, can be uploaded to the GDE Appliance. Once Interval is exceeded, the count specified by the Threshold parameter starts again. The default is 600 seconds (10 minutes). The maximum is 3600.

Network Diagnostics

The **System > Network Diagnostics** page provides a set of tools for diagnosing network related issues. This page can be accessed by GDE Appliance administrators of type System, All, Domain, Domain and Security, and Security. The available diagnostic tools are:

- **ping:** Checks if a system is up or available on the current subnet. It sends ICMP (Internet Control Message Protocol) echo request packets (ECHO_REQUEST) to the specified network host. ping sends six packets to the network host and reports the results.
- **ipAddress:** Shows the current IP address and related information.
- **arping:** Sends Address Resolution Protocol (ARP) requests to a neighbor host, pings the address on the device interface with ARP packets, and reports the current number of users with that IP address.
- **arp:** Displays the kernel's ARP cache.
- **traceroute :** Utilizes the IP protocol time-to-live field to elicit an ICMP time exceeded (TIME_EXCEEDED) response from each gateway along the path to a specified host.
- **checkport:** Scans a port on a network-accessible system to verify that a TCP connection can be made to the system using the specified port.
- **nslookup:** Returns the IP address associated with a given host name or conversely, the host name associated with a given IP address by querying the DNS.

Backing Up and Restoring the GDE Appliance

6

A backup of the GDE Appliance is a snapshot of the configuration at a point in time. When a backup is restored, the Management Console displays the same information captured at the time the backup was originally made, any changes made after the last backup will not be restored.

This chapter includes the following sections:

- "Overview"
- "Per Domain Backup and Restore"
- "Backing Up the GDE Appliance Configuration"
- "Restoring a GDE Appliance Backup"
- "Automatic Backup"

Overview

A GDE Appliance backup can be used to restore the hosts, encryption keys, policies, as well as other configuration information of a GDE Appliance in the event of a software crash recovery or system changes. A GDE Appliance Administrator of type *System* or *All* creates a system-level GDE Appliance backup, and a GDE Appliance Administrator of type *Domain*, *Domain and Security,* or *All* creates a domain-level backup via the Management Console.

Administrators of type *Domain*, *Domain and Security*, or *All* must be logged into the domain that is to be backed up or restored to perform these operations.
An administrator of type *All* can also perform a domain backup and restore operation, as long as that *All* administrator type is added to the domain.

System-level configuration such as network and timezone settings are ***not*** backed up—those remain unchanged after a restore operation.

Each backup is encrypted with a wrapper key. A wrapper key must be created before the GDE Appliance can be backed up. The same wrapper key is also required to restore the backup.

GDE Appliance backups can be restored at the system-level or at the domain-level.

- A system-level backup can only be restored to the same GDE Appliance or another GDE Appliance.
- A domain-level backup can only be restored to a domain—the same domain, or another domain on the same GDE Appliance, or a domain on another GDE Appliance.

Per Domain Backup and Restore

In addition to a creating a backup of the GDE Appliance, you can also back up and restore the configuration information of a single domain. A domain backup can be restored to:

- the same domain
- to a different domain on the same GDE Appliance

  If a domain backup is restored to a different domain on the same GDE Appliance, there may be a host name conflict, in which case the host names must be changed.
- to a different domain on another GDE Appliance

To create a backup of a domain and to restore that backup, a wrapper key must be created for the domain, and the domain must have an assigned Domain Administrator. The backup and restore operations are done by a Domain Administrator, Domain and Security Administrator, or an administrator of type All from within the domain to be backed up or restored.

Backing Up the GDE Appliance Configuration

When a backup is restored, the Management Console displays the same information captured at the time the backup was originally made.

You can create a backup of the GDE Appliance configuration at the system level or at the domain level. To create a backup of a domain, you must be logged into that domain.

Differences between System-level and Domain-level Backups

The following table lists the differences between system-level and domain-level backups:

Table 5: System-level vs domain-level backups

System-level backup	Domain-level backup
Administrators of type *System* or *All* create the backup.	Administrators of type *Domain* or *Domain and Security, or All* create the backup.

System-level backup	Domain-level backup
Backs up the configuration information for the complete GDE Appliance including; web server certificate, certificates, system preferences, log preferences, users, domains, hosts, encryption keys, signatures, policies, GuardPoints, and license information including all the configuration information in all the domains.	Backs up domain specific information including; web server certificate, certificates, system preferences, log preferences, domains, hosts, encryption keys, signatures, policies, GuardPoints, and license information.
GDE Appliance users can be backed up.	Domain level users cannot be backed up, they will need to be recreated or added back to the domain after a restore operation.
GuardPoints and host-sharing information are backed up.	GuardPoints and host-sharing information are not backed up. Host sharing will have to be re-established and GuardPoints recreated after the restore operation.

The procedures to create a wrapper key, create a backup, and restore a backup are the same at the domain level and at the system level.

Backup Encryption 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 GDE Appliance 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.

To backup system-level configuration, the wrapper key must be created at the system-level by a GDE Appliance Administrator of type *System* or *All*. To create a backup at the domain-level, a wrapper key must be created from within the domain to be backed up by a GDE Appliance Administrator of type *Domain*, or *Domain and Security,* or *All* at the domain level.

Create a wrapper key

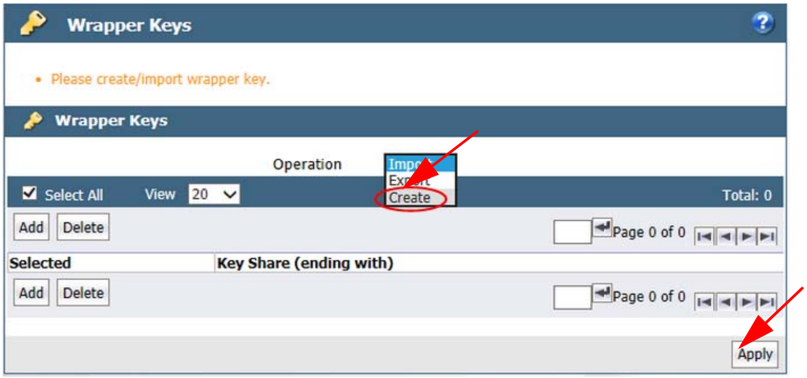
1. Log on to the Management Console as an administrator of type *System Administrator* or *All*.

   Or if you are creating a wrapper key at the domain level

   Log on or switch to a domain on the Management Console as an administrator of type *Domain*, *Domain and Security*, or *All.*

2. Select **System > Wrapper Keys** from the menu bar.
3. In the **Wrapper Keys** window, select **Create** from the **Operation** menu, then click **Apply** to create the wrapper key.

Figure 7: Wrapper Keys window



Wrapper Keys

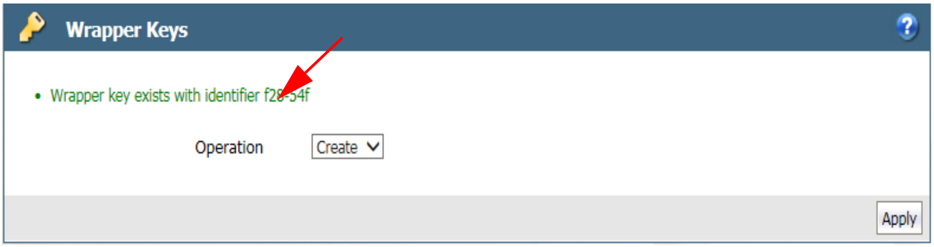
- Please create/import wrapper key.

Wrapper Keys

Operation: Create

You will see a confirmation message stating that the key exists, see Figure 8 below.

Figure 8: Wrapper Keys selection confirmation



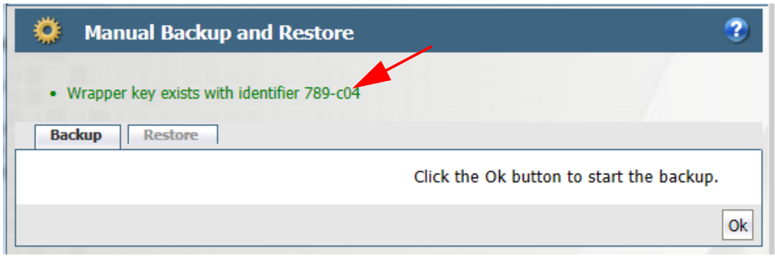
Wrapper Keys

- Wrapper key exists with identifier f28-54f

Operation: Create

4. Select **System > Backup and Restore > Manual Backup and Restore** from the menu bar. A confirmation message is also displayed on this tab, stating that the wrapper key exists. You can now proceed with creating a backup.

Figure 9: Manual Backup and Restore



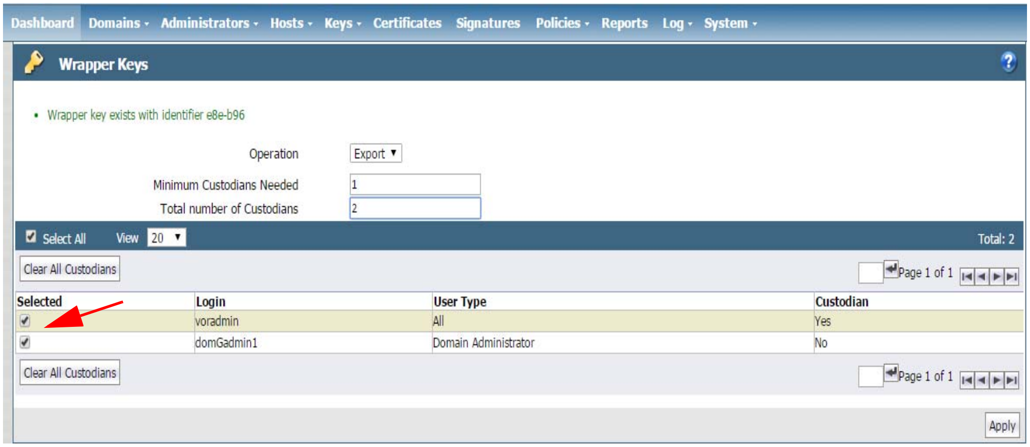
Manual Backup and Restore

- Wrapper key exists with identifier 789-c04

Click the Ok button to start the backup.

5. Return to the **System > Wrapper Keys** menu option and select **Export** from the **Operation** menu to export key shares.

Figure 10: Wrapper Keys window to select custodians for key shares



- Wrapper key exists with identifier e8e-b96

Operation: Export
Minimum Custodians Needed: 1
Total number of Custodians: 2

Selected	Login	User Type	Custodian
☑	voradmin	All	Yes
☑	domGadmin1	Domain Administrator	No

6. 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.

7. Select the check box next to the GDE Appliance 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* window when they log into the Management Console, see Figure 11. Each administrator must see a unique wrapper key share displayed on the dashboard beneath the fingerprint for the CA.

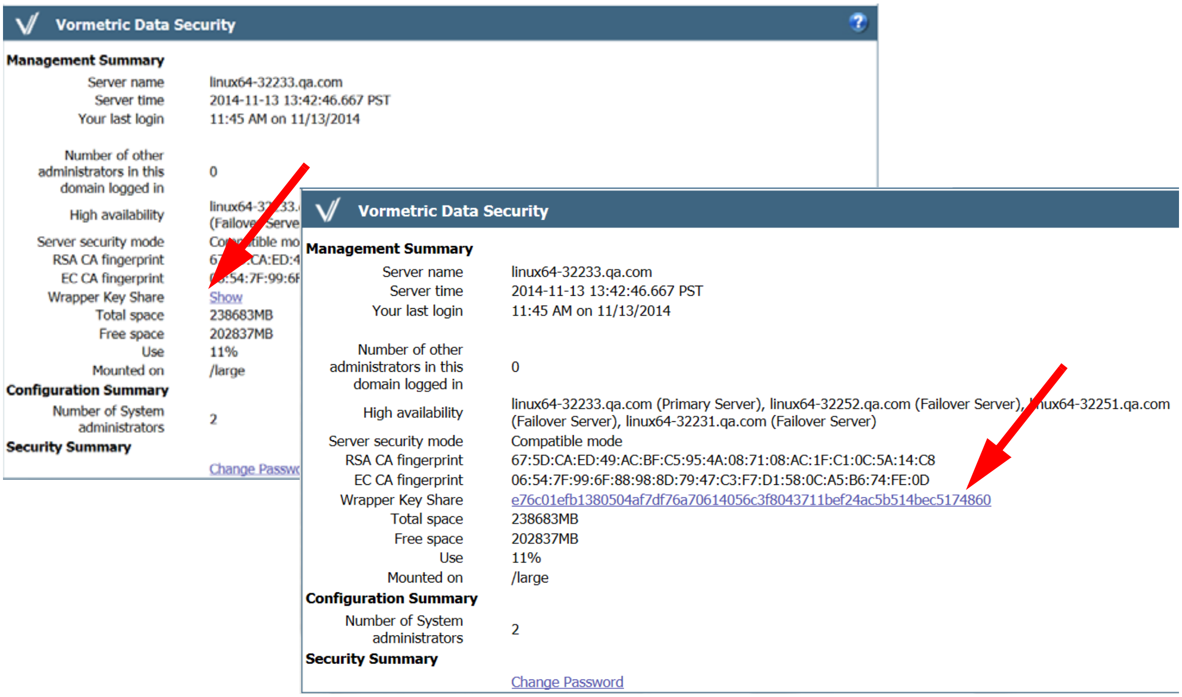
8. Click **Apply** on the bottom right hand corner.

   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**.

9. Ask each administrator to securely store a copy of this key share. They must provide this as part of their role in a GDE Appliance restore operation.

]

Figure 11: Management Console Dashboard showing the wrapper key share toggle



Vormetric Data Security

Management Summary

Server name	linux64-32233.qa.com
Server time	2014-11-13 13:42:46.667 PST
Your last login	11:45 AM on 11/13/2014
Number of other administrators in this domain logged in	0
High availability	linux64-32233.qa.com (Primary Server), linux64-32252.qa.com (Failover Server), linux64-32251.qa.com (Failover Server), linux64-32231.qa.com (Failover Server)
Server security mode	Compatible mode
RSA CA fingerprint	67:5D:CA:ED:49:AC:BF:C5:95:4A:08:71:08:AC:1F:C1:0C:5A:14:C8
EC CA fingerprint	06:54:7F:99:6F:88:98:8D:79:47:C3:F7:D1:58:0C:A5:B6:74:FE:0D
Wrapper Key Share	e76c01efb1380504af7df76a70614056c3f8043711bef24ac5b514bec5174860
Total space	238683MB
Free space	202837MB
Use	11%
Mounted on	/large

Configuration Summary

Number of System administrators	2

Security Summary

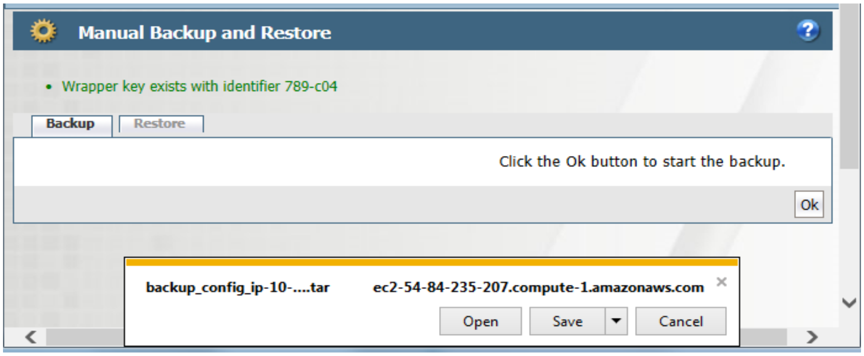
Change Password

A backup of the GDE Appliance can be created after the wrapper key has been created. The procedure to create a backup at the system level or at the domain level is the same.

System-level Backup

1. Log on to the Management Console as an administrator of type *System Administrator* or *All*.
2. Select the **System > Backup and Restore** menu option. The **Manual Backup and Restore** page opens.
3. Click the **Backup** tab and then select **Ok**.

Figure 12: Manual Backup and Restore dialog with File Download dialog displayed



Manual Backup and Restore

- Wrapper key exists with identifier 789-c04

Click the Ok button to start the backup.

backup_config_ip-10-....tar ec2-54-84-235-207.compute-1.amazonaws.com

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_<`*`server name`*`>_yyyy_mm_dd_hhmm.tar`

   Where <*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.

Domain-level Backup

Create a backup of a global domain

1. Log on to the Management Console as an administrator of type *Domain, Domain and Security* or *All*.

   Or switch to the domain that you want to backup.

2. Select the **System > Backup and Restore** menu option. The **Manual Backup and Restore** page opens.

3. Click the **Backup** tab and click **Ok** to start the backup.

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_<domain name>_<`*`server name`*`>_yyyy_mm_dd_hhmm.tar`

   Where <domain_name> is the name of the domain being backed up and <*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.

Restoring a GDE Appliance Backup

A backup of the GDE Appliance can be used to restore the hosts, encryption keys, and policies, as well as other configuration information of a GDE Appliance, after a software crash recovery or system changes. A GDE Appliance backup can be restored at the system level or at the domain level.

The procedure to restore a domain-level backup is the same as the procedure to restore a system-level backup. To restore a domain level backup, you must be logged into that domain.

The GDE Appliance backup is restored via the Management Console.

Restoring the GDE Appliance from a backup

The following procedures describe:

- how to do a system-level restore
- how to do a domain-level restore

NOTE: Following a restore operation, the GDE Appliance configuration in the Management Console is replaced by the configuration stored in the backup copy. Any new encryption keys, policies, hosts, or GuardPoints added since the last backup will be overwritten and lost.

NOTE: Unless this is a disaster recovery scenario where all GDE Appliances have been lost, always backup the current configuration before running a restore operation.

System-level restore

1. Locate the backup that is to be restored
2. Log on to the Management Console as an administrator of type *System Administrator* or *All*.

NOTE: If you already have the proper 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* pull-down menu.
5. Click the **Add** button.

6. 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**.

   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. If this is a disaster recovery, enable the **Include User(s)** check box.
12. Click the **Ok** button. The restored file uploads and the GDE Appliance disconnects from the Management Console.
13. Log back on to the Management Console as an administrator of type *Security* or *All*. Verify that the configuration is restored correctly.

Domain-level restore

When restoring a domain-level backup, all host sharing and GuardPoints on shared hosts are removed and users are not restored.

1. Locate the backup that is to be restored
2. Log on to the Management Console as an administrator of type *Domain*, *Domain and Security*, or *All*.

NOTE: If you already have the proper 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* pull-down menu.
5. Click the **Add** button.
6. 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**.

   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.

In the case of a domain-level restore, you will not be able to restore users and this option will not be available.

11. Click **Ok**.

Once the restore operation is complete, verify that the configuration is restored correctly.

Warning! Following a restore operation, the GDE Appliance configuration in the Management Console is replaced by the configuration stored in the backup copy. Any new encryption keys, policies, hosts, or GuardPoints added since the date/time of the backup file being used for the restore operation, will be overwritten and lost. If there is a reason to do a selective restore from backup, then the following procedure is recommended:
1. Export the keys created since the date/time of the backup file being used for restore operation. Refer to the section on exporting/importing keys in the chapter on “Configuring Keys and Key Groups”.
2. Restore from the backup file (note that this operation will replace the current GDE Appliance configuration).
3. Import the keys created in step 1.

Automatic Backup

The GDE Appliance system configuration information can be scheduled to be automatically backed up on a daily or weekly basis using the Automatic Backup feature.

Automatic backups can also be configured at the domain level. To schedule an automatic backup at the domain level, you must be logged into the domain for which the backup is to be scheduled.

In addition to scheduling a backup, there is also an option to run a scheduled backup immediately and push the backup file to a configured external file server. To do this, you must access a File Server (a UNIX or Windows host) that is network accessible by the GDE Appliance to store the backup files.

The procedure to schedule an automatic backup is the same at the system level and at the domain level.

Schedule an Automatic Backup

1. Select **System > Backup and Restore > Automatic Backup** in the Management Console, to open the **Automatic Backup** page.

2. Enter the settings for the **Automatic Backup Schedule** and the **External File Server** where the backup files will be stored.

   Enter the following information in the **Automatic Backup Schedule** section:

   a. **Active Schedule**: Choose either Daily or Weekly, the default is Weekly.

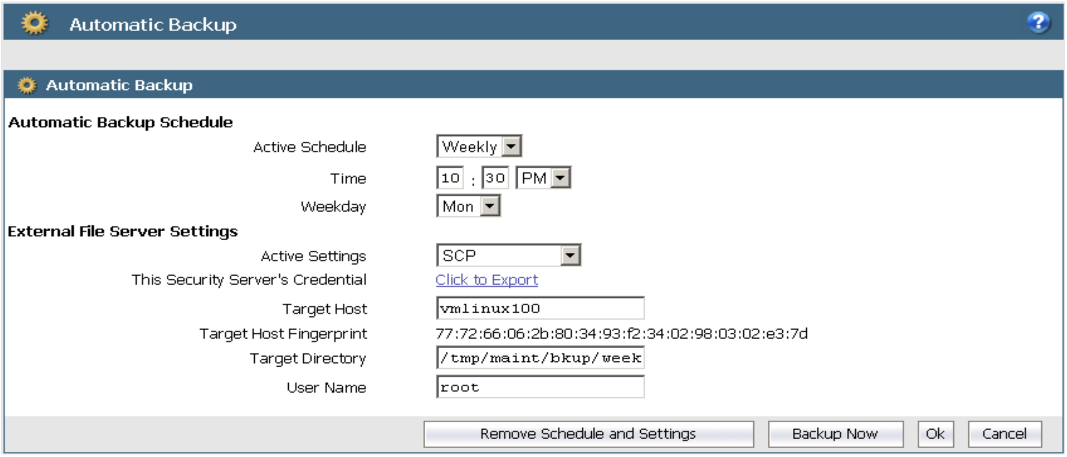
   b. **Time**: Based on a 12-hour clock and the A.M./P.M. modifiers. Time is relative to the GDE Appliance system clock.

   c. **Weekday**: Select the day of the week on which to backup the GDE Appliance.

   Enter the following information in the **External File Server Settings** section:

   d. **Active Settings**: Select SCP or Windows Share. This configures the mode in which to copy the generated backup file to the remote system. SSH must be configured on the destination system to use the SCP mode. The selected mode—SCP or Windows—determines the subsequent configuration parameters that must be entered

Figure 13: Automatic Backup Schedule for SCP



Automatic Backup

Automatic Backup

Automatic Backup Schedule

Active Schedule	Weekly
Time	10 : 30 PM
Weekday	Mon

External File Server Settings

Active Settings	SCP
This Security Server's Credential	Click to Export
Target Host	vmlinux100
Target Host Fingerprint	77:72:66:06:2b:80:34:93:f2:34:02:98:03:02:e3:7d
Target Directory	/tmp/maint/bkup/week
User Name	root

SCP

If you select **SCP**, enter the following information (all fields marked with a red asterisk are required):

- **This Server Security's Credential**: **Click to Export**. Click this to download the GDE Appliance server's public key. Copy the public key onto the destination system and into *~/user/.ssh/authorized_keys*. The public key is required to use SCP to copy the backup file to the external file server.

- **Target Host**: Enter the host name, IP address, or FQDN of the destination system. If the destination system has a File System Agent, you do not have to use the same host name as configured in the Hosts window. You can use any recognized means of addressing the destination system, just as long as it is recognized on your network.
- **Target Host Fingerprint**: The fingerprint value displayed is the fingerprint of the GDE Appliance public key that is currently on the destination system. The fingerprint is retrieved from the destination system and displayed in the Automatic Backup page during a backup. You can verify if the public key on the destination system is current by comparing the key in *~user/.ssh/authorized_keys* on the destination system with the key generated by **Click to Export**.
- **Target Directory**: Enter the full path of the directory in which to copy the backup file.
- **User Name**: Enter the name of the user to perform the copy operation. The name entered must be a valid user on the destination system. Also, copy the public key into the *~/.ssh/authorized_keys* file in the home directory of the user you specify in this text-entry box. A password is not required for the SCP user because a public key is used to authenticate the SCP user.

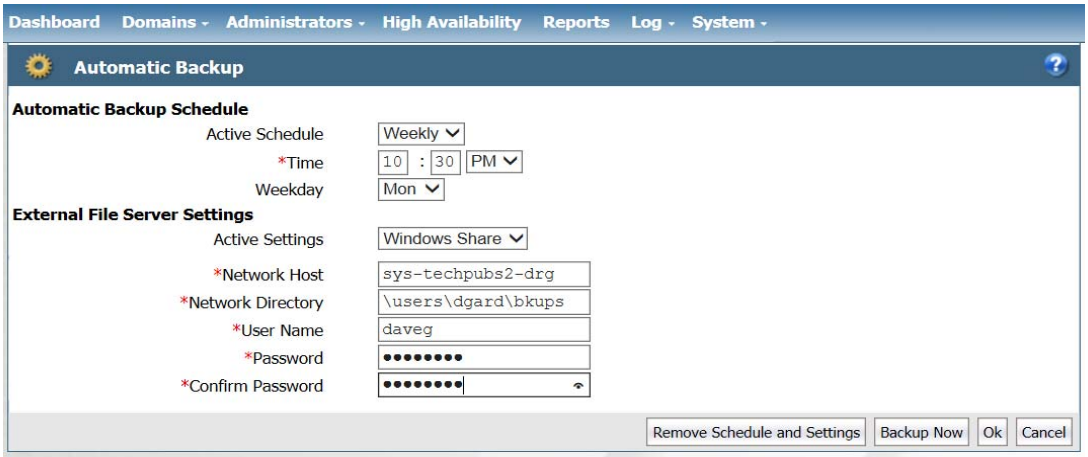
Windows Share

If you select **Windows Share**, enter the following information (all fields marked with a red asterisk are required):

- **Network Host**: Host name, IP address, or FQDN of the destination system.
- **Network Directory**: The shared folder path to which to copy the backup file.
- **User Name**: The name of the user to perform the copy operation. The name entered must be a valid user on the destination system.
- **Password**: The password for User Name. Sometimes a domain is required for user authentication. To include the user domain, append the domain to the user name in the form user @domain. For example, bubba@vormetric.com.
- **Confirm Password**: Re-enter the password for User Name.

Click **Ok** to save the configuration settings currently displayed on the Automatic Backup page, changes to the settings are stored in cache until you click **Ok**.

Figure 14: Automatic Backup schedule for Windows Share



Automatic Backup Schedule

Active Schedule: Weekly

*Time: 10 : 30 PM

Weekday: Mon

External File Server Settings

Active Settings: Windows Share

*Network Host: sys-techpubs2-drg

*Network Directory: \users\dgard\bkups

*User Name: daveg

*Password: ••••••••

*Confirm Password: ••••••••

1. Click **Ok** to save the configuration settings or click **Backup Now** to immediately create a backup using the current configuration. This is an easy way to the test network connection and login credentials of the configuration settings you just made.
2. After a successful backup, look in the specified Target Directory on the Target Host to see the backup files.

   Example:

   `backup_config_myCo.corp.com_v5.3.1.0_1716_yyyymmdd_hhmm.txt`

Schedule an immediate backup

You can also schedule an immediate backup once you have made all your selections:

- Click **Backup Now** to create a backup immediately using the current configuration.

  This is an easy way to the test network connection and login credentials of the configuration settings you just made.

Remove schedule and settings

Click **Remove Schedule and Settings** to clear all the fields in both the Daily and Weekly configurations. For SCP mode backups, this means the public key is removed, and a new one has to be generated. This new public key has to be copied to the destination system.

A new public key is automatically downloaded the next time you click **Click to Export**. If you create a new key this way, you must also update the *~/.ssh/authorized_keys* file on the destination system because the SSH credentials have changed and will no longer be valid.

Configuring High Availability (HA)

7

Two or more GDE Appliances can be configured as a High Availability (HA) cluster to provide redundancy.

The High Availability configuration consists of two or more GDE Appliances—one GDE Appliance installation acts as the primary server and the others become failover servers. All configuration settings, including changes to administrators, hosts, keys, and policies, occur on the primary GDE Appliance only. Configuration changes and updates on the primary GDE Appliance are pushed to the failover GDE Appliance at set intervals.

To ensure reliable operation, Thales recommends that the appliances or systems in an HA configuration run homogeneous configurations. If the primary GDE Appliance is a virtual applianceGDE Appliances, the failovers must all be virtual appliances.

This chapter contains the following sections:

- "GDE Appliance High Availability Overview"
- "High Availability Configuration"
- "Converting a Failover GDE Appliance to a Primary"
- "Assigning Hosts to a GDE Appliance in an HA cluster"
- "Pushing Configuration Changes to Hosts"
- "Reassigning Hosts to Another Node in the HA Cluster"
- "Displaying High Availability Configuration Status"

GDE Appliance High Availability Overview

Only GDE Appliance Administrators of type System or type All are permitted to configure High Availability (HA) for GDE Appliances.

All configuration settings, including changes to administrators, hosts, keys, and policies, are made on the primary GDE Appliance, failovers are read-only. Configuration changes and updates on the primary GDE Appliance are pushed to the failover GDE Appliances at set intervals.

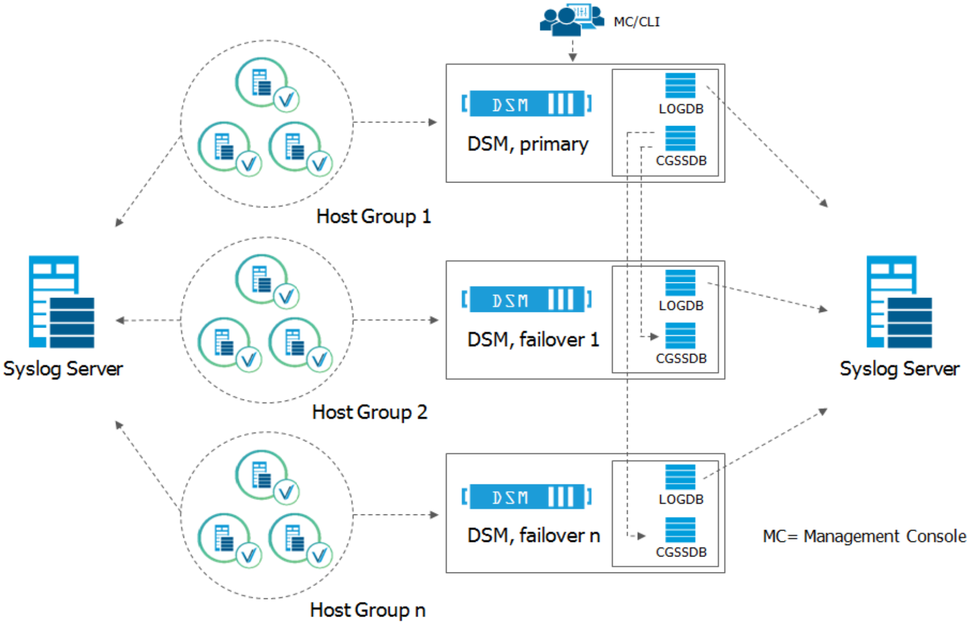
The primary GDE Appliance propagates configuration changes to the failover GDE Appliances using replication. Each failover GDE Appliance database is updated with the primary GDE Appliance database. The primary GDE Appliance acts as the Certificate Authority (CA) and creates signing certificates. The primary GDE Appliance must be installed and configured with its own certificates, before you can configure failover and agent certificates.

Replication is a one-way operation in which changes go only from the primary to the failover GDE Appliance. Data is not pushed back to the primary GDE Appliance. Therefore, log data generated on the failover GDE Appliances remains on the failovers—there is no record of failover GDE Appliance activity on the primary GDE Appliance. You must check the logs on the failover GDE Appliances for records of local agent activity or configure a Syslog server as a central repository for GDE Appliance log messages. Additionally, auto-backup settings are not replicated to the failover server, as backups are only done from the primary GDE Appliance.

Because a failover GDE Appliance is effectively a copy of the primary, both GDE Appliances have the same RSA CA and EC CA fingerprints (for example, `5X:5A:51:93:ED:53:B9:8A:1Z:FG:72:3A:BG:60:FV:3Q:CE:F7:69:95`). They continue to have the same RSA CA and EC CA fingerprints after converting a failover to a primary. Likewise for backup key shares—if a key share was displayed in the old primary, it will also be displayed in the new primary.

Replication between GDE Appliance high availability nodes can be secured by enabling TLS, this is described in the sections below.

Figure 15: High Availability configuration



Assigning agents to GDE Appliances in an HA cluster

You can assign VTE agents to any GDE Appliance in an HA cluster. The assigned GDE Appliance becomes the initial point-of-contact for those agents. The assigned GDE Appliance pushes configuration changes and encryption keys to the VTE Agent immediately.

A list of the GDE Appliances that the agent can communicate with is generated and downloaded to the agent. If a GDE Appliance in the list is not available when the agent tries communication, the agent tries the next GDE Appliance on the list.

NOTE: Agent logging occurs on the GDE Appliance to which the agent is assigned, not necessarily the primary GDE Appliance.

Each agent uses its own `agent.conf` file to identify the primary GDE Appliance. The most important line in this file specifies the protocol (HTTPS), the network name of the system running the Web application for the primary GDE Appliance, and the communication port (8446).

The FQDN of the primary GDE Appliance is required when an agent registers with the primary GDE Appliance. Once registered, the agent is automatically assigned to that primary GDE

Appliance. The agent is administered by the primary GDE Appliance without any additional configuration. That agent can be reassigned to a failover GDE Appliance later. If there are two agents running on the host, such as a VTE Agent and a Key Agent, the agents are assigned together to the same GDE Appliance.

The primary-secondary GDE Appliance relationship is active-passive. That is, the VTE agent and host configuration occur on the primary GDE Appliance and the changes are pushed to all the failover GDE Appliances. However, some load-balancing can be achieved by assigning VTE agents to specific failover GDE Appliances based on their proximity, availability, network speed, and system speed.

The list of GDE Appliances, both primary and failover, that an agent can access is configured on the primary GDE Appliance. The list is pushed to the host when a VTE Agent registers with the primary GDE Appliance.

Every GDE Appliance can check the status of every host in an HA configuration. Since configuration changes are done on the primary GDE Appliance only, and since each agent must first register with the primary GDE Appliance, each host must have network access to the primary GDE Appliance. It does not have to be an uninterrupted connection, but is required to register the agent and for the GDE Appliance to query the host status. Each host must be on the same network as every GDE Appliance that will check the host status.

Figure 16: Agent registration and failover pushes

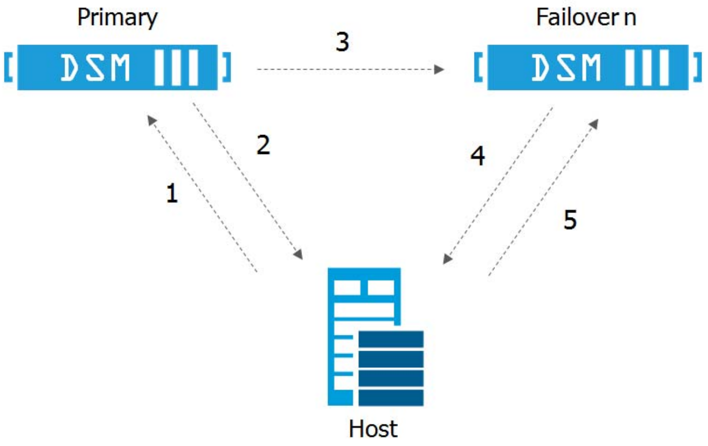


Figure 16 depicts the agent registration and host update flow:

1. The Management Console is used to add a host to the primary GDE Appliance and assign the host to a specific GDE Appliance in the HA configuration.
2. The VTE Agent on the host must be registered with the primary GDE Appliance (1).

3. If a VTE Agent is registered with the primary GDE Appliance, the primary GDE Appliance returns a list of GDE Appliances to the agent that the agent can use (2).
4. The primary GDE Appliance pushes configuration updates to all the failover GDE Appliances (3). The update includes a list of hosts whose agents are to be managed by each failover GDE Appliance. Each GDE Appliance knows the hosts that it can administer and each agent knows the GDE Appliances that are to administer it.
5. Each GDE Appliance pushes policy updates and configuration changes to the VTE Agents that the GDE Appliance administers (4).
6. The agent sends policy evaluation requests and activity messages to the first available GDE Appliance in the list (5).

Log information and activity are, by default, local to the GDE Appliance that is managing the agent. This makes tracking complicated because you must open a Management Console session on each GDE Appliance to monitor the activity and health of each host in the HA configuration.

Instead of running a Management Console session on each GDE Appliance, consider configuring a central Syslog server to receive log messages. You can view the host and agent activity in sequential order on the Syslog server. See “Configuring Syslog Servers for System-Level Messages” for information about configuring Syslog servers.

High Availability Configuration

You must have at least two GDE Appliances installed on the same network to create an HA system—a primary GDE Appliance and a failover GDE Appliance. The maximum number of nodes allowed in a GDE Appliance cluster is 8, including the primary node.

All GDE Appliance 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 node.

The following steps describe how to set up a HA cluster with two newly configured GDE Appliances. Replication between the primary and failover GDE Appliance nodes can be secured by enabling TLS between the nodes, see “Securing Replication” for more information.

Before you begin

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 also modify the 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.
- 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 this 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. *You must do this on EACH protected host making sure to add an entry for all GDE Appliance 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.

2. Open all required ports. The following table describes the communication direction and purpose of the ports that must be opened:

Table 6: Ports to configure

Port	Protocol	Communication Direction	Purpose
22	TCP	Management Console → GDE Appliance GDE Appliance → SSHD Server	CLI SSH Access Auto-backup via SCP
161	TCP/UDP	SNMP Manager → GDE Appliance	SNMP queries from an external manager
443	TCP	GDE Appliance → CIFS Server	Redirects to either port 8445 or 8448 depending on the security mode.
7025	UDP	GDE Appliance ↔ GDE Appliance	Uses SNMP to get failover node response time.

Port	Protocol	Communication Direction	Purpose
8443	TCP	Agent → GDE Appliance	Fallback RSA TCP/IP port through which the agent communicates with the GDE, in case 8446 is blocked. The agent establishes a secure connection to the GDE appliance, via certificate exchange, using this port.
8444	TCP	Agent → GDE Appliance	Fallback RSA port via which the Agent log messages are uploaded to GDE, in case 8447 is blocked.
8445	TCP	Browser → GDE Appliance GDE Appliance ↔ GDE (fallback)	Management Console, VMSSC, and fallback for RSA HA communication in case port 8448 is blocked.
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)
8448	TCP	Browser → GDE Appliance GDE Appliance ↔ GDE Appliance	GUI Management during enhanced security using Elliptic Curve Cryptography (Suite B). Also for secure communication between GDE Appliances in HA cluster.
50000	TCP	GDE Appliance (primary) → GDE Appliance (failover)	HA information exchange

3. Ensure that network communication between the designated primary and failover GDE Appliances is working, perform a 'ping' operation on all the GDE Appliances.

NOTE: If the network latency between the primary and the failover GDE Appliances 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. See Table 4, "General Preferences System tab attribute values and use," on page 25 for details about this setting. We recommend changing this value to 0 or 5 from the default of 10.

Securing Replication

You can choose to enable TLS to secure replication between GDE Appliance nodes in a high availability (HA) cluster. Prior to the current release, the replicated data was encrypted, now, the replication channel can also be encrypted. Should you choose to secure replication between nodes, this step must be done on *each* node that is to be part of the cluster *before* you create the cluster.

NOTE: If the GDE Appliance's outbound ports are filtered, then you must open the following outbound ports on the primary node: port 50501 for the first failover node, port 50502 for the second failover node and so on for each failover node. The GDE Appliance supports up to eight failover nodes. refer to the Ports Configuration table in the *Installation and Configuration Guide* for details.

Enabling TLSHA

Do the following on each node that is to be part of the HA cluster:

1. Log on to the CLI and type system at the prompt,

```
0000:vormetric$ system
0001:system$
```

2. Enable TLS, type security tlsha on at the prompt, you will be prompted to confirm that you want to continue,

```
0002:system$ security tlsha on
Enable TLS for HA replication for this DSM? The Security Server service
will restart automatically on failover DSMs.
Continue? (yes|no)[no]:yes
SUCCESS: Turned on TLS for HA replication.
Run this command on every server node in the cluster then run
convert2failover on failover servers.
0003:system$
```

3. You must run this on each node that is to be part of the cluster.

You can now proceed with creating the HA cluster. For details about using this command see, "System Category Commands".

Enabling TLSHA on existing HA deployment

If you have an existing HA deployment and want to enable this feature, you need to break up the cluster, enable TLS on each of the GDE Appliances that belong to the cluster, and then reconfigure HA.

Breaking up a 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.

Enabling TLSHA and reconfiguring the cluster

Next, enable TLS as described here, “Enabling TLSHA”. Once this has been done on each node, reconfigure the cluster as follows:

1. Log on to the CLI of the failover server.
2. Type ha to access the HA category of commands and type `convert2failover` at the prompt.
3. Follow the instructions to enter necessary data.
4. Wait until the conversion process is complete. This could take several minutes.
5. Log on to the Management Console on the primary GDE Appliance as a user of type System Administrator or All.
6. Select the failover server in the *High Availability Servers* window and click **Config Replication**.
7. Repeat the steps above each failover node, one at a time. Wait until synchronization is complete.

To check that TLS is enabled:

1. Log on the GDE Appliance CLI, type `security tlsha show` at the prompt,

```
0003:system$ security tlsha show
TLS for HA replication is enabled
SUCCESS: Showed TLS for HA replication.
0004:system$
```

To check whether TLS is running:

- Log on to the CLI, type:

```
# security tlsha status
```

```
0005:system$ security tlsha status
TLS HA replication has stopped
SUCCESS: Showed TLS for HA replication status.
0006:system$
```

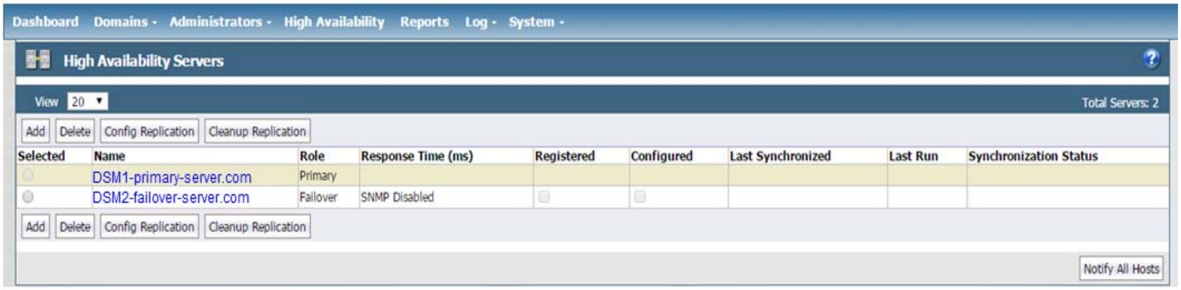
Adding GDE Appliance2 to GDE Appliance1

1. Install and configure two GDE Appliances as described in the *Installation and Configuration Guide*. The license must be installed on the primary GDE Appliance before HA can be configured.
2. On GDE Appliance1 (primary), 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.

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

4. Click **Add**. The **Add Server** window opens.
5. In **Server Name**, enter the host name or FQDN of GDE Appliance2 (failover).
6. Click **Ok**. GDE Appliance2 is listed in the **High Availability Servers** with the role of **Failover**.

Figure 17: Added but not registered failover node



Selected	Name	Role	Response Time (ms)	Registered	Configured	Last Synchronized	Last Run	Synchronization Status
○	DSM1-primary-server.com	Primary						
○	DSM2-failover-server.com	Failover	SNMP Disabled	□	□			

Registering GDE Appliance2 as a failover with GDE Appliance1

1. On GDE Appliance2, log on to the command line. 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 GDE Appliance1, the primary server.

   c. Type the name of an administrator of type System Administrator or All that is configured on GDE Appliance1.

   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 GDE Appliance will issue the certificate using the information you provide in the following steps:

   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. Type `yes` to continue. A warning is displayed asking you to confirm the primary server information that you entered in step 3. above, as well as the FQDN of the server designated as the failover, and the certificate information that you just entered. Click `yes` to continue.

   The installation utility creates certificates, completes the installation process, and then starts the GDE Appliance. This may take a few minutes.

   The CA certificate fingerprint is displayed.

   Sample output:

```
Primary_Server=DSM1
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 GDE Appliance1 on the Management Console, click the **Dashboard** tab.

7. Match the fingerprint from the output on GDE Appliance2 with the **RSA CA fingerprint** on the GDE Appliance1 **Dashboard**.

8. Click the **High Availability** tab. In the row for the failover GDE Appliance, the **Registered** check box should be selected.

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 GDE Appliance.

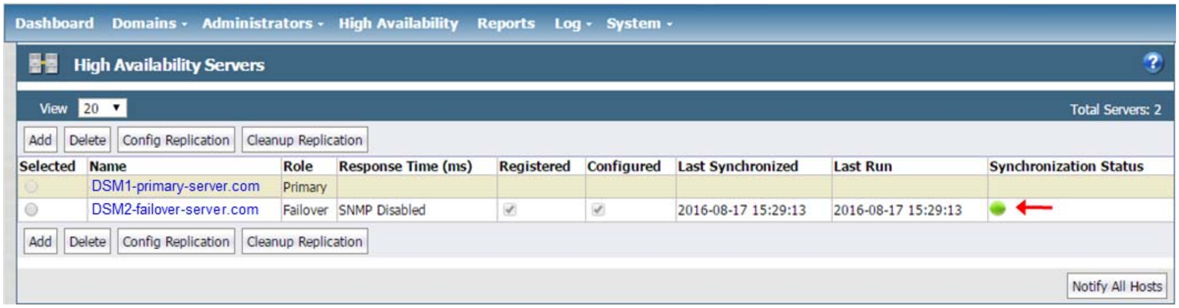
2. Click **Config Replication**. A dialog box opens, prompting you to continue.

3. Click **OK**. The **Configured** check box for the failover GDE Appliance should be enabled after configuration completes.

NOTE: After clicking OK, you will have to wait for the operation to complete and for the status to turn green, before you can verify the configuration changes.

4. Verify that the failover GDE Appliance configuration completed successfully. Check the *High Availability Servers* window on the primary GDE Appliance. Figure 18 shows a fully configured and operational failover GDE Appliance that has been synchronized with the primary GDE Appliance.

Figure 18: Configured and synchronized failover node



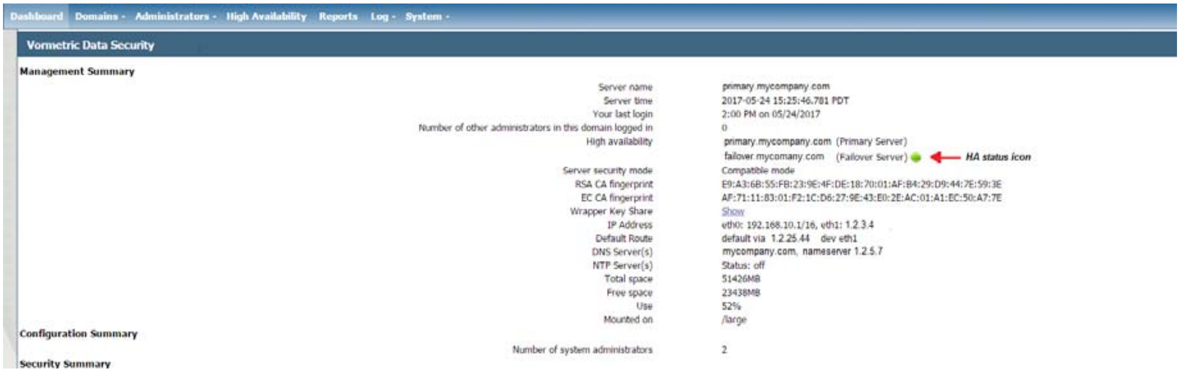
Selected	Name	Role	Response Time (ms)	Registered	Configured	Last Synchronized	Last Run	Synchronization Status
○	DSM1-primary-server.com	Primary						
○	DSM2-failover-server.com	Failover	SNMP Disabled	✓	✓	2016-08-17 15:29:13	2016-08-17 15:29:13	●

Synchronization Status on the Dashboard

The Management Console *Dashboard* page on both the primary and the failover nodes displays the high availability synchronization status, if high availability has been configured.

This field is not displayed if you are logged a domain. If a failover GDE Appliance has not been configured, a "No High Availability Setup" is displayed, clicking the red icon takes you to the *High Availability Servers* page of the primary server, from where you can configure failover GDE Appliances.

Figure 19: HA synchronization status on the Dashboard



Management Summary

Server name	primary.mycompany.com
Server time	2017-05-24 15:25:46.781 PDT
Your last login	2:00 PM on 05/24/2017
Number of other administrators in this domain logged in	0
High availability	primary.mycompany.com (Primary Server) failover.mycomany.com (Failover Server) ●
Server security mode	Compatible mode
RSA CA fingerprint	E9:A3:6B:55:FB:23:9E:4F:DE:18:70:01:AF:B4:29:D9:44:7E:59:3E
EC CA fingerprint	AF:71:11:83:01:F2:1C:D6:27:9E:43:E0:2E:AC:01:A1:EC:50:A7:7E
Wrapper Key Share	Show
IP Address	eth0: 192.168.10.1/16, eth1: 1.2.3.4
Default Route	default via 1.2.25.44 dev eth1
DNS Server(s)	mycompany.com, nameserver 1.2.5.7
NTP Server(s)	Status: off
Total space	51426MB
Free space	23438MB
Use	52%
Mounted on	/large

Configuration Summary

Number of system administrators	2

Security Summary

If high availability has been configured, the FQDN of the primary and failover GDE Appliance node(s) are displayed, with a synchronization status icon next to the failover node(s). The icon indicates the status of the failover;

Table 7: HA Synchronization Status Icons

Icon	Description
🟢	a green circle indicates that the failover has successfully synchronized with the primary within 30 minutes.
▲	a yellow triangle indicates that the failover has taken between 30 to 120 minutes to synchronize with the primary, and that there might be a problem.
🟥	a red square indicates that the failover is taking longer than 120 minutes to synchronize with the primary or a synchronization error.

Clicking the icon next to the failover node link takes you to the *High Availability Servers* page of the node that you are logged into, from where you can see the timestamp of the last time the failover server synchronized with the primary server.

The *High Availability* page on the primary displays the following:

- **Selected**: Shows which GDE Appliance(s) are selected.
- **Name**: Displays the name of the GDE Appliance.
- **Role**: Displays whether the current GDE Appliance is a primary or failover node.
- **Response Time (ms)**: If SNMP is enabled, the primary node polls each failover node using an SNMP GET request. The response time is displayed in milliseconds. If SNMP is disabled, the Response Time column will indicate “SNMP Disabled”. If the connection is lost, the Response Time column will indicate “Not Reachable”.
- **Registered**: A check mark in this column indicates that the failover node is registered with the primary node.

- **Configured**: A check mark in this column indicates that the failover node is configured and can be accessed by any registered Encryption Agents for policies and keys changes.
- **Last Synchronized**: The time shown in this column indicates the last successful synchronization between the primary and failover node.
- **Last Run**: The time in this column indicates the last attempt at synchronization between the primary and failover nodes.
- **Synchronization Status**: Shows the synchronization status between the primary and failover nodes, this indicated by an icon.

The *High Availability* page on the failover node displays the following:

- **Selected**: Shows which GDE Appliance(s) are selected.
- **Name**: Displays the name of the GDE Appliance.
- **Role**: Displays whether the GDE Appliance is a primary or failover node.
- **Registered**: A check mark in this column indicates that the failover node is registered with the primary node.
- **Configured**: A check mark in this column indicates that the failover node is configured and can be accessed by any registered Encryption Agents for policies and keys changes.
- **Last Synchronization Heartbeat from Primary**: The time, date and duration in this column indicates the last successful synchronization between the primary and failover nodes, and the time that has elapsed since the last synchronization. This status will also be reflected on the *Dashboard* page.
- **Synchronization Status**: Shows the synchronization status between the primary and failover nodes.

Configuring High Availability for network HSM-enabled

GDE Appliance appliances which do not have a built-in HSM can be configured use a network HSM via an nShield Connect HSM. For more about this feature, refer to the GDE Appliance Installation and Configuration Guide.

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

- Configure at least two nShield Connect appliances 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. Refer to the nShield Connect user documentation for a description of procedures to configure an nShield Connect HSM.

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

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

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

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

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

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

   Refer to the nShield user documentation for a description of how to configure and deploy the nShield Connect device and the associated RFS.
4. Add both nShield Connect appliances to each of the GDE Appliances as follows:

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

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 Connect device to be added to the GDE Appliance, it is not required for any subsequent nShield Connect appliances that are added.

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

```
0000:dsm$ hsm

0001:hsm$
```

c. Use the `connect add` command to add the nShield Connect to the GDE Appliance. 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 appliance 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
```

d. A warning is displayed, informing you that once this GDE Applianceis converted to a network HSM-enabled appliance, it cannot be rolled back. Type ‘yes’ to continue.

e. The GDE Appliance is restarted if the operation is successful.

f. Follow the prompts to add the nShield Connect appliance to the GDE Appliance.

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

h. If there are more nShield appliances in the same Security World you can add them now using the `connect add` command.

The second way to create a network HSM-enabled HA cluster is to configure a standalone network HSM-enabled GDE Appliance, this is your primary node. Then add non network HSM-enabled GDE Appliance 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 Connects that are configured on the primary node, and prompts you to add that nShield Connect appliance. If the primary is configured with more than one nShield Connect appliance, 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 that are not configured on the GDE Appliance 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.

Add the failover nodes as follows:

1. Log on to the GDE Appliance Web UI and click **High Availability** to navigate to the *High Availability Servers* page.
2. 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’.
3. 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.

4. Enter information about the primary GDE Appliance 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
```

5. Enter the failover GDE Appliance 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.

6. Type ‘`yes`’ to continue, the GDE Appliance server software, is stopped while the conversion to failover is done and the security certificate is signed.

7. A message is displayed informing you that the primary server has nShield Connect appliances configured with the IP addresses displayed, you will be prompted to add the first nShield Connect appliance in the list, type yes. In this case the `connect add` command is run automatically when you choose to add the nShield Connect appliance.

8. You will then be asked if you want to add the second nShield Connect, type ‘`yes`’.
If you have more than two nShield appliances 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 Connect appliances available in the same Security World. To ensure business continuity, Thales recommends that you connect each node to at least two nShield appliances.

9. Repeat these steps for each failover node.

Once a GDE Appliance is network HSM-enabled, it must be connected to at least one nShield Connect appliance. If you remove an nShield appliance from a Security World, you must make sure that any GDE Appliances that were connected to it, are now connected to another nShield appliance belonging to that same Security World.
In this case, if more than one nShield appliance is available in the Security World, a GDE Appliance Administrator could choose to use any of the available nShield appliances after the GDE Appliance has been converted to a failover node.

Converting a Failover GDE Appliance to a Primary

Reasons for changing a failover GDE Appliance to a primary GDE Appliance can include:

- The primary can fail unexpectedly and must be removed from service. A failover can then be reconfigured to act as a replacement primary GDE Appliance. This is particularly useful when you do not have a current backup of the primary node. The failover contains the same database information as the primary at the time the failover was last synchronized.
- The primary GDE Appliance can be fully operational but you want to create a new primary node for a different environment that contains the same database (namely, keys and policies)

as the existing primary GDE Appliance. You can configure a new primary node in this manner, though it is easier to just back up the old primary node and restore the backup on the new primary node.

The general reason for converting a failover to a primary GDE Appliance is because the primary is no longer operational.

To convert a failover GDE Appliance to a primary GDE Appliance:

1. If the primary GDE Appliance is still functioning and is available, do the following tasks on the primary:

   a. Reassign the hosts that are configured to the failover node to other another GDE Appliance.

      You cannot delete a failover from an HA configuration if there are hosts assigned to that GDE Appliance.

   b. Back up the primary GDE Appliance.

   c. Wait until the failover synchronizes with the primary.

   d. Run **Cleanup Replication** for the failover.

      Cleanup Replication deletes the failover configuration from the primary, and also deletes the failover registration.

   e. Delete the failover from the primary HA configuration.

      This removes everything associated with the failover, including the failover GDE Appliance’s certificate, and places the failover in an unregistered state.

2. Log on to the failover node CLI.

3. Execute the High Availability `convert2primary` command.

```
0001:ha$ convert2primary
WARNING: We will now convert this failover server to primary server.
This may take several minutes.
Continue? (yes|no)[no]:yes

SUCCESS: convert server to primary server. The server is restarted.

0002:ha$
```

4. Make any network changes that you need on the new primary GDE Appliance.

5. Open a Web browser session on the new primary GDE Appliance and log in.

NOTE: You have all the same keys, policies, and host records as the original primary GDE Appliance.

6. If you have not already done so, install a license.

   A license is optional for a failover node, but it is required for a primary server.

7. If you converted the failover to a primary because the original primary failed, reconfigure agent installations to use the new primary.

NOTE: If the primary node in a high availability deployment with several failover nodes fails, and a backup of that primary is restored to a new primary node with a different IP address and FQDN, which is *not* part of the HA configuration, then any agents running on hosts registered with the old primary will need to be re-registered with the new primary. The genca command will also have to be run on the CLI console to regenerate the CA certificate on the new primary. In the same scenario, if the primary backup is restored to a new primary with the same IP address and FQDN as the old primary, then the agents will not have to re-register, it will be as if nothing has changed

Assigning Hosts to a GDE Appliance in an HA cluster

The agents on a host are assigned to a primary or failover node in the Management Console. In an HA cluster, an agent and GDE Appliance association is characterized as follows:

- The agent is configured with the URL for the primary GDE Appliance in an HA cluster.
- The agent registers with the primary.
- The agent is implicitly assigned to the primary.
- The agent can be explicitly assigned to any GDE Appliance node in the HA cluster.
- The assigned GDE Appliance pushes updates and configuration changes to the agent.

GDE Appliances are selected for accessibility, speed, or simply convenience. If the GDE Appliance is not accessible, the agent accesses other GDE Appliances in the HA cluster in sequential order. The access order is a linear sequence when the agent is managed by the primary node, , or a loop sequence when the agent is managed by a failover node.

If the agent is assigned to a primary node, it accesses the primary first. If the primary is not available, the agent tries the failover nodes. The search will loop indefinitely, resuming with the primary.

If the agent is assigned to a failover node, it accesses that failover server first. If that failover is not available, the agent tries the remaining failover servers. After unsuccessfully looping through all the failover, the agent tries a connection with the primary. The search loops indefinitely, resuming with the assigned failover.

Failover server node order is based on an alphanumerically sorted list of failover servers automatically extracted from the primary node. You cannot configure the actual order in which servers are accessed.

If a failover cannot be synchronized, or if a failover is disconnected from the network, configuration changes are not pushed to the hosts that are configured with that failover. This is because only the configured GDE Appliance pushes changes to a host. Not until the host re-initializes, does it search for a GDE Appliance and then accept updates from the server node to which it successfully connects.

For a host to accept pushes from a different GDE Appliance, one option is to restart `secfs` on the host system. As `secfs` re-initializes, the VTE Agent searches for a GDE Appliance. It contacts the GDE Appliances in sequential alphanumeric order. The first GDE Appliance that the host can connect to, pushes the latest configuration changes to the host. Windows users may find it more convenient to reboot the Windows host.

If you are unsure of how many hosts may be out of sync with their assigned GDE Appliance, click the **Notify All Hosts** button in the *High Availability Servers* window. This pushes the latest configuration of every host, including their GDE Appliance assignment, to every host in the HA cluster.The agent is updated when it can communicate with an active GDE Appliance.

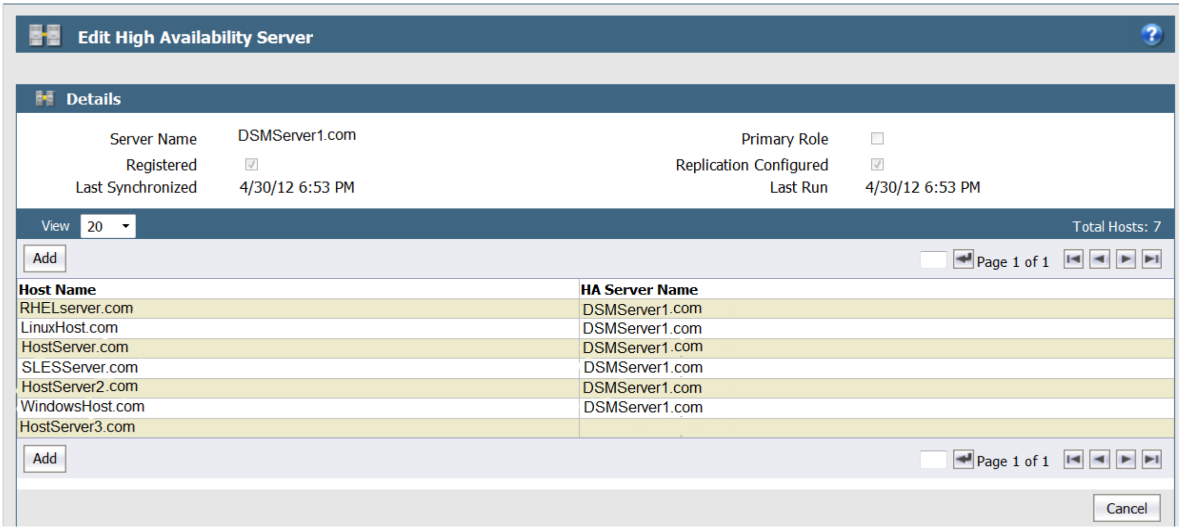
If you do not see log entries for an agent, the agent might be accessing the wrong GDE Appliance. Check the agent configuration. You can also check the logs on the other GDE Appliance.

You can configure a Syslog server to act as a central log repository for all GDE Appliances in an HA cluster. This enables you to monitor all the GDE Appliance from one location.

You can assign or reassign a host to any GDE Appliance at any time using the Management Console. Anticipate some delay before the host uses the new configuration. After you assign or reassign a host to a GDE Appliance, the GDE Appliance waits for the update interval to elapse before the primary pushes the configuration change to the assigned server node. Then, after another update interval, the assigned server node pushes the change to the VTE Agent on the host system. The agent begins using the new sever node after the change is downloaded and configured.

The *High Availability Server* window is the starting point for assigning agents to a GDE Appliance in the HA cluster. Click a GDE Appliance name to display the hosts that are assigned to that server node. The *Edit High Availability Server* window displays all the hosts that are assigned to the current GDE Appliance.

Figure 20: Displaying assigned VTE Agent hosts



Server Name DSMServer1.com
Registered ☑
Last Synchronized 4/30/12 6:53 PM
Primary Role □
Replication Configured ☑
Last Run 4/30/12 6:53 PM

Host Name	HA Server Name
RHELserver.com	DSMServer1.com
LinuxHost.com	DSMServer1.com
HostServer.com	DSMServer1.com
SLESServer.com	DSMServer1.com
HostServer2.com	DSMServer1.com
WindowsHost.com	DSMServer1.com
HostServer3.com	

Click **Add** to open the **Hosts for High Availability Server - serverName** window, where **serverName** is the selected GDE Appliance. The **Hosts for High Availability Server - serverName** window lists all the hosts in the HA configuration and the GDE Appliance to which each is assigned. If a GDE Appliance is not specified, it indicates that the host has not been explicitly assigned to a GDE Appliance and is therefore implicitly assigned to the primary.

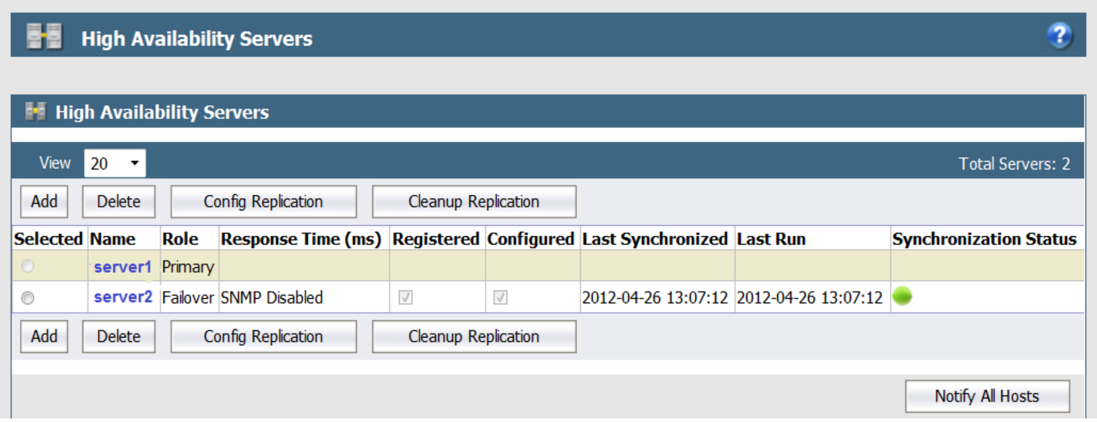
One or more of the displayed hosts can be selected at one time and assigned to the current GDE Appliance.

Assign a host to a GDE Appliance in an HA cluster

1. Log on to the Management Console on the primary node as an administrator of type Security Administrator or All.
2. Enter the domain.
3. Add the host.
4. Select **High Availability** in the menu bar.

   The *High Availability Servers* window opens.

Figure 21: Displaying the HA cluster



High Availability Servers

High Availability Servers

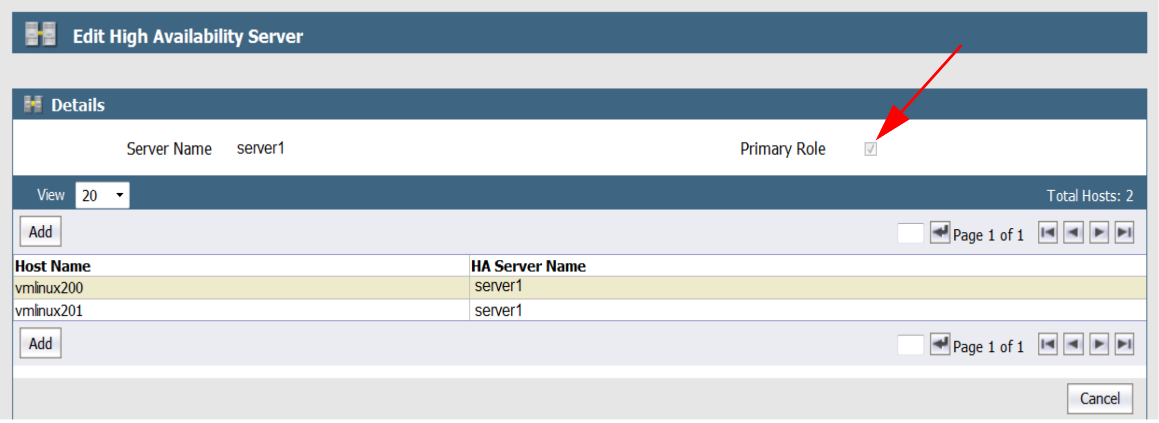
View 20 Total Servers: 2

Selected	Name	Role	Response Time (ms)	Registered	Configured	Last Synchronized	Last Run	Synchronization Status
○	server1	Primary						
○	server2	Failover	SNMP Disabled	☑	☑	2012-04-26 13:07:12	2012-04-26 13:07:12	●

5. Click the GDE Appliance in the **Name** column for which you want to administer the agents on the host.

   The *Edit High Availability Servers* window opens. The hosts already assigned to the current GDE Appliance are listed in the window.

Figure 22: Edit High Availability Server window, primary node indicated



Edit High Availability Server

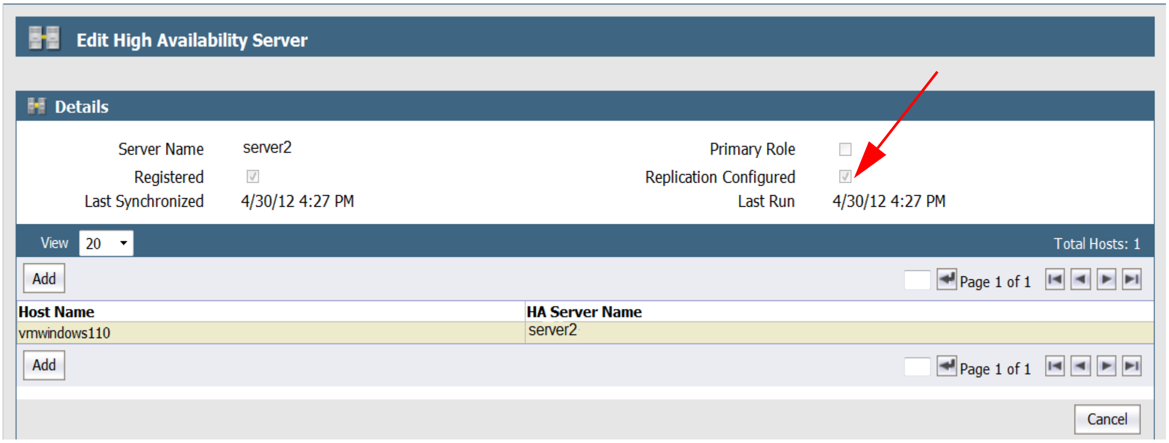
Details

Server Name server1 Primary Role ☑

View 20 Total Hosts: 2

Host Name	HA Server Name
vmlinux200	server1
vmlinux201	server1

Figure 23: Edit High Availability Server window, failover node indicated



Edit High Availability Server

Details

Server Name	server2	Primary Role	☐
Registered	☑	Replication Configured	☑
Last Synchronized	4/30/12 4:27 PM	Last Run	4/30/12 4:27 PM

View 20 Total Hosts: 1

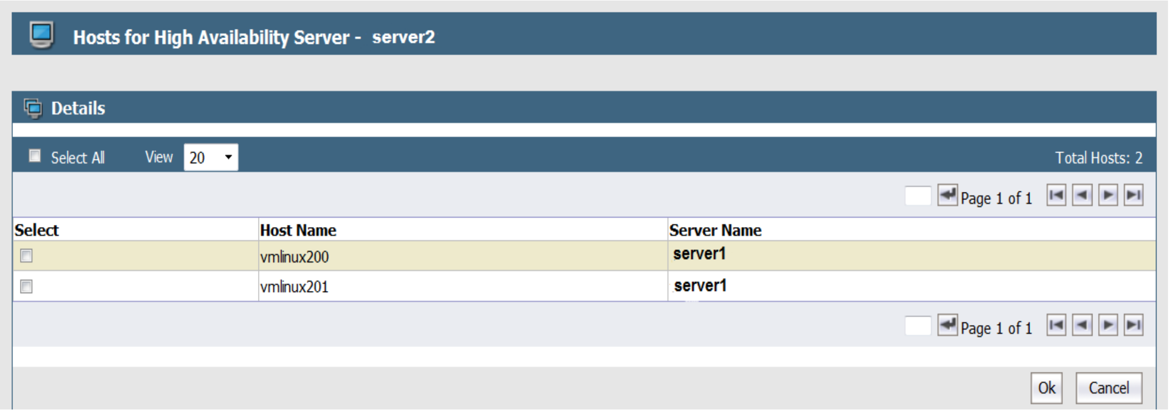
Host Name	HA Server Name
vmwindows110	server2

The *Edit High Availability Server* window for a failover node includes the **Replication Configured** checkbox. This checkbox is enabled by the GDE Appliance when a failover is registered and configured in the HA cluster. This checkbox must be enabled for the **Add** buttons to work. If the checkbox is not enabled, complete the failover registration and configuration process.

6. Click **Add**.

   The *Hosts for High Availability Server* window opens. All the hosts in the HA configuration, except those that are assigned to the current GDE Appliance, are listed.

Figure 24: Displaying hosts for selection and assignment



Hosts for High Availability Server - server2

Details

☐ Select All View 20 Total Hosts: 2

Select	Host Name	Server Name
☐	vmlinux200	server1
☐	vmlinux201	server1

7. Enable the **Select** checkbox of each host that is to be explicitly assigned to current GDE Appliance.

8. Click **Ok**.

The *Edit High Availability Server* window reopens and displays all the hosts that are assigned to the current GDE Appliance, including the host(s) that you just added.

9. (Optional) Once configured in the previous steps, you may test the VTE Agent host-to-GDE Appliance assignment as follows:

a. Wait for the process (configuration change push to the GDE Appliance and then from the GDE Appliance to the host) to complete (this may take between 1 and 15 minutes—depending on the configuration of your network).

b. Access a GuardPoint on the host system.

Do any action on that GuardPoint. The purpose of the action is to generate log messages and determine where the messages are sent.

NOTE: In order to view log messages, the policy applied to the GuardPoint needs to have the Audit role assigned.

c. Start a Management Console session on the GDE Appliance.

d. Open the *Logs* window.

e. Look for log entries from the assigned host system.

If you do not see any log entries for the host, the messages might have been sent to the original GDE Appliance or maybe the host system was assigned to the wrong GDE Appliance.

Since the failover is now the first GDE Appliance that the agent tries to communicate with, and the failover pushes configuration updates to the host, all agent activity is now logged on the failover. If log entries for the host do not appear in the *Logs* window for your GDE Appliance, check the host assignment. The log data may be going to a different GDE Appliance.

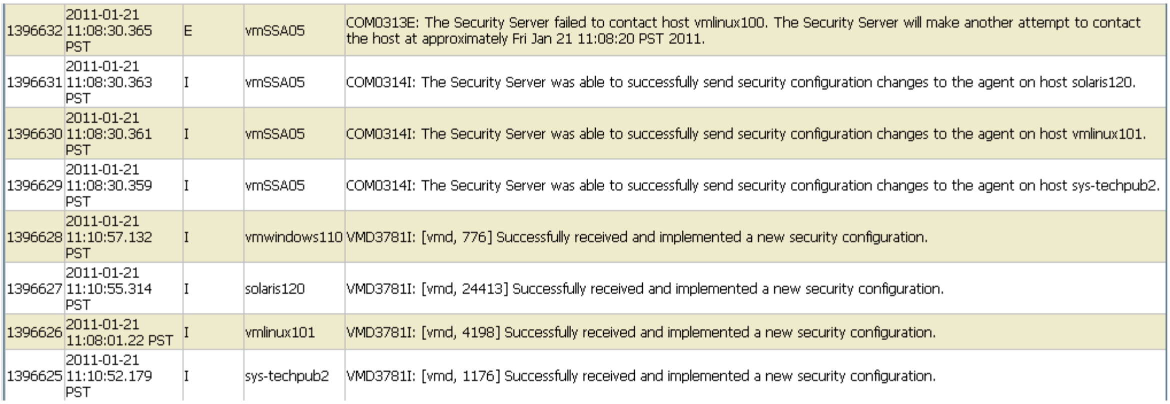
f. (Optional) Now that you know that the failover is servicing the host correctly, configure a Syslog server to consolidate all the log entries of all the GDE Appliance in one place.

Pushing Configuration Changes to Hosts

Once a host is assigned to a failover, instead of pushing changes directly from the primary node to the host, changes are pushed from the primary to the failover and then from the failover to the host. As long as there are reliable connections between the primary and failover, and failover and host, update pushes occur reliably. If a failover goes down unexpectedly, the assigned hosts might be temporarily orphaned. One workaround is to restart vmd on the host system. Another is to push the changes from the primary GDE Appliance.

The **Notify All Hosts** button in the *High Availability Servers* window pushes the latest host configurations directly from the primary GDE Appliance to every host in the HA cluster, regardless of whether the hosts are assigned to failover or not. This is a convenient way to push the latest host configuration changes to every host, including orphan hosts. Depending on the number of hosts in the HA cluster and network performance, this can take between a few minutes to a few hours (about 30 minutes for 5000 hosts). Check the push status in the *Logs* window. Messages are placed in the log at intervals to indicate the percentage of completion.

Figure 25: Example log entries for Notify All Hosts



1396632	2011-01-21 11:08:30.365 PST	E	vmSSA05	COM0313E: The Security Server failed to contact host vmlinux100. The Security Server will make another attempt to contact the host at approximately Fri Jan 21 11:08:20 PST 2011.
1396631	2011-01-21 11:08:30.363 PST	I	vmSSA05	COM0314I: The Security Server was able to successfully send security configuration changes to the agent on host solaris120.
1396630	2011-01-21 11:08:30.361 PST	I	vmSSA05	COM0314I: The Security Server was able to successfully send security configuration changes to the agent on host vmlinux101.
1396629	2011-01-21 11:08:30.359 PST	I	vmSSA05	COM0314I: The Security Server was able to successfully send security configuration changes to the agent on host sys-techpub2.
1396628	2011-01-21 11:10:57.132 PST	I	vmwindows110	VMD3781I: [vmd, 776] Successfully received and implemented a new security configuration.
1396627	2011-01-21 11:10:55.314 PST	I	solaris120	VMD3781I: [vmd, 24413] Successfully received and implemented a new security configuration.
1396626	2011-01-21 11:08:01.22 PST	I	vmlinux101	VMD3781I: [vmd, 4198] Successfully received and implemented a new security configuration.
1396625	2011-01-21 11:10:52.179 PST	I	sys-techpub2	VMD3781I: [vmd, 1176] Successfully received and implemented a new security configuration.

NOTE: Do not click **Notify All Hosts** more than once. Each time you click this button you spawn a new process and each new process slows the GDE Appliance.

Reassigning Hosts to Another Node in the HA Cluster

Hosts are implicitly assigned to the primary GDE Appliance once they are registered with that GDE Appliance. If you assign a host to a GDE Appliance, that host remains assigned to that GDE Appliance until it is acquired by another GDE Appliance or the host record is deleted. There is no delete button for removing host-to-GDE Appliance assignments and you cannot return the host to an implicitly assigned status.

Hosts are reassigned by clicking the name of the desired GDE Appliance in the *High Availability Servers* window and selecting the hosts. This is the same process whether assigning a host for the first time or reassigning it to another GDE Appliance.

Displaying High Availability Configuration Status

The primary server in an HA configuration automatically updates the failover nodes at set intervals. This ensures that the failovers possess the same keys, policies, and host configurations as the primary server node.

The Management Console on the primary is used to configure the failover nodes to be administered by that primary. Failovers are identified by their host name or FQDN. Failovers register with the primary and the Management Console displays the registration status of the configured failover node. The Management Console is also used for administrative tasks such as synchronizing the GDE Appliance, unregistering the GDE Appliance, and assigning the agents running on a host to a GDE Appliance. Additional HA configuration is done via the CLI.

Display HA configuration status

1. Log on to the Management Console on the primary as an administrator of type System Administrator or type All.
2. Select **High Availability** in the menu bar.

   The *High Availability Servers* window opens. It displays the primary and, if configured, the failover. The current GDE Appliance is always the primary GDE Appliance. If it is not, you are running the Management Console on a failover. You cannot make configuration changes on a failover node.

Table 8: High Availability Servers window fields information

Column Header	Description
Selected	Enable this check box to select a failover node. The next operation, such as delete and synchronize, is applied to the selected failover node.
Name	The network name of the appliance or system that is running the primary or failover node.
Role	The role of the GDE Appliance: either `Primary` or `Failover`.
Response Time (ms)	If SNMP is enabled, the primary polls each failover using an SNMP GET request at five-minute intervals. The response time for each failover is displayed in milliseconds. If SNMP is disabled, the Response Time column will display "`SNMP Disabled`". If the failover is not reachable, the Response Time column will display "`Not Reachable`".
Registered	Registration status. This checkbox becomes enabled after the failover successfully exchanges certificates with the primary. When enabled, the failover node can be configured for database replication and operation as a failover. Registration is initiated when the CLI `gencert` command is executed on the failover.

Column Header	Description
Configured	Configuration status. This checkbox is enabled after the failover node is configured for database replication and operation as a failover. Configuration is initiated by clicking **Config Replication**. Upon completion, this checkbox is enabled. The checkbox for the primary is always disabled. **Configured** check boxes are displayed on the primary only. Failover nodes must be configured and their **Configured** check boxes enabled before you can assign hosts to them.
Last Synchronized	The last time the failover successfully synchronized with the primary. Synchronization occurs at one-minute intervals automatically. Time is expressed in the form: *YYYY-MM-DD HH:MM:SS*, where *Y*=year, *M*=month, *D*=day, *H*=hour, *M*=minute, and *S*=second. For example, `2010-08-09 10:31:28`. **Last Synchronized** time is displayed on the primary only.
Last Run	The last time an attempt was made to synchronize the failover server with the primary. Time is expressed in the form: *YYYY-MM-DD HH:MM:SS.mm*, where *Y*=year, *M*=month, *D*=day, *H*=hour, *M*=minute, *S*=second, and *m*=millisecond. For example, `2010-08-09 10:31:28.838`. **Last Run** time is displayed on the primary only.
Synchronization Status	A green circle indicates that the last attempt to synchronize with the failover completed successfully. A red square indicates that the last attempt to synchronize with the failover failed. A yellow triangle indicates that the GDE Appliance is in the process of synchronizing with the failover, it turns to green if successful or red if it fails. Click the green ball or red square to display additional status information. Synchronization Status is displayed only on the primary. **Synchronization Status** icons are displayed on the primary only.

The buttons on the *High Availability Servers* window are:

- **Add**: Opens the *Add Server* window in which to the host name or FQDN of the GDE Appliance to be configured as a failover. Multiple failover nodes can be added.
- **Delete**: Removes the selected failover from the primary server node. GDE Appliance software remains intact on the deleted failover.
- **Config Replication**: Configures and runs replication on the selected and registered failover. Upon successful completion, the **Configured** checkbox for the failover is enabled, the failover operates as a failover, and can be accessed by the VTE agents to evaluate policies and dispense keys.
- **Cleanup Replication**: Removes the replication configuration and authentication credentials of the selected failover from the primary server node.
- **Notify All Hosts**: pushes the latest host configurations directly from the primary to every host in the HA cluster, whether the hosts are assigned to a failover or not. This is a convenient way to update orphan hosts. Depending on the number of hosts in the HA cluster and network performance, this can take between a few seconds to an hour (about 30 minutes for 5000 hosts).

If policy changes are not being applied to the hosts that are assigned to a failover, check the **High Availability** window.

- A green circle should be displayed for the failover in the **Synchronization Status** column.
- A red rectangle in the **Synchronization Status** column indicates that an error has occurred.
- The **Last Synchronized** column indicates the time and day of the last successful synchronization. The **Last Run** column indicates the time and day of the last attempt of the primary to synchronize with the failover.
- A message such as the following is entered in the **Logs** window when the primary is unable to synchronize with the failover.

  ```
  COM0628E: Primary Server failed to replicate configuration data to
  failover server "vmSSA06".
  ```
- Check the network connection between the two GDE Appliances and check that the software is running (for instance, open a Web browser to the failover). When a host is assigned to a failover, policy configuration changes are pushed from the primary, to the assigned failover, and then to the host. If the failover is going to be down for an extended period, reassign the hosts to another server. You can also click **Notify All Hosts** to push policy changes to all the hosts assigned to the GDE Appliance, regardless of which GDE Appliance they are assigned.

Recovering from incomplete synchronization of primary and failover nodes after replication

If the primary and failover server nodes do not synchronize completely after replication, do the following to re-initialize the failover node:

Run the CLI `config reset` command or run the CLI `convert2primary` and `convert2failover` commands. The `convert2failover` command wipes the existing database and restores it with a pristine copy of the primary GDE Appliance. Another option is to delete the failover installation and re-install it from scratch.

Afterwards, reconfigure replication on the failover.

See “config” on page 387 in the “Maintenance Category Commands” on page 386 for more information about using these commands.

Configuring SNMP

8

Simple Network Management Protocol (SNMP) is a full-featured protocol that is used to manage and monitor network nodes like hosts, routers, and appliances. The specific attributes of network nodes that can be managed and monitored by SNMP are configured as objects in a Management Information Base (MIB). The GDE Appliance can be enabled as an SNMP agent and then monitored by SNMP servers using the set of MIB objects described below.

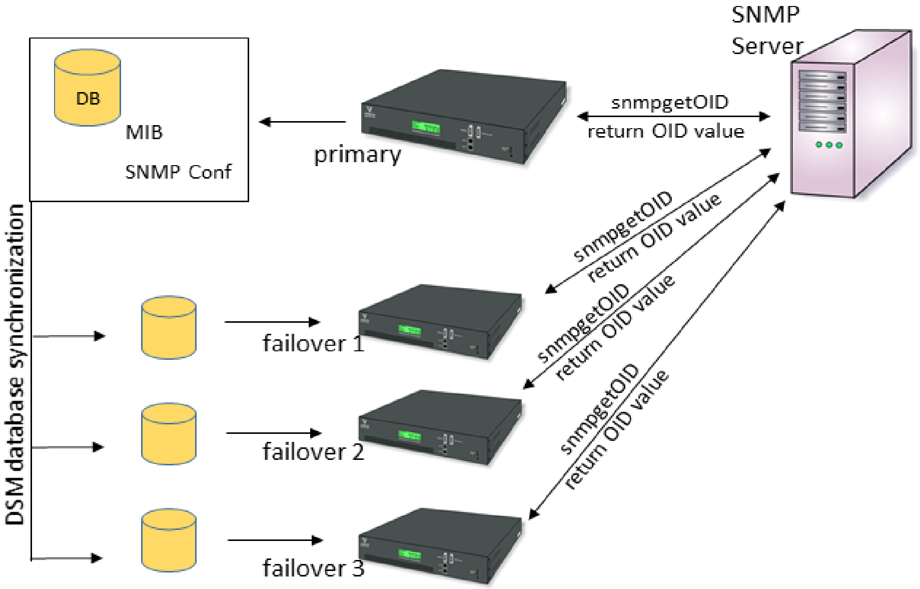
This chapter contains the following sections:

- "Overview"
- "Enabling SNMP on the GDE Appliance"
- "Changing OID Values"
- "Displaying Vormetric-specific SNMP Information"
- "Example SNMP Queries"

Overview

The GDE Appliance supports SNMP version 1 or 2. SNMP is not used to manage GDE Appliances. A small set of MIB objects are provided with which to query GDE Appliance configuration and status information. The primary GDE Appliance database is replicated to the failover GDE Appliances in an HA cluster, distributing the same SNMP configuration to all the failovers. Therefore, SNMP servers that can query the primary GDE Appliance can also query each failover GDE Appliance with the same community string.

Figure 26: SMNP configuration is replicated across failover GDE Appliances



When the GDE Appliance receives an SNMP GET request from an SNMP server, the GDE Appliance locates the Object IDentifier (OID) entry in the MIB and returns its value to the SNMP server.

If SNMP is enabled on the primary GDE Appliance, the primary GDE Appliance polls itself and each failover GDE Appliance using an SNMP GET request at five-minute intervals. The response time for each failover GDE Appliance is displayed in the High Availability Servers window in milliseconds. If SNMP is disabled, the Response Time column will display "SNMP Disabled". If the failover GDE Appliance is not reachable, the Response Time column will display "Not Reachable".

SNMP traps are not supported at this time and cannot be configured on the GDE Appliance.

Enabling SNMP on the GDE Appliance

SNMP is enabled via the **System > SNMP** page on the *Configuration* tab. You can define the SNMP community string with which to query the GDE Appliance.

If the SNMP Access Control List (ACL) is empty, SNMP requests from any IP address will be acknowledged. If the SNMP ACL is defined to allow only certain IP addresses (for example, 10.1.2.3) or IP address blocks (for example, 10.1.2.*) to go through, the GDE Appliance will only acknowledge requests from IP addresses specified in the SNMP ACL. The community string and IP address are the only credentials used to verify the legitimacy of the SNMP request. The community string is typically set to a factory default, value of “public”. This string must be the same for all devices in the same group for SNMP monitoring to function. For security reasons, the Network Administrator should change the community string from “public” to a custom value.

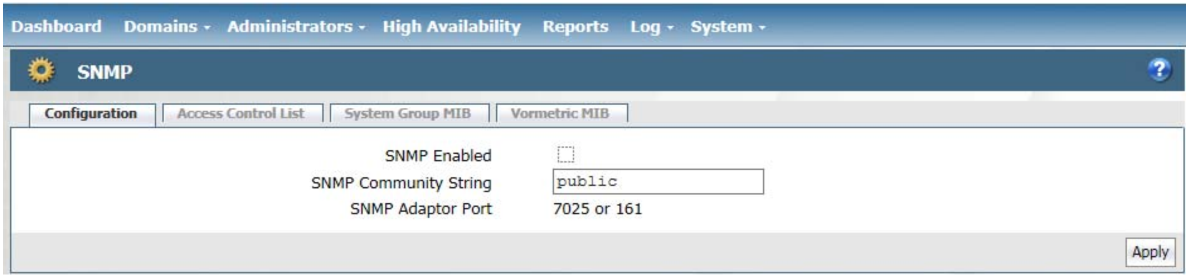
NOTE: We recommend that you do not enable SNMP on the GDE Appliance unless it is required, as this could pose a security risk. If you do enable SNMP on the GDE Appliance, we recommend that you use an SNMP ACL to restrict access to this service, and change the default community string from ‘public’ to a custom value.

The failover GDE Appliances in an HA cluster share the same SNMP configuration as the primary GDE Appliance. Enable SNMP listening on the primary GDE Appliance and SNMP listening is enabled on all the failover GDE Appliances. The community string that you enter is applied to the primary GDE Appliance and all the failover GDE Appliances in the HA cluster. This means that an SNMP server that is allowed to query the primary GDE Appliance can also query all the failover GDE Appliances in the HA cluster.

NOTE: If the failover GDE Appliances in an HA configuration do not respond to SNMP requests, restart the failover GDE Appliances to resolve the issue.

GET requests can be sent to port 161 or port 7025.

Figure 27: SNMP Configuration



SNMP Enabled □
SNMP Community String public
SNMP Adaptor Port 7025 or 161

To enable the GDE Appliance to listen for SNMP queries and to configure the SNMP community string:

1. Log on as an administrator of type System Administrator or All.
2. Do not enter a domain.
3. Select **System->SNMP**.
4. The SNMP window opens to the **Configuration** tab.

5. Check **SNMP Enabled** to make the GDE Appliance listen for SNMP queries.
6. Enter the community string, or password, with which all SNMP servers will query the GDE Appliance in the **SNMP Community String** field.
7. Click **Apply**.

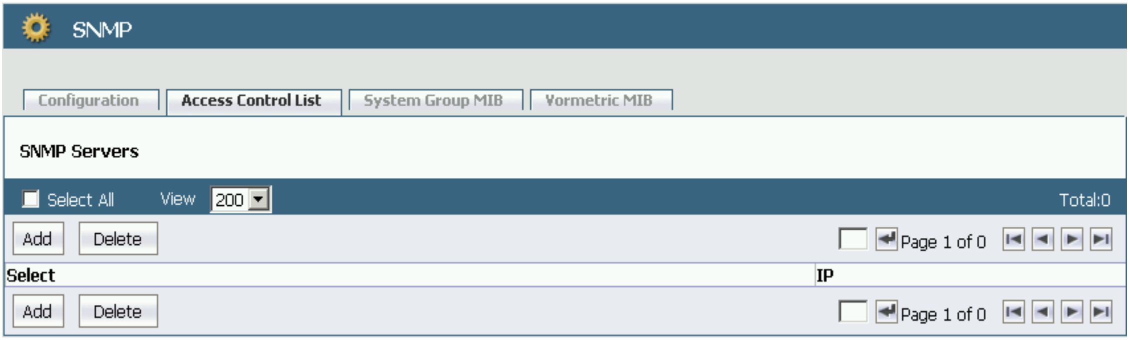
NOTE: Once SNMP is enabled, the GDE Appliance will respond to requests from any SNMP server unless a preferred SNMP server is specified in the Access Control List. Once the IP address of a SNMP Server is specified in the Access Control List, the GDE Appliance will only respond to that SNMP Server.

Adding SNMP Servers

Configure the SNMP servers that are allowed to query the GDE Appliance in the SNMP window, Access Control List tab.

SNMP servers can access the GDE Appliance using TCP or UDP.

Figure 28: SNMP Servers, Access Control List



To add a system to the list of SNMP servers that may submit SNMP queries to a GDE Appliance:

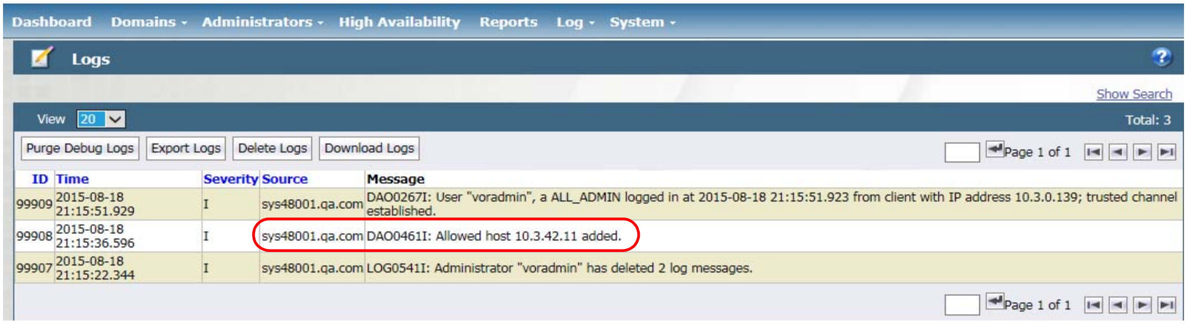
3. Click **Add**, the Add SNMP Server window opens.
4. Enter the IP address of the SMNP server to be granted access in the **IP Address** field.

   Host names and Fully Qualified Domain Names (FQDN) are not supported at this time.
5. Click **Ok**.

NOTE: The IP Address field currently supports the use of a “wild-card” in the 4th octet. For example: 10.1.2.*

Once an SNMP server has been added to the list of allowed servers, a corresponding log entry is created indicating an SNMP server has been added to the ACL.

Figure 29: Log entry indicating an SNMP server has been added to the ACL



ID	Time	Severity	Source	Message
99909	2015-08-18 21:15:51.929	I	sys48001.qa.com	DAO0267I: User "voradmin", a ALL_ADMIN logged in at 2015-08-18 21:15:51.923 from client with IP address 10.3.0.139; trusted channel established.
99908	2015-08-18 21:15:36.596	I	sys48001.qa.com	DAO0461I: Allowed host 10.3.42.11 added.
99907	2015-08-18 21:15:22.344	I	sys48001.qa.com	LOG0541I: Administrator "voradmin" has deleted 2 log messages.

There is no record of a failed status query in the Logs window; however, a record is entered in the server.log file. For example,

```
2011-09-23 17:41:13,267 ERROR [STDERR] Sep 23, 2011 5:41:13 PM
org.snmp4j.log.JavaLogAdapter log

WARNING: 10.3.244.200 not in ACL
```

The log entry indicates that an SNMP query was attempted from a system that is not configured in the Access Control List (ACL). Such a query is ignored by the GDE Appliance and, after the timeout interval has elapsed, the SNMP query is terminated and timeout message is returned. For example,

```
  # snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.2.1.1.4.0

Timeout: No Response from 10.3.48.1:7025

#
```

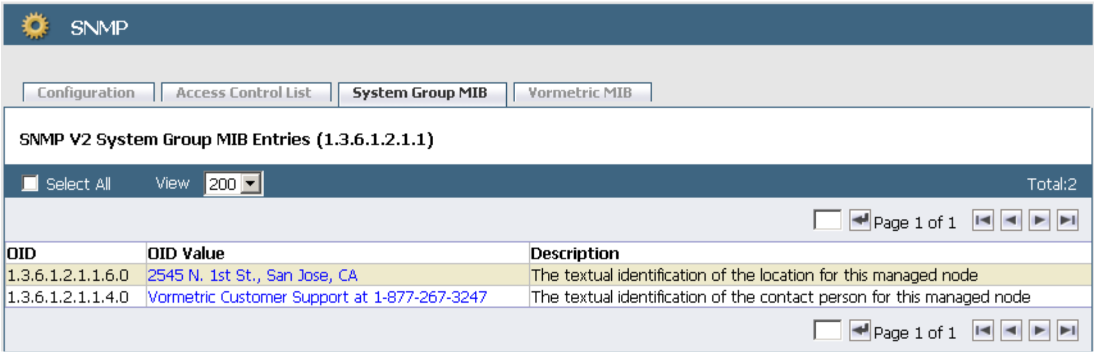
The following example from the server.log file indicates that an SNMP query had been submitted from a configured system. It indicates only that the system submitting the query is configured. It is no indication of the success or failure of the SNMP query itself; only that the SNMP server is allowed to query the GDE Appliance.

```
2011-09-23 17:41:49,964 ERROR [STDERR] Sep 23, 2011 5:41:49 PM
org.snmp4j.log.JavaLogAdapter log

WARNING: 10.3.244.200 passed ACL
```

Changing OID Values

The SNMP Object IDentifier (OID) values that can be changed are sysContact (1.3.6.1.2.1.1.4.0) and sysLocation (1.3.6.1.2.1.1.6.0). Customize the OID values so that the information collected by the SNMP server can include the contact for GDE Appliance questions and issues, plus the physical location of the GDE Appliance. These OIDs are part of the 1.3.6.1.2.1.1 MIB group defined in RFC 1213.

Figure 30: Customized contact and location information



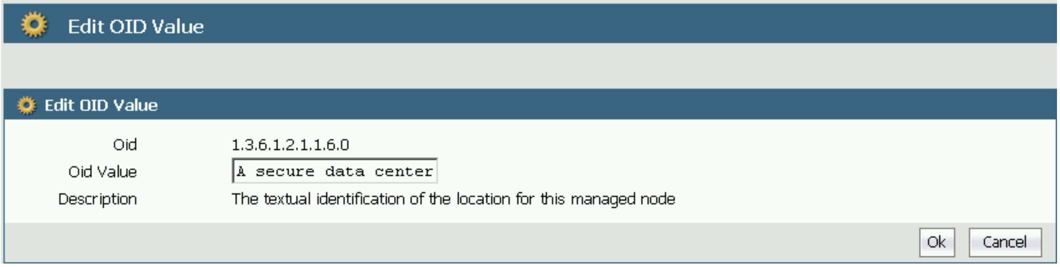
SNMP V2 System Group MIB Entries (1.3.6.1.2.1.1)

OID	OID Value	Description
1.3.6.1.2.1.1.6.0	2545 N. 1st St., San Jose, CA	The textual identification of the location for this managed node
1.3.6.1.2.1.1.4.0	Vormetric Customer Support at 1-877-267-3247	The textual identification of the contact person for this managed node

To configure the GDE Appliance contact and location information:

1. Open the System Group MIB tab.
2. Click a string in the **OID Value** column.
3. The **Edit OID Value** window opens.

Figure 31: Editing the OID value



Oid 1.3.6.1.2.1.1.6.0
Oid Value A secure data center
Description The textual identification of the location for this managed node

4. Select and delete the text string in the **OID Value** field.
5. Enter a new string in the **OID Value** field.
6. Click **Ok**.

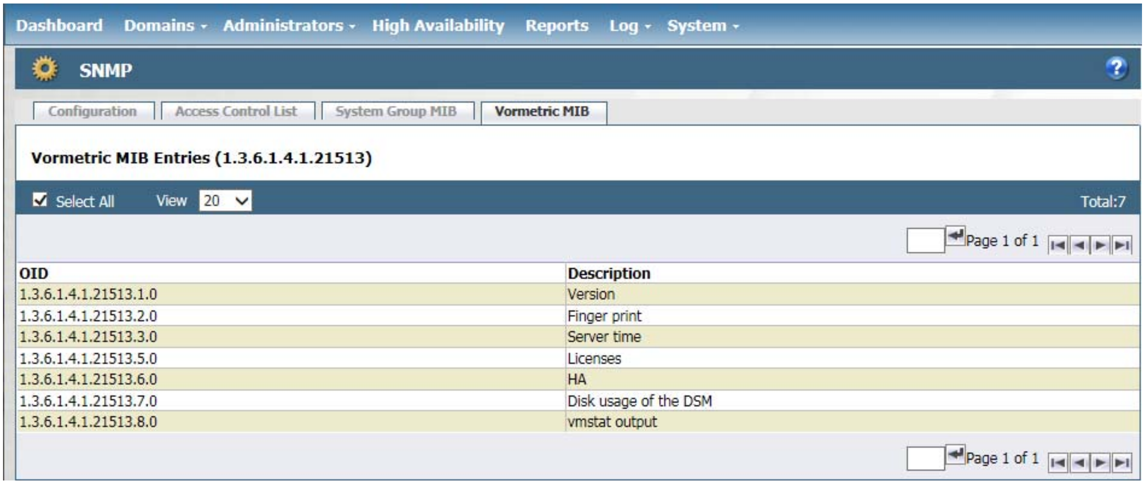
The text in the **Description** column is hard-coded and cannot be changed.

A log entry indicating the OID number and value change is entered in the *Logs* window.

Displaying Vormetric-specific SNMP Information

The Vormetric MIB tab displays the Vormetric-specific OIDs that can be queried by an SNMP server. The OIDs cannot be manually changed. The OID values are dynamic and change based upon the GDE Appliance state and configuration.

Figure 32: Vormetric-specific OIDs



Vormetric MIB Entries (1.3.6.1.4.1.21513)

OID	Description
1.3.6.1.4.1.21513.1.0	Version
1.3.6.1.4.1.21513.2.0	Finger print
1.3.6.1.4.1.21513.3.0	Server time
1.3.6.1.4.1.21513.5.0	Licenses
1.3.6.1.4.1.21513.6.0	HA
1.3.6.1.4.1.21513.7.0	Disk usage of the DSM
1.3.6.1.4.1.21513.8.0	vmstat output

The OIDs in the Vormetric group MIB begin with 1.3.6.1.4.1.21513. The following table lists the Vormetric OIDs and their purpose.

Table 9: OID Descriptions

OID	SNMP Object Type	Description
1.3.6.1.2.1.1.4.0	sysContact	The textual identification of the contact person for this managed node, together with information on how to contact this person. If no contact information is known, the value is a zero-length string. Max. length 256 characters.
1.3.6.1.2.1.1.6.0	sysLocation	The physical location of this node (e.g., 'telephone closet, 3rd floor'). If the location is unknown, the value is a zero-length string. Max. length 256 characters.
1.3.6.1.4.1.21513.2.0		Returns the fingerprint of the current GDE Appliance deployment. The fingerprint is also displayed in the Management Console *Dashboard* window.

OID	SNMP Object Type	Description
1.3.6.1.4.1.21513.3.0		Returns the time and date on the GDE Appliance at the time of the SNMP query.
1.3.6.1.4.1.21513.5.0		Returns the agent type (FS, or Key agent), the license installation state (true or false) of each agent type, and, for each installed license, the license expiration date. This information is also displayed in the Management Console *License* window.
1.3.6.1.4.1.21513.6.0		Returns the name of each node in a GDE Appliance HA cluster configuration.
1.3.6.1.4.1.21513.7.0		Returns disk usage information for each file system mounted on the GDE Appliance. This is the equivalent of running `df -hk -B 1024K` on the GDE Appliance command line.
1.3.6.1.4.1.21513.8.0		Returns GDE Appliance process, memory, paging, I/O, and CPU usage information. This is the equivalent of running vmstat on the GDE Appliance command line.

Example SNMP Queries

The following SNMP queries were made on Red Hat Enterprise Linux Server, release 6.0, using SNMPv2.

To display GDE Appliance contact information:

```
  # snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.2.1.1.4.0

SNMPv2-MIB::sysContact.0 = STRING: Vormetric Customer Support at 1-877-
267-3247

#
```

To display the physical location of the GDE Appliance:

```
  # snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.2.1.1.6.0

SNMPv2-MIB::sysLocation.0 = STRING: 2545 N. 1st St., San Jose, CA

#
```

To display the GDE Appliance version number:

```
  # snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.1.0

SNMPv2-SMI::enterprises.21513.1.0 = STRING: "5.3.0.1616"

#
```

To display the GDE Appliance fingerprint:

```
  # snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.2.0

SNMPv2-SMI::enterprises.21513.2.0 = STRING:
"D2:48:EF:E4:A2:B0:59:8C:5F:DB:9D:3B:30:41:0B:EE:BD:07:8D:67"

#
```

To display the current date and time on the GDE Appliance:

```
  # snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.3.0

SNMPv2-SMI::enterprises.21513.3.0 = STRING: "2015-08-18 20:56:53.135 PDT"

#
```

To display the GDE Appliance license configuration:

```
  # snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.5.0

SNMPv2-SMI::enterprises.21513.5.0 = STRING: "FS max # of agents: 30000;
Expires: Dec-31-2015; Key max # of agents: 30000; Expires: Dec-31-2015; FS
max # of agents: 30000; ; Key max # of agents: 30000; FS max # of agents:
30000; Max hours: 1000000; Key max # of agents: 30000; Max hours: 1000000;
Multi-domain enabled: true; max # of domains: 20000; Issued to: DSM522-
Performance-2015-12-31"

#
```

To display the GDE Appliance HA configuration:

```
  # snmpget -c public -v 2c 10.3.48.239:7025 1.3.6.1.4.1.21513.6.0

SNMPv2-SMI::enterprises.21513.6.0 = STRING: "Failover: sys15123.com;
Primary: sys48239.com; "

#
```

To display the mounted file systems and their disk usage:

```
  # snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.7.0

SNMPv2-SMI::enterprises.21513.7.0 = STRING: "

Filesystem           1M-blocks  Used Available Use% Mounted on

/dev/mapper/vg_sys48001-lv_root

                         50269  3006     44703   7% /

tmpfs                     1917     1      1917   1% /dev/shm

/dev/sda1                  477    38       414   9% /boot
```

```
/dev/mapper/vg_sys48001-lv_home
                         45867 15185     28346  35% /home
"#
```

To display GDE Appliance system usage information:

```
  # snmpget -c public -v 2c 10.3.48.1:7025 1.3.6.1.4.1.21513.8.0

SNMPv2-SMI::enterprises.21513.8.0 = STRING: "
procs -----------memory---------- ---swap-- -----io---- --system-- -----cpu-----
 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs us sy id wa st
 0  0  51040 130248 228572 1777640    0    0     1    12   11    4  0  0 100  0  0
"
#
```

9

Configuring Syslog Servers for System-Level Messages

This section describes how to add a remote Syslog server to your system, and how to control the severity level and format of the messages that the GDE Appliance sends to the Syslog server.

You can configure a Syslog server to receive the same messages that are sent to the Logs window of the Management Console. Use the **System> Log Preferences** menu to create templates that apply to logging configurations for all of the Agents.

This chapter contains the following sections:

- “Overview”
- “Supported Syslog Formats”
- “Adding a Syslog Server”
- “Using Syslog to Troubleshoot the GDE Appliance and Agents”
- “VTE Agent Log Files”
- “GDE Appliance Log Files”
- “Pruning the GDE Appliance Logs”
- “Exporting Logs”
- “Adding an Email Notification Group”

Overview

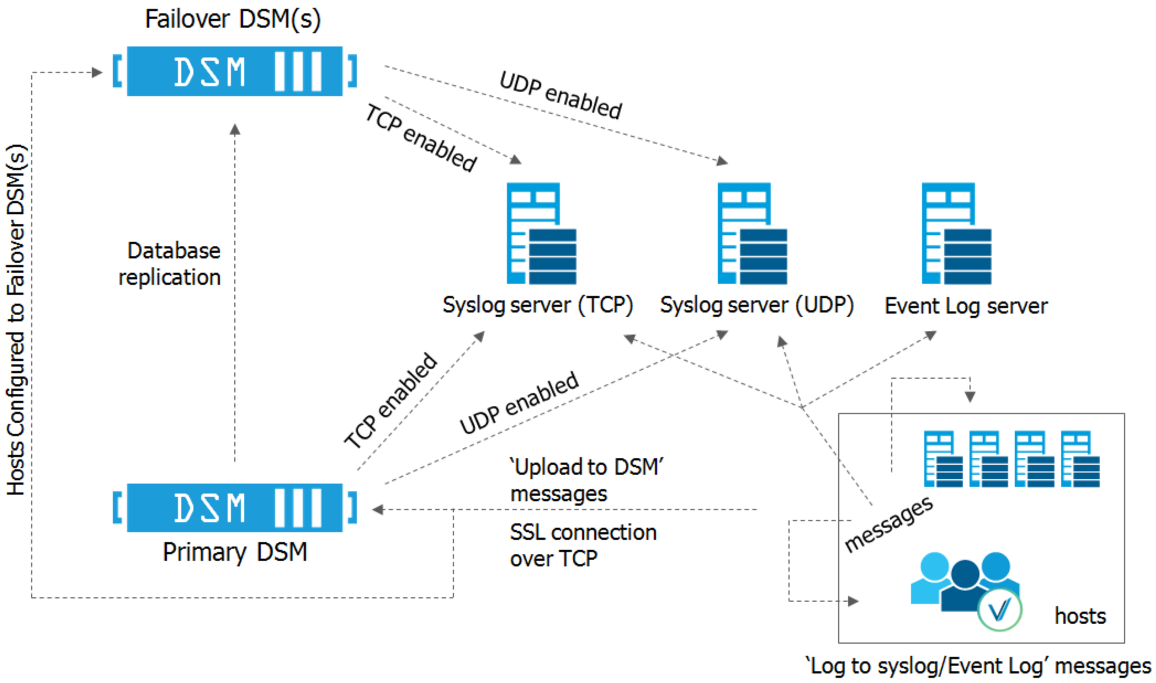
Agent log data is generated on agent hosts. The log data is placed in `/var/log/vormetric` on a UNIX system or in `C:\Documents` or `Settings\All Users\Application Data\Vormetric\DataSecurityExpert\agent\log` on a Windows system, when the **Log to File** logging preference is enabled. The log data can also be forwarded to a Syslog or Event Log server when the **Log to Syslog/Event Log** logging preference is enabled.

NOTE: Ensure that the `/var` directory in your system has 256KB to 1MB available for logging to ensure proper GDE Appliance logging behavior.

When **Log to Syslog/Event Log** is enabled, log data is placed into a local `/var/log/messages` or `/var/adm/messages` file, or into the local Windows Event Log. The host administrator can choose to configure the agent to forward log data to a remote Syslog server or Event Log server. The host administrator can upload the log data to a remote server with whichever transport protocol is preferred. The GDE Appliance is not used to configure the remote log servers for host systems.

The **Syslog Server** window in the Management Console lets you configure the remote Syslog servers to which to send GDE Appliance log data. The log data sent to remote Syslog servers consists of log data that is generated on the GDE Appliance and, when **Upload to Server** is enabled in the **Log Preferences** window, log data that is generated on hosts. The administrator then configures the GDE Appliance to forward log data to a Syslog server using either UDP protocol or TCP protocol.

Figure 33: Handling log messages



Items to consider before configuring Syslog logging include:

- Only administrators of type System Administrator or All (when not in a domain) can enable Syslog messaging.
- Only administrators of type System Administrator, Domain Administrator, or All (when in a domain) can configure Syslog messaging.

- If Syslog servers are configured in a domain, only events that take place in that domain are logged to the Syslog servers.
- If Syslog servers are configured outside of a domain, only events that take place at the system level are logged to the Syslog servers.
- A default Syslog port number is not provided. The usual industry standard port number for Syslog over UDP is 514. Port 1468 has been used successfully for TCP.
- Configuring a Syslog server is an effective way to consolidate the logs of all the GDE Appliances in an HA configuration in one central repository. The failover GDE Appliances in an HA cluster deployment have the same configuration as the primary server node. The failovers forward log data to the same Syslog server(s) as the primary. Therefore, each failover must have network access to the Syslog servers configured on the primary.

Supported Syslog Formats

The GDE Appliance supports the following log formats:

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

Plain Message

Originally, GDE Appliance Syslog support included only Plain Message format. While simple and efficient, this format did not allow for user enhanced reporting or customization.

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

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

Table 10: Syslog message parameters and descriptions

Parameter	Description
12-07-201216:53:02	Date and time
Local7.Debug	Message priority
10.3.32.231	Sending machine’s IP address

Parameter	Description
2012-12-08 01:01:58.709	Date and time of logged event
vormetric	Originator tag
SOURCE[linux64-32231.qa.com]	Source of message
DAO0445I	Unique message ID
Administrator voradmin added SysLog Host 10.3.25.168	Plain text message of the logged event

Common Event Format (CEF) log format

The GDE Appliance Syslog supports Common Event Format (CEF) log format. The CEF format is specified in the Arcsight "Common Event Format" standard.

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

```
<27> 2012-10-16T16:01:44.030Z centos-6-0 CEF:0|Vormetric, Inc.|vee-
fs|5.1.0.9026|CGP2604E| Reject access|7|logger=CGP spid=6362 cat=[ALARM]
pol=AuditAllExceptLp uinfo=lp,uid\=4,gid\=7\\lp\\ sproc=/bin/ls
act=read_dir_attr gp=/Guard filePath=/datafiles/file.dat denyStr=DENIED
showStr= Code (1M)
```

Table 11: CEF Log Format parameters and descriptions

Parameter	Description
<27>	A standard syslog facility/priority code
2012-10-16T16:01:44.030Z	Date and time
centos-6-0	The host name of the machine sending the message.
CEF:0	Version of the CEF
Vormetric, Inc.	Sending device vendor
vee-fs	Sending device product
5.1.0.9026	Sending device version
CGP2604E	Unique message ID
Reject access	Name: A human-readable and understandable description of the event.
7	Severity: An integer that reflects the importance of the event. Only numbers from 0 to 10 are allowed, where 10 indicates the most important event.

Parameter	Description
`logger=CGP spid=6362 cat=[ALARM] pol=AuditAllExceptLp uinfo=lp,uid\=4,gid\=7\\lp\\ sproc=/bin/ls act=read_dir_attr gp=/Guard filePath=/datafiles/file.dat denyStr=DENIED showStr= Code (1M)`	Extension: A collection of key-value pairs. The keys are part of a predefined set. The standard allows for including additional keys. An event can contain any number of key-value pairs in any order, separated by delimiting characters.

RFC5424

The GDE Appliance Syslog support includes the RFC5424 log format.

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

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

Table 12: CEF Log Format parameters and descriptions

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

Log Event Extended Format (LEEF)

The GDE Appliance Syslog support includes Log Event Extended Format (LEEF). The LEEF header is pipe (“|”) separated and attributes are tab separated.

Adding a Syslog Server

To add a syslog server:

1. Verify that one or more Syslog servers are accessible from the GDE Appliance. It is usually enough to ping the Syslog server and run ps to check the Syslog process on the Syslog server system.

   If you are going to send the messages to the local host, verify that the syslogd process on the local host is accepting messages. You may need to restart syslogd with the “-r” argument.

   NOTE: Record the Syslog transport protocols and port numbers of the Syslog server(s). You will need this information later.

2. Set the severity level at which to send messages to the Syslog server in the `/etc/syslog.conf` file on the agent host.

   Severity levels in the *Log Preferences* window are DEBUG, INFO, WARN, ERROR, and FATAL. Severity levels are cumulative, so each level includes the levels below it. For example, FATAL logs only FATAL messages, whereas WARN logs WARN, ERROR, and FATAL messages. To ensure that the syslog server gets the messages set in the *Log Preferences* window, set the level in the syslog.conf file to debug and direct the output to the local messages file. For example, on a Solaris system, set the output file path to /var/adm/messages.

   ```
   user.debug /var/adm/messages
   ```

3. Log on to the Management Console as an administrator of type System Administrator or All.

4. Select **System > General Preferences**. The **General Preferences** window opens to the **General** tab.

5. Click the **System** tab, and then select **Syslog Enabled**.

   This enables communication between the GDE Appliance and the Syslog server.

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

6. Click **Apply**.

7. Select **System > Log Preferences**. The *Log Preferences* window opens to the *Server* tab.
8. Set the **Logging Level** property.

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

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

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

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

    In the interests of security, we recommend that you use a root certificate rather than a non-root certificate.

NOTE: For syslog servers configured with the UDP transport protocol, ensure that UDP packets are not blocked by a firewall or switch rules. Also, verify that the Syslog server is logging messages as expected.
If you add a Syslog certificate when using TLS protocol, you may need to restart the server. To this you need to do a `system > server restart` from the CLI. After restart, verify that the Syslog server is logging messages as expected.

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

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

You may configure multiple Syslog servers per GDE Appliance however, each Syslog server must have a unique hostname or IP address.

12. Click **Ok**.

13. Do a task on an agent system that normally generates a Syslog entry, such as accessing a GuardPoint.
14. Check the `/var/log/messages` file on the Syslog server for GDE Appliance log entries.

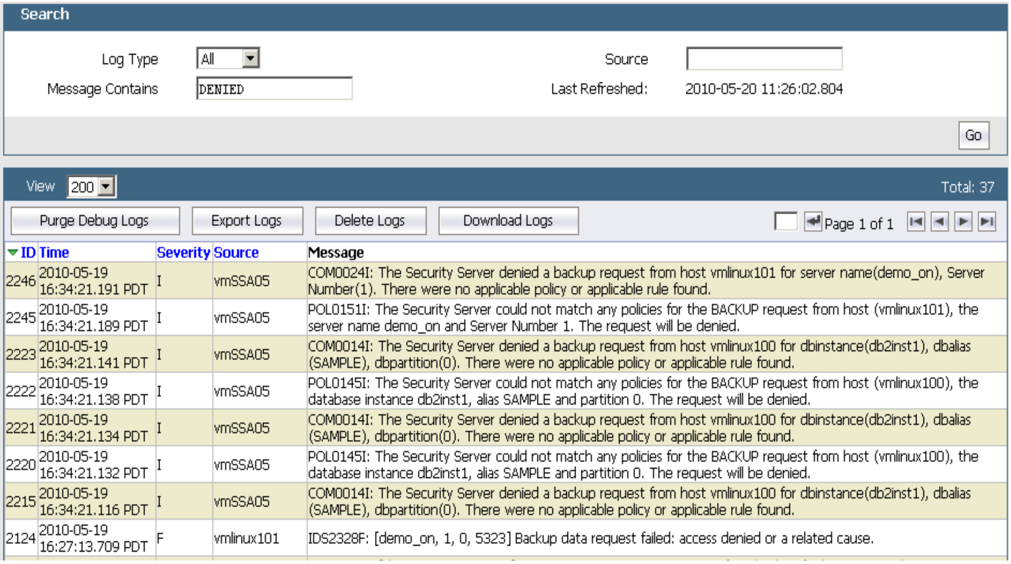
Using Syslog to Troubleshoot the GDE Appliance and Agents

Syslog entries for GDE Appliance activity indicate the source of the Syslog message (system name after the timestamp), the source of the message itself (SOURCE), the log level (AUDIT, ALARM, and so on), and much more.

Analyzing log entries

The format and content of log entries for VTE Agents are described below.

Figure 34: Message Log entries



Log Type: All
Message Contains: DENIED
Source:
Last Refreshed: 2010-05-20 11:26:02.804

View: 200
Total: 37

ID	Time	Severity	Source	Message
2246	2010-05-19 16:34:21.191 PDT	I	vmSSA05	COM0024I: The Security Server denied a backup request from host vmlinux101 for server name(demo_on), Server Number(1). There were no applicable policy or applicable rule found.
2245	2010-05-19 16:34:21.189 PDT	I	vmSSA05	POL0151I: The Security Server could not match any policies for the BACKUP request from host (vmlinux101), the server name demo_on and Server Number 1. The request will be denied.
2223	2010-05-19 16:34:21.141 PDT	I	vmSSA05	COM0014I: The Security Server denied a backup request from host vmlinux100 for dbinstance(db2inst1), dbalias (SAMPLE), dbpartition(0). There were no applicable policy or applicable rule found.
2222	2010-05-19 16:34:21.138 PDT	I	vmSSA05	POL0145I: The Security Server could not match any policies for the BACKUP request from host (vmlinux100), the database instance db2inst1, alias SAMPLE and partition 0. The request will be denied.
2221	2010-05-19 16:34:21.134 PDT	I	vmSSA05	COM0014I: The Security Server denied a backup request from host vmlinux100 for dbinstance(db2inst1), dbalias (SAMPLE), dbpartition(0). There were no applicable policy or applicable rule found.
2220	2010-05-19 16:34:21.132 PDT	I	vmSSA05	POL0145I: The Security Server could not match any policies for the BACKUP request from host (vmlinux100), the database instance db2inst1, alias SAMPLE and partition 0. The request will be denied.
2215	2010-05-19 16:34:21.116 PDT	I	vmSSA05	COM0014I: The Security Server denied a backup request from host vmlinux100 for dbinstance(db2inst1), dbalias (SAMPLE), dbpartition(0). There were no applicable policy or applicable rule found.
2124	2010-05-19 16:27:13.709 PDT	F	vmlinux101	IDS2328F: [demo_on, 1, 0, 5323] Backup data request failed: access denied or a related cause.

Analyzing VTE Agent log entries

The general format of a VTE Agent log entry is:

```
CGP2602I: [SecFS, 0] Level: Policy[policyName?] User[userID?]
Process[command?] Access[whatIsItDoing?] Res[whatIsItDoingItTo?]
Effect[allowOrDeny? Code (whatMatched?)]
```

where:

- SECFS indicates that the message was generated by a VTE Agent. You can enter `secfs` in the **Search Message** text-entry box in the **Logs** window to display VTE Agent policy evaluation and GuardPoint activity for all configured hosts.
- Level indicates the importance of the message. For example, AUDIT indicates an informational message, whereas ALARM indicates a critical failure that should not go ignored.
- Policy[] indicates the name of the policy that is being used to evaluate the access attempt.
- User[] identifies the system user attempting to access data in the GuardPoint. It typically displays the user name, user ID, and group ID.
- Process[] indicates the command, script, or utility being executed.
- Access[] indicates what is being attempted. Access may be read_dir, remove_file, write_file_attr, write_app, create_file, etc. These correspond to the Access methods that you configure in the policy. read_dir corresponds to d_rd. remove_file corresponds to f_rm. And so on.
- Res[] indicates the object being accessed by Process[].
- EFFECT[] indicates the rule that matched and, based upon that rule, whether or not the GDE Appliance grants access. Access states may be either PERMIT or DENIED.

For example:

```
CGP2606E: [SecFS, 0] [ALARM] Policy[allowAllRootUsers_fs]
User[bubba,uid=1111,gid=10\wheel\] Process[/usr/bin/vim]
Action[create_file] Res[/opt/apps/apps1/lib/file1.txt]
Effect[DENIED Code (1M)]
```

The format of a rule match is:

```
intchar
```

where:

- `int` is an integer representing the security rule being used or violated. Security rules are numbered sequentially from top to bottom in the Online Policy Composer window.
- `char` is an uppercase letter indicating the item that is using or violating the policy.

Table 13: Character Codes and Their Descriptions

Character Code	Description
A	The **Action** component of a security rule failed to match.
M	All security rule components match and, unless overridden, the **Effect** for that security rule is applied.
P	The **Process** component of a security rule failed to match.
R	The **Resource** component of a security rule failed to match.

Character Code	Description
T	The time specified in the **When** component of a security rule failed to match.
U	The **User** component of a security rule failed to match.

For example, the following match codes indicate:

- **1R** – Mismatch in Resource for Security Rule 1.
- **3U** – Mismatch in User for Security Rule 3.
- **4A** – Mismatch in Action for Security Rule 4.
- **2M** – All components matched for Security Rule 2. Since all the rules matched, Security Rule 2 will be used and no other rules will be evaluated.

Log message levels

The detail and extent of information logged is determined by the selected log level. The agent supports five log levels as listed in Table 14.

Table 14: The Agent-Supported 5 Log Levels

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

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

Using log files

Check the log files to verify the successful installation and configuration of the GDE Appliance software, to determine why a backup or restore operation failed, or to monitor GDE Appliance activity.

A logged event falls into one of the following categories:

- **Operational status.** The result of any significant action performed by an VTE Agent or GDE Appliance is logged.
- **Administrative activity.** The result of any maintenance or administrative activity on the GDE Appliance is logged (for example, a key has been created or exported).
- **System status.** The result of any system errors are logged (for example, if the database connection is interrupted).
- **Policy-specified audit.** If the result of a policy evaluation specifies that it should be audited, then a suitable message is logged.

Several logs files are provided. Each serves a different purpose. (Windows only) The `\ProgramData` folder on Windows Vista and Windows Server 2008, and the `\Documents and Settings\All Users\Application Data` folder for all other supported Windows platforms, are hidden by default. VTE Agent logs, configuration data, and certificates are stored under that folder. If you cannot browse the folder for your platform, enable the **Show hidden files and folders** radio button in the **Folder Options** menu to view the folder and its contents.

Active logs are log files that being currently written to and updated by GDE Appliance processes. Inactive logs are logs that have been filled to capacity and then closed. The name of the closed log file is the original name usually appended with the date and some random numbers. For example, the name of an active agent log is vordb2_usr.log. When it reaches the configured capacity, it is made inactive and usually renamed to `vordb2_usr.log.YYYY-MM-DD-MM-SS.tar.gz`. For example, the archive file for `vordb2_db2inst1.log` can be `vordb2_db2inst1.log.2011-01-19-12-25-32`.

Do not try to manually modify or remove active logs. Use the Management Console interface to configure server and VTE Agent logs. Regularly back up and delete inactive logs to maximize available hard disk space.

The Windows system event log can fill quickly. If a Windows host runs out of system event log space, the vmd service does not start and issues an error: "`The service did not respond to the start or control request in a timely fashion.`" To prevent the system event log from running out of space, the current event log is archived to a file when it reaches 20MB, all archived entries are then purged from the event log, and logging continues as usual. Archive files are placed in `%SystemRoot%\System32\Config`. The archive file is named `Archive-Vormetric Encryption Expert-timestamp.evt`. For example, `Archive-Vormetric Encryption Expert-2010-05-14-18-14-30-171.evt`. The file is archived in a binary format that you can open in the Event Viewer. Check disk space availability during periods of heavy load and extensive logging. Back up and delete the archive files.

VTE Agent Log Files

The agent logs are the first places to check when communication between the GDE Appliance and VTE agent system fails. Also, you may want to check these logs after setting up a new agent or changing the agent configuration.

Sample logging formats include the following:

vorvmd.log (Windows)/vorvmd_root.log (UNIX)

(UNIX)

`/var/log/vormetric/vorvmd_root.log`

(Windows)

```
\Documents and Settings\All Users\Application
Data\Vormetric\DataSecurityExpert\Agent\log\vorvmd.log
```

(Windows XP)

```
\Documents and Settings\All Users.WINDOWS\Application
Data\Vormetric\DataSecurityExpert\agent\log\vorvmd.log
```

(Windows Vista and Windows Server 2008)

`\ProgramData\Vormetric\DataSecurityExpert\Agent\log\vorvmd_root.log`

(Windows) The same information that is sent to `vorvmd.log` can also be sent to the Windows Event Viewer. Enable **Log to Syslog/Event Log** logging options for the agents and open **Event Viewer > Vormetric Encryption Export** to view log events on the host system.

`vorvmd_root.log` contains the VTE Agent transactions for the root user. Transactions consist of a record of vmd actions, such as starting the vmd daemon and setting up communication links with the GDE Appliance.

messages (UNIX only)

`/var/log/messages`

messages is a Syslog-generated file. It contains standard Syslog entries. It contains kernel entries for enabling/disabling the log service, memory usage, CPU usage, system calls, device initialization, etc. It also contains log entries that are also displayed in the Message Log.

secfs.log (AIX only)

The `secfs.log` file contains kernel-related messages, and the `secfsd.log` file contains process-related messages. The `secfs.log` file is generated only on AIX systems. The secfs.log file is maintained in the `./agent/secfs/tmp` directory. It is used instead of Syslog to log kernel messages. The same log messages are placed in both `/var/log/messages` and `secfs.log`. The `secfs.log` file is archived at 32MB and renamed to `secfs.log.archive`. Only one archive file is maintained.

secfsd.log

(UNIX)

`/opt/vormetric/DataSecurityExpert/agent/secfs/tmp/secfsd.log`

(Windows Server 2003)

```
C:\Documents and Settings\All Users\Application
Data\Vormetric\DataSecurityExpert\agent\log\secfsd.log
```

(Windows Vista and Windows Server 2008)

`C:\ProgramData\Vormetric\DataSecurityExpert\agent\log\secfsd.log`

(Windows XP)

```
C:\Documents and Settings\All Users.WINDOWS\Application
Data\Vormetric\DataSecurityExpert\agent\log\secfsd.log
```

The `secfs.log` file contains kernel-related messages, and the `secfsd.log` file contains process-related messages. secfsd.log contains a record of GuardPoint mounts and GuardPoint dismounts (GuardPoints are mounted file systems). Entries are added to this file when you add and remove GuardPoints, as well as when you reboot the agent system.

statusfile

`/opt/vormetric/DataSecurityExpert/agent/secfs/tmp/statusfile`

`\Program Files\Vormetric\DataSecurityExpert\agent\secfs\tmp\statusfile`

`statusfile` is a current record of the local VTE Agent configuration. View this file after updating the VTE Agent configuration on the GDE Appliance to verify that the changes have actually been applied. This file should always be checked when the configuration of the VTE Agent is in question. This file lists:

- Each GuardPoint and GuardPoint properties, such as the lock status, protection status, and GuardPoint directory
- The names of applied policies
- The logging information that is captured
- Where captured log information is sent
- Hosts settings

You can also display the file timestamp to see when the agent was last updated.

This file is deleted each time the VTE Agent configuration is updated. You must manually regenerate it using the “`secfsd -status`” command. If you want to keep records of VTE

Agent configuration changes, either copy the `statusfile` to a different name, or run “`vmsec status`” and assign the output to a different file.

(Windows) The `secfsd` command has limited support on Windows platforms. You can use the `secfsd -status lockstat` command or use the Vormetric Data Security tray to open the status window. Look for strings like `coreguard_locked=true` and `system_locked=true`. (`false` indicates that a lock is not applied. `true` indicates that a lock is applied.).

You may view the file contents using an ASCII display command, such as `cat`.

GDE Appliance Log Files

GDE Appliance logs are logs on the GDE Appliance system. The primary log is viewed in the **Logs** window of the Management Console. This log is generally the first log that you check to diagnose GDE Appliance problems. Check the GDE Appliance log after making or restoring a database backup. Look for entries like “`Backup Request for SAMPLE from host vmSSA06 is allowed.`” and “`Backup/Restore completed successfully.`” Messages like “`Backup data request failed: access denied or a related cause.`” indicate a problem has occurred and some debugging on your part is required.

Appliance-based GDE Appliance installations must use the `diag` CLI command to list and view the log files. However, the log files can be exported from an appliance using the various export features in the Logs window. Appliance-based server administrators cannot delete log files.

The GDE Appliance server creates three log files in

- `boot.log` contains JBoss startup information.
- `cgss.log` contains server information.
- `server.log` contains system-level information.

`boot.log` is managed as a single file. It is not expected to ever become a large file nor is it rotated. The `cgss.log` and `server.log` files can become large and are rotated.

The `cgss.log` and `server.log` files are important log files that can grow quickly under heavy load. Because these logs are vital to analyzing GDE Appliance behavior, they should be monitored and backed up regularly.

The names of the active files are `cgss.log` and `server.log`. When either file contains 10MB of log data it is made inactive and renamed to `cgss.log.1` or `server.log.1`, respectively. And a new active `cgss.log` or `server.log` file is opened. When the new active log file reaches 10MB it is made inactive and renamed to `cgss.log.2` or `server.log.2`. And a new active log file is opened. This process continues until there are a total of 10 inactive log files. When there are 10 inactive log files, and the active log file reaches its full 10MB capacity, the first inactive file is discarded, all the other log file names are decremented by one, and the former active log becomes the 10th inactive log file. Using `cgss.log` as an example, when `cgss.log` fills, `cgss.log.1` is thrown away, all the other log file names are decremented by one, and `cgss.log` becomes `cgss.log.10`. Depending on how much load you place on the server, and if your policies audit a lot of data, these files can grow and rotate quickly.

badlog.log

Log files with unparsable data are “bad logs”. A badlog.log file contains log data from an agent that is intended for display in the Logs window but which cannot be displayed because the log data cannot be parsed due to format irregularities. Each attempt by an agent to upload an unparsable log file to the server is placed in the badlogs directory as a unique file. Regardless of the number of failed attempts to parse incoming log files, the GDE Appliance will continue to accept uploaded logs from the agent.

cgss.log

The cgss.log file contains a record of the events that make up the BEK generation process for an agent requesting to make a backup, as well as the names of uploaded audit files. This file does not contain events that pertain to restore operations. Check this file if the agent fails to back up a database, even though agent/server authentication is correctly configured and the policy for this agent permits the backup operation.

jboss.log

The `jboss.log` file contains information that is related to starting and stopping the JBoss Web application server. This file is generated when the `/etc/init.d/cgss` command is used to start and stop JBoss. Check this log file for problems that are related to JBoss, such as when you are unable to initiate a Management Console session.

This file is located in `/tmp`.

server.log

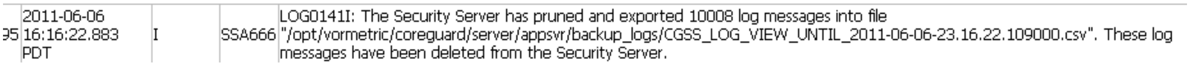
The server.log file contains details about agent backup and restore requests, connection status, Management Console interaction, Java exceptions, JBoss start and stop processes, and more. This file contains diverse information and should be checked for almost any problem that is related to the GDE Appliance. Sometimes it is easier to `grep` a specific error level, like WARN, INFO, or DEBUG, than it is to view the entire file.

Pruning the GDE Appliance Logs

After about 10,000 entries in the **Message Log**, the existing logs are automatically pruned (removed) from the database and written to the backup directory, `/opt/vormetric/coreguard/server/jboss-5.1.0.GA/server/default/backup_logs`. (`/opt/vormetric/coreguard/server/appsvr/backup_logs` is a symbolic link to this directory).

The output file name is `CGSS_LOG_VIEW_UNTIL_YYYY-MM-DD-NN.NN.NN.NNNNNN.csv`. For example, `CGSS_LOG_VIEW_UNTIL_2011-06-06-23.16.22.109000.csv`.

Figure 35: A pruning entry in the Message Log



95	2011-06-06 16:16:22.883 PDT	I	SSA666	LOG0141I: The Security Server has pruned and exported 10008 log messages into file "/opt/vormetric/coreguard/server/appsvr/backup_logs/CGSS_LOG_VIEW_UNTIL_2011-06-06-23.16.22.109000.csv". These log messages have been deleted from the Security Server.

Each output file averages 10, 000 lines and 4.3 MB disk space. Each is owned by `db2fenc1`, with a mod of 644 (`rw-r--r--`). The output file is a comma-separated list comprising the entries in the Logs window and is saved as a `.csv` file.

Up to ten log files can reside in the `backup_logs` directory at one time. The first log file is deleted when the eleventh log file is generated.

Pay attention to this directory. If you are generating a massive amount of log data, as can occur when running a lot of `dataxform` sessions or when GuardPoints are under heavy loads, the log files can come and go quickly. Once gone, there is no record of the activity that had occurred.

The output file column organization is the same as the output of the **Export Logs** button on the **Logs** window.

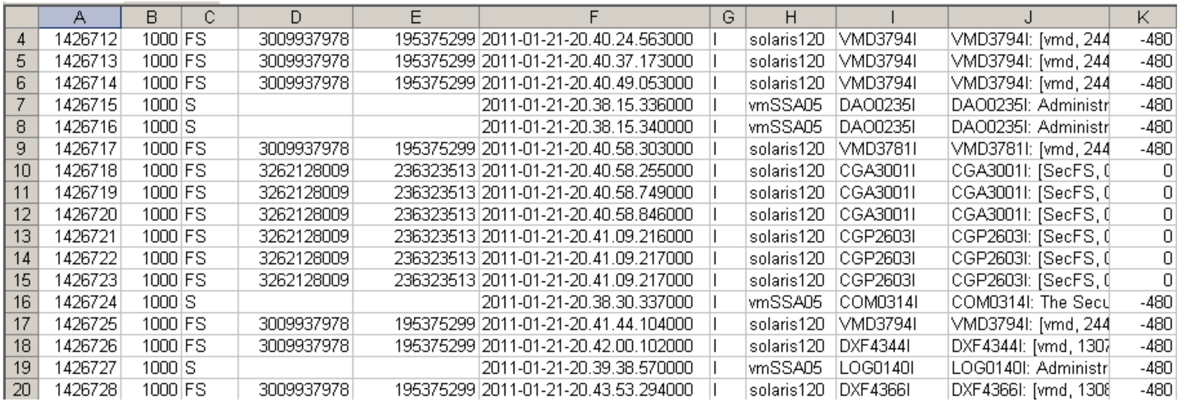
Exporting Logs

You can export the log entries that are displayed in the **Logs** window to maintain a separate record of server and agent activity at the application level. Administrators of type System Administrator can also export log files that track the internal operations of the GDE Appliance at the system level.

The data displayed in the **Logs** window can be exported to a file for archival or analysis. Only the entries in the **Logs** window that are appropriate for the administrator type and domain can be saved to a text file. The output file is formatted as a comma-separated list and is usually viewed in a spreadsheet application.

The following example is an excerpt of a .csv file generated by an administrator of type All that is inside a domain.

Figure 36: Figure 158: Excerpt of a log .csv file



	A	B	C	D	E	F	G	H	I	J	K
4	1426712	1000	FS	3009937978	195375299	2011-01-21-20.40.24.563000	I	solaris120	VMD3794I	VMD3794I: [vmd, 244	-480
5	1426713	1000	FS	3009937978	195375299	2011-01-21-20.40.37.173000	I	solaris120	VMD3794I	VMD3794I: [vmd, 244	-480
6	1426714	1000	FS	3009937978	195375299	2011-01-21-20.40.49.053000	I	solaris120	VMD3794I	VMD3794I: [vmd, 244	-480
7	1426715	1000	S			2011-01-21-20.38.15.336000	I	vmSSA05	DAO0235I	DAO0235I: Administr	-480
8	1426716	1000	S			2011-01-21-20.38.15.340000	I	vmSSA05	DAO0235I	DAO0235I: Administr	-480
9	1426717	1000	FS	3009937978	195375299	2011-01-21-20.40.58.303000	I	solaris120	VMD3781I	VMD3781I: [vmd, 244	-480
10	1426718	1000	FS	3262128009	236323513	2011-01-21-20.40.58.255000	I	solaris120	CGA3001I	CGA3001I: [SecFS,	0
11	1426719	1000	FS	3262128009	236323513	2011-01-21-20.40.58.749000	I	solaris120	CGA3001I	CGA3001I: [SecFS,	0
12	1426720	1000	FS	3262128009	236323513	2011-01-21-20.40.58.846000	I	solaris120	CGA3001I	CGA3001I: [SecFS,	0
13	1426721	1000	FS	3262128009	236323513	2011-01-21-20.41.09.216000	I	solaris120	CGP2603I	CGP2603I: [SecFS,	0
14	1426722	1000	FS	3262128009	236323513	2011-01-21-20.41.09.217000	I	solaris120	CGP2603I	CGP2603I: [SecFS,	0
15	1426723	1000	FS	3262128009	236323513	2011-01-21-20.41.09.217000	I	solaris120	CGP2603I	CGP2603I: [SecFS,	0
16	1426724	1000	S			2011-01-21-20.38.30.337000	I	vmSSA05	COM0314I	COM0314I: The Secu	-480
17	1426725	1000	FS	3009937978	195375299	2011-01-21-20.41.44.104000	I	solaris120	VMD3794I	VMD3794I: [vmd, 244	-480
18	1426726	1000	FS	3009937978	195375299	2011-01-21-20.42.00.102000	I	solaris120	DXF4344I	DXF4344I: [vmd, 1307	-480
19	1426727	1000	S			2011-01-21-20.39.38.570000	I	vmSSA05	LOG0140I	LOG0140I: Administr	-480
20	1426728	1000	FS	3009937978	195375299	2011-01-21-20.43.53.294000	I	solaris120	DXF4366I	DXF4366I: [vmd, 1308	-480

The format of this table is subject to change. At this time, the columns indicate:

Table 15: Exported Message Log Headings and Description

Column Heading	Description
A	ID number in the Management Console (LOG_ID)
B	Internal domain identifier. If you are not in a domain this is zero. (DOMAIN_ID)
C	Entity that generated the message. For example, S (**GDE Appliance**), FS (VTE Agent) (SOURCE)
D	Internal tag (TAG)
E	Internal subtag (SUBTAG)
F	Time of action in UTC (LOG_TIMESTAMP)
G	Severity in the Management Console (SEVERITY)
H	Source in the Management Console (HOST_NAME)
I	GDE Appliance or agent Message ID. For example, DAO0239I or CGP2603I.The Message ID also identifies the log service. For example, CGP2603I was generated by the CGP (Policy Evaluation Service) log service. (MESSAGE_ID)
J	Message in the Management Console (MESSAGE)
K	Time offset in minutes. Subtract this number from the time in column F to determine local time. F - K = local time. For example, 22:40:19 UTC - 420 offset = 15:40:19 PDT = 3:40 PM PDT. (TIMEZONE_OFFSET)

Exporting the Message Log

To export the Message Log:

1. Log on to the Management Console as an administrator of the appropriate type for the data you want to export.
2. Enter a domain if you want to export domain-related log entries.
3. Open the **Logs** window.
4. Click **Export Logs**. The **File Download** window opens.

   The options are:

   - **Open** to display the log entries to be exported in the default spreadsheet application. Usually this is Excel.
   - **Save** to export the log to a file on the system running the Management Console Web session or on another network accessible system. The default output file name is `log.csv`.
   - **Cancel** to close the window and stop the export operation.
5. Click **Save**. The **Save As** window opens.
6. Enter the name and path for the export file. The default file name is `log.csv`.
7. Click **Save**. The **Download Complete** window opens. It displays statistical information about the exported log, such as its location and size.

   The options are:

   - **Open** to open the exported log file in the default spreadsheet application used to process CSV format files.
   - **Open Folder** to open a Windows Explorer window in which to select and view the exported log in an application of your choice.
   - **Close** to close the window.
8. Click an option to open the exported log in the default spreadsheet application, open the exported log file in a different application, or to close the window and continue other Management Console operations.

Exporting GDE Appliance system logs

The Management Console enables GDE Appliance administrators of type System to export a collection of log files that track the GDE Appliance’s installation, configuration, and internal operations at the system level.

NOTE: If there is a major application or server failure, the Management Console graphic interface can stop working and you will be unable to use this feature to export the system.

Periodically export the server log files, and archive them. Later, the exported files may be useful to Thales Customer Support for diagnosing and resolving system related problems. You may also want to use this as an alternative to the CLI `diag` log view command because here you can download all the server and `cgss` logs at one time in one file, including other files that aren't viewable from the CLI. You can unzip the exported file and view the individual log files in your favorite editor, rather than "`more`" through them in the CLI.

The contents and analysis of these files are not described in this document. Should a major problem occur, analyze these files with Thales Customer Support.

This function exports just a subset of the total log files that are on the system. Included in the export file are log files such as:

- `alters.log`
- `boot.log`
- `cgss.log`
- `cgssdb_start_replication_2009-10-30.log`
- `cgssdb_stop_replication_2009-11-15.log`
- `convert_failover_to_primary.log`
- `convert_primary_to_failover.log`
- `db2setup.log`
- `delver.log`
- `jboss.log`
- `security_server_install.log`
- `security_server_uninstall.log`
- `security_server_upgrade.log`
- `server.log`
- `server_replication_2009-10-30.log`
- `vor_cert.log`
- `vor_est_trust.log`

More and diverse log files are generated on the server during the course of normal usage and maintenance. System administrators on software-only installations can view the additional log files located in `/tmp` and `/var/log`.

Exporting the GDE Appliance system log files

1. Log on to the Management Console as an administrator of type System Administrator or All.

   NOTE: This export system logs feature is not available to administrators of type Domain Administrator and Security Administrator.

   It does not matter if you enter a domain or not. The same log files are exported.

2. Select **Log > Logs**. The Logs window opens.

3. Click **Download Logs**. The **File Download** window opens.

   The options are:

   - **Open** to place the individual log files in a cached archive file without saving the archive file. The files can then be extracted and saved as desired.
   - **Save** to export a diverse collection of internal log files to a single zip file. The file may be saved on the system running the Management Console Web session or on another network accessible system.
   - **Cancel** to close the window and stop the export operation.

4. Click **Save**. The **Save As** window opens.

5. Enter the name and path for exporting the file. The default file name is `logs.zip`.

6. Click **Save**. The **Download Complete** window opens. It displays statistical information about the exported log, such as its location and size.

   The options are:

   - **Open** to open the exported log file in the default archive utility used to process zip format files.
   - **Open Folder** to open a Windows Explorer window in which to select and view the exported log in an application of your choice.
   - **Close** to close the window.

7. Click an option to open the exported log in the default archive application, open the exported log file in a different application, or to close the window.

Adding an Email Notification Group

Email Groups are per domain. You can set up email groups for domains of System, Security, Domain, Domain/Security and All Administrators.

Enabling email notification for log messages

You can automatically send email notifications to a set of administrators if the GDE Appliance generates a serious log message.

You need to configure an SMTP server first. Navigate to *System > Email Notification* and click the **SMTP Server** tab. Enter the information for the following tabs:

- **SMTP Server**—SMTP server that will send the email notification. SMTP Servers are per appliance and you must be signed in with System Administrator privileges to modify this setting. If you don't have these privileges, the SMTP server setting is grayed out. Note that the appliance does not come with a default SMTP server and that the SMTP server settings are initially empty.
- **SMTP Server Port**—Port used by the SMTP server.

To bring up the Email Notification interface, select **System > Email Notification** when outside a domain. The attributes and interface information for the Email Notification are as follows:

- **Email Group Name**—Name of the email group which will receive the email notification. Email Groups are per domain. You can set up email groups for domains of System, Security, Domain, Domain/Security and All Administrators.
- **Email Threshold Level**—If the GDE Appliance generates a log message with a severity of this specified threshold level, then an email notification is generated. Can be ERROR or FATAL.
- **Email Address List**—Email addresses that will receive this email notification. Separate addresses with commas. If LDAP is configured, you can select addresses from your LDAP address book by pressing **Select**. If it's not configured, you can enter your login and password to access it.
- **Email Subject**—Text you want on the subject line.
- **Message Contains**—This is a string filter that works with the Email Threshold Level. Only messages containing this string will be sent as an email notification. If blank, then all messages meeting the threshold criteria will be sent.
- **Enabled**—A checkbox that enables or disables email notification to the group.

To add an email notification group:

1. Select **System > Email Notification**. The **Email Notification** window displays.
2. Under the **Email Notification List** tab, click **Add**. The **Add Email Notification Group** window displays.
3. Enter the information and click **Ok**.

Changing the SMTP server and port for email notification

You must be signed in with System Administrator privileges to modify this setting.

To change the SMTP server and port for email notification:

1. Select **System > Email Notification**. The **Email Notification** window displays.
2. Click the **SMTP Server** tab
3. Enter the SMTP server and server port and click **Ok**.

10 External Certificate Authority

You can configure the GDE Appliance to have certificates signed by an external Certificate Authority (CA).

You can configure an external CA on a single node or high availability (HA) deployments. You can set up the GDE Appliance to have certificates signed by an external Certificate Authority when the system is set up for the first time, when the system is upgraded, or when the system is in production.

This chapter contains the following sections:

Overview

To configure the GDE Appliance to work with an external CA, you must have:

- A valid account with an external CA that is network accessible
- Instructions from the CA explaining how to transfer a certificate request file and a signed certificate file to and from the GDE Appliance.

The high-level steps for signing the GDE Appliance's Web server certificate with an external Certificate Authority are as follows:

1. Use the CLI `genca` command to generate the GDE Appliance's self-signed internal certificate authority and Web server certificates.

   This enables access to the Web-based Management Console.

2. Install the license. In HA systems, install the license only on the primary GDE Appliance.
3. Generate the Certificate Signing Request (CSR) file, and save it as a Privacy Enhanced Mail (PEM) file.

   The PEM file contains the information you must submit to the external CA to obtain an approved and signed certificate.

4. Import the signed certificate and the signer's certificate(s).

5. Allow the GDE Appliance to restart.
6. If the CA is to be used in an HA environment, repeat steps 4 through 6 for each failover server.

Installing an External Certificate Authority

Installing an External CA on a Single Node

You can create a new single node system or modify an existing single node system to work with an External Certificate Authority.

Generate a self-signed certificate (genca)

1. Log on to the GDE Appliance CLI.
2. Generate the self-signed Certificate Authority certificate. Type:

```
dsm$ system
system$ security genca
```

   This command regenerates the CA on the GDE Appliance. Refer to the “System Category Commands” on page 364, for more information about the genca command.
3. Log on to the Management Console as an administrator of type System Administrator or All. Do not enter a domain.
4. Click **System > License > Upload License File** to upload the license file. This step is required only if this is a new installation or a GDE Appliance software upgrade.

NOTE: Run the `gencert` command instead of the genca command when converting a primary GDE Appliance to a failover GDE Appliance, and you only need to re-validate the server certificate. This will prevent the need to re-register agents.

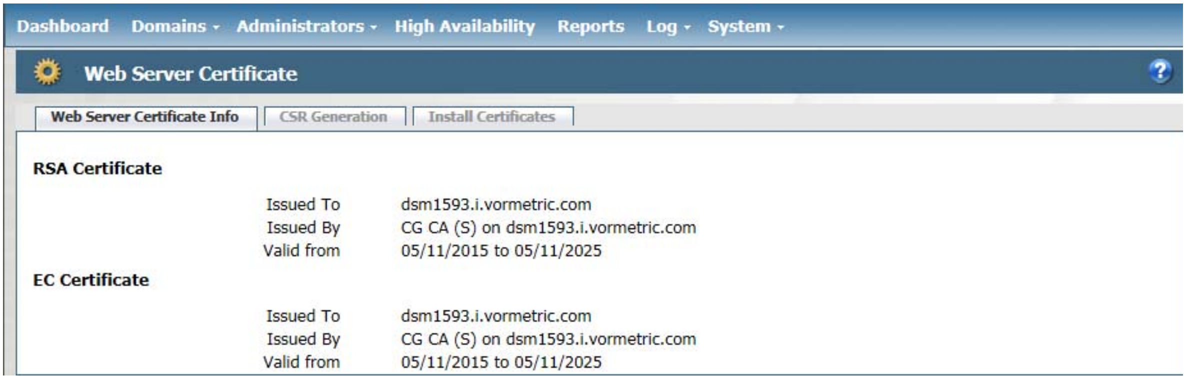
Web Server Certificate Information

The *Web Server Certificate Info* tab displays status information about the existing Web server certificate. It can be used to determine if the certificate has been self or externally signed. It also shows the GDE Appliance operating mode with respect to Suite B and consists of the following three fields:

- **Issued To**—Displays a summary of the data required to generate a CSR including Common Name (CN). CN in this field represents the host name of the device requesting the CSR.
- **Issued By**—Displays the CN of the Certificate Authority issuing the certificate

- **Valid From**—Displays the certificate's start and expiration date

Figure 37: Web Server Certificate



RSA Certificate

Issued To dsm1593.i.vormetric.com
Issued By CG CA (S) on dsm1593.i.vormetric.com
Valid from 05/11/2015 to 05/11/2025

EC Certificate

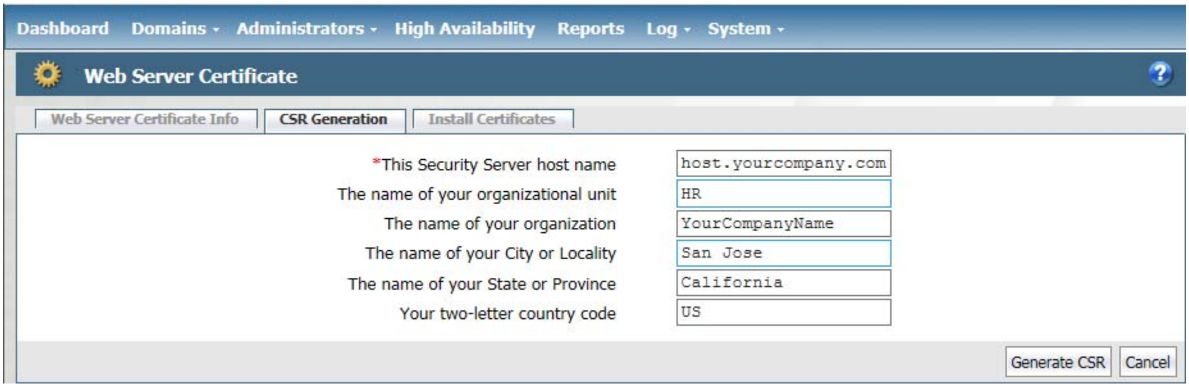
Issued To dsm1593.i.vormetric.com
Issued By CG CA (S) on dsm1593.i.vormetric.com
Valid from 05/11/2015 to 05/11/2025

Generate a CSR

1. Select **System > Web Server Certificate** from the Management Console. The Web Server Certificate window opens.
2. Click the **CSR Generation** tab. Enter the information in the fields. If you entered this information while running the genca command, the fields (other than the hostname which is updated automatically, but can also be changed) on this tab will contain that same information. You can modify this information if required. Verify that the following pre-populated entries are consistent with the requirements of your external CA. For instance, some CAs will not accept an abbreviation for the name of the city or state.
    - **Host Name**: Network name of the GDE Appliance (up to 64 characters). It is possible to edit this field, however it is recommended that you do not change this name.
    - **Organizational Unit**: Typically a department or group name (up to 64 characters)
    - **Organization**: Typically, this is the company name (up to 64 characters)
    - **City or locality**: Location of the Organization (up to 128 characters)
    - **State or province**: Location of the Organization. Refer to external CA for format requirements. Some CAs will not accept an abbreviation for the name of the city or state. (up to 128 characters)
    - **Country Code**: Abbreviation for the country where the Organizational Unit is located (up to 2 characters).

NOTE: Strings that contain a comma (,) are permitted; however, the use of single or double-quotes in any field on the CSR Generation tab is not allowed.

Figure 38: Certificate Signing Request Tab Information



*This Security Server host name: host.yourcompany.com
The name of your organizational unit: HR
The name of your organization: YourCompanyName
The name of your City or Locality: San Jose
The name of your State or Province: California
Your two-letter country code: US

If you are running the GDE Appliance in Suite B or Compatibility mode, when you click Generate CSR, the GDE Appliance generates a .zip file containing two PEM files:

- tserver-csr.pem
- EC_tserver-csr.pem

If you are operating in compatibility mode, you will need both PEM files signed. After you receive the signed Web server certificates, install both on the GDE Appliance.

3. Click **Generate CSR**. The **File Download** window opens.
4. Click **Save**. The **Save As** window opens.
5. Enter the name and path for the certificate request file. The default file name is *servercsr_<hostname_YYYY_MM_DD_HHMM>.pem*.
6. Click **Save**. The **Download Complete** window opens. It displays statistical information about the exported PEM file, such as its location and size.
7. Know where the PEM file is saved so you can find it later. Click **Open Folder** to verify the location.
8. Click **X** to close the window.
9. Submit the new CSR to a Certificate Authority for signing/approval.

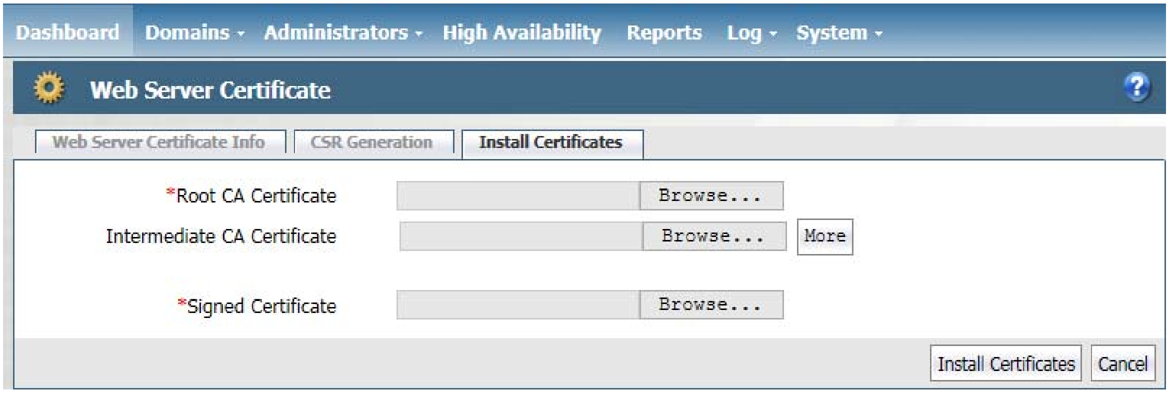
NOTE: Be sure to follow the procedures of the CA to obtain valid certificates. Each CA may have different procedures to obtain the Root certificate, Intermediate certificate, and signed CSR certificate.

Install certificates

1. In the Management Console, on the *Web Server Certificate* page, click the **Install Certificates** tab.

2. Click **Browse** for the **Root CA Certificate** field and load the Root CA Certificate. The Root CA Certificate is required.
3. If needed, click **Browse** for the **Intermediate CA Certificate** field and load the Intermediate CA Certificate.
4. If needed, click **More** to browse for additional Intermediate CA Certificates. You can select up to ten Intermediate CA Certificates.
5. Click **Browse** for the **Signed Certificate** field and load the Signed Certificate. This is required.

Figure 39: Install certificates



NOTE: When you copy a certificate, be certain to copy and paste the certificate just as it appeared originally. Make sure that there are no extra characters or leading spaces as this will invalidate the certificate.

6. Click **Install Certificates**, and then click **OK** to install the certificate and restart the server. The restart takes several minutes.

NOTE: During restart, do not close the browser. Do not select Back, Refresh, or the browser Stop buttons.

7. After the server restarts, log on again.
8. To verify the certificate status, click the **Web Server Certificate Info** tab.
   - If the Common Name (CN) entry in the **Issued To** and **Issued By** fields shows the same information, the current certificate has been self-signed.
   - If the CN entry in the **Issued To** and **Issued By** fields shows different values the current certificate was not self-signed.

If you are running the GDE Appliance in Suite B or Compatibility mode, you need to send both the RSA and EC CSRs to be signed by your CA, in which case you need to import both signed certificates; an RSA certificate and an EC certificate.

Installing an external CA in a high availability system

The external Certificate Authority GDE Appliance HA system is similar to that of a self-signed GDE Appliance HA cluster. To register the agents assigned to a failover server, the failover server must initially have an active connection to the primary server.

Once you disable the HA configuration, and convert the primary server to a failover or back to a primary server, the hosts assigned to the primary server must re-register before they can operate again. If you anticipate an extended delay in configuring failover servers, you should reassign the agents to the primary server before you reconfigure the failover server.

You can create a new HA environment or modify an existing HA environment to work with an External Certificate Authority.

Generate a self-signed certificate (genca)

NOTE: This needs to be done only on the primary node.

1. Log on to the GDE Appliance CLI.
2. Generate the self-signed Certificate Authority certificate. Type:

```
system
security genca
```

3. Log on to the Management Console as an administrator of type System Administrator or All. Do not enter a domain.
4. Click **System > License > Upload License File** to upload the license file. This step is required only if you are doing a new installation, or if you are upgrading the GDE Appliance software.

Create a new HA configuration

1. Log on to the GDE Appliance as an administrator of type System Administrator or All. Do not enter a domain.

NOTE: The first GDE Appliance software version to support an external Certificate Authority is 5.1.1. Be sure the primary and all failover GDE Appliance servers are already running the same software version that supports external Certificate Authority. If needed, upgrade the primary and all failover GDE Appliance software.

2. Click **High Availability**, and then click **Add**, the **Add High Availability Server Details** screen opens.
3. Enter the host name or the FQDN in the **Server Name** field, and then click **OK**.
4. Convert the primary to a failover server. Repeat this step for all servers you want to use as failover servers.

Modify an existing HA configuration for an External CA

If you want to configure an external CA for an existing HA configuration, you need to generate a CSR and

1. Log on to the Management Console as an administrator or type System Administrator or All. Do not enter a domain.
2. From the Management Console on the primary server, disable communication between the primary server and all the failover servers (Cleanup Replication).
3. Make sure that the primary and failover servers are at the same GDE Appliance version.
4. The genca command only needs to be run on a new server added as the primary server, not for an existing failover. See “Generate a CSR”
5. Confirm that the designated failover servers have been added to the primary, then convert each of these servers to failovers.
6. Install the certificates on all the failover servers, see “Install certificates”.

Administrative Tasks

Tasks in this section are done as required to administer or maintain an external CA environment.

Changing to another external CA

To reconfigure the GDE Appliance to use a different CA:

1. Generate a new Certificate Signing Request, see “Generate a CSR”.
2. Submit the new CSR to a Certificate Authority for signing/approval.
3. Install the new signed certificates from the **Install Certificates** window, see “Install certificates” on page 112.

Restoring the GDE Appliance to a self-signed Certificate Authority

You can restore the GDE Appliance to a self-signed Certificate Authority at any time. To revert a GDE Appliance to a self-signed Certificate Authority, run the CLI `genca` command. For example:

```
system$ security genca
```

NOTE: Reverting to a self-signed Certificate Authority invalidates all configured certificates, including agent and failover certificates, and they will all have to be regenerated.

The CLI `genca` command overwrites the current server certificate, and must be run to generate a new signer certificate.

Converting a primary GDE Appliance to a failover

When you convert the primary to a failover, you must reinstall the external CA. You need to do the following:

1. Generate a new Certificate Signing Request, see “Generate a CSR”.
2. Submit the new CSR to a Certificate Authority for signing/approval.
3. Install the new signed certificates from the **Install Certificates** window, see “Install certificates”.

NOTE: If the Certificate Authority changes, there is no need to re-register all the agents that are assigned to the primary server. If you run the genca command to revert an external CA GDE Appliance to a self-signed CA GDE Appliance, you must re-register the agents.

Converting a failover GDE Appliance to a primary

Convert an external CA failover GDE Appliance to a primary GDE Appliance as you would a self-signed CA failover GDE Appliance. No additional configuration is required after running the `convert2primary` command. The converted GDE Appliance retains its external CA configuration, and the server and agent remain valid.

Intermediate Certificate Authority

Use the *Intermediate Certificate Authority* page to configure the GDE Appliance to have the internal GDE Appliance CA signed by an external Certificate Authority (CA).

- "Intermediate CA Info"
- "CSR Generation"

NOTE: Use of the Intermediate CA is optional.

Intermediate CA Info

The *Intermediate Certificate Authority* tab displays the following information about the Server/Agent RSA Certificate and the Server/Agent EC Certificate:

- **Issued To**: Displays the host name of the GDE Appliance to which the certificate has been issued
- **Issued By**: Displays the name of the CA that has signed this intermediate certificate
- **Fingerprint**: Displays the SHA-256 digest of the certificate
- **Valid From**: Displays the period for which the certificate is valid

CSR Generation

Use the *CSR Generation* tab to generate a certificate signing request.

1. Navigate to **System > Intermediate CA**.
2. Click **CSR Generation** tab.
3. Fill out the form and click **Generate RSA CSR** or **Generate EC CSR**.

   If the GDE Appliance is in compatibility mode, generate both types of certificates. If using Suite B mode, use the EC certificates. If using RSA mode, use the RSA certificates.

NOTE: If certificate information was filled in during the initial configuration of the GDE Appliance when running the genca command, the form on this page is pre-populated with that information.

4. After generating the CSR, a file download dialog box displays, prompting you to select a location to save the .zip file that contains the CSR. The file format is `hostname-<YYYY_MM_DD_HHMM>-ec-csr.zip` or `hostname-<YYYY_MM_DD_HHMM>-rsa-csr.zip`, depending on the type of CSR generated. Each zip file contains two CSRs, each of which must be signed by the external CA.

5. Download the resulting zip file and extract the two CSRs inside.
6. For each CSR, open it in a text editor and copy the contents.

Obtaining and Installing External Certification

NOTE: The following example uses Microsoft Active Directory Certificate Services through Certification Authority Web Enrollment. Other certificate services will differ slightly in their methods.

1. Navigate to your web enrollment URL and login.
2. Click **Request a certificate** which takes you to the Request a Certificate page.
3. Click **advanced certificate request**, which opens the Submit a Certificate Request or Renewal page.
4. Paste your CSR into the certificate request box.
5. Select **Subordinate Certification Authority** in the Certificate Template pull-down menu.
6. Click **Submit** to request your certificate.
7. In the Certificate Issued screen, select the **Base 64 encoded** option.
8. Click **Download certificate chain** to download your new certificate chain.
9. Repeat the previous steps for any remaining CSRs.
10. **Return to the** GDE Appliance and click System > Intermediate CA.

Install Certificates

The file containing the GDE Appliance CA signed certificates for installation must also contain the entire certificate chain of CAs back to a root CA. The certificates must be in PEM format, must have keyCertSign and CRLSign key usages, and must also be in the correct signing order, with the GDE Appliance CA certificate at the top, followed by its signer certificate and so on until the root CA certificate which must be the last certificate at the end of the file.

Install Certificate Chain

NOTE: This certificate chain format is for Unix only.

For example, for a GDE Appliance CA certificate signed by CA1, where CA1 is signed by CA2, which in turn is signed by CA3, which is signed by the root CA, then the order of certificates in the file must be the following:

```
-----BEGIN CERTIFICATE-----
```

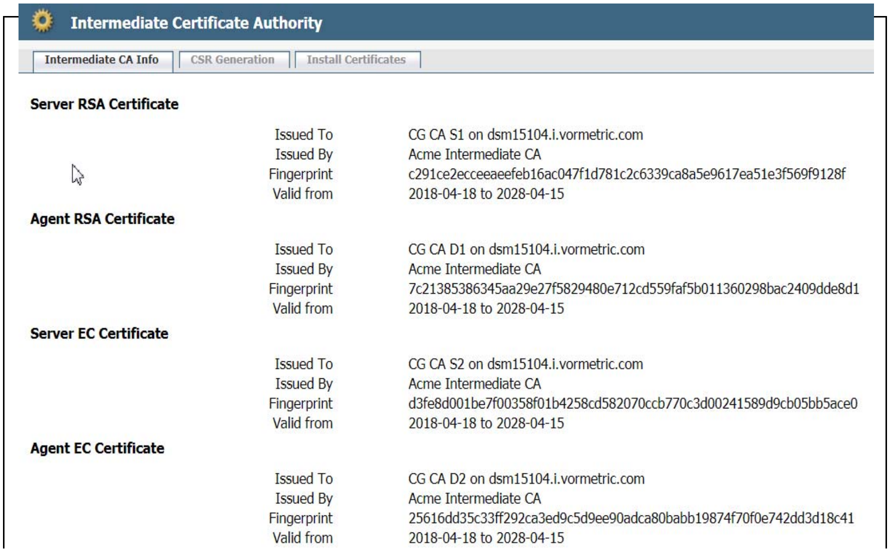
```
     (DSM CA cert)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 (CA1 cert)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 (CA2 cert)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 (CA3 cert)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
 (RootCA cert)
-----END CERTIFICATE----
```

To install the certificate:

1. On the GDE Appliance, click the **Install Certificates** tab.
2. Click **Choose File/Browse** to select the certificate chains (RSA or EC) to upload.

NOTE: You can upload both pairs at once, or only the RSA pair or only the EC pair.

3. Click **Install Certificates** and wait for the GDE Appliance to restart before logging in again.
4. Click **Intermediate CA Info tab**. The content should look like the following:



Server RSA Certificate

Issued To	CG CA S1 on dsm15104.i.vormetric.com
Issued By	Acme Intermediate CA
Fingerprint	c291ce2ecceeaeefeb16ac047f1d781c2c6339ca8a5e9617ea51e3f569f9128f
Valid from	2018-04-18 to 2028-04-15

Agent RSA Certificate

Issued To	CG CA D1 on dsm15104.i.vormetric.com
Issued By	Acme Intermediate CA
Fingerprint	7c21385386345aa29e27f5829480e712cd559faf5b011360298bac2409dde8d1
Valid from	2018-04-18 to 2028-04-15

Server EC Certificate

Issued To	CG CA S2 on dsm15104.i.vormetric.com
Issued By	Acme Intermediate CA
Fingerprint	d3fe8d001be7f00358f01b4258cd582070ccb770c3d00241589d9cb05bb5ace0
Valid from	2018-04-18 to 2028-04-15

Agent EC Certificate

Issued To	CG CA D2 on dsm15104.i.vormetric.com
Issued By	Acme Intermediate CA
Fingerprint	25616dd35c33ff292ca3ed9c5d9ee90adca80babb19874f70f0e742dd3d18c41
Valid from	2018-04-18 to 2028-04-15

NOTE: The **Issued To** and **Issued By** fields are different which indicates the certificates are no longer self-signed.

Importing the Root Certificate and Verifying a Secure Connection

To obtain a secure connection (green lock status) in your browser, import the "root CA" certificate into either your browser's certificate store, or the Windows certificate store.

NOTE: Some browsers have their own certificate store like Firefox. Chrome and IE/Edge use the Windows certificate store.

The following example is from Firefox.

1. Select **options** from the menu and enter **cert** in the search field.
2. Click **View Certificates > Authorities** tab.
3. Click **Import** and import the root ca certificate: *_root_ca.cer
4. Click **Ok** and then browse to your GDE Appliance using its hostname, which must match the hostname in the certificate.
5. In the URL field, you should see a green lock icon next to the URL. This indicates a secure connection.

LDAP Configuration

11

The GDE Appliance allows for integration with Lightweight Directory Access Protocol (LDAP) directory services such as Active Directory (AD) and OpenLDAP. This feature allows the GDE Appliance Administrator to import user criteria instead of recreating it from scratch.

This chapter contains the following sections:

Configuring LDAP

An LDAP server must be configured and authenticated before any information can be imported.

Configure LDAP server settings

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

   Examples:

   ```
   ldap://ldapserver.mycorp.com:389

   ldaps://ldapserver.mycorp.com:636
   ```

   NOTE: The default LDAP port is 389. The default LDAPS port is 636.

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

5. (Optional) Enter up to a 256 character string to filter searches, in the **LDAP Query** field.
6. (Optional) Enter the LDAP user login name in the **Login** field.

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

   jsmith@mycorp.com
7. Enter the LDAP password in the **Password** field. Enter it again in **Confirm Password**.

NOTE: The LDAP user name and password details entered here are cached, so that you do not need to enter them every time you import an administrator or an email address for email notifications.
You may also enter a different Login and Password in place of these stored values when you import administrators.

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

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

9. The **CA Certificate Exists** box will be checked if the LDAPS Server Certificate has been uploaded to the GDE Appliance.

User Schema Settings

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

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

   For example: sAMAccountName or commonName

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

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

   For example: name or description

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

Group Schema Settings

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

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

Importing LDAP Administrators

The Import function allows Administrators to import data from an LDAP server such as Active Directory (AD) or OpenLDAP. Once an LDAP server has been identified and configured, the GDE Appliance Administrator can import the desired values. To set up access to an AD/LDAP repository, see, “Configuring LDAP” on page 121. You will need an LDAP login ID and password.

To import values from an LDAP directory:

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

Selecting LDAP administrators

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

- **LDAP Query**—Use the field to filter searches using the LDAP query language. Results depend on how the LDAP service is set up. See RFC2307 for full details on syntax.
- **Group**—Select a group from the drop down list.
- **User**—Enter a user name.
- **Maximum number of entries to return**— Limits the maximum number of records to import or display. The default value is 300. The minimum value is 1 and the maximum value is 10,000. A high integer value may result in a delay depending on the database size.
- **Go**—Click to refresh the screen

- **Select All**—Click to select all values on that page
- **View**—Select a value from this drop down box to control how many values appear on any page
- **Selected**—Click to select individual values.
- **User Type**—Select a value from this drop down box to define the type of Administrator or role of the values you import.
- **Add/Cancel**—Select to add or cancel your selections.

NOTE: The introduction of the multi-tenancy feature allows the creation of local domains. Each local domain can have its own specific LDAP server. The LDAP server can be configured by the local domain administrator, or a local administrator of type Domain and Security.

Selecting LDAP users for email notifications

The GDE Appliance can be configured to send email notifications about fatal and error conditions on the GDE Appliance. This can be done at a system level outside a domain, at a global domain level, or at a local domain level. System level and global domain level administrators use system level LDAP servers and local domain level administrators use local domain level LDAP servers.

To select LDAP users to receive email notifications, do the following:

1. Select **System > Email Notification**.

NOTE: If an SMTP server has not been configured, the following message is displayed “SMTP is not set.” Click the **SMTP Server** tab to configure an SMTP server. A warning will also be displayed if the SMTP server is not correctly configured.

2. Click **Add** to add a group of users who will receive an email notification

   The *Add Email Notification Group* window has the following fields that must be configured to enable notifications:

   - **Email Group Name**—Name of the email group that will receive the email notification.
   - **Email Address List**—Email addresses that will receive this email notification. Separate addresses with commas.

     If LDAP is configured, you can select addresses from your LDAP address book by clicking **Select**. The *Connect to AD/LDAP Server* window opens. If the Login and Password were entered under **LDAP Server Settings** on the *AD/LDAP Details* window, these values will be populated and do not need to be re-entered. If it’s not configured, you can enter your login and password to access it. Select the check boxes for those users who are to receive the notifications and click **Add**.

- **Email Subject**—Text you want on the subject line.
- **Notification Type**—Generic, Key Expiration, Certificate Expiration. The Generic option is visible both inside and outside a domain, the Key Expiration and Certificate Expiration options are visible only inside a domain.
- **Email Threshold Level**—Select either ERROR or FATAL. If the GDE Appliance generates a log message with a severity of this specified threshold level, then an email notification is generated. The ERROR threshold option sends log messages about errors and fatal errors since fatal is a subset of error. The FATAL threshold option sends only log messages about fatal errors.
- **Message Contains**—This is a string filter that works with the Email Threshold Level. Only messages containing this string will be sent as an email notification. If left blank, then all messages meeting the threshold criteria will be sent.
- **Enabled**—A check box that enables or disables email notification to the group.

3. Click **OK**.

12 Multifactor Authentication

Multifactor authentication increases access control to the GDE Appliance Management Console by requiring GDE Appliance administrators to enter the value or token code displayed on an RSA SecurID token, along with the administrator name, each time the administrator logs into the Management Console.

This chapter contains the following sections:

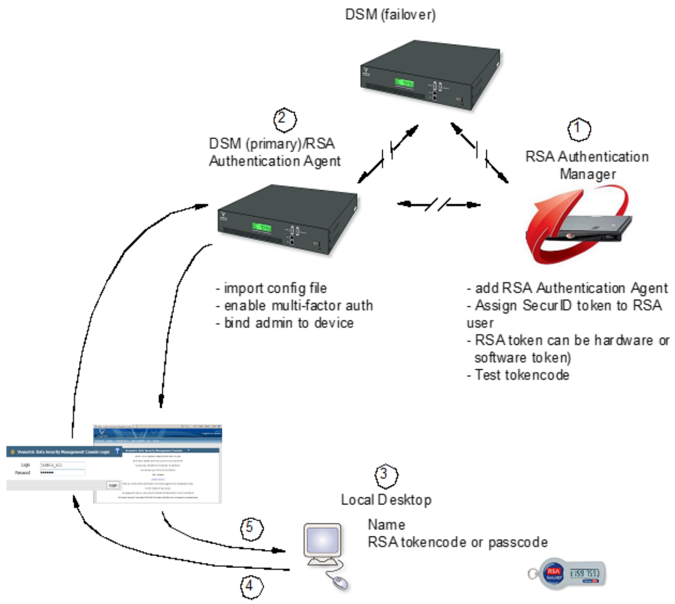
Overview

Multifactor authentication on the GDE Appliance comprises the GDE Appliance, the RSA Authentication Manager, the RSA Authentication Agent, and an RSA SecurID token. The usual sequence is:

- Configure the primary and failover GDE Appliances in the same cluster as RSA Authentication Agents in the RSA Security Console.
- Create an RSA user ID in the RSA Security Console window.
- Assign the SecurID token to the RSA User ID.
- Test the SecurID token in the RSA self-service console to make certain it is working properly.
- Import the RSA Authentication Agent file into the Management Console.
- Associate the RSA user ID to a GDE Appliance administrator.
- Enable multifactor authentication.

From this point on, a GDE Appliance administrator must enter the GDE Appliance administrator name, the RSA static PIN (if the GDE Appliance administrator ID requires the use of one), and the value displayed on the SecurID token known as a token code, to log into the GDE Appliance Management Console.

Figure 1: Configuring multifactor authentication


DSM (failover)
2
DSM (primary)/RSA Authentication Agent
1
RSA Authentication Manager
- import config file
- enable multi-factor auth
- bind admin to device
- add RSA Authentication Agent
- Assign SecurID token to RSA user
- RSA token can be hardware or software token)
- Test tokencode
3
Local Desktop
Name
RSA tokencode or passcode
5
4

Configuring RSA Authentication

The RSA Authentication Agent is the intermediary between GDE Appliance and the RSA Authentication Manager. The RSA Authentication Agent intercepts an access request from the GDE Appliance and directs the request to the RSA Authentication Manager server for authentication.

An initial link between GDE Appliance and the RSA Authentication Manager is created when an RSA configuration file, `sdconf.rec`, is imported into the GDE Appliance Management Console. The first time the RSA Authentication Agent authenticates an administrator with the RSA Authentication Manager, the RSA Authentication Agent node secret is copied and embedded in the GDE Appliance.

The `mfauth` CLI command is run *only* on the primary GDE Appliance—the `mfauth` command cannot be run on the failover—to enable multifactor authentication for the entire HA cluster.

You can delete the node secret using the `mfauth clean` CLI command. If you delete the node secret, also delete it from the RSA Security Console, and vice versa. This command removes the SecurID file from GDE Appliance. A replacement node secret file is automatically downloaded to GDE Appliance the next time a GDE Appliance administrator logs in with an RSA token code

You must regenerate the node secret file in the RSA Authentication Manager if the GDE Appliance installation is destroyed and rebuilt because the GDE Appliance authentication credentials are no longer valid.

Multifactor authentication status information is displayed on the GDE Appliance *Logs* page.

Once multifactor authentication is configured, RSA Authentication Manager and GDE Appliance startup/shutdown sequence is important.

- Start the RSA Authentication Manager *before* the GDE Appliance.
- Shutdown the GDE Appliance *before* the RSA Authentication Manager.

This sequence is required to ensure that the RSA Authentication Agent can reliably access the RSA Authentication Manager.

Applying RSA authentication to a GDE Appliance administrator

Check the following before you configure multifactor authentication:

- Ensure that the RSA server and the GDE Appliance can communicate with each other via FQDN.
- If multifactor authentication is already configured, delete the node secret.

NOTE: You will also have to clear the node secret on the RSA Authentication Manager server as well if multifactor authentication is already configured.

```
0001:system$ mfauth clean
WARNING: Cleaning RSA secret file will break the communication between
the security server and RSA server!
Continue? (yes|no)[no]:yes
SUCCESS: RSA secret file is removed.
0002:system$
```

If multifactor authentication is already configured you will also have clear the node secret on the RSA Authentication Manager Security Console. Click **Access > Authentication Agents > Manage Existing**. Select **Authentication Agent > Manage Node Secret**. Check **Clear the node secret** box and click **Save**.

Configuring multifactor authentication

1. Log on to the RSA Authentication Manager Security Console.
2. Add the GDE Appliance as an RSA Authentication Agent. Click **Access > Authentication Agents > Add New**.

When adding the Agent Host Record, you should configure the Agent Type as a Communication Server. This setting is used by the RSA Authentication Manager to determine how communication with the GDE Appliance will occur.

3. Enter the GDE Appliance's IP address, resolve the IP address, then click **Save**.

   GDE Appliance host names configured in the RSA Authentication Manager must resolve to valid IP addresses on the local network.

4. Generate the configuration file from the RSA Authentication Manager Security Console, under **Access > Authentication Agents > Generate Config File**.

5. Upload the generated configuration file (`sdconf.rec`) to the GDE Appliance. **Click System > Upload RSA Configuration File**. On the Upload RSA Configuration File page, click **Browse** to select the file, click **Ok**.

   If the GDE Appliance has more than one IP address configured, select the IP address that was used to configure the GDE Appliance on the RSA Authentication Manager server from the pull-down menu

   The `sdconf.rec` file is stored in a .zip file and must be extracted. Each GDE Appliance instance in the RSA realm must use the same `sdconf.rec` file.

6. On the GDE Appliance Management Console, open the Add Administrator or Edit Administrator window.

   a. Enter the usual GDE Appliance administrator name, description, password and confirm password in the respective text-entry boxes, and select the desired administrator type.

   b. Enter the RSA User ID provided by the RSA administrator in the RSA User ID text-entry field.

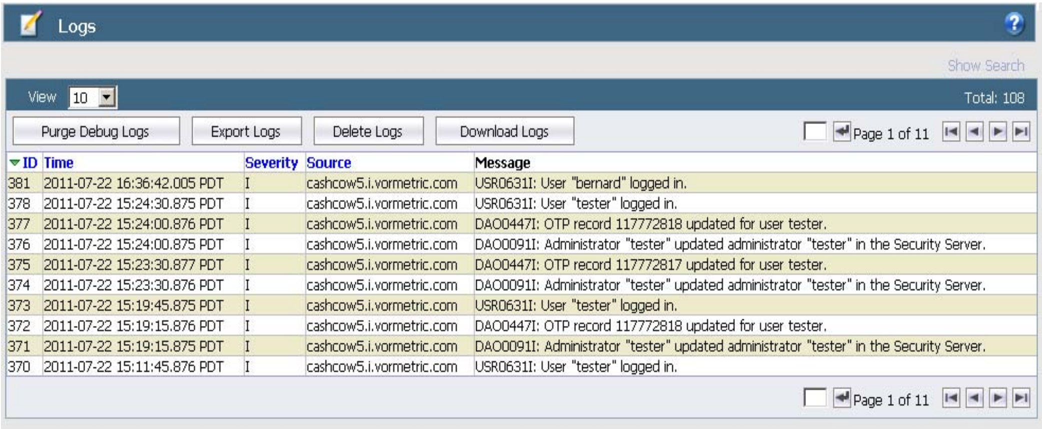
   c. Click **Ok**.

7. Enable multifactor authentication. This is done via the GDE Appliance CLI console on the primary GDE Appliance server. Access the CLI console and type;

```
0009:vormetric$ system

0010:system$ mfauth on

WARNING: After enabling the administrator multiple factor authentication, the
security server software will start to validate the extra one-time password!

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

SUCCESS: administrator multiple factor authentication enabled.

0011:system$
```

You can view multifactor authentication activity in the Logs window from outside a domain.

Figure 2: Log entries showing administrator login activity



ID	Time	Severity	Source	Message
381	2011-07-22 16:36:42.005 PDT	I	cashcow5.i.vormetric.com	USR0631I: User "bernard" logged in.
378	2011-07-22 15:24:30.875 PDT	I	cashcow5.i.vormetric.com	USR0631I: User "tester" logged in.
377	2011-07-22 15:24:00.876 PDT	I	cashcow5.i.vormetric.com	DAO0447I: OTP record 117772818 updated for user tester.
376	2011-07-22 15:24:00.875 PDT	I	cashcow5.i.vormetric.com	DAO0091I: Administrator "tester" updated administrator "tester" in the Security Server.
375	2011-07-22 15:23:30.877 PDT	I	cashcow5.i.vormetric.com	DAO0447I: OTP record 117772817 updated for user tester.
374	2011-07-22 15:23:30.876 PDT	I	cashcow5.i.vormetric.com	DAO0091I: Administrator "tester" updated administrator "tester" in the Security Server.
373	2011-07-22 15:19:45.875 PDT	I	cashcow5.i.vormetric.com	USR0631I: User "tester" logged in.
372	2011-07-22 15:19:15.876 PDT	I	cashcow5.i.vormetric.com	DAO0447I: OTP record 117772818 updated for user tester.
371	2011-07-22 15:19:15.875 PDT	I	cashcow5.i.vormetric.com	DAO0091I: Administrator "tester" updated administrator "tester" in the Security Server.
370	2011-07-22 15:11:45.876 PDT	I	cashcow5.i.vormetric.com	USR0631I: User "tester" logged in.

Additional RSA configuration notes

The following are additional points to consider when configuring or troubleshooting an RSA configuration.

- If you are configuring an existing GDE Appliance Authentication Agent setup, go to Access -> Authentication Agents -> Manage Existing. Choose Authentication Agent -> Manage Node Secret, check Clear the node secret, and save it.
- If you are configuring a new GDE Appliance Authentication Agent setup, you do not need to go to Manage Node Secret.

The RSA Authentication Manager server requires the IP address and hostname of the GDE Appliance. If DNS is configured, the IP address or hostname can be resolved from the RSA Authentication Manager Security Console.

Or you can edit the `/etc/hosts` file on the GDE Appliance and add the GDE Appliance IP address and host name. Use the host name to configure the RSA Authentication Agent.

Viewing and Downloading System-Level Reports

13

The GDE Appliance comes with pre-configured reports that display system information. All reports can be downloaded and saved locally in CSV format.

This chapter includes the following sections:

- “Overview”
- “Viewing and Downloading Reports”
- “System-Level Reports”

Overview

All reports are under the **Reports** tab. The availability of reports depends on the GDE Appliance administrator type and privileges, and whether the administrator is currently in or out of a domain.

- Administrators of type All can access all system reports and global domain reports. See “Viewing and Downloading Domain-Level Reports” for more information about domain-level reports.
- Administrators of type System can access system reports outside global domains.

Viewing and Downloading Reports

To view a report, click the **Report** tab on the Management Console, and then click the name of the report.

To save the report as a CVS file to your local machine, click **Download** at the top left of the report table.

System-Level Reports

The following reports are available to administrators of type All and System:

- "Administrators"
- "Servers"
- "Security Domains"
- "System License Usage Summary"
- "Executive Summary"

You must be outside of a domain to access system-level reports.

Administrators

The Administrators report is a table of administrators with access to the GDE Appliance.

Column Name	Description
User Name	Login
User Type	System Administrator, Security Administrator, Domain Administrator, Domain and Security Administrator, and All
LDAP User ID	The UserID of a user imported from LDAP
Last Login Time	The time of this user's last login. Timestamps are in the form *YYYY-MM-DD HH:MM:SS* where *Y*=year, *M*=month, *D*=day, *H*=hour, *M*=minute, *S*=second

Servers

The GDE Appliance Servers report is a table of primary and failover GDE Appliance servers.

Column Name	Description
Server Name	FQDN of the GDE Appliance
Up Time	How long the GDE Appliance has been active
Role	Primary or failover

Security Domains

The Security Domains report is a table of Security domains managed by this GDE Appliance.

Column Name	Description
Organization	Name of the organization responsible for this domain
Domain Name	Name of the domain set when the domain was created.
Description	User added information
Help Desk Information	Phone number of tech support
Domain Administrators	Names of the Domain Administrators assigned to this domain.
Security Administrators	Names of the Security Administrators assigned to this domain.
Domain and Security Administrators	Names of the GDE Appliance administrators of type Domain and Security assigned to this domain.
All Administrators	Names of the GDE Appliance administrators of type All who can access this domain.

System License Usage Summary

The System License Usage Summary report provides a system level overview of all licenses used by the GDE Appliance.

Column Name	Description
Agent Type	Type of agent license; VTE (FS), VAE (Key)
License Type	Type of license used in a domain; Perpetual, Term, or Hourly
Total Agents Licensed	Total number of agent licenses available on the system
Agents Licensed to Domains	Total number of agent licenses available to domains
Agent Licenses Used	Total number of agent licenses used
Logical Cores Used	Total number of logical CPU cores used by the GDE Appliance
Total Logical Core Hour Licenses	Total number of logical CPU core hour licenses available
Logical Core Hours Licensed to Domains	Total number of logical CPU core hour licenses allocated to domains
Logical Core Hour Licenses Used	Total number of logical CPU core licenses used by the GDE Appliance
LDT Enabled Hosts	Total number of hosts using VTE Agent licenses with LDT enabled
Docker Enabled Hosts	Total number of hosts using VE Agent licenses with Docker enabled

Column Name	Description
Term Expiration Date	Expiration date of a term license used in a domain, if applicable

Executive Summary

The Executive Summary Report shows the totals for the following entities:

- Asymmetric Keys
- GuardPoints
- Hosts (Encryption Expert agents)
- Policies
- Security Domains
- Security Server Administrators
- Security Servers
- Symmetric Keys

Part II: GDE Appliance Domain Administrators

GDE Appliance System Administrators create domains but do not operate within them; however, all tasks done by the GDE Appliance Domain Administrators and GDE Appliance Security Administrators occur within domains. The GDE Appliance Domain Administrators and GDE Appliance Security Administrators must always know what domain they are in before doing any task. If you log in as a GDE Appliance Domain Administrator or a GDE Appliance Security Administrator, and you notice that the administrator, host, or log data is unexpected, you are most likely in the wrong domain.

GDE Appliance Domain Administrators add additional Domain Administrators to each domain. A Global Domain Administrator can be a member of multiple domains. GDE Appliance Domain Administrators who are members of multiple domains can easily switch between the domains. GDE Appliance Domain Administrators also add GDE Appliance Security Administrators to a domain and assign *roles* to these Security Administrators (for example, *Audit*, *Key*, *Policy*, *Host*, *Challenge & Response,* and/or *Client Identity*) that are applied only within that domain. Local or restricted Domain Administrators are restricted to a particular domain. The first Domain Administrator is added to a restricted domain by the GDE Appliance System Administrator. After that the local Domain Administrator creates and adds other Domain or Security Administrators to the Domain as required. Local Domain Administrators and Security Administrators are members of the local domain they are created within, they cannot be members of any other domain. Once created and assigned to a local domain, they are not visible to administrators of other domains.

GDE Appliance Domain Administrators cannot remove domains and cannot perform in any of the domain security roles.

GDE Appliance Domain Administrators do the following tasks:

- "Adding and Removing GDE Appliance Domain Administrators"
- "Configuring Syslog Server for Application-Level Messages"
- "Viewing and Downloading Domain-Level Reports"
- "Viewing GDE Appliance Preferences and Logs"

Adding and Removing GDE Appliance Domain Administrators

14

A GDE Appliance Domain Administrator can:

- Enable and disable GDE Appliance Domain Administrator and Security Administrator accounts in the current domain (global Domain Administrators).
- Create, delete, import, enable or disable GDE Appliance Domain Administrator and Security Administrator accounts in the current domain (local or restricted Domain Administrators).
- Configure GDE Appliance Security Administrator roles (Audit, Key, Policy, Host, Challenge & Response, Client Identity).

When a GDE Appliance Domain Administrator changes the configuration of a Security Administrator or another Domain Administrator, the current Management Console session for that administrator is terminated and that administrator must log back in. If a Domain Administrator is removed from a domain, the Domain Administrator cannot switch to or do any work in that domain.

Assigning Domain Administrators or Security Administrators to Domains

There are two types of Domain Administrators that can be created on the GDE Appliance, global Domain Administrators and Local (or restricted) Domain Administrators.

A GDE Appliance System Administrator adds the first Domain Administrator to a global domain. A global Domain Administrator can add additional administrators (Domain, and Domain and Security) to domains and remove these administrators from domains. But, a global Domain Administrator cannot delete administrator accounts.

A GDE Appliance System Administrator adds the first Domain Administrator to the restricted domain. The local Domain Administrator can then create new administrators (Domain, Security, or Domain and Security), in the domain, or import LDAP users and make them Domain, Security, or Domain and Security Administrators within the local domain. A local Domain Administrator can also delete those administrator accounts.

A GDE Appliance System Administrator, can delete global Domain Administrators, but cannot delete local Domain Administrators as they are not visible to the System Administrator. The

GDE Appliance System Administrator can, however, disable the local Domain Administrator that they added to a local domain.

Add Global Domain or Security Administrators to a domain

1. Log in as an administrator of type Domain, Domain and Security, or All. The *Dashboard* window opens.
2. Switch to the domain to which you want to add Domain or Security Administrators.

   a. Select **Domains > Switch Domains**.

   The *Domains* window opens. All the domains in which the current GDE Appliance Administrator (of type Domain, Security, Domain and Security, or All) is a member, are displayed. The **Selected** radio button of the current domain is grayed out and cannot be selected.

   b. Select the radio button of the domain.

   If the domain is not listed, ask the GDE Appliance Administrator (of types Domain, Security, Domain and Security, or All) for that domain to add you to it.

   c. Click **Switch to Domain**. The *Domains* window is redisplayed.
3. Select **Administrators > Domain**. The *Administrators* window opens and displays all the GDE Appliance Administrators (of types Domain, Security, Domain and Security, or All) who are members of the current domain.
4. Click **Add to Domain**. The *Available Administrators* window opens. This window lists all the GDE Appliance Administrators (of types Domain, Security, Domain and Security, and All) who are not already assigned to the current domain.
5. Enable the **Selected** check box of the Administrator you want to add to the current domain.
6. If you are adding an administrator of type Security Administrator, you also need to assign roles to that Security Administrator. Select the administrator role check boxes (Audit, Key, Policy, Host, Challenge & Response, and/or Client Identity) to enable these features.

   Administrators of type Domain and Security Administrator are automatically assigned the following roles: Key, Policy, Host, Challenge & Response and Client Identity. If you want a Domain and Security Administrator to have the Audit role, you must enable that role by selecting the checkbox for Audit.
7. Click **Ok**. The GDE Appliance Administrators added to the domain are now active.

Add Local Domain or Security Administrators to a restricted domain

1. Log on to the GDE Appliance as an administrator of type Domain, Domain and Security, or All with your local Domain Administrator credentials. You must select the **I am a local domain**

administrator check box, and then enter the local domain name in the **Domain Name** field. The *Dashboard* window opens.

2. Navigate to the *Administrators* window.
3. Click **New** to create a new Domain, Security, or Domain and Security Administrator.
4. In the *Add Administrators* window, enter the following information:
    - **Login**—Type a user name for the administrator, it must contain at least 5 characters with an upper limit of 36 characters. Only one instance of an administrator name is allowed.
    - **Description**—(Optional) Enter a description that helps you identify the administrator. The maximum number of characters for this field is 256.
    - **Password**—Enter a password for the administrator. The password must conform to the attributes defined in the password preferences, the maximum password length is 256 characters. The newly created administrators will have to change this password the first time they log on to the GDE Appliance.
    - **Confirm Password**—Re-type the password to confirm.
    - **User Type**—Select the type of administrator to create; Domain Administrator, Security Administrator, or Domain and Security Administrator.
    - **Read-Only User**—Select this check box to create an administrator with read-only privileges. You can assign read-only privileges to any type of administrator—except for Local Domain administrators that are the first administrators to be assigned to a domain. If the first administrator added to a local domain is read-only, that administrator will not be able to create any more administrators for that domain.
5. Click **Ok**. The new administrator is displayed in the table on the Administrators page.
6. Click **Import** to import LDAP users to assign as GDE Appliance Administrator types. You have to have an LDAP Server configured in order to import these users, see “LDAP Configuration” on page 121 for details.
7. Enter the Login and Password for the LDAP server. If the Login and Password were entered under **LDAP Server Settings** on the AD/LDAP Details window, these values will be populated and do not need to be re-entered. You may also enter a different Login and Password in place of these stored values when you import administrators. Click **Connect**. The *LDAP Users* window displays LDAP user names.
8. Select LDAP Users:

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

    - **LDAP Query**—Use the field to filter searches using the LDAP query language. Results depend on how the LDAP service is set up. See RFC2307 for full details on syntax.
    - **Group**—Select a group from the drop down list.
    - **User**—Enter a user name.

- **Maximum number of entries to return**— Limits the maximum number of records to import or display. The default value is 300. The minimum value is 1 and the maximum value is 10,000. A high integer value may result in a delay depending on the database size.
- **Go**—Click to refresh the screen
- **Select All**—Click to select all values on that page
- **View**—Select a value from this drop down box to control how many values appear on any page
- **Selected**—Click to select individual values.
- **User Type**—Select a value from this drop down box to define the type of Administrator or role of the values you import.
- **Add/Cancel**—Select to add or cancel your selections.

GDE Appliance Security Administrator Roles

A GDE Appliance Security Administrator can be configured with one or more roles. Domain Administrators assign roles when they assign a Security Administrator to a domain. The roles are applicable only in the current domain. A Security Administrator can be assigned different roles in different domains. Table 1 lists the GDE Appliance Security Administrator roles.

Table 1: Security Administrator roles and permitted tasks

Role	Description
Audit	The audit role can only view log data.
Key	The key role can create, edit, and delete local key-pairs, public keys, and key groups. Administrators with this role can also view log data.
Policy	The policy role can create, edit, and delete policies. Administrators with this role can also view log data.
Host	The Host role can configure, modify, and delete hosts and host groups. Administrators with this role can also view log data. The Challenge & Response role is automatically selected when the Host role is selected.

Role	Description
Challenge & Response	The Challenge & Response role must be enabled for a Security Administrator to view the Host Password Challenge & Response window. The window is used to enter a challenge string and display the response string. The response string is a temporary password that a system user enters to decrypt cached encryption keys when there is no connection to the GDE Appliance. The Challenge & Response role is automatically enabled when the Host role is enabled. You may disable the Host role afterwards to leave just the Challenge & Response role enabled. With just this role enabled, the Security Administrator has access to the Dashboard, **Domains > Switch Domains**, and **Hosts > Host Password Challenge & Response** menus only. A Security Administrator can open both the **Hosts > Host Password Challenge & Response** window and the **Hosts > Hosts > Challenge Response** tab with the Host and Challenge & Response roles assigned. With just the Challenge & Response role assigned, the Security Administrator can open only the **Hosts > Host Password Challenge & Response** window.
Client Identity	The Client Identity role must be enabled for a Security Administrator to create Identity-Based Key Access. A client identity is used to control access to encryption keys on the GDE Appliance by VAE host administrators.

Assigning Security Administrator Roles

NOTE: If a GDE Security Administrator is logged in when you assign or change their role(s), that administrator’s Management Console session is terminated and they must log on again.

To assign role(s) to a Security Administrator:

1. Log on as a Domain Administrator. The *Dashboard* window opens.
2. If you are not already in it, switch to the desired domain.
   a. Select **Domains > Switch Domains**. The *Domains* window opens. All domains in which the current Domain Administrator is a member are displayed. The **Selected** radio button of the current domain is opaque and cannot be selected.
   b. Select the radio button of the desired domain. If the desired domain is not listed, ask the GDE Appliance Domain Administrator to add you to that domain.
   c. Click **Switch to Domain**. The **Domains** window opens.
3. Select **Administrators > Domain**. The *Administrators* window opens and displays all the Domain Administrators and Security Administrators who are members of the current domain.
4. Select an administrator in the **Login** column. The *Assign Roles* window opens.
5. Enable or disable the **Selected** check boxes for the roles that you want to assign the current administrator. Click **Ok**.

Configuring Syslog Server for Application-Level Messages

15

This section describes how to add a remote Syslog server to your system, and how to control the severity level and format of the messages that the GDE Appliance sends to the Syslog server.

You can configure a Syslog server to receive the same messages that are sent to the Logs window of the Management Console. Use the **System> Log Preferences** menu to create templates that apply to logging configurations for all of the Agents.

This chapter contains the following sections:

Overview

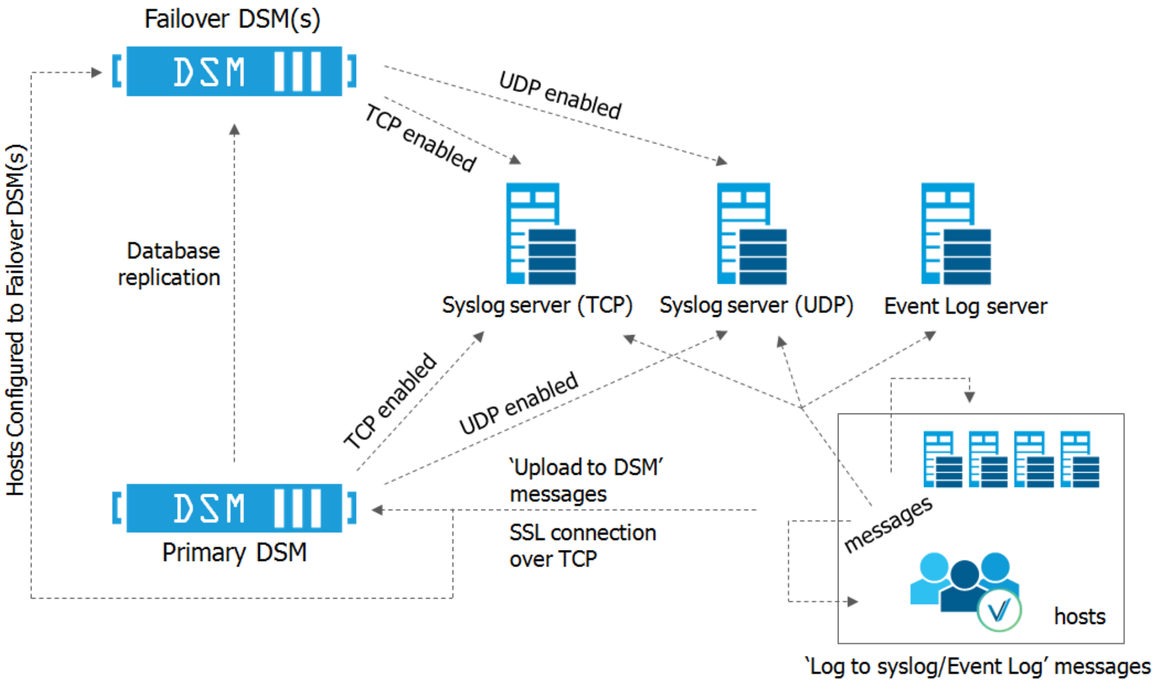
Agent log data is generated on agent hosts. The log data is placed in `/var/log/vormetric` on a UNIX system or in `C:\Documents` or `Settings\All Users\Application Data\Vormetric\DataSecurityExpert\agent\log` on a Windows system, when the **Log to File** logging preference is enabled. The log data can also be forwarded to a Syslog or Event Log server when the Log to **Syslog/Event Log** logging preference is enabled.

NOTE: Ensure that the `/var` directory in your system has 256KB to 1MB available for logging to ensure proper GDE Appliance behavior.

When **Log to Syslog/Event Log** is enabled, the host administrator can choose to do nothing, which causes log data to be placed into a local `/var/log/messages` or `/var/adm/messages` file, or into the local Windows Event Log, or the host administrator can configure the agent to forward log data to a remote Syslog server or Event Log server. The host administrator can upload the log data to a remote server using the preferred transport protocol. The GDE Appliance is not used to configure the remote log servers for host systems.

The **Syslog Server** window in the Management Console lets you configure the remote Syslog servers to which to send GDE Appliance log data. The log data sent to remote Syslog servers consists of log data that is generated on the GDE Appliance and, when **Upload to Server** is enabled in the **Log Preferences** window, log data that is generated on hosts. The GDE Appliance administrator then configures the GDE Appliance to forward log data to a Syslog server using either UDP protocol or TCP protocol.

Figure 3: Handling log messages



Items to consider before configuring Syslog logging include:

- Only administrators of type System Administrator, Domain Administrator, or All can configure Syslog messaging within a domain.
- If Syslog servers are configured in a domain, only events that take place in that domain are logged to the Syslog servers.

- A default Syslog port number is not provided. The usual industry standard port number for Syslog over UDP is 514. Port 1468 has been used successfully for TCP.
- Configuring a Syslog server is an effective way to consolidate the logs of all the GDE Appliances in an HA configuration in one central repository. The failover GDE Appliances in an HA cluster deployment have the same configuration as the primary server node. The failover nodes forward log data to the same Syslog server(s) as the primary GDE Appliance. Therefore, each failover must have network access to the Syslog servers configured on the primary.

Supported Syslog Formats

The GDE Appliance supports the following log formats:

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

Plain Message

Originally, GDE Appliance Syslog supported only Plain Message format. While simple and efficient, this format did not allow for user enhanced reporting or customization.

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

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

Table 2: Syslog message parameters and descriptions

Parameter	Description
`12-07-201216:53:02`	Date and time
`Local7.Debug`	Message priority
`10.3.32.231`	Sending machine’s IP address
`2012-12-08 01:01:58.709`	Date and time of logged event
`vormetric`	Originator tag
`SOURCE[linux64-32231.qa.com]`	Source of message

Parameter	Description
DAO0445I	Unique message ID
Administrator voradmin added SysLog Host 10.3.25.168	Plain text message of the logged event

Common Event Format (CEF) log format

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

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

```
<27> 2012-10-16T16:01:44.030Z centos-6-0 CEF:0|Vormetric, Inc.|vee-
fs|5.1.0.9026|CGP2604E| Reject access|7|logger=CGP spid=6362 cat=[ALARM]
pol=AuditAllExceptLp uinfo=lp,uid\=4,gid\=7\\lp\\ sproc=/bin/ls
act=read_dir_attr gp=/Guard filePath=/datafiles/file.dat denyStr=DENIED
showStr= Code (1M)
```

Table 3: CEF Log Format parameters and descriptions

Parameter	Description
<27>	A standard Syslog facility/priority code
2012-10-16T16:01:44.030Z	Date and time
centos-6-0	The host name of the machine sending the message.
CEF:0	Version of the CEF
Vormetric, Inc.	Sending device vendor
vee-fs	Sending device product
5.1.0.9026	Sending device version
CGP2604E	Unique message ID
Reject access	Name: A human-readable and understandable description of the event.
7	Severity: An integer that reflects the importance of the event. Only numbers from 0 to 10 are allowed, where 10 indicates the most important event.

Parameter	Description
`logger=CGP spid=6362 cat=[ALARM] pol=AuditAllExceptLp uinfo=lp,uid\=4,gid\=7\\lp\\ sproc=/bin/ls act=read_dir_attr gp=/Guard filePath=/datafiles/file.dat denyStr=DENIED showStr= Code (1M)`	Extension: A collection of key-value pairs. The keys are part of a predefined set. The standard allows for including additional keys. An event can contain any number of key-value pairs in any order, separated by delimiting characters.

RFC5424

Vormetric Syslog supports RFC5424 log format.

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

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

Table 4: CEF Log Format parameters and descriptions

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

Log Event Extended Format (LEEF)

The GDE Appliance supports Log Event Extended Format (LEEF). The LEEF header is pipe (“|”) separated and attributes are tab separated.

Adding a Syslog Server

To add a Syslog server:

1. Verify that one or more Syslog servers are accessible from the GDE Appliance system. It is usually enough to ping the Syslog server and run ps to check the Syslog process on the Syslog server system.

   If you are going to send the messages to the local host, verify that the syslogd process on the local host is accepting messages. You may need to restart syslogd with the “-r” argument.

   NOTE: Record the Syslog transport protocols and port numbers of the Syslog server(s). You will need this information later.

2. Set the severity level at which to send messages to the Syslog server in the /etc/syslog.conf file on the agent host.

   Severity levels in the Log Preferences window are DEBUG, INFO, WARN, ERROR, and FATAL. Severity levels are cumulative, so each level includes the levels below it. For example, FATAL logs only FATAL messages, whereas WARN logs WARN, ERROR, and FATAL messages. To ensure that the Syslog server gets the messages set in the Log Preferences window, set the level in the syslog.conf file to debug and direct the output to the local messages file. For example, on a Solaris system, set the output file path to /var/adm/messages.

   ```
   user.debug /var/adm/messages
   ```

3. Log on to the Management Console as an administrator of type System Administrator or All.
4. Select **System > General Preferences**. The **General Preferences** window opens to the **General** tab.
5. Click the **System** tab, and then select **Syslog Enabled**.

   This enables communication between the GDE Appliance and the Syslog server.

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

6. Click **Apply**.

7. Select **System > Log Preferences**. The *Log Preferences* window opens to the *Server* tab.
8. Set the **Logging Level** property.

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

   Redundant Syslog failure messages are filtered so that only one out of every fifty redundant messages is sent to `/var/log/messages` and the *Logs* window. All the redundant Syslog failure messages are sent when the level is set to DEBUG.
9. Click **Apply**.
   - If you are configuring a Syslog server to receive domain-level log data, and are logged in as an administrator of type All, remain logged in and enter the domain to be configured.
   - If you are configuring a Syslog server to receive domain-level log data, and are logged in as an administrator of type System Administrator, log out and log back in as a user of type Domain Administrator, or All, and enter the domain to be configured.
10. Select **Log > Syslog**. The **Syslog Server** window opens.
11. Click Add and enter the following information:

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

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

    In the interests of security, Vormetric recommends that you use a root certificate rather than a non-root certificate.

NOTE: For Syslog servers configured with the UDP transport protocol, ensure that UDP packets are not blocked by a firewall or switch rules. Also, verify that the Syslog server is logging messages as expected.
If you add a Syslog certificate when using TLS protocol, you may need to restart the server. To this you need to do a `system > server restart` from the CLI. After restart, verify that the Syslog server is logging messages as expected.

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

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

    You may configure multiple Syslog servers but only one instance of a Syslog server name is allowed in the GDE Appliance database.

12. Click **Ok**. Perform a task on an agent system that normally generates a Syslog entry, such as accessing a GuardPoint.
13. Check the `/var/log/messages` file on the Syslog server for GDE Appliance log entries.

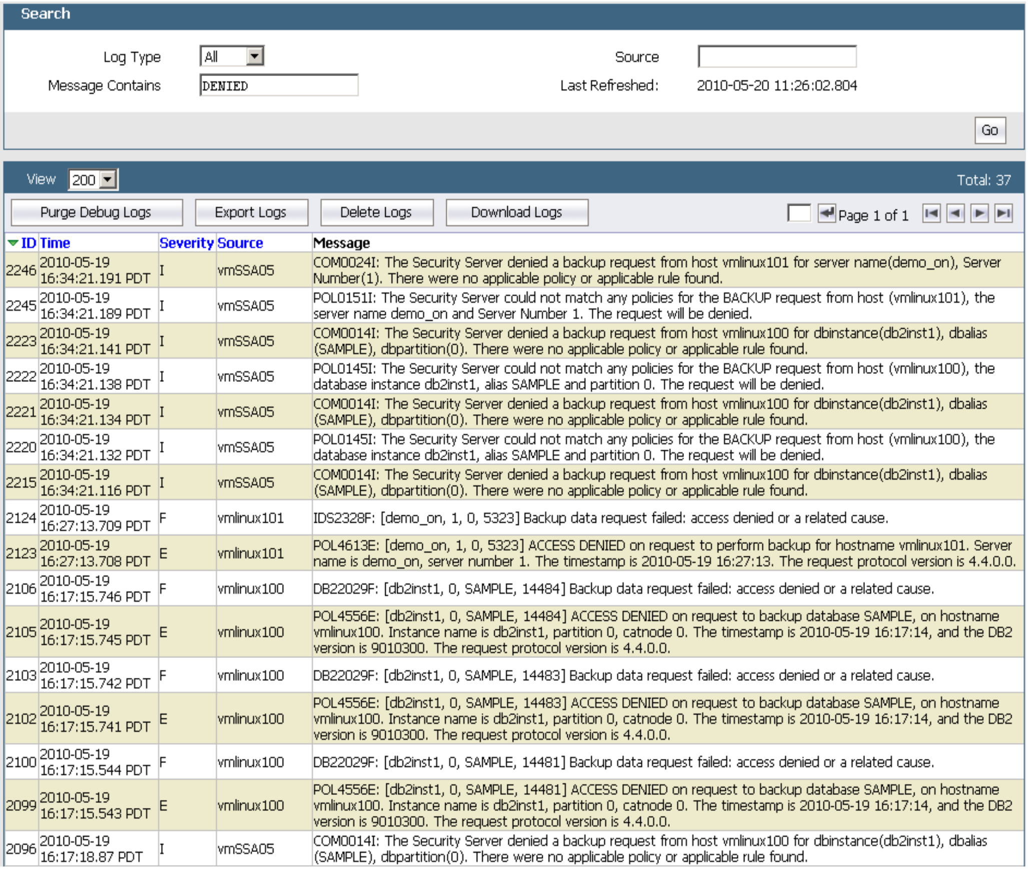
Using Syslog to Troubleshoot the GDE Appliance and Agents

Syslog entries for GDE Appliance activity indicate the source of the Syslog message (system name after the timestamp), the source of the message itself (SOURCE), the log level (AUDIT, ALARM, and so on), and much more.

Analyzing log entries

The format and content of log entries for File System Agents are described below.

Figure 4: Message Log entries



Log Type: All
Message Contains: DENIED
Source:
Last Refreshed: 2010-05-20 11:26:02.804

ID	Time	Severity	Source	Message
2246	2010-05-19 16:34:21.191 PDT	I	vmSSA05	COM0024I: The Security Server denied a backup request from host vmlinux101 for server name(demo_on), Server Number(1). There were no applicable policy or applicable rule found.
2245	2010-05-19 16:34:21.189 PDT	I	vmSSA05	POL0151I: The Security Server could not match any policies for the BACKUP request from host (vmlinux101), the server name demo_on and Server Number 1. The request will be denied.
2223	2010-05-19 16:34:21.141 PDT	I	vmSSA05	COM0014I: The Security Server denied a backup request from host vmlinux100 for dbinstance(db2inst1), dbalias (SAMPLE), dbpartition(0). There were no applicable policy or applicable rule found.
2222	2010-05-19 16:34:21.138 PDT	I	vmSSA05	POL0145I: The Security Server could not match any policies for the BACKUP request from host (vmlinux100), the database instance db2inst1, alias SAMPLE and partition 0. The request will be denied.
2221	2010-05-19 16:34:21.134 PDT	I	vmSSA05	COM0014I: The Security Server denied a backup request from host vmlinux100 for dbinstance(db2inst1), dbalias (SAMPLE), dbpartition(0). There were no applicable policy or applicable rule found.
2220	2010-05-19 16:34:21.132 PDT	I	vmSSA05	POL0145I: The Security Server could not match any policies for the BACKUP request from host (vmlinux100), the database instance db2inst1, alias SAMPLE and partition 0. The request will be denied.
2215	2010-05-19 16:34:21.116 PDT	I	vmSSA05	COM0014I: The Security Server denied a backup request from host vmlinux100 for dbinstance(db2inst1), dbalias (SAMPLE), dbpartition(0). There were no applicable policy or applicable rule found.
2124	2010-05-19 16:27:13.709 PDT	F	vmlinux101	IDS2328F: [demo_on, 1, 0, 5323] Backup data request failed: access denied or a related cause.
2123	2010-05-19 16:27:13.708 PDT	E	vmlinux101	POL4613E: [demo_on, 1, 0, 5323] ACCESS DENIED on request to perform backup for hostname vmlinux101. Server name is demo_on, server number 1. The timestamp is 2010-05-19 16:27:13. The request protocol version is 4.4.0.0.
2106	2010-05-19 16:17:15.746 PDT	F	vmlinux100	DB22029F: [db2inst1, 0, SAMPLE, 14484] Backup data request failed: access denied or a related cause.
2105	2010-05-19 16:17:15.745 PDT	E	vmlinux100	POL4556E: [db2inst1, 0, SAMPLE, 14484] ACCESS DENIED on request to backup database SAMPLE, on hostname vmlinux100. Instance name is db2inst1, partition 0, catnode 0. The timestamp is 2010-05-19 16:17:14, and the DB2 version is 9010300. The request protocol version is 4.4.0.0.
2103	2010-05-19 16:17:15.742 PDT	F	vmlinux100	DB22029F: [db2inst1, 0, SAMPLE, 14483] Backup data request failed: access denied or a related cause.
2102	2010-05-19 16:17:15.741 PDT	E	vmlinux100	POL4556E: [db2inst1, 0, SAMPLE, 14483] ACCESS DENIED on request to backup database SAMPLE, on hostname vmlinux100. Instance name is db2inst1, partition 0, catnode 0. The timestamp is 2010-05-19 16:17:14, and the DB2 version is 9010300. The request protocol version is 4.4.0.0.
2100	2010-05-19 16:17:15.544 PDT	F	vmlinux100	DB22029F: [db2inst1, 0, SAMPLE, 14481] Backup data request failed: access denied or a related cause.
2099	2010-05-19 16:17:15.543 PDT	E	vmlinux100	POL4556E: [db2inst1, 0, SAMPLE, 14481] ACCESS DENIED on request to backup database SAMPLE, on hostname vmlinux100. Instance name is db2inst1, partition 0, catnode 0. The timestamp is 2010-05-19 16:17:14, and the DB2 version is 9010300. The request protocol version is 4.4.0.0.
2096	2010-05-19 16:17:18.87 PDT	I	vmSSA05	COM0014I: The Security Server denied a backup request from host vmlinux100 for dbinstance(db2inst1), dbalias (SAMPLE), dbpartition(0). There were no applicable policy or applicable rule found.

Analyzing VTE Agent log entries

The general format of a VTE Agent log entry is:

```
CGP2602I: [SecFS, 0] Level: Policy[policyName?] User[userID?]
Process[command?] Access[whatIsItDoing?] Res[whatIsItDoingItTo?]
Effect[allowOrDeny? Code (whatMatched?)]
```

where:

- SECFS indicates that the message was generated by a VTE Agent. You can enter `secfs` in the **Search Message** text-entry box in the **Logs** window to display VTE Agent policy evaluation and GuardPoint activity for all configured hosts.
- Level indicates the importance of the message. For example, AUDIT indicates an informational message, whereas ALARM indicates a critical failure that should not go ignored.
- Policy[] indicates the name of the policy that is being used to evaluate the access attempt.
- User[] identifies the system user attempting to access data in the GuardPoint. It typically displays the user name, user ID, and group ID.
- Process[] indicates the command, script, or utility being executed.
- Access[] indicates what is being attempted. Access may be read_dir, remove_file, write_file_attr, write_app, create_file, etc. These correspond to the Access methods that you configure in the policy. read_dir corresponds to d_rd. remove_file corresponds to f_rm. And so on.
- Res[] indicates the object being accessed by Process[].
- EFFECT[] indicates the rule that matched and, based upon that rule, whether or not the GDE Appliance grants access. Access states may be either PERMIT or DENIED.

For example:

```
CGP2606E: [SecFS, 0] [ALARM] Policy[allowAllRootUsers_fs]
User[bubba,uid=1111,gid=10\wheel\] Process[/usr/bin/vim]
Action[create_file] Res[/opt/apps/apps1/lib/file1.txt]
Effect[DENIED Code (1M)]
```

The format of a rule match is:

```
intchar
```

where:

- `int` is an integer representing the security rule being used or violated. Security rules are numbered sequentially from top to bottom in the Online Policy Composer window.

- `char` is an uppercase letter indicating the item that is using or violating the policy.

Table 5: Character Codes and Their Descriptions

Character Code	Description
A	The **Action** component of a security rule failed to match.
M	All security rule components match and, unless overridden, the **Effect** for that security rule is applied.
P	The **Process** component of a security rule failed to match.
R	The **Resource** component of a security rule failed to match.
T	The time specified in the **When** component of a security rule failed to match.
U	The **User** component of a security rule failed to match.

For example, the following match codes indicate:

- **1R** – Mismatch in Resource for Security Rule 1.
- **3U** – Mismatch in User for Security Rule 3.
- **4A** – Mismatch in Action for Security Rule 4.
- **2M** – All components matched for Security Rule 2. Since all the rules matched, Security Rule 2 will be used and no other rules will be evaluated.

Log message levels

The detail and extent of information logged is determined by the selected log level. The agent supports five log levels as listed in Table 6.

Table 6: The Agent-Supported 5 Log Levels

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

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

Using log files

Check the log files to verify the successful installation and configuration of the Vormetric Data Security software, to determine why a backup or restore operation failed, or to monitor Vormetric Data Security activity.

A logged event falls into one of the following categories:

- **Operational status.** The result of any significant action performed by an VTE Agent or GDE Appliance is logged.
- **Administrative activity.** The result of any maintenance or administrative activity on the GDE Appliance is logged (for example, a key has been created or exported).
- **System status.** The result of any system errors are logged (for example, if the database connection is interrupted).
- **Policy-specified audit.** If the result of a policy evaluation specifies that it should be audited, then a suitable message is logged.

Several logs files are provided. Each serves a different purpose. The log files are:

(Windows only) The `\ProgramData` folder on Windows Vista and Windows Server 2008, and the `\Documents and Settings\All Users\Application Data` folder for all other supported Windows platforms, are hidden by default. VTE Agent logs, configuration data, and certificates are stored under that folder. If you cannot browse the folder for your platform, enable the **Show hidden files and folders** radio button in the **Folder Options** menu to view the folder and its contents.

Active logs are log files that being currently written to and updated by GDE Appliance processes. Inactive logs are logs that have been filled to capacity and then closed. The name of the closed log file is the original name usually appended with the date and some random numbers. For example, the name of an active agent log is vordb2_usr.log. When it reaches the configured capacity, it is made inactive and usually renamed to `vordb2_usr.log.YYYY-MM-DD-MM-SS.tar.gz`. For example, the archive file for `vordb2_db2inst1.log` can be `vordb2_db2inst1.log.2011-01-19-12-25-32`.

Do not try to manually modify or remove active logs. Use the Management Console interface to configure server and VTE Agent logs. Regularly back up and delete inactive logs to maximize available hard disk space.

The Windows system event log can fill quickly. If a Windows host runs out of system event log space, the vmd service does not start and issues an error: "`The service did not respond to the start or control request in a timely fashion.`"

To prevent the system event log from running out of space, the current event log is archived to a file when it reaches 20MB, all archived entries are then purged from the event log, and logging continues as usual. Archive files are placed in `%SystemRoot%\System32\Config`.

The archive file is named `Archive-Vormetric Encryption Expert-timestamp.evt`. For example, `Archive-Vormetric Encryption Expert-2010-05-14-18-14-30-171.evt`. The file is archived in a binary format that you can open in the Event Viewer. Check disk space availability during periods of heavy load and extensive logging. Back up and delete the archive files.

VTE Agent Log Files

The agent logs are the first places to check when communication between the GDE Appliance and VTE Agent system fails. Also, you may want to check these logs after setting up a new agent or changing the agent configuration.

vorvmd.log (Windows)/vorvmd_root.log (UNIX)

(UNIX)

```
/var/log/vormetric/vorvmd_root.log
```

(Windows)

```
\Documents and Settings\All Users\Application
Data\Vormetric\DataSecurityExpert\Agent\log\vorvmd.log
```

(Windows XP)

```
\Documents and Settings\All Users.WINDOWS\Application
Data\Vormetric\DataSecurityExpert\agent\log\vorvmd.log
```

(Windows Vista and Windows Server 2008)

```
\ProgramData\Vormetric\DataSecurityExpert\Agent\log\vorvmd_root.log
```

(Windows) The same information that is sent to `vorvmd.log` can also be sent to the Windows Event Viewer. Enable **Log to Syslog/Event Log** logging options for the agents and open **Event Viewer > Vormetric Encryption Export** to view log events on the host system.

`vorvmd_root.log` contains the VTE Agent transactions for the root user. Transactions consist of a record of vmd actions, such as starting the vmd daemon and setting up communication links with the GDE Appliance.

messages (UNIX only)

```
/var/log/messages
```

messages is a syslog-generated file. It contains standard syslog entries. It contains kernel entries for enabling/disabling the log service, memory usage, CPU usage, system calls, device initialization, etc. It also contains log entries that are also displayed in the Message Log.

secfs.log (AIX only)

The `secfs.log` file contains kernel-related messages, and the `secfsd.log` file contains process-related messages. The `secfs.log` file is generated only on AIX systems. The secfs.log file is maintained in the `./agent/secfs/tmp` directory. It is used instead of syslog to log kernel messages. The same log messages are placed in both `/var/log/messages` and `secfs.log`. The `secfs.log` file is archived at 32MB and renamed to `secfs.log.archive`. Only one archive file is maintained.

secfsd.log

(UNIX)

`/opt/vormetric/DataSecurityExpert/agent/secfs/tmp/secfsd.log`

(Windows Server 2003)

```
C:\Documents and Settings\All Users\Application
Data\Vormetric\DataSecurityExpert\agent\log\secfsd.log
```

(Windows Vista and Windows Server 2008)

`C:\ProgramData\Vormetric\DataSecurityExpert\agent\log\secfsd.log`

(Windows XP)

```
C:\Documents and Settings\All Users.WINDOWS\Application
Data\Vormetric\DataSecurityExpert\agent\log\secfsd.log
```

The `secfs.log` file contains kernel-related messages, and the `secfsd.log` file contains process-related messages. secfsd.log contains a record of GuardPoint mounts and GuardPoint dismounts (GuardPoints are mounted file systems). Entries are added to this file when you add and remove GuardPoints, as well as when you reboot the agent system.

statusfile

`/opt/vormetric/DataSecurityExpert/agent/secfs/tmp/statusfile`

`\Program Files\Vormetric\DataSecurityExpert\agent\secfs\tmp\statusfile`

`statusfile` is a current record of the local VTE Agent configuration. View this file after updating the VTE Agent configuration on the GDE Appliance to verify that the changes have actually been applied. This file should always be checked when the configuration of the VTE Agent is in question. This file lists:

- Each GuardPoint and GuardPoint properties, such as the lock status, protection status, and GuardPoint directory
- The names of applied policies
- The logging information that is captured
- Where captured log information is sent
- Hosts settings

You can also display the file timestamp to see when the agent was last updated.

This file is deleted each time the VTE Agent configuration is updated. You must manually regenerate it using the "`secfsd -status`" command. If you want to keep records of VTE Agent configuration changes, either copy the `statusfile` to a different name, or run "`vmsec status`" and tee the output to a different file.

(Windows) The `secfsd` command has limited support on Windows platforms. You can use the `secfsd -status lockstat` command or use the Vormetric Data Security tray to open the status window. Look for strings like `coreguard_locked=true` and `system_locked=true`. (`false` indicates that a lock is not applied. `true` indicates that a lock is applied.).

You may view the file contents using an ASCII display command, such as `cat`.

GDE Appliance Log Files

The primary GDE Appliance log is viewed in the *Logs* window of the Management Console. This log is generally the first log that you check to diagnose server problems. Check the GDE Appliance log after making or restoring a database backup. Look for entries like "`Backup Request for SAMPLE from host vmSSA06 is allowed.`" and "`Backup/Restore completed successfully.`" Messages like "`Backup data request failed: access denied or a related cause.`" indicate a problem has occurred and some debugging on your part is required.

Viewing the log files is easier on a software-only server than an appliance-based server. On a software-only server you can use a favorite editor to search a log or copy logs nightly as part of a batch process. Use the `diag` CLI command to list and view the log files. However, the log files can be exported from an appliance using the various export features in the *Logs* window. GDE Appliance administrators cannot delete log files.

The JBoss application server creates three log files in `/opt/vormetric/coreguard/server/jboss-5.1.0.GA/server/default/log`.

- `boot.log` contains JBoss startup information.
- `cgss.log` contains GDE Appliance information.

- server.log contains system-level information.

boot.log is managed as a single file. It is not expected to ever become a large file nor is it rotated. The cgss.log and server.log files can become large and are rotated.

The three log files are physically stored in /opt/vormetric/coreguard/server/jboss-5.1.0.GA/server/default/log. Alternate access is provided through the symbolic link, /opt/vormetric/coreguard/server/log.

The cgss.log and server.log files are important log files that can grow quickly under heavy load. Because these logs are vital to analyzing GDE Appliance behavior, they should be monitored and backed up regularly.

The names of the active files are cgss.log and server.log. When either file contains 10MB of log data it is made inactive and renamed to cgss.log.1 or server.log.1, respectively. And a new active cgss.log or server.log file is opened. When the new active log file reaches 10MB it is made inactive and renamed to cgss.log.2 or server.log.2. And a new active log file is opened. This process continues until there are a total of 10 inactive log files. When there are 10 inactive log files, and the active log file reaches its full 10MB capacity, the first inactive file is discarded, all the other log file names are decremented by one, and the former active log becomes the 10th inactive log file. Using cgss.log as an example, when cgss.log fills, cgss.log.1 is discarded, all the other log file names are decremented by one, and cgss.log becomes cgss.log.10. Depending on the load you place on the server, and if your policies audit a lot of data, these files can grow and rotate quickly.

badlog.log

Log files with unparsable data are “bad logs”. A badlog.log file contains log data from an agent that is intended for display in the Logs window but which cannot be displayed because the log data cannot be parsed due to format irregularities. Each attempt by an agent to upload an unparsable log file to the server is placed in the badlogs directory as a unique file. Regardless of the number of failed attempts to parse incoming log files, the GDE Appliance will continue to accept uploaded logs from the agent.

Log files are in an XML format. Log files originate on the UNIX agent in the /var/log/vormetric directory and they are removed from the agent after they are successfully uploaded to the GDE Appliance. If the GDE Appliance cannot parse the file, it is placed in
/opt/vormetric/coreguard/server/jboss-5.1.0.GA/server/default/auditlog/badlogs/vmd_upload_hostName.num. For example, vmd_upload_vmlinux101.374.

This file is located in
/opt/vormetric/coreguard/server/jboss-5.1.0.GA/server/default/log.

cgss.log

The cgss.log file contains a record of the events that make up the BEK generation process for an agent requesting to make a backup, as well as the names of uploaded audit files. This file does not contain events that pertain to restore operations. Check this file if the agent fails to back up a database, even though agent/server authentication is correctly configured and the policy for this agent permits the backup operation.

This file is located in:
`/opt/vormetric/coreguard/server/jboss-5.1.0.GA/server/default/log`.

server.log

The server.log file contains details about agent backup and restore requests, connection status, Management Console interaction, Java exceptions, JBoss start and stop processes, and more. This file contains diverse information and should be checked for almost any problem that is related to the GDE Appliance. Sometimes it is easier to `grep` a specific error level, like WARN, INFO, or DEBUG, than it is to view the entire file.

This file is located in:
`/opt/vormetric/coreguard/server/jboss-as/standalone/log`.

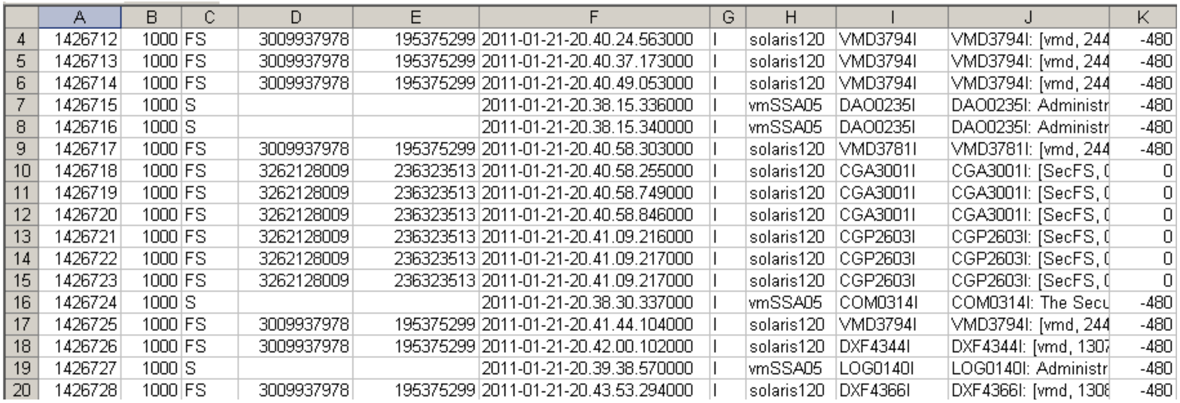
Exporting Logs

You can export the log entries that are displayed in the *Logs* window to maintain a separate record of server and agent activity at the application level.

The data displayed in the *Logs* window can be exported to a file for archival or analysis. Only the entries in the *Logs* window that are appropriate for the administrator type and domain can be saved to a text file. The output file is formatted as a comma-separated list and is usually viewed in a spreadsheet application.

The following example is an excerpt of a .csv file generated by an administrator of type All that is inside a domain.

Figure 5: Figure 158: Excerpt of a log .csv file



	A	B	C	D	E	F	G	H	I	J	K
4	1426712	1000	FS	3009937978	195375299	2011-01-21-20.40.24.563000	I	solaris120	VMD3794I	VMD3794I: [vmd, 244	-480
5	1426713	1000	FS	3009937978	195375299	2011-01-21-20.40.37.173000	I	solaris120	VMD3794I	VMD3794I: [vmd, 244	-480
6	1426714	1000	FS	3009937978	195375299	2011-01-21-20.40.49.053000	I	solaris120	VMD3794I	VMD3794I: [vmd, 244	-480
7	1426715	1000	S			2011-01-21-20.38.15.336000	I	vmSSA05	DAO0235I	DAO0235I: Administr	-480
8	1426716	1000	S			2011-01-21-20.38.15.340000	I	vmSSA05	DAO0235I	DAO0235I: Administr	-480
9	1426717	1000	FS	3009937978	195375299	2011-01-21-20.40.58.303000	I	solaris120	VMD3781I	VMD3781I: [vmd, 244	-480
10	1426718	1000	FS	3262128009	236323513	2011-01-21-20.40.58.255000	I	solaris120	CGA3001I	CGA3001I: [SecFS, (	0
11	1426719	1000	FS	3262128009	236323513	2011-01-21-20.40.58.749000	I	solaris120	CGA3001I	CGA3001I: [SecFS, (	0
12	1426720	1000	FS	3262128009	236323513	2011-01-21-20.40.58.846000	I	solaris120	CGA3001I	CGA3001I: [SecFS, (	0
13	1426721	1000	FS	3262128009	236323513	2011-01-21-20.41.09.216000	I	solaris120	CGP2603I	CGP2603I: [SecFS, (	0
14	1426722	1000	FS	3262128009	236323513	2011-01-21-20.41.09.217000	I	solaris120	CGP2603I	CGP2603I: [SecFS, (	0
15	1426723	1000	FS	3262128009	236323513	2011-01-21-20.41.09.217000	I	solaris120	CGP2603I	CGP2603I: [SecFS, (	0
16	1426724	1000	S			2011-01-21-20.38.30.337000	I	vmSSA05	COM0314I	COM0314I: The Secu	-480
17	1426725	1000	FS	3009937978	195375299	2011-01-21-20.41.44.104000	I	solaris120	VMD3794I	VMD3794I: [vmd, 244	-480
18	1426726	1000	FS	3009937978	195375299	2011-01-21-20.42.00.102000	I	solaris120	DXF4344I	DXF4344I: [vmd, 1307	-480
19	1426727	1000	S			2011-01-21-20.39.38.570000	I	vmSSA05	LOG0140I	LOG0140I: Administr	-480
20	1426728	1000	FS	3009937978	195375299	2011-01-21-20.43.53.294000	I	solaris120	DXF4366I	DXF4366I: [vmd, 1308	-480

The format of this table is subject to change. At this time, the columns indicate:

Table 7: Exported Message Log Headings and Description

Column Heading	**Description**
A	ID number in the Management Console (LOG_ID)
B	Internal domain identifier. If you are not in a domain this is zero. (DOMAIN_ID)
C	Entity that generated the message. It can be S (GDE Appliance), FS (VTE Agent). (SOURCE)
D	Internal tag (TAG)
E	Internal subtag (SUBTAG)
F	Time of action in UTC (LOG_TIMESTAMP)
G	Severity in the Management Console (SEVERITY)
H	Source in the Management Console (HOST_NAME)
I	GDE Appliance or agent Message ID. For example, DAO0239I or CGP2603I.The Message ID also identifies the log service. For example, CGP2603I was generated by the CGP (Policy Evaluation Service) log service. (MESSAGE_ID)
J	Message in the Management Console (MESSAGE)
K	Time offset in minutes. Subtract this number from the time in column F to determine local time. F - K = local time. For example, 22:40:19 UTC - 420 offset = 15:40:19 PDT = 3:40 PM PDT. (TIMEZONE_OFFSET)

Exporting the Message Log

1. Log on to the Management Console as an administrator of the appropriate type for the data you want to export.
2. Enter a domain if you want to export domain-related log entries.
3. Open the *Logs* window.
4. Click **Export Logs**. The *File Download* window opens.

   The options are:

   - **Open** to display the log entries to be exported in the default spreadsheet application. Usually this is Excel.
   - **Save** to export the log to a file on the system running the Management Console Web session or on another network accessible system. The default output file name is `log.csv`.
   - **Cancel** to close the window and stop the export operation.
5. Click **Save**. The *Save As* window opens.
6. Enter the name and path for the export file. The default file name is `log.csv`.
7. Click **Save**. The *Download Complete* window opens. It displays statistical information about the exported log, such as its location and size.

   The options are:

   - **Open** to open the exported log file in the default spreadsheet application used to process CSV format files.
   - **Open Folder** to open a Windows Explorer window in which to select and view the exported log in an application of your choice.
   - **Close** to close the window.
8. Click an option to open the exported log in the default spreadsheet application, open the exported log file in a different application, or to close the window and continue other Management Console operations.

Adding an email Notification Group

Email Groups are per domain. You can set up email groups for domains of System, Security, Domain, Domain/Security and All Administrators.

Enabling email notification for log messages

You can automatically send email notifications to a set of administrators if the GDE Appliance generates a serious log message.

You need to configure an SMTP server first. Navigate to **System > Email Notification** and click the SMTP Server tab. Enter the information for the following tabs:

- **SMTP Server**—SMTP server that will send the email notification. SMTP Servers are per appliance and you must be signed in with System Administrator privileges to modify this setting. If you don’t have these privileges, the SMTP server setting is grayed out. Note that the appliance does not come with a default SMTP server and that the SMTP server settings are initially empty.
- **SMTP Server Port**—Port used by the SMTP server.

To bring up the Email Notification interface, select **System > Email Notification** when outside a domain. The attributes and interface information for the Email Notification are as follows:

- **Email Group Name**—Name of the email group which will receive the email notification. Email Groups are per domain. You can set up email groups for domains of System, Security, Domain, Domain/Security and All Administrators.
- **Email Threshold Level**—If the GDE Appliance generates a log message with a severity of this specified threshold level, then an email notification is generated. Can be ERROR or FATAL.
- **Email Address List**—Email addresses that will receive this email notification. Separate addresses with commas. If LDAP is configured, you can select addresses from your LDAP address book by pressing Select. If it’s not configured, you can enter your login and password to access it.
- **Email Subject**—Text you want on the subject line.
- **Message Contains**—This is a string filter that works with the Email Threshold Level. Only messages containing this string will be sent as an email notification. If blank, then all messages meeting the threshold criteria will be sent.
- **Enabled**—A checkbox that enables or disables email notification to the group.

To add an email notification group:

1. Select **System > Email Notification**. The **Email Notification** window displays.
2. Under the **Email Notification List** tab, click **Add**. The **Add Email Notification Group** window displays.
3. Enter the information and click **Ok**.

Viewing and Downloading Domain-Level Reports

16

The GDE Appliance comes with pre-configured reports that display system information. All reports can be downloaded and saved locally in CSV format.

This chapter includes the following sections:

Overview

All reports are under the **Reports** tab. The availability of reports depends on the GDE Appliance administrator type and privileges, and whether the administrator is currently in or out of a domain. You must be in a domain to access the domain-level reports.

GDE Appliance Administrators of type Security and type Domain and Security must have AUDIT privileges to access the reports inside domains (for both global and restricted domains).

Viewing and Downloading Reports

To view a report, click the **Report** tab on the Management Console, and then click the name of the report.

To save the report as a CVS file to your local machine, click **Download** at the top left of the report table.

Domain-Level Reports

The following security reports are available inside any domain:

- “Keys”
- “Key-Policy”
- “Policies”
- “Policy-Key”
- “Policy-Host”
- “Hosts”
- “GuardPoints”
- “Certificates”
- “License Usage by Hosts”
- “Host Registration Activities”
- “Hosts with GuardPoint Status”

The reports displayed depend on the roles assigned to an Administrator of type Security or Domain and Security, in addition to the ‘Audit’ role.

Keys

The *Keys* report is a table of keys available in the current domain.

The Keys report can generate more specific views through use of the following **Search** fields in the report's top panel.

- **Key Name**—Enter a specific key name.
- **Source**—Enter the source, either IP address or FQDN.
- **Key Flavor**—Select All, Symmetric or Asymmetric from the drop-down menu.
- **Key Algorithm**—Select All, 3DES, AES128, AES256, ARIA128, ARIA256, RSA1024, RSA2048, or RSA4096 from the drop-down menu.
- **Key Usage**—Select All, Vault-Keys or Non-Vault-Keys from the drop-down menu.

Click **Go**.

Table 8: Keys Report

Column Name	Description
Name	Name of the key
Source	The origin of the key, e.g., from GDE Appliance

Column Name	Description
Description	User defined description for the key
Algorithm	Algorithm used to create the key. Available options are: 3DES, AES128, AES256, ARIA128, ARIA256, RSA1024, RSA2048, RSA4096
Key type	Indicates whether the keys are; > Stored on server—each time the key is needed, it retrieved from the GDE Appliance and downloaded to non-persistent memory on the host. > Cached on Host—downloads and stores the key in persistent memory on the host. > Cached, Unique to Host—generated key is unique to the host and downloaded and stored in persistent memory.
Flavor	Whether the key is Symmetric or Asymmetric
Creation Time	Time stamp of when the key was created. Format of the time stamp is YYYY-MM-DD HH:MM:SS:ms
Time Expired	Time and date when the key expires or has already expired
Number of Policies	Number of policies that use this key

Key-Policy

The *Key-Policy* report lists keys and the policies that use the key. The Key-Policy report can generate a more specific view through use of the **Search** field in the report's top panel.

In the **Key Name** field, enter the specific key name you want to search for. Click **Go**.

Table 9: Key-Policy report

Column Name	Description
Key Name	Name of the key
Algorithm	Algorithm used to create the key; 3DES, AES128, AES256, ARIA128, ARIA256, RSA1024, RSA2048, RSA4096
Policy Name	Name of the policy that uses the key
Policy Type	The type of policy that uses the key, e.g., FS

Policies

The *Policies* report is a table of available policies. This report can generate more specific views through use of the following **Search** fields in the report's top panel.

- **Policy Name**—Enter a policy name.

- **Policy Type**—Select from available options, click **Go**.

Table 10: Policies Report

Column Name	Description
Policy Name	Name of the policy
Policy Type	The type of policy that uses the key, e.g., FS
Creation Time	Time stamp of when the key was created. Format of the time stamp is YYYY-MM-DD HH:MM:SS:ms
Keys Used	Number of keys used by this policy
Total GuardPoints	Number of GuardPoints using this policy
GuardPoints Enabled	Number of GuardPoints where this policy is enabled
GuardPoints Disabled	Number of GuardPoints where this policy is disabled

Policy-Key

The *Policy-Key* Report is a table of Key Names associated with Policy Names. This report can generate a more specific view through use of the **Search** field in the report's top panel.

In the **Policy Name** field, enter the specific policy name you want to search for, click **Go**.

Table 11: Policy Key Report

Column Name	Description
Policy Name	Name of the Policy
Policy Type	The type of policy that uses the key, e.g., FS
Key Name	Name of the key
Algorithm	Algorithm used to create the key: 3DES, AES128, AES256, ARIA128, ARIA256, RSA1024, RSA2048, RSA4096

Policy-Host

The *Policy-Host* report is a table of Host Names associated with Policy Names. This report can generate a more specific view through use of the **Search** field in the report's top panel.

In the **Policy Name** field, enter the specific policy name you want to search for, click **Go**.

Table 12: Policy Host Report

Column Name	Description
Policy Name	Name of the policy
Policy Type	The type of policy that uses the key, e.g., FS
Host Name	IP address or FQDN of the host on which the policy is applied
OS Type	Operating System running on the host: for example, UNIX, Windows, Linux
GuardPoint Enabled	Yes (Y) or No (N)

Hosts

The *Hosts* report is a table of Hosts and the registration status of the agents installed on them. This report can generate a more specific view through use of the **Search** field in the report's top panel.

In the **Host Name** field, enter the specific Host name (IP address or FQDN) you want to search for, click **Go**.

Table 13: Hosts Report

Column Name	Description
Host Name	IP address or FQDN of the host on which the policy is applied
OS Type	Operating System running on the host: for example, UNIX, Windows, Linux, or OFFLINE if the host OS cannot be detected.
FS Agent Registration Status	Registration status of the agent on the host. Possible values are; Registered, Registration Allowed, Registration Not Allowed.
FS Agent Version	Version of the VTE (FS) Agent installed on the host
Key Agent Registration	Registration status of the agent on the host. Possible values are; Registered, Registration Allowed, Registration Not Allowed.
Key Agent Version	Version of the Key (VAE) Agent installed on the host
Last Policy Update	Time of the last policy update. Format of the time stamp is YYYY-MM-DD HH:MM:SS:ms
Number of Policies	Total number of policies on the host
Number of Enabled Policies	Total number of enabled policies on the host

GuardPoints

The *GuardPoints* report is a table of GuardPoints associated with each host. This report can generate more specific views through use of the following **Search** fields in the report's top panel.

- **Host Name**—Enter a host name (IP Address or FQDN).
- **Guard Path**—Enter the path for the folder location where the GuardPoint is installed.

Click **Go**.

Table 14: GuardPoints Report

Column Name	Description
Host Name	IP address or FQDN of the host on which the GuardPoint has been created
GuardPoint Type	Type of GuardPoint created. Options are DIR, RAWDEVICE
Guard Path	GuardPoint location
Guard Enabled	Yes (Y) or No (N)
Policy Name	Name of the policy that applies to the GuardPoint

Certificates

The *Certificates* report is a table that describes certificates in the Certificate Vault. This report can generate more specific views through use of the following **Search** fields in the report's top panel.

- **Subject**—Enter the certificate name.
- **Issuer**—Enter the entity that issued the certificate.
- **Valid from**—Enter the date in the following format MM/DD/YY or select a day from the calendar button at the right of the field.
- **Valid to**—Enter the date in the following format MM/DD/YY or select a day from the calendar button at the right of the field.
- **Public Key Algorithm**—Enter the type of key you want to search for: RSA or DSA

Click **Go**.

Table 15: Certificates Report

Column Name	Description
ID	Identification number of the certificate
Subject	Name of the certificate

Column Name	Description
Issuer	Entity that issued the certificate
Valid From	Issuing date of the certificate
Valid To	Expiration date of the certificate
Public Key Algorithm	Algorithm used to sign the certificate, e.g., RSA or DSA
Public Key Size	512, 1024, 2048, 4096, etc.
Signature Algorithm	Algorithm for creating digital signatures, such as Sha1 with RSA, MD2 with RSA
CA	Certificate authority such as VeriSign, AT&T, GoDaddy, etc.
Type	Root, intermediate, leaf, unknown
Extended Key Usage	Server authentication and/or client authentication, code signing, email, time stamping, OCSP signing, unknown
CRL	Certificate revocation list
OCSP	Online Conflict Status Protocol
Format	Format of the vaulted certificate, such as PEM, DER, PKCS#7, PKCS#11, PKCS#12
With Private Key	Contains a private key? Y or N
File Name	Name of file
Description	Information that more fully describes the certificate

License Usage by Hosts

The *License Usage by Hosts* report is a table of license usage by hosts in this domain. For more information about core hour licensing, see “Logical core hour usage” on page 17.

Table 16: License Usage by Hosts report information

Column Name	Description
Organization	Name of the organization responsible for this domain
Domain	Name of the domain set when the domain was created
Agent Type	FS (VTE), Key (VAE)
License Type	Perpetual, Term, or Hourly
Host Name	Name of the host

Column Name	Description
Agent Licenses Used	Number of agents used
Logical Cores Used	Total number of cores used
Logical Core Hour Licenses Used	Total number of core hours used
LDT Enabled Hosts	Total number of hosts using VTE Agent licenses with LDT enabled
Docker Enabled Hosts	Total number of hosts using VTE Agent licenses with Docker enabled

Host Registration Activities

The Host Registration Activities report is a table of host registrations and deregistrations for hosts under hourly licenses.

Table 17: Host Registration Activities report information

Column Name	Description
Organization	Name of the organization responsible for this domain
Domain	Name of the domain set when the domain was created
Agent Type	VTE (FS), VAE (Key)
Host Name	Name of the host
Agent Licenses Used	Number of agent licenses used
Logical Cores	Number of logical cores
Logical Core Hour Licenses Used	Number of logical core hours used within this registration period
Registration Start (UTC)	Date host was registered
Registration End (UTC)	End date of the registration

Hosts with GuardPoint Status

The Hosts with GuardPoint Status report is a table of the total number of hosts with the status of their GuardPoints. This report helps with facilitating audits and other compliance metrics.

The Hosts with GuardPoint Status report features an overall status panel at the top that has the following fields:

- **Report ID:** The ID of the current report being generated
- **State:**
  - **QUEUED**—when the request has been submitted and is waiting in the queue.

- **STARTED**—when the request is being processed.
- **COMPLETED**—when the report has been generated without errors found.
- **CANCELLED**—when the request in the queue has been canceled before completion by the administrator.
- **ERROR**—when errors have been found on the hosts or when a timeout or GDE Appliance internal error occurred during processing.

NOTE: If State indicates an ERROR, check the fields for Total Hosts and Completed Hosts. If Total Hosts and Completed Hosts are equal, then the report table will show those host(s) indicating an ERROR condition. When Total Hosts and Completed Hosts are NOT equal, this indicates a problem with the GDE Appliance and host communication connections or another issue that should be troubleshooted.

- **Total Hosts**—the total number of hosts being queried by the report.
- **Completed Hosts**—the total number of hosts that have been queried to create the report.
- **Creation Time**—the month, day, year, and hour and minute that the query was started.
- **Completion Time**—the month, day, year, and hour and minute that the query ended with results.
- **Position in Queue**—if multiple requests for reports have come in to the GDE Applianc for processing, this is the number this request is that reflects how many other requests are already lined up.
- **Total Tasks**—if multiple requests for reports have come in to the GDE Appliance for processing, this is the total number of requests that are in the queue.
- **Remaining Tasks**—if multiple requests for reports have come in to the GDE Appliance for processing, this is the number of requests that are yet to be worked on.
- **Last Update Time**—this field indicates the month, day, year, hour, minute (and AM/PM) that the GDE Appliance report database was last updated.

Report Tasks

- To start a query and generate a report, click **Generate Report**.
- To update the GDE Appliance database, click on **Refresh**.
- To cancel a query report generation request, click **Cancel**.

- To download the results of this report, click **Download** to produce a CSV text file.

Table 18: Hosts with GuardPoint Status Report

Column Name	Description
Report ID	Unique identifier for this report view
Host Name	IP address or FQDN of the host
Host Description	(Optional) User-entry field for more clearly defining the host during provisioning
OS Type	Operating System installed on the host
Port	Port number used for GDE Appliance <-> Agent communication
One-Way Enabled	The agent was registered with One-Way Communication enabled between the Agent and the GDE Appliance (Yes—Y) or not (N).
FS Agent Registration Status	Registered, Allowed, Not Allowed
FS Agent Version	Version of the VTE (FS) Agent installed on the host
Key Agent Registration Status	Registered, Allowed, Not Allowed
Key Agent Version	Version of the VAE (Key) Agent installed on the host
Last Policy Update	Timestamps are in the form `YYYY-MM-DD HH:MM:SS:ms`
Docker Image ID	Unique identifier for the Docker image. This column is displayed only if you have a VTE Agent license with a Docker Extension
Docker Container ID	Unique identifier for the Docker container. This column is displayed only if you have a VTE Agent license with a Docker extension
GuardPoint Type	DIR, RAWDEVICE
Guard Path	GuardPoint location
Policy Name	Name of the GuardPoint policy
Guard Enabled	Indicates whether or not the GuardPoint is enabled. Values; Y or N
GuardPoint Status	Up, Down, Server Pending, Agent Pending, Error, or Unavailable
Transformation Status	Indicates the transformation status of a rekey operation. Displayed only if you have a VTE Agent license with an LDT extension and an LDT policy applied to a GuardPoint
Transformation Progress	If a rekey operation is underway, this indicates the percentage of the operation completed. Displayed only if you have a VTE Agent license with an LDT extension and an LDT policy applied to a GuardPoint
Estimated Rekey Completion Time	Provides an estimate of the time it will take to transform the data in the GuardPoint based on the available resources and the size of the data.

Table 18: Hosts with GuardPoint Status Report

Column Name	Description
Transformation Error	Indicates whether there was an error in the transformation operation.
Last Transformation Start Time	Date and time the last data transformation started.
Last Transformation Completion Time	Date and time when the last data transformation was done.
Total Files to be Transformed	The total number of files in that GuardPoint to be transformed by the policy.
Totals Files Transformed	Total number of files in that GuardPoint transformed by the policy. If the rekey operation is successful, this should match the number in the Total Files to be Transformed field.
Total Bytes to be Transformed	Total number of Bytes to be transformed.
Total Bytes Transformed	Total number of bytes transformed. If the rekey operation is successful, this should match the number in the Total Bytes to be Transformed field.
Total Files Skipped	Indicates the number of files skipped during data transformation. If any files were skipped, use the `voradmin ldt skip` command from the CLI on the host to see why these files were skipped.
Error Reason	If the Guard Status reads “Error” and Guarded reads “N”, the reason will be indicated here

Viewing GDE Appliance Preferences and Logs

17

Viewing GDE Appliance Preferences

Preferences for viewing the various windows and panels on the Management Console are set by the GDE Appliance System Administrator, as a GDE Appliance Domain Administrator you can still set some viewing preferences within the domains you are authorized to access.

You can set Log viewing preferences from the Edit Host page for the available agent log tabs. You can also configure Docker log settings from the Docker Log tab. Docker support is a separately licensed feature, see "Enabling Docker Support" for more information about this feature.

Setting Log Preferences on a Host

Log settings for the VTE Agent (FS Agent Log) are configured at the System level on the GDE Appliance. These settings are inherited by all the hosts on the GDE Appliance. However, you can fine those tune log settings for a specific host, and those settings will override the system settings.

Navigate to the *Hosts* page and click on the name of the host in the **Host Name** column for which you want to set log viewing preferences. Click the agent log that you want to configure (e.g., FS Agent Log, Key Agent Log, Docker Log). From this page, you can set the following parameters for the host:

1. **Message Type**
   - Management Service: Logs messages that are related to the agent and VMD process server interaction in the agent logs. Log to File and Upload to Server are enabled by default. The default log message level is INFO.
   - Policy Evaluation: Logs messages that are related to policy evaluation in the agent log. Set the log message level to desired setting. The default log message level is ERROR.
   - System Administration: Logs messages that are related to system level events. The default log message level is ERROR.
   - Security Administration: Logs messages that are related to security related events. The default log message level is INFO.

2. **Message Destination**

   Log Messages can be stored in several locations.

   - **Log to File**: Send log messages to the /var/log/vormetric/vorvmd_root.log file of a UNIX host, or a Windows equivalent, such as \Documents and Settings\All Users.WINDOWS\Application\Data\Vormetric\DataSecurityExpert\agent\log\vorvmd.log.
   - **Log to Syslog**: Send log messages to the syslog server for a UNIX host. If a syslog server is not configured, it is sent to the host 'messages' file, such as /var/adm/messages. On a Windows host, the messages are sent to the Event Viewer (Application events).
   - **Upload to Server**: Upload to the GDE Appliance and display in the Management Console Logs window.

     Level: Sets the level of error messages to be sent.

     Duplicates: Allow or suppress duplicate messages:

     - **Allow**: All duplicate messages of the corresponding Message Type are captured and displayed in the log.
     - **Suppress**: Messages of the corresponding Message Type will follow the configured Threshold as to how many times duplicate messages are sent to the GDE Appliance during the given Interval.

3. **File Logging Settings**

   - **Maximum File Size (bytes)**: The agent starts a new, empty log file when the specified limit is exceeded. The default is 1000000 bytes.
   - **Delete Old Log Files**: Select this check box to delete old FS agent logs. This check box works in conjunction with the **Number of Old Log Files to Keep** field. For example, Select this check box and enter 3 as the **Number of Old Log Files to Keep** value. After 3 logs are generated, the first log, log1, is deleted and a new log, log4, is created. If you do not Select this check box, log files will continue to accumulate in the server database and you will have to remove them manually.
   - **Number of Old Log Files to Keep**: Appears only when you select **Delete Old Log Files**. Specifies the maximum number of agent log files to leave in the server database. This text-entry box is only displayed when the **Delete Old Log Files** check box is enabled. The default is 5.

4. **Syslog Settings**

   - Local: Send Syslog messages to the local machine.
   - Server (1, 2, 3, 4): Enter the hostname of the Syslog server
   - Protocol: UDP or TCP
   - Message Format: Specifies the format of the message; Plain Message, CEF, or RFC5424.

5. **Upload Logging Settings**

- **Maximum Number of Messages to Upload At Once**: Limits the number of messages sent to the GDE Appliance at one time. When the specified number of log entries is reached, those entries are uploaded to the GDE Appliance. The default is 1000.
- **Upload Messages At Least Every (seconds)**: The maximum interval to wait before the agent is to upload messages to the GDE Appliance. Use this attribute to update the log viewer even when the Maximum Number of Messages to Upload At Once has not been reached. You can lower the interval if there is little agent activity. The default is 10 seconds.
- **Upload Messages At Most Every (seconds)**: The minimum interval to wait before the agent is to upload messages to the GDE Appliance. You can increase the interval if there is considerable agent activity, so the agents do not flood the network with log messages. The default is 1.
- **Normal Time Out (seconds)**: The maximum interval of time the agent is to wait for the GDE Appliance to acknowledge a backup or restore request and upload related message data. If the agent cannot connect to the GDE Appliance within the specified interval, the agent will try again after the interval configured by the Upload Messages At Least Every attribute. The default is 2 seconds.
- **Shutdown Time Out (seconds)**: The maximum interval of time the agent is to wait for the GDE Appliance to acknowledge job completion and upload related message data. If the agent is unable to upload the log messages within the specified interval, they are left on the agent system. The agent will resend the messages at the beginning of the next job. The default is 30 seconds.
- **Drop If Busy**: Select to slow log message generation and drop log files during periods of extreme logging.

6. **Duplicate Message Suppression Settings**

   - **Enable Concise Logging**: When enabled, audit log messages are reduced. This option is disabled by default. Instead of logging messages for each file system operation, only the following types of audit messages are logged;

     - only one audit message for each read or write activity is logged at the start of that activity.
     - audit messages for reading file status information and setting file attributes (and extended attributes) are not logged.
     - audit messages for directory open, close and read attributes are not logged.

     These settings can be customized on each host and the host setting will override the system level settings. Note that this feature is not available for VTE versions prior to v6.0.

   - **Threshold**: Used when the Duplicates value is set to Suppress. Specifies the maximum number of duplicate messages the agent is to send to the GDE Appliance within the amount of time specified by the Interval parameter. The default is 5 messages. The maximum is 100.

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

NOTE: We recommend turning on **Log to File** or **Log to Syslog** instead of **Upload to Server** for INFO and DEBUG levels. And, for general day-to-day operation, we recommend enabling and setting only ERROR Level (so that only ERROR, WARNING, and FATAL log entries are received). Setting Upload to Server to INFO or DEBUG level for policy evaluation can degrade GDE Appliance performance.

Configure Docker Log Settings

With the introduction of Docker support, you can now configure log settings for Docker images and containers. Docker logs evaluate GuardPoint policies.

1. Log on to the Management Console and switch to a domain or log on to a GDE Appliance as a local domain administrator of type Security with a Host role.
2. Navigate to the *Hosts* page.
3. Click the name of your Docker host in the **Host Name** column, the *Edit Host* page opens.

   Enter the following information in the **Configure Docker Log Setting** panel:

   - **Docker Image/Container**: Click **Browse** to select an image or container from the Docker host. If you select an image the **Docker Image ID** field displays the image ID. If you select a container, the **Docker Image ID** field displays the image from which the container was spawned and the **Docker Container ID** displays the container ID. You can use these IDs to search for Docker specific logs on the *Logs* page later.
   - **Policy Evaluation Level**: Select a log message level. For more information about log levels, refer to the *Administrators Guide*.
   - **Policy Evaluation Duplicated**: You can choose to suppress or allow duplicate messages. Select SUPPRESS or ALLOW, the default is SUPPRESS.
4. Click **Ok**. The Policy Evaluation settings are saved in a table under the **Configure Docker Log Setting** panel.

Docker log messages are displayed on the Logs page. To search for Docker specific log messages:

1. Navigate to the *Logs* page.
2. Enter the following information in the **Search** panel:

- **Log Type**: Select whether you want to display logs from both the GDE Appliance and the agents, only the GDE Appliance, or only the agents. The default is All, which means from both GDE Appliance and agents.
- **Source**: Enter the hostname of the GDE Appliance or agent for which you want to return log files.
- **Last Refreshed**: Displays the date and time of when the displayed log files were last refreshed. Format is YYYY-MM-DD HH:MM:SS
- **Message Contains**: Type in text string that you want to search for in the log messages.
- **Docker Host**: Click **Browse** to select the Docker Host for which you want to return log files.
- **Docker Image/Container**: Click **Browse** to select an image or container for which you want to display logs.
- **Docker Image ID**: Displays the ID for the selected Docker image.
- **Docker Container ID**: Displays the ID of the selected Docker container.

3. Click **Go**. The relevant logs are displayed in the table under the **Search** panel.

Viewing Logs

The entries displayed in the Message Log depend on the GDE Appliance administrator type (System, Domain, Security, All), the domain in which that administrator is working, and, for Security Administrators, that administrator’s role (Audit, Key, Policy, Host, Challenge & Response, Client Identity).

A GDE Appliance Administrator of type Domain cannot view the log entries that can be viewed by an administrator of type System or Security (and vice versa). By design, entries exported to a Syslog log file will have gaps in the number sequence depending on which domains and roles the GDE Appliance Administrators are actively logging.

The Domain Administrator sees log entries such as Domain Administrator and Security Administrator logins, SSL handshaking, and policy evaluation.

Log entries are displayed in the Management Console based on the current administrator type and the domain in which the administrator is working. However, all this log information combined is available in the server.log file on the GDE Appliance.

Part III: GDE Appliance Security Administrators

GDE Appliance Security Administrators have only the roles that were assigned to them when a GDE Appliance Domain Administrator designated them to be a member of that domain. GDE Appliance Security Administrators can be assigned to multiple domains and the same GDE Appliance Security Administrator can have different roles in those different domains.

GDE Appliance Security Administrators do the following tasks:

- "Creating and Configuring Signature Sets"
- "Managing Keys"
- "Configuring Policies"
- "Configuring Hosts and Host Groups"
- "Managing GuardPoints"
- "Security Administrator Preferences & Logs"

Creating and Configuring Signature Sets

18

File signing checks the authenticity and integrity of executables and applications before they are allowed to access GuardPoint data. When you initiate file signing on the GDE Appliance, the VTE Agent calculates the cryptographic signatures of the executables that are eligible to access GuardPoint data. Files are individually signed as part of a set and the set is configured in a policy that defines the processes to allow.

When an executable tries to access a GuardPoint, the `secfs` service checks the fingerprint, a SHA-2 (Secure Hashing Algorithm) message digest, of the executable against the fingerprint stored in the GDE Appliance database. If they match, the executable's authenticity is verified and it can be allowed to access protected data. A hostile or compromised executable, such as a Trojan application, malicious code, or rogue process, with a missing or mismatched signature, is denied access.

Once a set of files to be signed is created, the executables are signed on a selected host and a copy of each signature is stored on the GDE Appliance. This is done as a background process on the selected host. The time it takes to complete signing depends upon the number of files to be signed, the response time of the host system, and other load factors. The completion status is indicated in the *Signature Sets* window.

Completed signature sets are configured in a (VTE Agent) policy so that not only are the executables attempting GuardPoint access identified, but their signatures are checked to ensure that they had not been compromised.

Creating Signature Sets

A signature set is a collection of file names and/or directory names. You can enter the full path of files and directories manually or use the browser to locate and select them. Specify a directory to sign all the files in that directory and all the subdirectories that it may contain.

Signing many files can take a while. To shorten processing time, verify that the files and directories in the signature set exist. It takes longer to process non-existent files. If they do not exist, we recommend that you delete them as sources from the signature set.

By default, a generic error message is generated and displayed in the *Logs* window about a non-existent source being detected; the name of the offending file or directory is not specified.

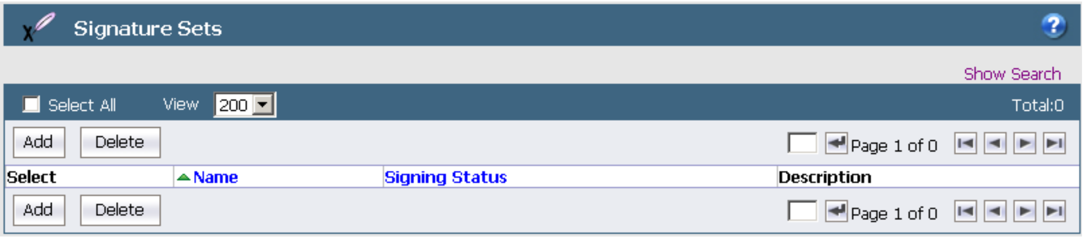
However, it is specified in the agent log on the host. To identify the offending file or directory, open the agent log file `vorvmd.log/vtray > View > File System > Log` on Windows systems. Look for "`Number of failed files`" to determine how many files were affected and "`is invalid for the signature request`" to identify the files that were not signed.

To create a signature set:

1. Log on to the Management Console as an administrator of type Security with `Host` role permissions, type Domain and Security with `Host` role permissions, or type All.
2. From the menu bar, select **Signatures**.

   The *Signature Sets* window opens. All configured signature sets are displayed.

Figure 6: Default Signature Sets window



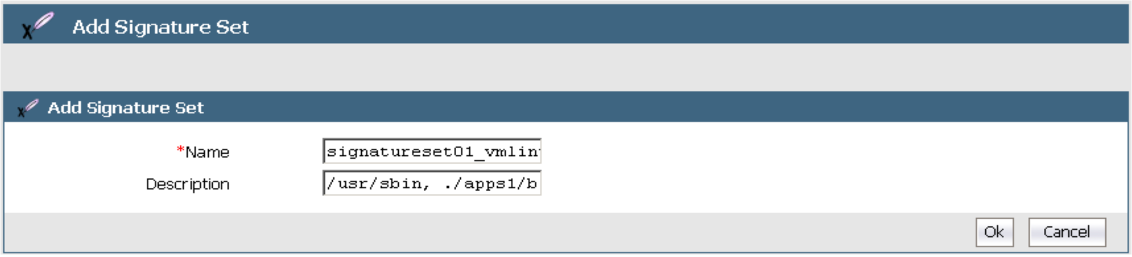
3. (Optional) Display only specific signature sets by entering all or part of a signature set name, and select the completion status, in the **Search** panel to display a subset of all signature sets in the GDE Appliance database.

   The **Show Search** label located below the **Signature Sets** banner opens the **Search** panel. You can enter a string and/or limit the search to sets with a specific completion status, and then click **Go** to display only those signature sets that match the search criteria. Click **Hide Search** to conceal the **Search** panel. The **Search** panel is not displayed to reduce graphic size.
4. Click **Add**. The **Add Signature Set** window opens.
5. Enter a name to assign the signature set in the **Name** text-entry box.

   Enter a unique string for the signature set name. The string you enter cannot exist in the current domain nor any other domain.

   This field is mandatory. The name must consist of alpha-numeric characters; starting with an alphabet character. The only non-alpha-numeric characters allowed are underscore (_) and dash (-). The maximum number of characters is 64.
6. (Optional) Enter a brief phrase or string in the **Description** text-entry box to make signature set identification easier. The maximum number of characters is 256.

Figure 7: Adding a signature set



Add Signature Set

Add Signature Set

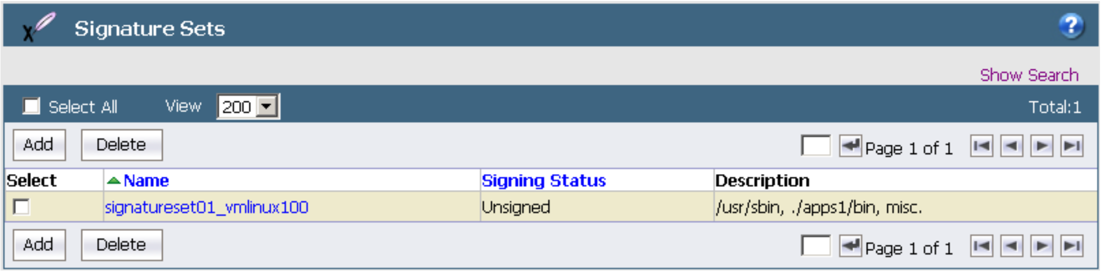
*Name: signatureset01_vmlin

Description: /usr/sbin, ./apps1/b

7. Click **Ok**.

   The **Signature Sets** window reopens and displays all the signature sets, including the one you just created.

Figure 8: Unsigned signature set



Signature Sets

Select	Name	Signing Status	Description
□	signatureset01_vmlinux100	Unsigned	/usr/sbin, ./apps1/bin, misc.

   By default, the signature set has an *Unsigned* status.

8. Add the files to be signed and directories whose files are to be signed to the signature set.

Adding files to a set

You can enter the full path of files or directories manually or use the browser to locate and select the files. It is quicker and easier to manually enter the paths of files; however, manual entry is prone to typographic errors and incorrect paths. Browsing can take longer but it ensures that the files exist and paths are entered correctly.

A cryptographic hash is created for each file in a signature set that meets a specific criteria. It would take longer, bloat the GDE Appliance database, and reduce performance to sign all the files in a signature set, especially when the set consists of top-level directories. The criteria is listed below. All other files are skipped.

- On a Windows host, all the files in the signature set that are inside a GuardPoint are signed. Only the compiled Windows executable files in the signature set that are located outside a GuardPoint are signed.

- On UNIX, it makes no difference if the files are inside or outside a GuardPoint. Only the files in the signature set with one or more of the execute bits (for example, `-rwxrwxrw-`) set on a UNIX host are signed.
- File extension has no impact. Files like `.bat` and visual basic programs on Windows, and files that end with `.so` on UNIX, are skipped.

Each instance of a file that has been copied to a different location or to a different name will have the same signature. This can be convenient way to detect duplicate files on your system.

To add files and/or directories to the signature set:

1. Select **Signatures** in the menu bar.
2. Click the name of a signature set in the **Name** column.
3. Click the *Source* tab in the **Edit Signature Set** window.
4. Select the host that contains the files to be signed.

   You must specify a host before you can browse for sources or initiate the signing process. You cannot enter the host name manually in the **Host** text-entry box.

   a. Click **Select** next to the **Host** test-entry box.

   The **Select a host to continue** window opens. All configured hosts are displayed and available for selection.

   b. Enable the **Select** radio button for the host that contains the files to be signed.

   Do not click the name of a host—that will open the **Edit Host** window.

   c. Click **Select** on the bottom of the window.

   The **Edit Signature Set** window is redisplayed and includes the name of the selected host in the **Host** text-entry box. The files on this host will be signed.
5. Click **Add**.

   The **Add Sources** window opens. Do one of the following:

   - Enter file names and directory paths manually in the **Sources** scroll-list
   - Select files and directories by browsing the host
   - Do a combination of the two

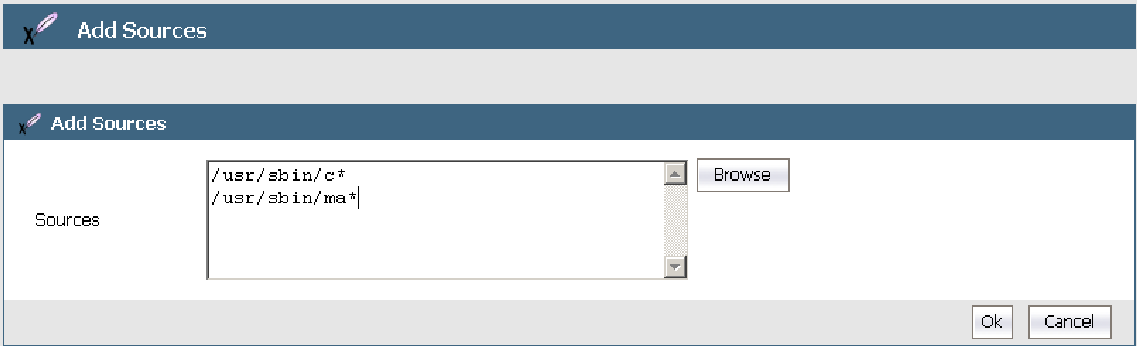
   Adding sources is cumulative.
6. To add sources manually:

   a. Enter the full paths to files and directories in the **Sources** scroll-list (Enter one file or directory per line).

   The asterisk can be used in a limited capacity as a wildcard character in file name searches. Place it somewhere in a file name string. Any executable or application file in the specified directory, and in every subdirectory, that matches the string will be located and can be signed. The wildcard is ignored when used in directory names. Directories that would normally match the wildcard are ignored. Check the logs for skipped files and directories.

A trailing slash (/) or backslash (\) at the end of directory paths is optional.

Figure 9: Manual source entry



```
/usr/sbin/c*
/usr/sbin/ma*
```

If you plan to add sources using both the manual and browser methods, be sure to click **Ok** before you open the browser. If you do not, all the sources that you had manually entered in the **Sources** scroll-list will be deleted and only the browser-selected sources will be listed. Inversely, you can browse for sources first and then manually add additional sources later without losing browser-selected and manually-entered sources.

b. Click **Ok**.

The **Source** tab displays the added sources.

7. To add sources using the browser:

a. Display the **Source** tab of a signature set.

b. Click **Add**.

The **Add Sources** window opens.

c. Click **Browse**.

The **Remote File Browser** window opens.

The **Type** scroll-list is hardwired to `Directory and File`.

The **Start Directory** text-entry box displays the top-level directory that is appropriate to the platform type: Windows (\) or UNIX (/).

d. (Optional) Enter a start point in the **Start Directory** text-entry box.

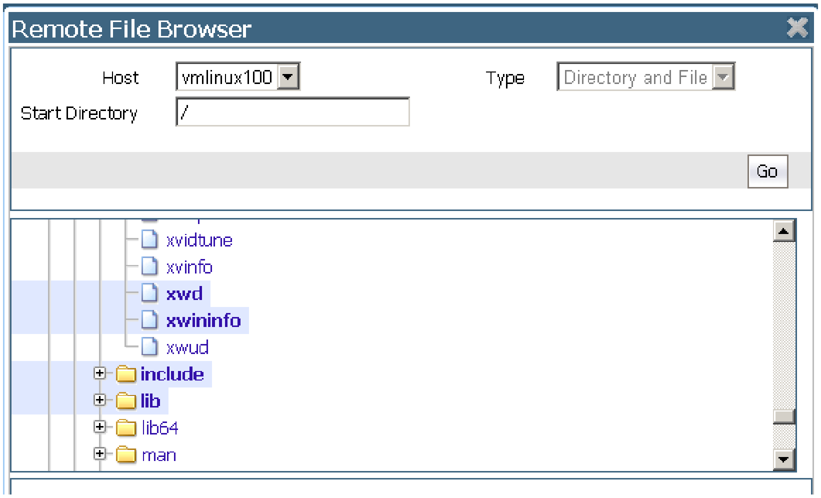
You cannot browse above the **Start Directory**. Enter a start point that is higher in the directory hierarchy than all the directories and files that you want to select, or you will have to re-enter start points to locate and select the desired files. The default is the top-level, either slash or backslash.

e. Click **Go** or, with the mouse cursor in the **Start Directory** text-entry box, press the <`Enter`> key.

f. Navigate to and select the desired files.

Click the plus symbol (+) next to a folder to display the next level of the directory hierarchy. Click the minus symbol (-) to collapse the hierarchy. Click a folder or file name to select that directory or file.

Figure 10: Adding files/directories to the set, browser method



Remote File Browser

Host: vmlinux100

Type: Directory and File

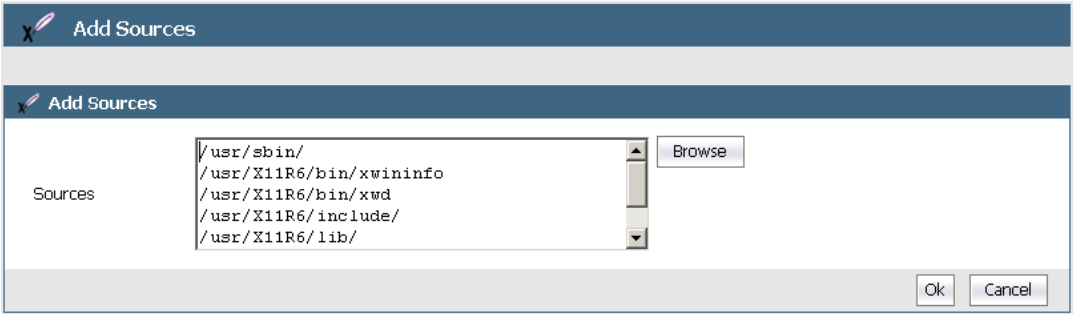
Start Directory: /

Single-click one or more files and/or directories. When you select a directory, all the files in all the subdirectories are also added to the set.

g. Click **Ok**.

The **Source** scroll-list displays the new additions.

Figure 11: Displaying browser-selected sources



Add Sources

Add Sources

Sources:

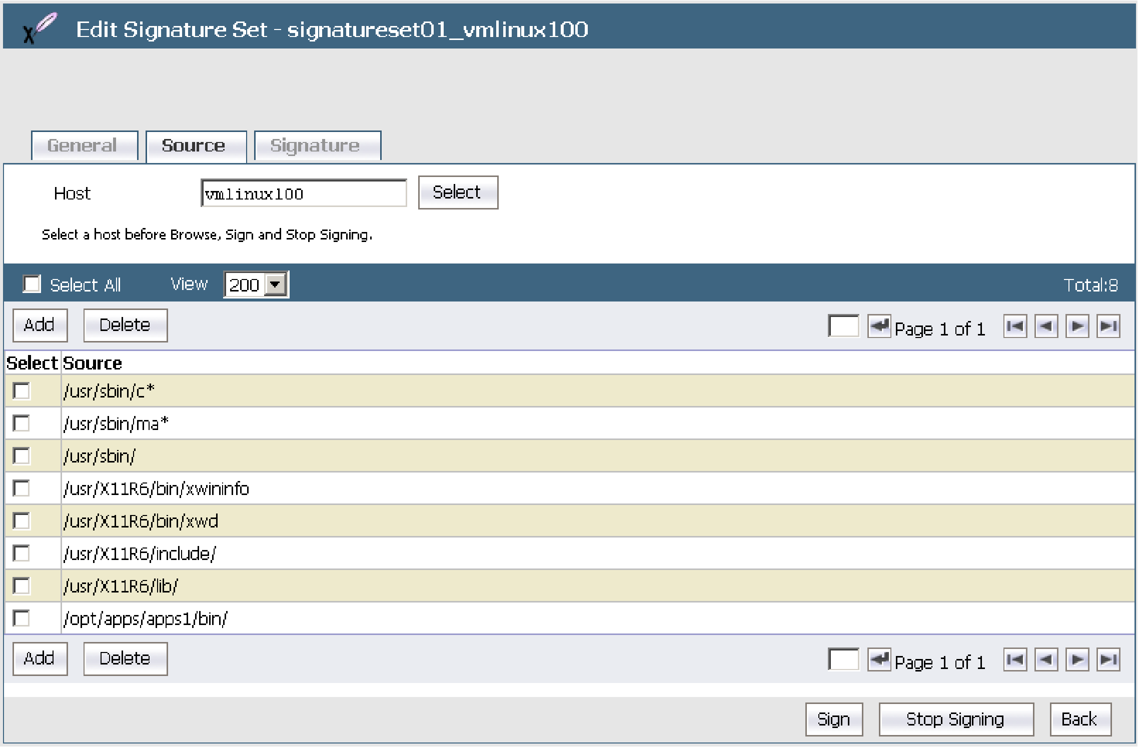
```
/usr/sbin/
/usr/X11R6/bin/xwininfo
/usr/X11R6/bin/xwd
/usr/X11R6/include/
/usr/X11R6/lib/
```

You can make changes by single, double, or triple clicking a source in the **Sources** scroll-list. Single-click to add or delete individual characters. Double-click to select a word. Triple-click to select an entire line.

h. Click **Ok**.

The **Source** tab displays the added sources.

Figure 12: Signature set with files



Edit Signature Set - signatureset01_vmlinux100

Host: vmlinux100

Select a host before Browse, Sign and Stop Signing.

Total:8

Select	Source
□	/usr/sbin/c*
□	/usr/sbin/ma*
□	/usr/sbin/
□	/usr/X11R6/bin/xwininfo
□	/usr/X11R6/bin/xwd
□	/usr/X11R6/include/
□	/usr/X11R6/lib/
□	/opt/apps/apps1/bin/

Signing Files in a Signature Set

Signing involves calculating a hash value for a file and storing the value on the GDE Appliance. Later, when a policy checks signatures, the signature of the process or executable accessing the GuardPoint is calculated and compared against the value in the GDE Appliance. If the two values match, the process or executable satisfies the Process requirement of a policy and may be granted access to the guarded data.

NOTE: If the executable itself is volatile, or subject to frequent change, it may not be worthwhile to use a file signature as a criteria in a policy because you have to re-sign the executable after each change. If the volatile executables are members of a large signature set, it can take a while to re-sign the files because the signature of every file in the signature set is recalculated. If the volatile files are few, it might be quicker to add the volatile files to a different signature set and sign that set, rather than re-sign all the files in the original signature set.

To sign the files in a signature set:

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions, type Domain and Security Administrator with `Host` role permissions, or type All.
2. Select **Signatures** in the menu bar.

   The **Signature Sets** window opens. Note the completion status of the desired signature set in the **Signing Status** column.
3. Click the name of the signature set in the **Name** column.

   The **Edit Signature Set** window opens to the **General** tab.
4. Click the **Source** tab.

NOTE: Do not enable any of the **Select** check boxes. The **Select** check boxes are used only to delete sources from the set.

5. If not already selected, specify a host that contains the files to be signed.

   You must specify a host before you can start signing. You cannot enter the host name manually in the **Host** text-entry box.

   a. Click the **Select** button next to the **Host** test-entry box.

   The **Select a host to continue** window opens. All configured hosts are displayed and available for selection.

   b. Enable the **Select** radio button for the host that contains the files to be signed.

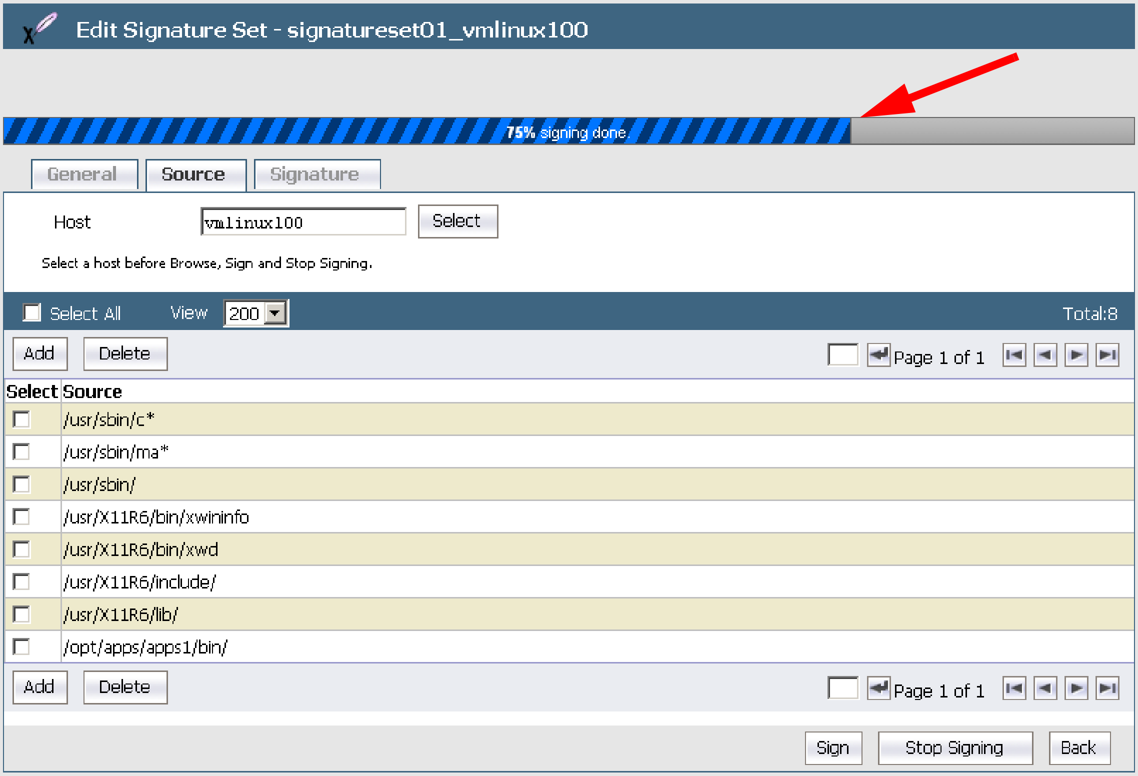
   Do not click the name of a host—that will open the **Edit Host** window.

   c. Click **Select** on the bottom of the window.

   The **Edit Signature Set** window is redisplayed and includes the name of the selected host in the **Host** text-entry box. The files on this host will be signed.
6. Click **Sign**.

   The time for this process to complete depends on how many files are being processed. The percentage of files in the signature set that have been signed is indicated in the status bar on the **Edit Signature Set** window. Also, you can view signing status in the **General** tab.

Figure 13: Signing progress indicator



Edit Signature Set - signatureset01_vmlinux100

75% signing done.

Host: vmlinux100

Select a host before Browse, Sign and Stop Signing.

□ Select All   View 200   Total:8

Select	Source
□	/usr/sbin/c*
□	/usr/sbin/ma*
□	/usr/sbin/
□	/usr/X11R6/bin/xwininfo
□	/usr/X11R6/bin/xwd
□	/usr/X11R6/include/
□	/usr/X11R6/lib/
□	/opt/apps/apps1/bin/

The signing status for the set in the **Signature Sets** window and the **Edit Signature Set** window, **General** tab, is IN_PROGRESS. Signing occurs as a background process, so you can use the Management Console for other administrative functions during this operation.

7. When signing completes, display the **General** tab and note both the signing status and percentage of completion.

   These should be FINISHED and 100 percent respectively.

8. View the resulting file: signature pairs in the **Signature** tab.

Using signature sets in a policy

Policies can be configured to identify the executables trying to access GuardPoint data and to verify that the executables themselves are unchanged since they were signed. You must, however, anticipate the effect of encryption on file signatures.

When a file inside a GuardPoint is copied to a location outside the GuardPoint, the two files will have different signatures because the file in the GuardPoint is encrypted and the file outside the GuardPoint is not.

Encryption makes the two files different, and the vmd process does not decrypt guarded files before checking their signatures. This means that when you rekey guarded files their signatures also change, and you must re-sign the files that use the signatures of those files in Process sets.

If both files, the one inside the GuardPoint and the one outside, must access GuardPoint data, add both files to the signature set and sign them. If encryption is not applied, both files will have the same signature and a signature mismatch should not occur.

Checking the agent logs if signing fails

If signing fails, or you want more information about the signing process such as which files were skipped, check the agent logs.

Messages are logged to:

(UNIX) /var/log/vormetric/vorvmd_root.log with **Log to File** enabled, and to messages with **Log to Syslog/Event Log** enabled.

(Windows) \Documents and Settings\ ...\agent\log\vorvmd.log with **Log to File** enabled.

In the Management Console, look for messages like:

```
COM0591W: The agent at host sys-techpub2 failed to generate the signature on
this file E:\apps\lib\dataxform_auto_config. Please check the VMD log for the
cause.
```

In the host vorvmd_root.log/vorvmd.log file, look for messages like:

```
[VMD] [WARN ] [3732] [VMD3824W] Failed to create the signature for
E:\apps\lib\dx1\aa_dir\dataxform_auto_config for the signature request 9,
error code 3
```

Table 19: Error Codes

Code	Description
0	System is okay.
1	Does not exist.
2	DO NOT USE.
3	Invalid argument.
4	Operation not supported.
5	Out of memory.
6	No space left on device.

Code	Description
7	Timeout reached.
8	I/O error.
9	Interrupted.
10	Permission denied.
11	Too many keys in key group.
12	Error in soap rpc layer.
13	Returned buffer is partially full.
14	Given target buffer is too small.
15	Unable to compress buffer.
16	Internal test failed.
17	Overflow.
18	Error setting up logging.
19	Overloaded error.
20	Server responded to a file upload with “bad request”.
21	Unknown user name or bad password.
22	The directory service is not available.

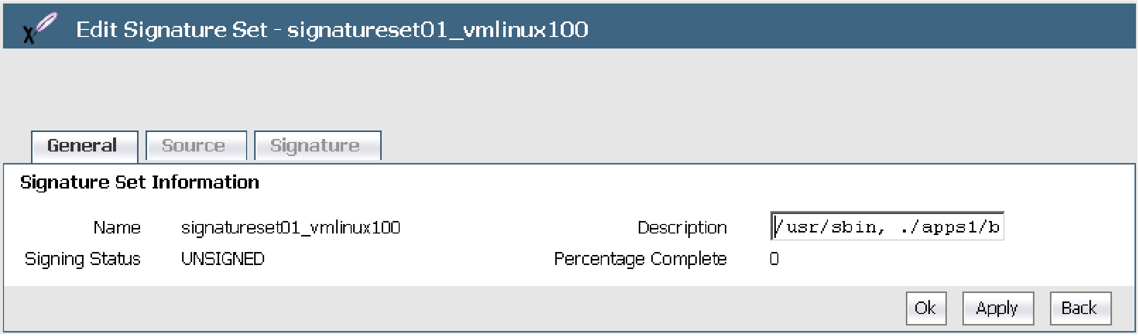
Checking Signing Completion Status

To display the completion status of a signature set:

1. Select **Signatures** in the menu bar.
2. Click the name of a signature set in the **Name** column.

   The **Edit Signature Set** window opens. The **General** tab is displayed.

Figure 14: The Edit Signature Set window, General tab


Edit Signature Set - signatureset01_vmlinux100

Signature Set Information

Name signatureset01_vmlinux100

Description /usr/sbin, ./apps1/b

Signing Status UNSIGNED

Percentage Complete 0

The **General** tab displays the file signing status and the percentage of files in the signature set that have been signed. The parts of the **General** tab are described below.

Table 20: General tab information for the Signatures page

Field	Description
Name	The name of the signature set.
Description	(Optional) Descriptive string to simplify set identification.
Signing Status	A signature set can be in one of five states: `UNSIGNED`—there may or may not be files in this signature set. If there files in the set, no attempt has been made to sign them. `IN_PROGRESS`—the GDE Appliance is actively signing the files in the set. This can take a while depending upon system load, accessibility, and the number of files being signed at one time. `FINISHED`—all the files in the set have been successfully signed and the set is ready to be used. `FINISHED_WITH_WARNING`—the VTE Agent was able to process each file in the signature set, but that one or more files in the set could not be signed. Possible causes are missing files or inadequate access permissions. Check the `vmd` log for details — `vorvmd_root.log` on UNIX and **Event Viewer > Vormetric Encryption Expert** on Windows. `ABORTED`—signing had been started but was stopped before completing.
Percentage Complete	Indicates the percentage of files that had been signed relative to the total number of files in the set.

The only field you can modify on the **General** tab is **Description**.

Stopping Signing

You can interrupt signing at any time by clicking **Stop Sign** in the **Source** tab. You are not prompted to verify your choice.

It takes a while for signing to stop. Once it does, the **Signing Status** displayed in the **General** tab is set to ABORTED and the **Percentage Complete** indicates the percentage of files that have been successfully signed. All the files that were signed remain intact and can be viewed in the **Signature** tab.

Re-Signing Files in a Signature Set

Signatures are computed values and, unless the files in a set have been compromised or modified, the signature should always be the same for a given file. If files have been modified, they must be resigned so that their signatures match the signatures in the GDE Appliance.

To re-sign files, you can:

- Create and sign a new signature set with the files and the directories to be signed. If there are only a few files and directories in the set, this can be the easiest solution.
- Create and sign a new signature set with the paths of the directories that contain the files to be signed. If there are only a few files in the directories, or most of the files in the directories need re-signing, this can be the easiest solution.
- Open and re-sign the same signature set that was originally used to sign the files. If you have the time, or the signature set is small, this can be the easiest solution.

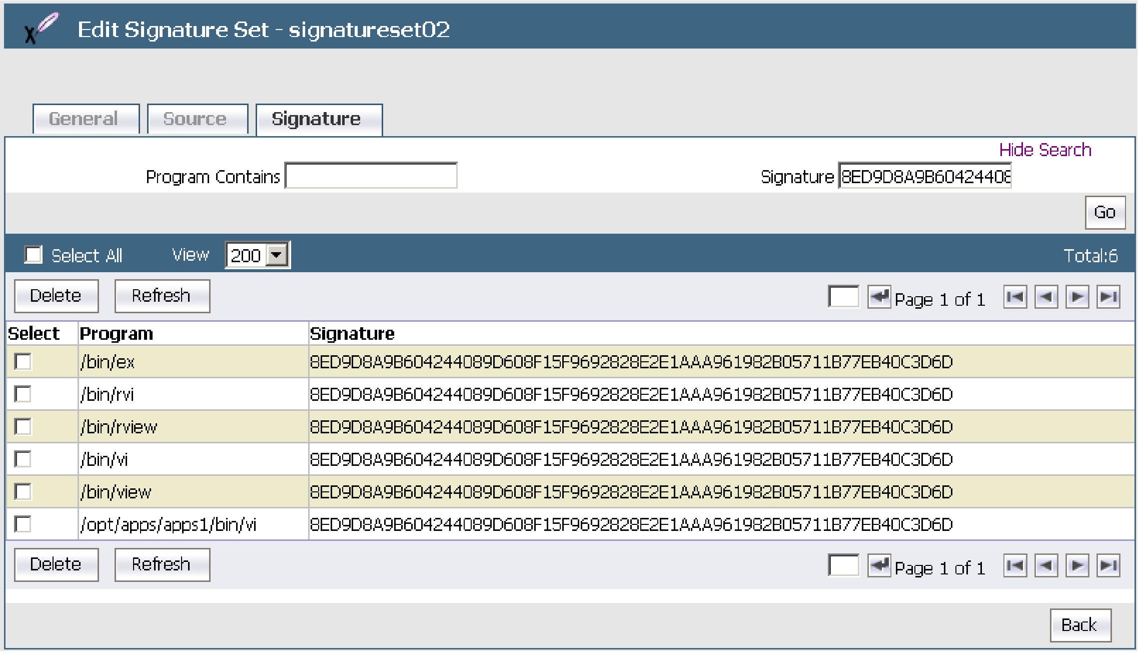
Signatures are computed values. It takes a long time to compute the signature of every file in a large signature set. It takes longer to re-sign the files in a set than it does to sign the files the first time because of the additional handling required to update information on the GDE Appliance. If you plan to re-sign many files, on the scale of hundreds of thousands, it can be quicker to delete the signature set that was initially used to sign the files, recreate the signature set from scratch, and sign the members of the signature set as if it were a new signature set.

Displaying Signatures, Detecting Duplicate Files

You can display up to 200 files of a signature set on one page, or you can display a subset of the files across multiple pages. You can specify a search criteria to display a subset of the signed files. The search criteria can be a case-insensitive string that is in all or part of a file name, and/or it can be the signature itself. String search is a convenient way to display signed files with a specific extension, such as "`.exe`", or signed files with names that contain a specific string, such as "`lib`".

Displaying files based on their signature is one way to locate identical files, regardless of name differences. If you search using a signature, you must enter the entire signature.

Figure 15: Displaying identical files based on their signature—Same file in different locations and with different names



Program Contains

Signature 8ED9D8A9B60424408

□ Select All View 200 Total:6

Select	Program	Signature
□	/bin/ex	8ED9D8A9B604244089D608F15F9692828E2E1AAA961982B05711B77EB40C3D6D
□	/bin/rvi	8ED9D8A9B604244089D608F15F9692828E2E1AAA961982B05711B77EB40C3D6D
□	/bin/rview	8ED9D8A9B604244089D608F15F9692828E2E1AAA961982B05711B77EB40C3D6D
□	/bin/vi	8ED9D8A9B604244089D608F15F9692828E2E1AAA961982B05711B77EB40C3D6D
□	/bin/view	8ED9D8A9B604244089D608F15F9692828E2E1AAA961982B05711B77EB40C3D6D
□	/opt/apps/apps1/bin/vi	8ED9D8A9B604244089D608F15F9692828E2E1AAA961982B05711B77EB40C3D6D

Displaying Specific Signed Files in a Signature Set

To display specific signed files in a signature set:

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions, type Domain and Security Administrator with `Host` role permissions, or type All.
2. Select **Signatures** in the menu bar.

   The **Signature Sets** window opens.
3. Click the name of a signature set in the **Name** column.

   The **Edit Signature Set** window opens.
4. Click the **Signature** tab.

   By default, all signed files in the set are displayed in alphanumeric order.
5. Click **Show Search** to display the **Search** panel.

6. To search for files with a specific string in their names, enter the string in the **Program Contains** text-entry box.

   Enter all or any part of the desired file name. Case does not matter. All files that contain the string and, if configured, match the signature in the **Signature** text-entry box, will be displayed.

7. To search for files with a specific signature, enter the entire signature in the **Signature** text-entry box.

   Enter the entire signature. Unlike the **Program Contains** text-entry box, the **Signature** text-entry box is case-sensitive. All files that have the same signature and, if configured, match the string in the **Program Contains** text-entry box, will be displayed.

8. Click **Go**.

Deleting Signatures from a Set

Delete signatures from a signature set when you want to continue to use the signature set to authenticate processes, and you no longer want to authenticate the files that you are deleting from the set.

You can delete signatures individually or one page at a time.

To delete individual signatures from a signature set:

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions, type Domain and Security Administrator with `Host` role permissions, or type All.

2. Select **Signatures** in the menu bar.

   The **Signature Sets** window opens.

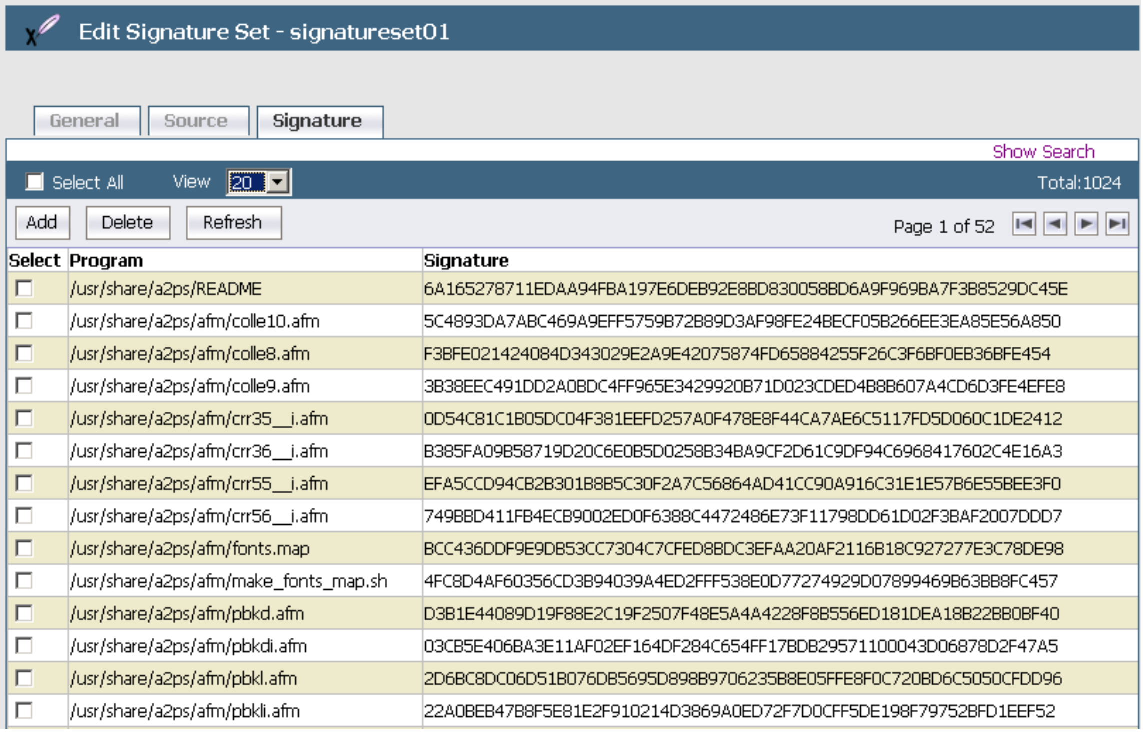
3. Click a signature set in the **Name** column.

   The **Edit Signature Set** window opens.

4. Click the **Signature** tab.

   The signed files in the signature set are displayed, along with their signatures.

Figure 16: Signed signature set



Edit Signature Set - signatureset01

Select	Program	Signature
□	/usr/share/a2ps/README	6A165278711EDAA94FBA197E6DEB92E8BD830058BD6A9F969BA7F3B8529DC45E
□	/usr/share/a2ps/afm/colle10.afm	5C4893DA7ABC469A9EFF5759B72B89D3AF98FE24BECF05B266EE3EA85E56A850
□	/usr/share/a2ps/afm/colle8.afm	F3BFE021424084D343029E2A9E42075874FD65884255F26C3F6BF0EB36BFE454
□	/usr/share/a2ps/afm/colle9.afm	3B38EEC491DD2A0BDC4FF965E3429920B71D023CDED4B8B607A4CD6D3FE4EFE8
□	/usr/share/a2ps/afm/crr35__i.afm	0D54C81C1B05DC04F381EEFD257A0F478E8F44CA7AE6C5117FD5D060C1DE2412
□	/usr/share/a2ps/afm/crr36__i.afm	B385FA09B58719D20C6E0B5D0258B34BA9CF2D61C9DF94C6968417602C4E16A3
□	/usr/share/a2ps/afm/crr55__i.afm	EFA5CCD94CB2B301B8B5C30F2A7C56864AD41CC90A916C31E1E57B6E55BEE3F0
□	/usr/share/a2ps/afm/crr56__i.afm	749BBD411FB4ECB9002ED0F6388C4472486E73F11798DD61D02F3BAF2007DDD7
□	/usr/share/a2ps/afm/fonts.map	BCC436DDF9E9DB53CC7304C7CFED8BDC3EFAA20AF2116B18C927277E3C78DE98
□	/usr/share/a2ps/afm/make_fonts_map.sh	4FC8D4AF60356CD3B94039A4ED2FFF538E0D77274929D07899469B63BB8FC457
□	/usr/share/a2ps/afm/pbkd.afm	D3B1E44089D19F88E2C19F2507F48E5A4A4228F8B556ED181DEA18B22BB0BF40
□	/usr/share/a2ps/afm/pbkdi.afm	03CB5E406BA3E11AF02EF164DF284C654FF17BDB29571100043D06878D2F47A5
□	/usr/share/a2ps/afm/pbkl.afm	2D6BC8DC06D51B076DB5695D898B9706235B8E05FFE8F0C720BD6C5050CFDD96
□	/usr/share/a2ps/afm/pbkli.afm	22A0BEB47B8F5E81E2F910214D3869A0ED72F7D0CFF5DE198F79752BFD1EEF52

5. If you plan to delete many file signatures, set the **View** number high because file selection applies only to the files on the current page. Files are deselected when you go to another page.

6. Select the file signatures to be deleted.

   You can click the **Select** check boxes of individual files on the current page or you can enable the **Select All** checkbox to select all the files on the current page.

7. Click **Delete**.

   A dialog box opens and prompts you to verify that you want to delete the selected signatures.

8. Click **OK**

   The signatures are removed from the GDE Appliance database.

Deleting Signature Sets

You can delete individual signatures within a set or whole signature sets.

You cannot delete an active signature set. If it is defined in a VTE Agent policy, it must be removed from the policy before the set can be deleted from the GDE Appliance.

To delete one or more signature sets

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions, type Domain and Security Administrator with `Host` role permissions, or type All.
2. Select **Signatures** in the menu bar.

   The **Signature Sets** window opens. All configured signature sets are displayed.
3. Enable the **Select** checkbox of each signature set to be deleted.
4. Click **Delete**.

   A dialog box opens that prompts you to verify that you want to delete the selected signature sets.
5. Click **OK**.

Managing Keys

19

The GDE Appliance can be used to create agent keys, as a secure centralized repository for storing and retrieving third-party encryption keys, and to create key templates.

This chapter includes the following sections:

- "Overview"
- "Agent Keys"
- "Key Templates"
- "Identity-Based Key Access"

Overview

Encryption keys are required for ensuring data integrity and privacy as well as user authentication.

Types of keys used by the GDE Appliance include:

- **Authentication keys**—verify the identity of the GDE Appliance, to the host and visa versa. The GDE Appliance and host cannot communicate without valid authentication keys. Authentication keys are referred to as ***authentication certificates***.
- **Symmetric encryption keys**—randomly generated AES keys that encrypt and decrypt data, whether the data resides on a file system or it is part of a database backup.
- **Asymmetric (public and private) keys**—encrypt and decrypt the randomly generated AES symmetric keys that encrypt and decrypt backed up data. The public RSA key encrypts the symmetric key. The private RSA key decrypts the symmetric key.
- **Imported symmetric encryption keys**—as of release v6.0.3, the GDE Appliance allows the import of externally generated symmetric keys to encrypt data.

Warning! Once encryption is applied, you must keep track of the encryption keys you are using. Encrypted data is unusable without the proper keys. Missing or improperly applied keys are the primary source of data retrieval problems.
Back up encryption keys to a secure location without encrypting them. This way, if

you must build a new GDE Appliance from scratch, you have the keys in a usable form.

Agent Keys

The GDE Appliance creates two types of agent keys; symmetric and asymmetric.

Symmetric keys that can be used by:

- VTE agent
- VAE agent
- Key agent for Oracle TDE

Asymmetric keys can be used by;

- Key agent for Microsoft TDE
- VAE agent

NOTE: Keys created via the Management Console do not have all the required Key Identifier attributes for certain VAE use cases. Refer to the *VAE Guide* for details about key usage.

Keys are partitioned into their own GDE Appliance domains. In other words, an agent that is registered to Domain-A can not retrieve, delete, or modify keys stored in Domain-B and vice versa. This applies to keys created by the GDE Appliance and agents. The key name does not have to be globally unique but must be unique within a domain. Therefore, you can have duplicated key names across different domains but key names must be unique within a domain.

The VTE Agent policies use symmetric keys. Since security policies are only applicable to the VTE agent, the GDE Appliance is aware that a symmetric key is used by the VTE Agent, once a key has been assigned to a policy. An attempt to delete a key used by a policy will fail until the key is removed from the policy.

Importing Externally Generated Keys (BYOK)

The GDE Appliance provides a Bring Your Own Key (BYOK) solution for enterprises that want to use their own keys for encryption operations on the GDE Appliance. These externally generated symmetric keys i.e., not generated on the GDE Appliance, can be imported to the GDE Appliance and used in security policies.

To import an externally generated key, you must first create an asymmetric RSA key pair (using either the RSA2048, or the RSA4096 algorithm), on the GDE Appliance. The public key component of this key pair is then used to wrap the external symmetric key which is to be imported. This wrapped key can then be imported to the GDE Appliance. See "Importing Symmetric Keys (BYOK)" for the procedure.

Externally generated symmetric keys can be imported using the Management Console or via the GDE Appliance RESTful API. To use the GDE Appliance RESTful API, refer to the GDE Appliance RESTful API docs located at https://<*dsm_IP_address*|*FQDN*>/doc/.

Versioned Keys

You can create 'versioned' keys to use with Live Data Transformation policies. The LDT feature, enables GDE Appliance Security Administrators to encrypt or rekey GuardPoint data without blocking user or application access to that data. Standard (non-LDT) policies require you to associate a non-versioned key with a policy to transform your data, while user and application access to the data is blocked during the transformation process. Transforming this data to use a new key would require a separate policy with this new key to be applied to the data.

With LDT you create a 'versioned' key for an LDT policy and define a life span for the key. The key is then automatically rotated when it reaches its expiry date. When the key rotates, all its properties including the key name and cryptographic algorithm remain unchanged, except the cryptographic key material that changes output of the key's cryptographic algorithm. Under LDT policy the new key material is applied to transform data to the new key version, as part of the same LDT policy that also protects data. You can still manually rotate the key if circumstances require it.

The **Automatic Key Rotation** option on the *Symmetric* tab of the *Add Agent Key* page must be selected in order to create a versioned key. See Table 21, "Symmetric Key Fields," on page 207 for more about this option.

Refer to the *Live Data Transformation Guide* for information about implementing LDT and to the "Configuring Policies" chapter for procedures to create LDT policies.

Enhanced Encryption Mode

As of GDE Appliance v6.1, a new encryption mode has been introduced for symmetric keys; AES CBC-CS1.

This new encryption mode is supported only by VTE v6.1.0 and GDE Appliance v6.1. If you have a host group that contains a mix of VTE 6.1.0 and earlier versions of VTE, and you apply a policy containing keys that use the CBC-CS1 encryption mode, the policy will not apply and will fail with an error message to the effect that the new encryption mode is not supported by all of the protected hosts in the host group. Similarly if you add a CBC-CS1 encryption key to a host group that has older registered hosts (earlier than v6.1), it will fail as the new encryption mode is not supported by all the hosts.

Warning! Once data is encrypted with keys that use a selected encryption mode (either legacy CBC or the new CBC-CS1), the mode is permanent—you cannot switch between encryption modes.
To change the encryption mode, i.e. move from using the new CBC-CS1 encryption mode to the legacy CBC mode, then you must transform the data using keys that use the legacy CBC encryption mode using the offline data transform tool or LDT.

Symmetric keys that use the new CBC-CS1 encryption mode are only supported on GDE Appliance v3.x. If you try importing keys that use this new encryption mode, to an earlier version of the GDE Appliance, the import will fail. These keys are not recognized by earlier versions of the GDE Appliance. The legacy CBC encryption mode is the default mode when creating a new encryption key.

Adding Agent Keys

Creating symmetric keys

The GDE Appliance lets you manually create (or add) symmetric keys and import symmetric keys. You can create your own keys or copy third-party keys to the GDE Appliance. Symmetric keys are based on 3DES, AES, and ARIA algorithms and are used to encrypt the data in GuardPoints. You can configure symmetric keys for VTE Agents only.

Create a symmetric key

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

   The *Agent Keys* page displays.
3. Click **Add**. The *Add Agent Key* window opens.
4. Select the **Symmetric** tab.

5. Complete the fields in this window by using the information in Table 21.

Table 21: Symmetric Key Fields

Field	Description
Name	Enter a name for the key in the **Name** field. This field is mandatory. The maximum number of characters is 64.
Description	(Optional) Enter a phrase or string in the **Description** text-entry box that helps you to identify the key. The maximum number of characters is 256.
Template	(Optional) A key template with a set of pre-defined attributes. Key templates are useful for creating keys of a specific type with specific attributes. Default Microsoft SQL Symmetric and Asymmetric key templates are also provided. If you use this template do NOT modify any of the template attributes. You can create your own templates by selecting Keys > Key Template. To create a Microsoft SQL Server TDE agent symmetric or asymmetric key, choose this template and do not change any of the custom attribute values.
Expiration Date	Date the key expires. Set a date per your security policies, when the expiry date is reached, it is displayed in red. Once an expiration date is set for a non-versioned key, when the key expires, you can reset the expiry date. You can also choose to create a new key for your policy, in which case you must rekey your data with the new key. Once an expiration date is set for a versioned key, when the key expires, you can rotate the key and set a new expiry date, or have the expiry date update automatically to a value that equals the date the key is rotated plus the period defined in **Key Version Life Span**. **IMPORTANT!** You must assign an expiration date to a versioned key. Without an expiration date, the key does not contain all of the properties required for versioned keys. As a result, LDT does not recognize the files that need transforming in a GuardPoint when using that key.
Algorithm	Select an encryption algorithm from the **Algorithm** list. Your choices are 3DES, AES128, AES256, ARIA128, and ARIA256. The default is AES256.
Key Type	Select the location for the generated key from the **Key Type** scroll-list. Your choices are **Stored on Server** and **Cached on Host**. The default is **Stored on Server**. **Stored on Server** keys are downloaded to non-persistent memory on the host. Each time the key is needed, the host retrieves the key from the GDE Appliance. Stored on Server requires a constant network connection to the GDE Appliance. **Cached on Host** downloads and stores (in an encrypted form) the key in persistent memory on the host. The cached keys are used when there is no network connection between the host and GDE Appliance. All hosts using the same encryption key can access encrypted data on other hosts that use the same key. The **Unique to Host** checkbox is displayed when **Cached on Host** is selected.
Unique to Host	This check box is displayed when the **Key Type** is set to **Cached on Host**. When enabled, this check box uses a token that is stored in the host record on the GDE Appliance to make the encryption key unique. The unique host encryption key is downloaded to the host and stored in an encrypted manner using the host password. These keys are used for locally attached devices, as files encrypted by them can be read by only one machine. Therefore, do not enable this checkbox for cloned systems, RAID configurations, clustered environments, or any environment that uses host mirroring. The **Unique to Host** checkbox can be enabled only when the **Key Type** is set to **Cached on Host** and the **Key Creation Method** is set to **Generate**.

Field	Description
Key Creation Method	Select if the key is to be generated automatically using a random seed or if it is to be generated by importing a file. Your choices are **Generate** and **Manual Input**. **Generate** is the default. The **Unique to Host** check box is disabled when **Key Creation Method** is set to **Manual Input**.
Key String	This list is displayed when **Key Creation Method** is set to **Manual Input**. Enter a hex string `[0-9, a-f, A-F]` for the key in the **Key String** text-entry box. - Enter 32 hex characters (128 bits) if the selected algorithm is AES128 or ARIA128. - Enter 48 hex characters (192 bits) if the selected algorithm is 3DES. - Enter 64 hex characters (256 bits) if the selected algorithm is AES256 or ARIA256. Re-enter the string in the **Confirm Key String** field.
Key Refresh Period (minutes)	When an Agent Key is cached on host, a GDE Appliance administrator can define the refresh period. This setting only applies to VAE keys. Values are from 1 to 44640 minutes, with 10080 minutes as the default value. When set outside of a domain (on the General Preferences page, System tab), the refresh period is applied globally, that is for all keys.
Automatic Key Rotation	Selecting this option creates a ‘versioned’ key required for a Live Data Transformation (LDT) policy. The key is automatically rotated based on the expiry date and the period defined in the **Key Version Life Span** option. Refer to the *Live Data Transformation Guide* for more information about using this option with LDT policies.
Key Version Life Span	This field is displayed once you enable the **Automatic Key Rotation** check box. This option specifies the frequency of key rotation in days. Refer to the *Live Data Transformation Guide* for more information about using this option for LDT policies.

6. Click **Ok**.

The GDE Appliance creates new versions of keys which have expired or are about to expire in 24 hours. It computes a new expiration date for the newly created (rotated) key version as follows:

`(version creation date) + (key version life span)`

For example;

a. Create a versioned key, `TestKey`, on 2/21/2018.

b. Set the key **Expiration Date** to a week after the date you create the key, for our example that would be 2/28/2018.

c. Set the **Key Version Life Span** to 10 days.

d. The key is created with the **Current Version** as ‘0’ to indicate this is the base version of the key.

The GDE Appliance creates the first version of the key 24 hours before expiration on 2/27/2018, with a new expiration date of 03/09/2018. The **Current Version** column for `TestKey`, on the *Agent Keys* page, displays ‘1’ indicating this is the first version of the key.

The GDE Appliance creates a second version of this key on 03/08/2018 (24 hours before expiration) with a new expiration date of 03/18/2018. The **Current Version** column for

`TestKey`, on the *Agent Keys* page, displays ‘2’ indicating that this is the second version of the key.

Importing Symmetric Keys (BYOK)

Import an external symmetric key to the GDE Appliance:

1. Click **Import Symmetric Key**.
2. Enter the required information in the following fields:
   - **Name**: type a name for the key to be imported. This field is required.
   - **UUID**: enter the unique identifier of the externally generated key. This field is optional.
   - **Description**: type a description for the key to be imported. This field is optional.
   - **Algorithm**: select the algorithm that was used to create the key to be imported (AES128, or AES256). This field is required.
   - **Key type**: select whether the imported key should be of the type that is stored on the GDE Appliance, or whether it should be of the type that is cached on the host, the default option is cached on host. This field is optional.
   - **Hash Padding Algorithm**: select the padding algorithm used to wrap the key. Supported algorithms are, SHA256, SHA 384, SHA512, the default value is SHA256. This field is required.
   - **Mask Gen Function**: select the mask generation function used to wrap the key. Supported algorithms are, SHA256, SHA 384, SHA512, the default value is SHA256. This field is required.

NOTE: You must use the same algorithm for the Hash Padding Algorithm and Mask Gen Function when you wrap the key, for example, if you select SHA512 for Hash Padding Algorithm, you must select SHA512 for the Mask Gen Function. When you import the wrapped key, it will be unwrapped using the same information.

   - **Wrapper Key**: Click Select to select the public key used to wrap the external key. This field is required.
   - **Symmetric Key Material**: Base 64 encoded symmetric key material, wrapped by the public key. This field is required.
3. Click **Ok** to import the key. The imported key is displayed on the *Agent Keys* page, with the **Source** field value of External.

Creating asymmetric keys

Asymmetric keys are based on the RSA algorithm and are used to encrypt the symmetric keys. You can configure the symmetric keys for VTE Agents only.

The public half of an RSA key-pair can be imported into other GDE Appliances so that these other GDE Appliances can encrypt data but not decrypt it. A GDE Appliance with the private half of the RSA key-pair is required to decrypt data.

Create an asymmetric key

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

   The **Add Agent Key** window opens.
3. Click **Add**.
4. Select the **Asymmetric** tab.
5. Complete the fields displayed with the information described in Table 22.

Table 22: Asymmetric Key Fields

Field	Description
Name	Enter the name for the key in the **Name** text-entry box. This field is mandatory. The maximum number of characters is 64.
Description	(Optional) Enter a phrase or string in the **Description** text-entry box that helps you to identify the key. The maximum number of characters is 256.
Template	A key template with a set of pre-defined attributes. Key templates are useful for creating keys of a specific type with specific attributes. Pre-defined template are provided for Microsoft SQL Server TDE agent asymmetric keys called *Default_SQL_Asymmetric_Key_Template*. To create a Microsoft SQL Server TDE agent asymmetric key, choose this template and do not change any of the custom attribute values.
Key Type	Select the type of RSA key to generate. The choices are **Key Pair** and **Public Key**. **Key Pair** creates a standard RSA key in two parts: a public key and a private key. The **Public Key File** text-entry box is displayed when you select **Public Key**. Use the browser to locate and select a public key file that was generated by another server. The default is **Key Pair**. The key format should be “PEM”, which is a base64 encoded format.
Algorithm	Select an encryption algorithm from the **Algorithm** scroll-list. Your choices are RSA1024, RSA2048, and RSA4096. The default is RSA1024.
Public Key File	This text-entry box is displayed when **Key Type** is set to **Public Key**. Click **Browse...** to select the X.509 certificate file that contains the public key.

6. Click **Ok**.

Importing Symmetric Keys

The GDE Appliance allows the import of symmetric keys that are generated externally, i.e. not generated on the GDE Appliance, but generated on another HSM. You can use these keys in

GDE Appliance policies. To import an externally generated key, you must first create an asymmetric RSA key pair (using either the RSA2048, or the RSA4096 algorithm) on the GDE Appliance. The public key component of this key pair is used to wrap the external symmetric key to be imported. The wrapped external key can then imported to the GDE Appliance from the **Import Symmetric Key** button.

To import an external symmetric key into the GDE Appliance:

1. Click **Import Symmetric Key**.
2. Enter the required information in the following fields:
   - **Name**: type a name for the key to be imported. This field is required.
   - **UUID**: enter the unique identifier of the externally generated key. This field is optional.
   - **Description**: type a description for the key to be imported. This field is optional.
   - **Algorithm**: select the algorithm that was used to create the key to be imported. This field is required.
   - **Key type**: select whether the imported key should be of the type that is stored on the GDE Appliance, or whether it should be of the type that is cached on the host, the default option is cached on host. This field is required.
   - **Hash Padding Algorithm**: select the padding algorithm used to wrap the key. Supported algorithms are, SHA256, SHA384, SHA512, the default value is SHA256. This field is required.
   - **Mask Gen Function**: select the mask generation function used to wrap the key. Supported algorithms are, SHA256, SHA384, SHA512, the default value is SHA256. This field is required.

NOTE: You must use the same algorithm for the Hash Padding Algorithm and Mask Gen Function when you wrap the key, for example, if you select SHA512 for Hash Padding Algorithm, you must select SHA512 for the Mask Gen Function. When you import the wrapped key, it will be unwrapped using the same information.

   - **Wrapper Key**: Click Select to select the public key used to wrap the external key. This field is required.
   - **Symmetric Key Material**: Enter the base 64 encoded symmetric key material, wrapped by the public key. This field is required.
3. Click **Ok** to import the key. The imported key is displayed on the *Agent Keys* page, with a **Source** field value of *External*.

Storing and Caching Encryption Keys

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

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

Stored on Server keys

- Stored only on the GDE Appliance.
- Downloaded to non-persistent memory on the host.
- Remain in effect if they were used before losing the GDE Appliance connection.
- A connection to the GDE Appliance is required to download keys after a system reboot in order to access encrypted data.

NOTE: Do not apply **Stored on Server** keys to offline host files because, even if you enter the offline password, when there is no network connection and an attempt is made to access the files, the window making the attempt may wait indefinitely for the online keys.

Cached on Host keys

- Stored on the host for offline use.
- A host encryption key, encrypted using the host password, is downloaded to the host. All hosts using the same encryption key can encrypt/decrypt data on other hosts that use the same key.
- When needed, the key is decrypted and cached. When the host is disconnected from the GDE Appliance, the current policy remains in effect because the encryption key is locally available.
- If the VTE Agent cannot connect to the GDE Appliance after a reboot or `secfs` restart, any attempt to access the contents of an encrypted file on an unconnected host will not complete. The application hangs until the host password is provided to unlock the encryption keys. The application resumes accessing the contents of an encrypted file once the password is provided.
- Can be reestablished after a reboot without access to the GDE Appliance by entering the host password. You can specify the host password using the “`vmsec passwd`” utility, or, you can display the challenge string in challenge-response host deployments using the "`vmsec challenge`" utility.

Cached on Host with Unique to Host

- Unique key stored on the host for offline use.
- Using a token stored with the host record on the GDE Appliance, the encryption key is made unique to each host.
- This unique host encryption key is downloaded to the host and stored and encrypted using the host password.
- When the key is needed, it is decrypted and cached. If the host goes offline and is disconnected from the GDE Appliance, the current policy remains in effect because the encryption key is locally available in the system cache.
- If the VTE Agent cannot connect to the GDE Appliance after a reboot, any attempt to access the contents of an encrypted file on an unconnected host will not complete. The application will hang until the VTE Agent host password is entered in another terminal window. The application resumes execution once the password is provided.
- The key can also be reestablished after a reboot without access to the GDE Appliance through the use of the host password. You can specify the host password using the "`vmsec passwd`" utility, or, you can display the challenge string in challenge-response host deployments using the "`vmsec challenge`" utility.
- These keys are used for locally attached devices, as files encrypted by them can be read by only one host. Therefore, do not use **Cached on Host** with **Unique to Host** keys in any situation where data may be shared by more than one host, such as in clustered environments or any environment that uses host mirroring.
- These keys provide greater security because a key compromised on one host does not compromise the keys on other hosts.

Modifying and Displaying Key Configuration

The following information is displayed in tabular format on the *Agent Keys* page, about the keys on the GDE Appliance (both symmetric and asymmetric).

- **UUID**: The Universally Unique Identifier of the generated key.
- **Name**: Name assigned to the key when created. Names must be unique within a domain but can be repeated across different domains.
- **Versioned Key**: This column indicates whether a key is a 'versioned' key, which means that it can be automatically rotated and a new version created. It contains two sub-columns:
- **Versioned**: Indicates if a key can be versioned. If it is a versioned key, a check mark is displayed.

- **Current Version**: Indicates the version of the key. When a versioned key is created for the first time, the version number is ‘0’. When the key is rotated, the version number increments by 1. Refer to the LDT Guide for more information about versioned keys.
- **Algorithm**: The algorithm used to create the key.
- **Key Type**: If a symmetric key algorithm is configured, Stored on Server or Cached on Host can be selected. 'Stored on Server' keys are downloaded to non-persistent memory on the host. Each time the key is needed, the host retrieves the key from the Security Server. 'Cached on Host' downloads and stores (in an encrypted form) the key in persistent memory on the host.
- **Encryption**: Indicates whether the key is symmetric or asymmetric.
- **Creation Time**: Date and time the key was created.
- **Expiration Date**: Date the key expires. This is set when creating a key. Set the date per your security policies, when the expiry date is reached, it is displayed in red.

  When you set an expiration date for a non-versioned key, when the key expires, you can reset the expiry date. You can also choose to create a new key for your policy, in which case you must rekey your data with the new key. You can create an email notification to alert you when a key is due to expire from the **System > Email Notification** option, at the system level or at the domain level.

  When you set an expiration date for a versioned key, when the key expires, you can rotate the key and set a new expiry date, or have the expiry date update automatically to a value that equals the date the key is rotated plus the period defined in **Key Version Life Span** setting.

NOTE: You must set an expiration date for a versioned key, if you do not set an expiration date, the key will *not* be rotated.

- **Source**: The server that requested the key creation. This can be from a key agent host that submits a request to the GDE Appliance, or from the GDE Appliance itself if the request is generated through the Management Console or vmssc. This field is for informational purposes only and is not editable.
- **Description**: Optional text description of the key.

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

- Description (both symmetric and asymmetric keys)
- Expiration date
- Key type
- Key Refresh Period

Modify and display key information

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

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

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

   The *Edit Agent Key* window displays. The content of this window changes based on the type of key (symmetric or asymmetric) being modified. The Agent Key fields are detailed in Table 23.

Table 23: Edit Agent Key window field information

Field	Description
UUID	The key’s Universally Unique Identifier used to generate a license file.
Name	Name assigned to the key when it was first created. Names must be unique within a domain but can be repeated across different domains.
Source	The machine that requested the key creation. This can be from a key agent host that submits a request to the GDE Appliance, or from the GDE Appliance itself if the request is generated through the Management Console or vmssc. This field is for informational purposes only and is not editable.
Description	(Optional) Text description of the key. The maximum number of characters is 256.
Creation Date	Date the key was created.
Expiration Date	Date the key expires. This is the only field on this screen you can modify.
Algorithm	Algorithm used to create the key. The symmetric key algorithms are 3DES, AES128, AES256, ARIA128, and ARIA256. The asymmetric key algorithms are RSA1024, RSA2048, and RSA4096.

Field	Description
Key Type	If a symmetric key algorithm is configured, `Stored on Server` or `Cached on Host` can be displayed. `Stored on Server` keys are downloaded to non-persistent memory on the host. Each time the key is needed, the host retrieves the key from the GDE Appliance. `Cached on Host` downloads and stores (in an encrypted form) the key in persistent memory on the host. For symmetric keys without `Unique to Host` enabled, you can toggle between `Cached on Host` and `Stored on Server` only. You can enable/disable `Unique to Host` only when configuring a new key. When you switch between `Stored on Server` and `Cached on Host` symmetric keys, the configuration change is pushed to the host. If an asymmetric key algorithm is configured, `Key Pair` or `Public Key` can be displayed. `Key Pair` is a standard RSA key in two parts: a public key and a private key. The GDE Appliance with this type of key can allow an Encryption Agent to back-up and restore data. `Public Key` indicates that key contains only the public key component of a public:private key pair. The GDE Appliance with this key can allow an Agent to back-up data only.
Export Key	(Asymmetric keys only) This button opens or saves the key file. Public key only.
Unique to Host	(Symmetric keys only) When activated, unique keys are stored on the host for offline use when there is no connection to the GDE Appliance. This option can only be enabled/disabled when configuring a new key.
Key Version	(Versioned keys only) Indicates the version of the key. Any time a versioned key is rotated, the version number increments by 1.
Key Hash	(Versioned keys only) The hash value of the key generated using the key string. If the key is a versioned key, this value changes when the key is rotated. This attribute is not applicable to asymmetric keys.
Automatic Key Rotation	(Versioned keys only) If checked, indicates that the key is a versioned key.
Key Refresh Period (minutes)	(Symmetric keys only) When the Agent Key is cached on host, the administrator can define the refresh period. This setting only applies to VAE keys. Values are from 1 to 44640 minutes with 10080 minutes as the default value. When set outside of a domain under *General Preferences*, the refresh period is applied globally, for all new keys. The refresh period is not reset for existing keys.
Key Version Life Span (days)	This field is displayed once you enable the **Automatic Key Rotation** check box. This option specifies the frequency of key rotation in days. You can edit this field. Refer to the *Live Data Transformation Guide* for more information about using this option for LDT policies.

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

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

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

9. Click **Save** to save the public key component of the asymmetric key.

   The **Save As** dialog box opens.

   a. Specify a path and name for the file.

   b. Click **Save**.

   The **Download Complete** dialog box opens.

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

10. Click **Back** to return to the **Keys** window.

Deleting keys

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

Delete keys

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

   The **Agent Keys** window opens.
3. Enable the **Selected** checkbox for those keys you want to delete.
4. Click **Delete**.

Key Groups

Key groups are used to control access to encryption keys by VAE or VKM host administrators. To control access to encryption keys, keys are grouped into key groups, and the key group is then associated with a Client Identity. The Client identity can only access keys in the associated key group. Only Administrators of type Security with the 'Key' role, or type All, can create key groups. See “Identity-Based Key Access” for more information about creating and managing identities.

Only Administrators of type Security with the 'Key' role, or type All, can create key groups and associate key groups with identities. A key group can be associated with multiple client identities, and a key can be part of multiple key groups.

For example, create a key group `keyGrp1` and add two encryption keys to this group. Associate `keyGrp1` with a specific Client Identity. When a user logs on with those Client Identity credentials, that user can only access encryption keys associated with `keyGrp1`.

Key groups can be assigned to more than one client identity, they can be reassigned to different client identities, or can be deleted. Keys in a key group can also belong to more than one key group, and can be removed and reassigned to different key groups.

This functionality is also available via the GDE Appliance REST API, refer to the GDE Appliance REST API documentation for more information (https://<*dsm_IP_address*|*FQDN*>/doc/.

Add Key Group

1. Log on to the GDE Appliance as a Security Administrator with the ‘Key’ role.
2. Navigate to **Keys > Agent Keys > Key Groups** and on the *Key Groups* page, click **Add**.
3. On the *Add Key Group* page, enter a name for the key group. This field is required.
4. Add a description. This field is optional.
5. Click **Add Keys**. Select keys to add to this key group from the **Keys** list on the *Add Keys to Key group* page.
6. Click **Add Selected Keys to Key Group**. The *Add Key Group* page displays.
7. In the **Assigned Client Identities** section of the page, click **Add**, the *Available Client Identities* page displays.
8. Select one or more identities to assign to the key group from the list, click **Ok**.
9. Click **Ok** to create the key group and associate it with a client identity or identities.

Edit Key Group

Keys can be added or deleted from a key group.

1. Click the name of the key group on the Name column of the table on the Agent Key Groups page.
2. Add keys to a key group:
   - Click **Add Keys**.
   - Select the keys to add to this key group from the list on the *Add Keys to Key Group* page and click **Add Selected Keys to Key Group**. You are returned to the *Add Key Group* page.
3. To delete keys from a key group, select the keys and click **Delete Selected**.
4. To remove assigned client identities, select one or more identities from the **Assigned Client Identities** table and click **Delete**.

5. To add client identities:
   - Click **Add** and select one or more identities to assign to the key group from the list, then click **Ok**.
   - Click **Ok** again to confirm the changes.

Delete Key Group

To delete a key group, select the key group name (s) on the *Agent Key Groups* page and click **Delete**.

Exporting and Importing Keys

This section describes exporting and importing symmetric and asymmetric keys for archival, key restoration, or distribution to other GDE Appliances.

You can export, import, and archive the symmetric keys used to encrypt GuardPoint data. You can export and import symmetric keys between GDE Appliances in different HA clusters. You can export the keys of a server to a file in a secure location to ensure that you always have the keys needed to restore encrypted archive data. Without the right keys, encrypted backups are worthless.

NOTE: Keys that use the new CBC-CS1 encryption mode are only supported by and VTE v6.1. If you attempt to import keys that use the new encryption mode to versions earlier than 6.1, the import will fail.

The exported key file is itself encrypted. Before you export any keys, create and distribute the key shares of the wrapper key that will be used to encrypt the key file.

Caution: If you are going to import the keys on another GDE Appliance, be sure to import the wrapper key(s) into the other GDE Appliance *before* you import the key file. Do not lose the key shares or you will be unable to decrypt the key file wrapper.

Exporting keys

1. Log on to the Management Console as an administrator of type Security with Key role permissions, type Domain and Security with Key role permissions, or type All.
2. If you are not already in the appropriate domain, switch to it.
3. Select **Keys > Agent Keys > Export Import Keys**.

The **Export Import Keys** window opens and displays the **Export** tab.

4. If the message “`Export/Import Wrapper Key set.`” is not displayed, create or import a wrapper key before proceeding.

   Create and distribute the wrapper key.

   If the symmetric keys are to be exported to a different server, rather than restored on the originating server, be sure to import the same key shares to the other server to make an identical wrapper key. This way both servers will use the same wrapper key and should be able to successfully encrypt the exported key file on one server and decrypt it on the other.

5. In the **Export** tab, select the check boxes of the keys you want to export.

6. Click **Ok**.

   The **File Download** window opens.

   The options are:

   - **Open** to open the `.dat` file. It will be encrypted so this option is pointless at this time.
   - **Save** to save the `.dat` file on the system running the Management Console Web session, or on another network-accessible system.
   - **Cancel** to close the window and stop the export operation.

7. Click **Save**.

   The default file name is `<`*`server name`*`>_keys_YYYY_MM_DD_HHMM.dat`. For example, `server1.domain.com_keys_2016_05_11_1252.dat`.

   The **Download Complete** window opens. You can view the file location of the downloaded file.

8. Click **Close**.

9. (Optional) Check the **Logs** window for additional information about the key export process.

   A log entry should be generated that identifies who initiated the key export process, the number of keys in the file, the SHA hash of the key file, the file size, and the names of the keys in the file. The following example is for successfully exporting a small file that contains nine keys:

```
KMG0610I: Administrator "admin1" exported 9 symmetric keys to a file with
sha1=8c6c3544bd4352f3a8e93a3f478c16489ecd97e5 and size=3524 bytes, containing
the following keys: aes128, aes128_1, aes128_100901, aes128_StoredOnServer,
aes256, aria128, testkey2aes128, testkeyaes128, testkeyaes128_1
```

Importing keys

1. Log on to the Management Console as an administrator of type Security with `Key` role permissions, type Domain and Security with `Key` role permissions, or type All.

2. Select **Keys > Agent Keys > Export Import Keys**.

   The **Export Import Keys** window opens and displays the **Export** tab.

3. If the message “`Export/Import Wrapper Key set.`” is not displayed, set the wrapper key before proceeding.

   Configure the same wrapper key that you used to create the key file. Copy and paste the same key shares in the **Wrapper Keys** window that you used to make the wrapper file for the exported key file, otherwise you will be unable to import the key file.

4. In the **Import** tab, click **Browse**.
5. Locate and select the key file.
6. Click **Open**.
7. Click **Ok**.

   The **Keys** window opens. If a problem occurs, either real or potential, the **Export Import Keys** window remains open and displays a message. A warning message is displayed if keys in the imported file already exist on the GDE Appliance.

   Another typical warning message is "`Wrong path/file name.`" that is displayed when the specified file cannot be accessed. It is also displayed if there is a wrapper key mismatch. If you get this error message, and you are sure that the path and file name are correct, verify that the same key share used to export the key file is also used to import the key file.

   Upon completion without errors or warnings, the **Keys** window is opened. It shows all configured keys, including the imported keys. Similarly named keys are imported with the same name and appended with *_X*, where *X* is an integer. Each time a key with the same name is imported, *X* increments by `1`.

8. (Optional) Check the **Logs** window for additional information about the key import process. A log entry should be generated for each key that is created on the GDE Appliance. For example:

```
DAO0239I: Administrator "alladmin" created Symmetric Key "testkeyaes128".
```

   Also, a log entry should be generated that identifies the user who initiated the key import process, the number of keys in the file, the SHA hash of the key file, the file size, and the names of the keys in the file. The following example is for successfully importing a small file that contains only three keys:

```
KMG0611I: Administrator "alladmin" imported the following 3 symmetric keys:
testkey2aes128, testkeyaes128, testkeyaes128_1
```

Exporting a public key

A public key is the public-key component of a public:private RSA key-pair. The public key of an RSA key-pair is used to make backups only. The private key of an RSA key-pair is used to restore backups. The public key can be imported into other GDE Appliances to enable them as backup-only GDE Appliances. Shared public keys are for environments in which data is backed up in one place with one set of policy constraints, and the backup is restored in another place with a different set of policy constraints.

Export the public key of an RSA key pair

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

   The **Agent Keys** window opens.
3. Click the RSA key-pair or RSA public key in the **Name** column that you want to export.

   The **Edit Agent Key** window opens.
4. Click **Click to Export**.

   The **File Download** window opens, prompting you to save the public key.
5. (Optional) Click **Open** to display the public key.

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

   The file locater opens.
7. Enter the path and name for the file.

   The default file name is `PublicKey.xml`.
8. Click **Save**.

Importing a public key

Import the public key of an RSA key pair

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

   The **Agent Keys** window opens.
3. Click **Add**.
4. Select the **Asymmetric** tab.
5. Select **Public Key** from the **Key Type** scroll-list.

   The **Algorithm** scroll-list is replaced with the **Public Key File** text-entry box.
6. Enter the name to assign the imported public key in the **Name** text-entry box.
7. Click **Browse...** to open the file locater.
8. Locate and select the public key file.
9. Click **Open**.

10. (Optional) To set an expiration date for the key, enter the date manually in the **Expiry Date** text-entry box in the form *MM/DD/YY*, or click the calendar icon, 📅, and select the expiration date from the graphic interface.
11. Click **Ok**.

    The **Agent Keys** window opens and displays the imported key. The key type is **Public Key**.

Key Templates

Key templates let you quickly add agent 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. This is particularly helpful for applications with keys that have customized attributes.

NOTE: Pre-defined templates for Microsoft SQL Server TDE agent keys are provided: `Default_SQL_Asymmetric_Key_Template` and `Default_SQL_Symmetric_Key_Template`.

Warning! DO NOT modify any of the attributes in either of the Microsoft SQL Server TDE key templates or you may prevent access to the database.

You can also enforce key template usage when creating keys. This means that GDE Appliance administrators creating keys must select a key template to define the key's attributes.

The key templates feature allows you to specify common attributes (for example, name, description and algorithm) and custom attributes (that is, attributes specific to certain types of keys such as Microsoft SQL Server TDE keys). The attributes and interface information for key templates are as follows:

Common template attributes:

- **Name**—Name you assigned the key template when you created it. Names must be unique within a domain but can be repeated across different domains.
- **Description**—Optional text description of the key template.
- **Algorithm**—Algorithm used to create the key. The symmetric key algorithms are `3DES`, `AES128`, `AES256`, `ARIA128`, and `ARIA256`. The asymmetric key algorithms are `RSA1024`, `RSA2048`, and `RSA4096`.

- **Key Type**—Stored on Server, Cached on Host, Key Pair, Public Key.
- **Unique to Host**—This can be selected with `Cached on Host`.
- **Expiry Date**—Date the key expires.
- **Application Specific Information**—Optional data that is specific to the application.
- **Contact Information**—Optional contact information.
- **Attribute Name**—Name of the added custom attribute.
- **Attribute Value**—Value of the added custom attribute.

Default Microsoft SQL Server TDE symmetric key template attributes:

- **Attribute Index**—Value indicating whether a key is `supported` (0x01), `volatile` (0x02), `exportable` (0x04) or `importable` (0x08). The attribute value can be any combination of these bit masks. For example, an attribute that is supported and exportable would be 0x05.
- **Cryptographic Usage Mask**—A bit mask to define the key cryptographic usage. The first 7 bits indicate Sign, Verify, Encrypt, Decrypt, Wrap Key, Unwrap key, and Export. The SQL server requires that a symmetric key can be used for all those purposes. The cryptographic usage mask value in binary bits is 1111111 (decimal value is 127).
- **Object Type**—The type of object. Values can be `SymmetricKey`, `PublicKey` or `PrivateKey`. Since this is the key template for symmetric key, the value must always be `SymmetricKey`.
- **x-VormCanBePlainText**—Specifies whether the key value can be revealed in plain text outside the GDE Appliance (`true`) or not (`false`). This value is always set to `true`.
- **x-VormCanNeverBeExported**—Specifies whether the GDE Appliance can never export key values, and will return an error when a user tries to do an export (`true`) or not (`false`). This attribute protects sensitive key material from being exported outside the server. In general, only public keys can be exported. This value is always set to `true` (you cannot export key values).
- **x-VormCanNeverBePlainText**—Specifies whether the key value can never be revealed in plain text outside the GDE Appliance (`true`) or if revealing it in plain text is allowed (`false`). This value is always set to false (key values can be revealed in plain text).
- **x-VormCanObjectPersist**—Specifies whether the GDE Appliance can store the key after it creates it (`true`) or does it create the key and return it to Key Agent without storing it (`false`). This value is always set to `true`.
- **x-VormID**—This is the SQL-server-customized key identifier that the SQL server uses to locate the key. The value must be unique in GDE Appliance.

Default Microsoft SQL Server TDE asymmetric key template attributes:

- **Attribute Index**—Value indicating whether a key is `supported` (0x01), `volatile` (0x02), `exportable` (0x04) or `importable` (0x08). The attribute value can be any combination of these bit masks. For example, an attribute that is supported and exportable would be 0x05.
- **Cryptographic Usage Mask**—A bit mask to define the key cryptographic usage. The first 7 bits indicate Sign, Verify, Encrypt, Decrypt, Wrap Key, Unwrap key, and Export. The SQL server requires an asymmetric private key be used for signing, decryption, unwrapping and exporting purposes. The cryptographic usage mask value in binary bits is 1101001 (decimal value is 105).
- **Object Type**—The type of object. Values can be `SymmetricKey`, `PublicKey` or `PrivateKey`. Since this is the key template for asymmetric key, the value here will always be `PrivateKey`.
- **x-VormID**—This is the SQL server customized key identifier that the SQL server uses to locate the key. The value must be unique in GDE Appliance.

Common Key Template Procedures

Use the following procedures to manage your key templates.

Adding a key template

1. Select **Keys > Key Template.** The **Key Templates** window opens.
2. Click **Add.** The **Add Key Template** window opens.
3. Fill in the desired standard attributes.
4. Click **Add** to add customized attributes. The **Key Template Attribute** window appears.
5. Add the attribute name and attribute value and click **Ok**. Add as many customized attributes as desired.
6. Click **Ok** in **Add Key Template** window. The **Key Templates** window appears with the new template listed.

Deleting a key template

1. Select **Keys > Key Template**. The **Key Templates** window opens.
2. Select the template you want to delete.
3. Click **Delete**.

Modifying a key template

1. Select **Keys > Key Template.** The **Key Templates** window opens.
2. Click on the template name to modify existing attributes or add custom attributes.

NOTE: DO NOT modify any of the attributes in either of the Microsoft SQL Server TDE key templates called `Default_SQL_Asymmetric_Key_Template` and `Default_SQL_Symmetric_Key_Template`. Doing so may prevent access to the database.

Using a key template

1. Select **Keys > Agent Keys > Keys**.
2. Click **Add**. This displays the **Add Agent Key** window
3. Click the **Template** pull down menu and select a key template.

Enforcing a key template to define a key

1. Select **System > General Preferences > System Tab.** The **General Preferences** window opens.
2. Click on **Enforcing Using Key Template to Define Key**.
3. Click **Apply**.

Identity-Based Key Access

The VAE and VKM agents provide identity-based access control to encryption keys stored on the GDE Appliance. The identity of a VAE or VKM user is established using credentials; user name and password, and a corresponding identity profile is created on the GDE Appliance. This GDE Appliance identity profile is then associated with a key group that contains the keys that client identity is allowed to access. When a VAE or VKM user logs in with a Client Identity profile and tries to access keys, the GDE Appliance verifies that identity profile and then grants access to keys in key groups associated with that identity profile. For more about creating and managing key groups see the section “Key Groups” above.

An identity can be associated with multiple key groups. Only Administrators of type Security with the 'Client Identity' role or an Administrator of type All, can create client identities.

NOTE: Security Administrators with just the Client Identity role assigned can only create identities and cannot perform any other tasks on the GDE Appliance. Additionally, Security Administrators with just the Client Identity role assigned can view only limited menu options. As a best security practice, Thales recommends that you do not assign both ‘Key’ and ‘Client Identity’ roles to a single Security administrator.

Username Requirements

The identity’s username requirements are as follows:

- May contain the following non-alpha-numeric characters:
  - at (@)
  - dot (.)
  - underscore (_)
  - dash (-)

Password Requirements

The password restrictions are:

- Cannot allow colon ":"
- Min password length: 1 character
- Maximum password length: 256 characters

For password requirements:

- Your application may contain other requirements for passwords. Follow the requirements provided in the application documentation.

Add Client Identity

Log on to the GDE Appliance as an Administrator of type Security with the 'Client Identity' role or an Administrator of type All. If you log in as a Security Administrator with the 'Client Identity' role, only the Dashboard, Domain and Keys menu options are available.

1. Navigate to the **Keys > Identities** page.
2. On the *Client Identities* page, click **Add**, the *Add Client Identity* page displays.
3. Enter the following information:
   - **Identity Name**: name of the VAE/VKM user.
   - **Description**: a description for the identity profile, this is optional.
   - **User password**: the user password, enter the password again to confirm
4. Click **Ok** to add that identity profile to the GDE Appliance.

Edit Client Identity

Edit a client identity to change the password or description.

To change the password:

1. On the *Client Identities* page, click the client identity in the **Name** column, the *Edit Client Identity* page displays.
2. Select the **Update User Credentials** check box.
3. Enter the new password information in the **User Password** and **Confirm User Password** fields.
4. Click **Ok** to confirm the update.

To change the description:

1. On the *Client Identities* page, click the client identity in the **Name** column, the *Edit Client Identity* page displays.
2. Edit the contents of the **Description** field and click **Ok** to confirm the update.

Delete Client Identity

To delete a client identity or identities:

1. Select the identity to remove.
2. Click **Delete**.

Configuring Policies

20

The primary job of a GDE Appliance Security Administrator is to create policies that protect data. Policies govern access to, and encryption of, the files in VTE-protected directories. VTE-protected directories are called GuardPoints.

This chapter contains the following sections:

Overview

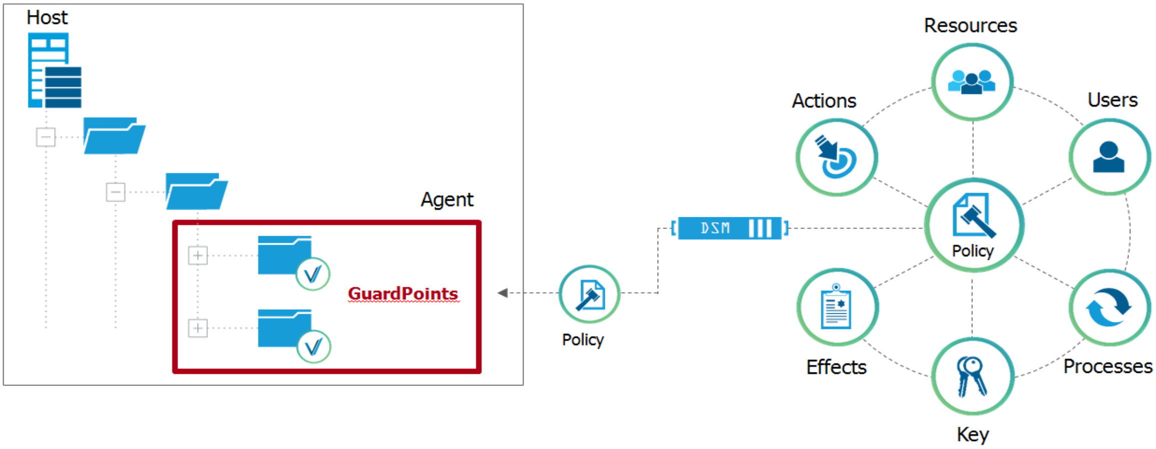
A Data Security policy is a collective set of rules that govern data access and encryption. Think of a policy as an if-then statement. The rules are processed sequentially. If the criteria of rule one are not met, the policy enforcement engine moves on to the second rule and so on. The following criteria are processed by the policy enforcement engine:

- **Order**: Security rule enforcement sequence.
- **Resource**: Files and/or directories to which the policy will apply, plus key rules that govern those files and directories.
- **User**: Users and user groups authorized to access the resources.
- **Process**: Executables which will access the files.
- **Action**: Type of user access being made (read, write, copy, move etc.). Before you can define Data Transformation Rules, you must select an Action type of Key_op.
- **Effect**: When all the other rules match, this describes the type of access granted or denied per the rule.
- **When**: Time frame within which the action occurs.
- **Browsing**: Allow browsing is enabled by default, while the Enable Communication check box is enabled on the host. This allows the server to browse the host's file system. This option can be deselected even if host communication is still enabled.

A policy comprises 'Security Rules' and 'Key Rules'. A security rule defines the users or user groups authorized to have specified access to specific files or directory paths for a designated period of time. In short, it defines who is accessing data (**User**), what they can do with the data (**Action**), which applications or executables have access to the data (**Process**), where the data is located (**Resource**), the time frame that the 'Security Rule' is applicable (**When**), and how the data can be accessed (**Effect**), and if it can be viewed from the GDE Appliance (**Browsing**).

A key rule defines the encryption key to apply to a specific resource set or the encryption key to use as the default key, in the event that no other key rule matches. It defines the sequence in which the key rules are to be executed (**Order**), the location of the data to be encrypted (**Resource**), the encryption key to be applied to the resource set (**Key**). When defining a key rule for a Live Data Transformation (LDT) policy, you can select a key that is applied to the resource set (**Current Key**) and the key to use to rekey that resource set (**Transformation Key**).

Figure 17: Policies and how they relate to the GuardPoints, Hosts, and the GDE Appliance



Policy Rule Criteria and Effects

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

Table 24: Policy Rule Criteria

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

Table 25: Policy Rule Effects

Effect	Action
Permit	Permit access to the data.
Deny	Deny access to the data.
Apply Key	Encrypt data written into GuardPoint with the key specified in the *Key Selection Rules* tab. Decrypt data that is accessed using the same key.
Audit	Creates an entry in the Message Log that describes what is being accessed, when it is being accessed, the security rule being applied.

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

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

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

Creating and Configuring VTE Policies

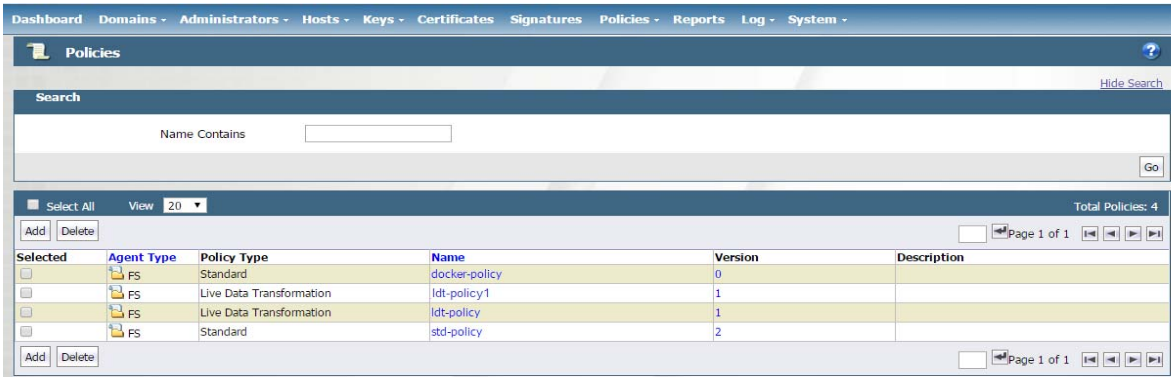
Access the Domain to be Protected

1. Log on to the Management Console as a GDE Appliance Security Administrator to the domain containing your protected host. Or log into the local (restricted) domain to which you belong.
2. Switch to the domain containing the host you want to protect. Click **Domains > Switch Domains.** The **Switch Domains** window opens.
3. Select the domain containing the protected host and click **Switch to domain**. The domain to which you switched, is displayed in the upper right corner of the Management Console.

Add a Policy

1. Click **Policies > Manage Policies** to list the policies available to this domain.

Figure 18: Policies, Management window



Name Contains

View 20

Total Policies: 4

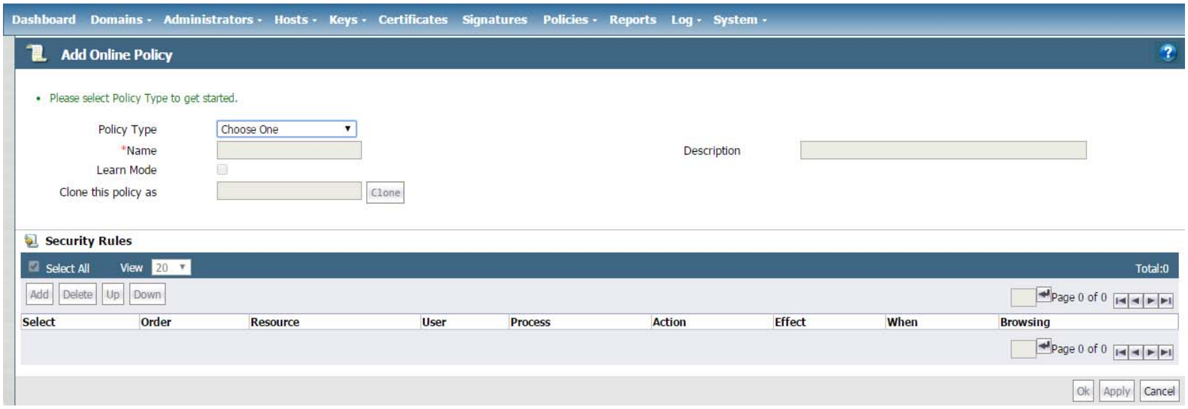
Page 1 of 1

Selected	Agent Type	Policy Type	Name	Version	Description
□	FS	Standard	docker-policy	0	
□	FS	Live Data Transformation	ldt-policy1	1	
□	FS	Live Data Transformation	ldt-policy	1	
□	FS	Standard	std-policy	2	

Page 1 of 1

2. Click **Add**. The *Add Policy* page displays.

Figure 19: Add Policy window



- Please select Policy Type to get started.

Policy Type: Choose One

*Name:

Learn Mode: □

Clone this policy as: Clone

Description:

3. Add a policy by selecting and entering the following information.

   a. Select a policy type from the **Policy Type** drop-down list. The available options are **Standard** and **Live Data Transformation** (LDT). The LDT policy type is only available if you have a valid LDT license.

   See “Enabling Live Data Transformation” for more information about LDT. Refer to the *Live Data Transformation Guide* for information about implementing LDT.

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

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

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

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

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

4. Clicking **Ok** at this point creates a blank policy called `basic-access-policy` if you are creating a standard policy. This policy has no rules.

If you selected an LDT policy, `ldt-policy`, per our example, this policy has one security rule added to it by default—key_op—that cannot be deleted, edited or reordered.

To add rules to the policy, click **Add**. The **Add Security Rule** window opens.

Add Security Rules to a Policy

Security rules specify how the GDE Appliance will respond to an access request.

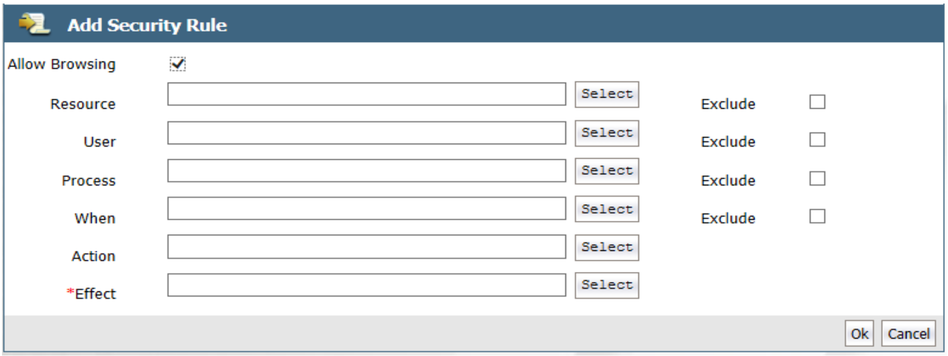
To add security rules to a policy:

1. Open the **Add Security Rule** window if it is not displayed. Click the policy name in the **Policies** window if the policy has already been created. Click **Add** in the **Security Rules** panel. The **Add Security Rule** window opens.

   If you chose a **Live Data Transformation** policy type, then the first security rule for the policy is created by default. This rule permits key operations on all resources for that policy, without denying user or application access to resources, so that a rekey operation can be done whenever the encryption key is versioned. This rule is *always* the first rule in an LDT policy and cannot be edited.

For more information about creating policies for Live Data Transformation, refer to the *Live Data Transformation Guide.*

Figure 20: Add Security Rule window



Add Security Rule

Allow Browsing	☑			
Resource		Select	Exclude	□
User		Select	Exclude	□
Process		Select	Exclude	□
When		Select	Exclude	□
Action		Select		
*Effect		Select		

2. Click **Allow Browsing** to enable the user to access and traverse directories below the GuardPoint, leading down to the resources in the rule. Users that match the criteria set by the security rule can access the directories between the GuardPoint and the resource. If you define a resource, then that resource should exist in the GuardPoint. The files in these directories can be listed like any file in a browser, but they cannot be modified, copied, or deleted.

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

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

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

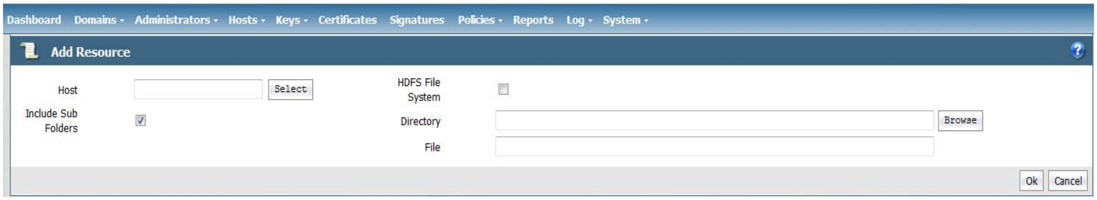
   To define specific resources in a GuardPoint, select **Resource**. The **Select Resource Set** window opens.

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

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

   c. Click **Add**. Here you specify the **Host**, **Directory** and **Files** on which to apply the rule. If your host is a Docker host, another field is displayed; **Docker Image/Container**.

Figure 21: Add Resource window



Host

Include Sub Folders ☑

HDFS File System □

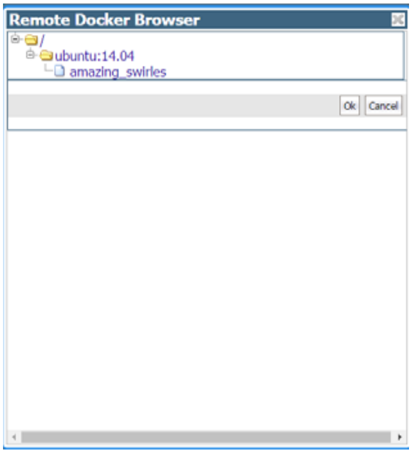
Directory

File

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

Host is the hostname containing the directory. Enter the hostname and click **Browse** to browse for the directory. If your host is a Docker host, another field is displayed; **Docker Image/Container**. Click **Browse** to open the **Remote Docker Browser** to select a Docker image or container, from which to select a resource.

Figure 22: Remote Docker Browser



```
/
  ubuntu:14.04
    amazing_swirles
```

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

Directory is appended to the GuardPoint. If the GuardPoint is `/mnt/remote2` and the directory is `/remoteDir`, then the policy applies to the files and directories in `/mnt/remote2/remoteDir`. If your host is a Docker host, clicking **Browse** opens the **Remote File Browser**, select a Docker image or container, from which to select a resource.

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

`sales/` — Access limited to `sales` directory under the GuardPoint.

`*sales/` — Access limited directories that end in "`sales`" under the GuardPoint. If you omit a leading path delimiter (back slash or forward slash) in a directory name before an asterisk e.g., `*sales`, a pop-up will prompt you to select whether the directory is on a Windows or non-Windows OS, and a '`/`' or '`\`' will be added accordingly as follows; for example if you select Windows the result will be `*\sales.`

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

The variables `|uname|` (user name) and `|gname|` (group name) can be used. On UNIX systems, `|uid|` and `|gid|` may also be used.

When the security rule is applied, the variable is replaced by the actual user name or user group name.

For example, if **Directory** is set to `/opt/local/ |gname|`, when you later make `/opt/local` the GuardPoint, only the members of the group specified as "engineering" in **Users** are allowed access to `/opt/local/engineering`.

`uname` and `gname` are like macros. Another example: if you want to define a policy to protect all the user directories under `/home`, you do not need enumerate `/home/steve`, `/home/george`, `/home/Richard`, and so on. You only need to define `/home/|uname|`, When the agent evaluates the policy, it replaces `|uname|` with the actual user, so when Steve logs on, the agent evaluates the policy with `/home/steve`, and they will not be able to access `/home/george`.

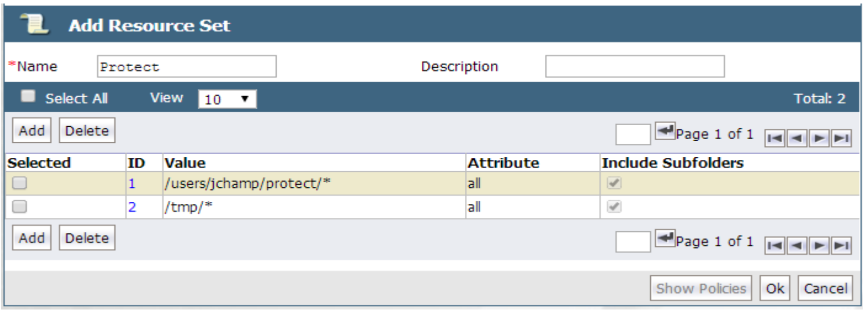
When a resource set is defined with a leading asterisk in the directory path, a leading path delimiter (back slash or forward slash) is inserted at the beginning of the string, e.g., `*/sales` results in `/*/sales`. If the **File** field is left blank, a trailing delimiter and asterisk are added to the path, the asterisk indicating that all files under that directory are included in the definition. For example, if a directory path is defined as `*/sales/*` and the **File** field is blank, it results in `/*/sales/*/*`.

File is the filename and can include variables or patterns.

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

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

Figure 23: Add Resource Set window



*Name: Protect
Description:

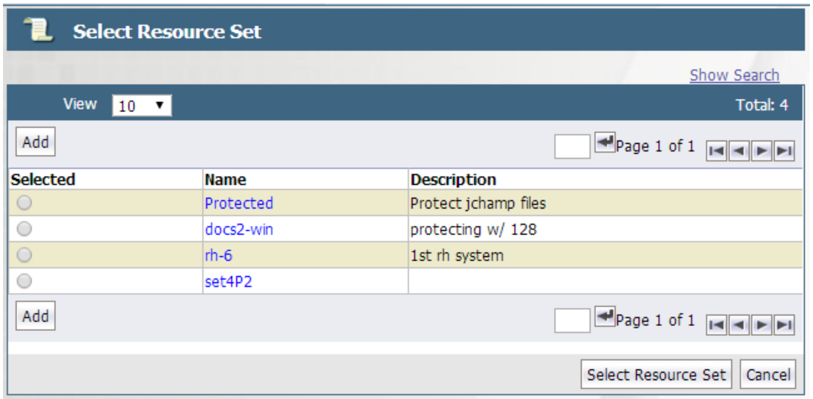
View: 10 — Total: 2

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

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

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

Figure 24: Select Resource Set window with new resource set added.



View: 10 — Total: 4

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

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

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

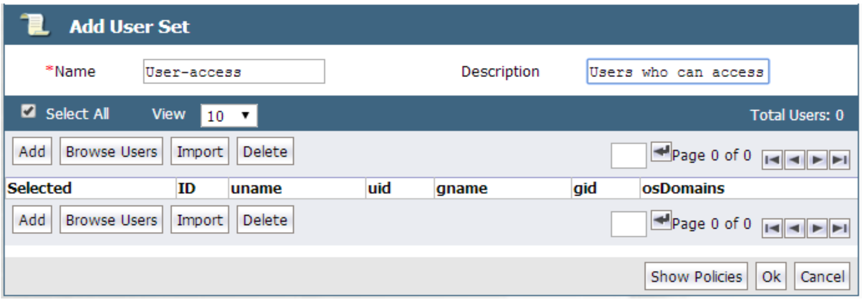
4. Specify the **User** criteria. **User** allows you to specify the users that are permitted or denied GuardPoint access.

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

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

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

Figure 25: Add User Set window



*Name: User-access

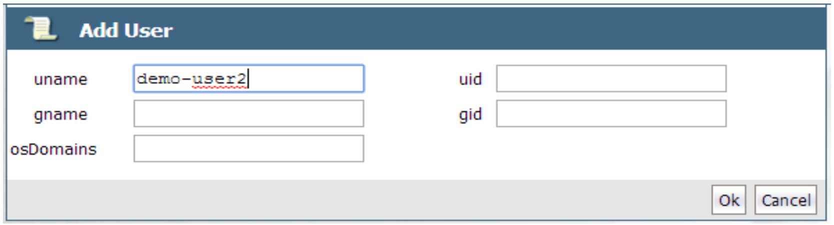
Description: Users who can access

☑ Select All View 10 ▾ Total Users: 0

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

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

Figure 26: Add User window



uname: demo-user2

uid:

gname:

gid:

osDomains:

uname—login name.

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

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

gname—comma-separated list of group names.

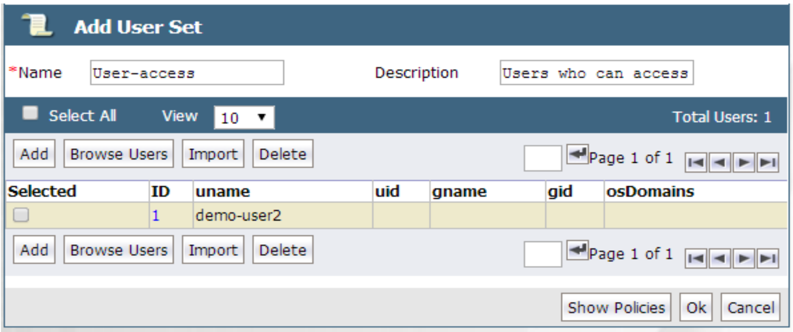
osDomain (*Windows only*)—network domain of the user. Multiple domain names, separated by commas, may be entered. Enter the string **`localhost`** to configure a generic domain.

If you click **Browse Users**, the *Add Users* page opens, you can select users from an LDAP server if configured, or from a selected host. To select users from docker images or containers, use the default Agents selection and select the host name (FQDN) of the Docker host from the list. Since this a Docker host, another field is displayed; Docker Image/Container. Click **Browse** to open the Remote Docker Browser to select a Docker image or container from which to select users.

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

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

Figure 27: Add User Set window



Add User Set

*Name: User-access

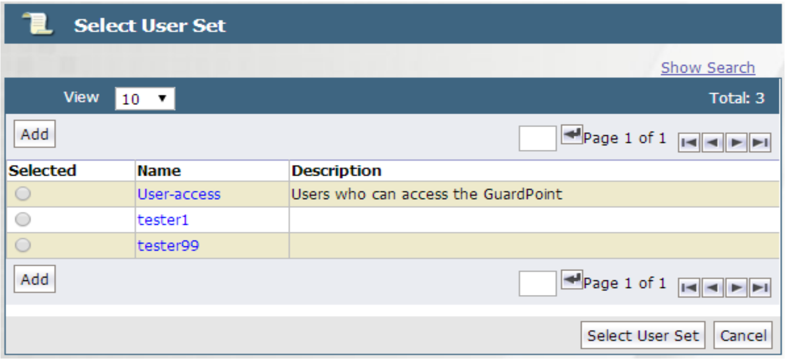
Description: Users who can access

Total Users: 1

Selected	ID	uname	uid	gname	gid	osDomains
□	1	demo-user2				

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

Figure 28: Select User Set window



Select User Set

Total: 3

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

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

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

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

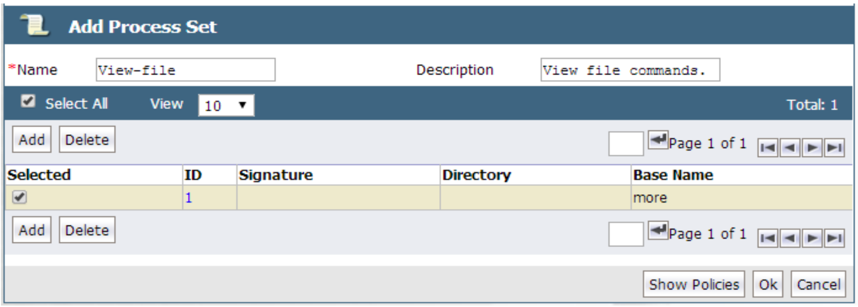
5. Specify the **Process** criteria. **Process** allows you to specify the executables that are permitted or denied access to the GuardPoint data.

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

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

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

Figure 29: Add Process Set window



*Name View-file

Description View file commands.

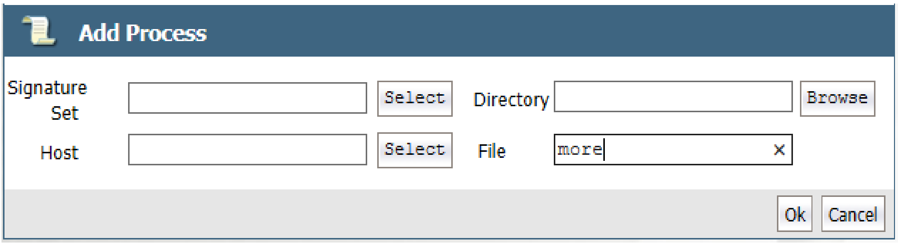
☑ Select All View 10 Total: 1

Selected	ID	Signature	Directory	Base Name
☑	1			more

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

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

Figure 30: Add Process window



Signature Set

Directory

Host

File more

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

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

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

or left blank.

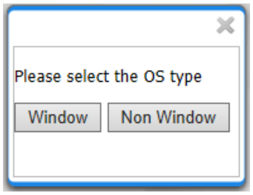
File—name of the executable. The `more` command is used in the example.

Click **Ok** to add this process to the Process Set.

If you select a Docker host, the **Docker Image/Container** field is displayed, select a Docker image or container, in the **Directory** field, click **Browse** and select a directory from the **Remote File Browser**, fill in the file name field as required. Click **Ok** to return to the *Add Process Set* page.

If you get the pop-up as shown in Figure 31, click **Windows** for Window hosts and **Non-Windows** for Linux hosts.

Figure 31: OS Type Pop-Up dialog



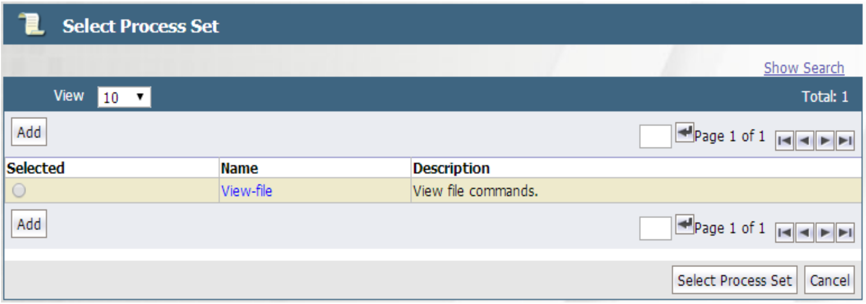
Please select the OS type

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

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

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

Figure 32: Select Process Set window



Select Process Set

Selected	Name	Description
○	View-file	View file commands.

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

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

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

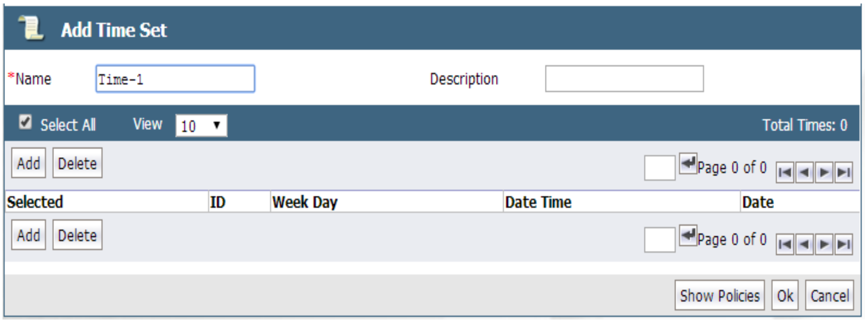
6. Specify the **When** criteria. **When** enables you to specify when GuardPoint access is allowed.

a. To specify *all* times, i.e. 24-hour access, leave **When** blank.

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

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

Figure 33: Add Time Set



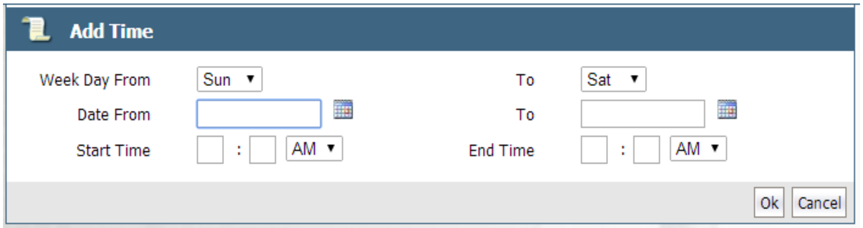
*Name: Time-1

☑ Select All View: 10 Total Times: 0

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

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

Figure 34: Add Time window



Week Day From: Sun To: Sat

Start Time: AM End Time: AM

Week Day From - To is a range of days of the week during which access is denied or permitted. Values are Sunday through Saturday. Enter a day of the week to begin allowing access and a day of the week to stop access.

Date From - To is a range of dates during which access is denied or permitted. Enter a calendar dates to from when to begin allowing access and when to stop.

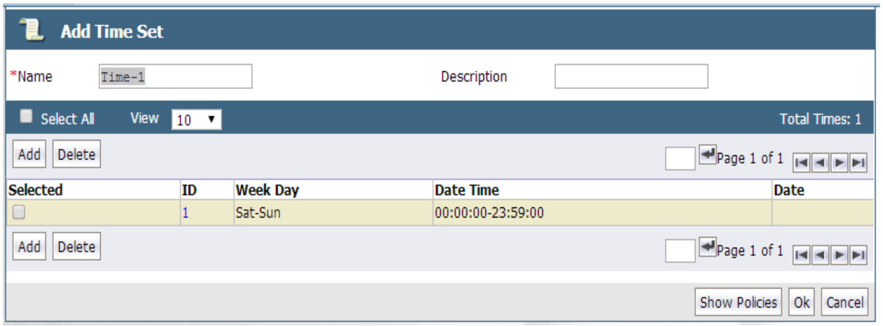
Start Time - End Time is a range of times during which access is denied or permitted. Enter a start time in the format *hh:mm*, select AM/PM, to allow access, and an end time in the format *hh:mm*, select AM/PM. This defines the exact start time and end time during which access is permitted.

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

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

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

Figure 35: Add Time Set window



*Name: Time-1

Description:

View: 10

Total Times: 1

Selected	ID	Week Day	Date Time	Date
□	1	Sat-Sun	00:00:00-23:59:00	

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

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

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

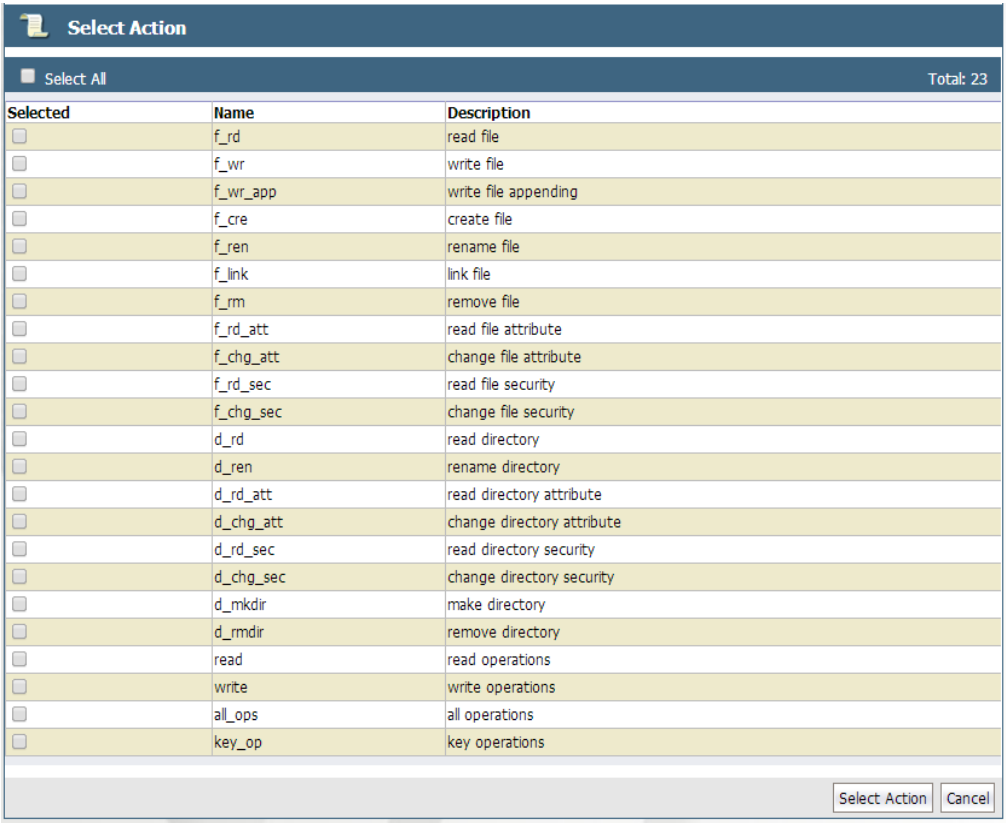
You can also create or select Time Sets directly, without creating a policy, by clicking **Policies > Manage Policies > Time Sets** to bring up the *Time Sets* window.

7. Specify the **Action** criteria. **Action** allows you to specify the type of file and directory action allowed in a GuardPoint.

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

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

Figure 36: Select Action window



Select Action

□ Select All Total: 23

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

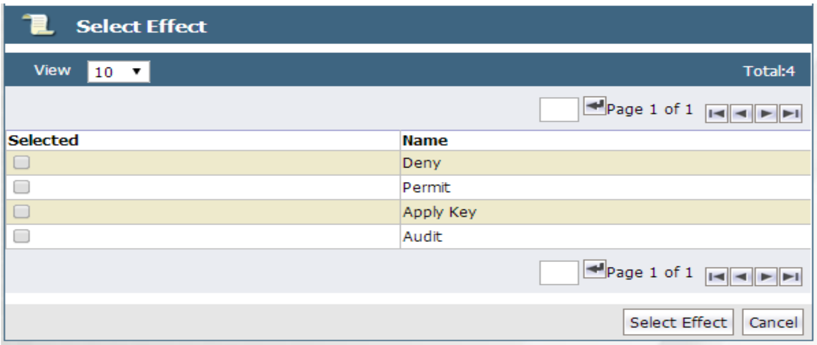
i. Select the allowable actions, and click **Select Action**. The **Add Security Rule** window opens with the allowable actions.

NOTE: key_op is used for the `dataxform` command. If you select key_op and click **Ok** on the **Edit Security Rule** window, you must add a Data Transformation Rule.

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

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

Figure 37: Select Effect window



Selected	Name
□	Deny
□	Permit
□	Apply Key
□	Audit

Deny—Denies the access attempt to the resource.

Permit—Grants the access attempt to the resource.

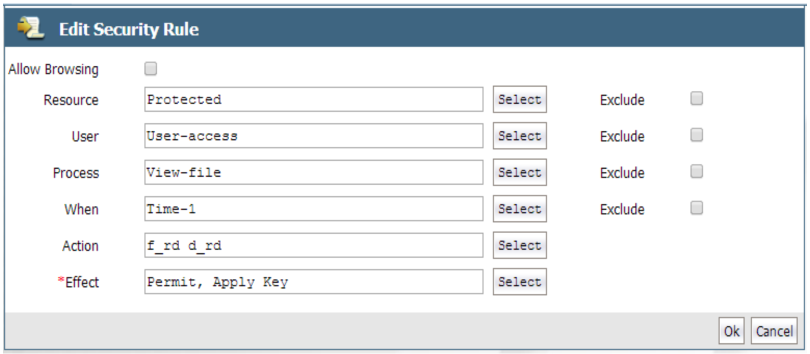
Audit—Used in conjunction with **permit** or **deny**, **audit** creates an entry in the Message Log that describes what is being accessed, when it is being accessed, and the security rule being applied.

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

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

b. Select desired effects and click **Select Effect**. The *Edit Security Rule* window opens with all criteria and the effects displayed (Figure 38).

Figure 38: *Edit Security Rule* window



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

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

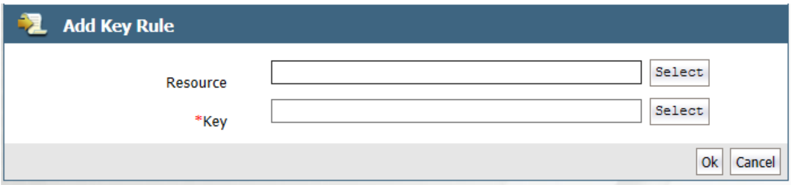
Add Key Selection Rules

After setting up the Security Rules, set up your *Key Selection Rules*.

1. Click **Add** in the **Key Selection Rules** panel at the bottom of the *Add Policy* window.

   The **Add Key Rule** window opens.

Figure 39: Add Key Rule window



- **Resource**—(Optional) Opens the **Resource Set List** window from which you can select or create the resource set whose members are to be encrypted. If you do not specify a resource set in the **Key Selection Rules** tab, encryption is applied to the resources specified in the **Security Rules** tab.
- **Key**—Enables you to enter a key name, or, if selected, the **Select Symmetric Key** window opens allowing you to select an existing key.

If you selected a Live Data Transformation policy type, instead of **Key**, the following fields are displayed:

- **Resource**—(Optional) Opens the **Resource Set List** window from which you can select or create the resource set whose members are to be encrypted. If you do not specify a resource set in the **Key Selection Rules** tab, encryption is applied to the resources specified in the **Security Rules** tab.
- **Current Key**—The current key specifies the key applied to existing data prior to application of LDT policy. The current key can be a clear key or a non-versioned key. When a policy is applied to protect data, Live Data Transformation uses the current key to transform data to the current version of the Transformation Key.

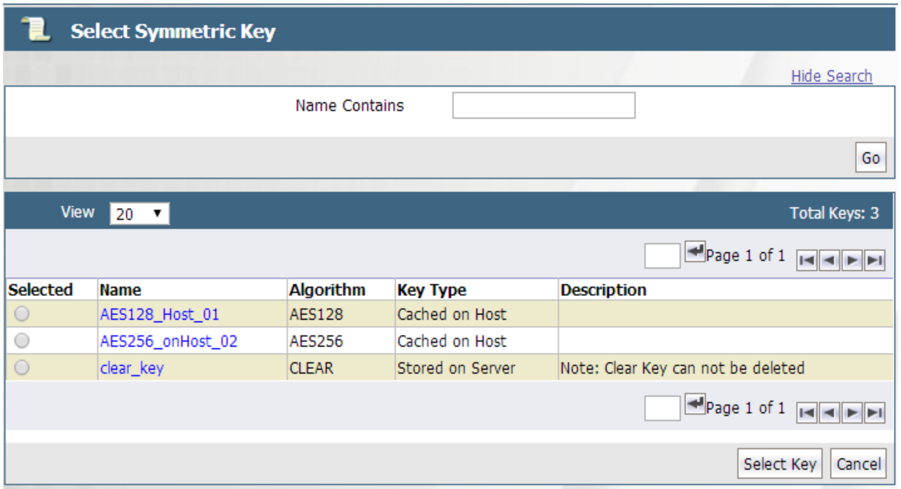
  Enter a key name, or, if selected the **Select Symmetric Key** window displays, allowing you to select a non-versioned key.
- **Transformation Key**—This is the versioned key applied to data for initial transformation from current key and subsequent rekeying to the next version of Transformation Key.

  Click **Select** to open the **Select Symmetric Key** window, and select a versioned key.

See “Versioned Keys”, for more information about LDT versioned keys.

2. Select a **Resource**, if desired, then select **Key**. The **Select Symmetric Key** window opens. If this is a key rule for an LDT policy, then select **Current Key**.

Figure 40: Select Symmetric Key window



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

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

b. If this is a key rule for an LDT policy, after selecting a **Current Key**, you must select a **Transformation Key** on the *Add Key Rule* page. Once you've selected both keys, click **Ok** to return to the *Edit Policy* page.

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

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

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

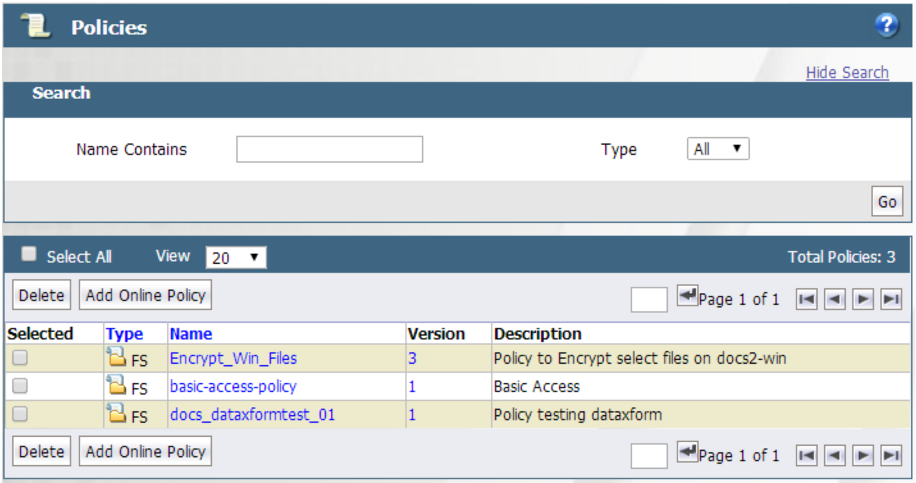
- Set **Action** to **all_ops**

Set **Effect** to **deny audit**

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

The **Policies** window opens (Figure 41) and the policy you just created can be applied to a GuardPoint.

Figure 41: Policies window



Name Contains:

Type: All

View: 20

Total Policies: 3

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

Displaying Policies

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

Display Policies

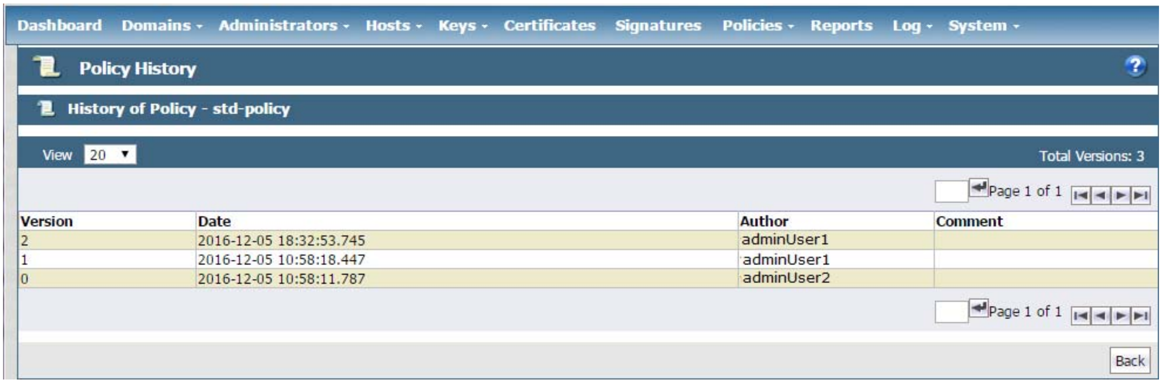
1. Log on to the Management Console as an administrator of type Security with `Policy` role permissions, type Domain and Security with `Policy` role permissions, or type All.
2. Select **Policies** in the menu bar.

   The *Policies* window opens. Configured policies are displayed.

Policy History

The number of times a policy has been changed is displayed in the **Version** column of the **Policies** window. This number indicates the current revision only. It cannot be used to roll-back to a previous version. Restore a backup to revert to a previous online policy version. The version count starts at zero when the online policy is initially created and increments by one each time it is saved thereafter. Click the policy version number in the **Version** column to view the version history of a policy.

Figure 42: Policy version history



Policy History

History of Policy - std-policy

View 20

Total Versions: 3

Page 1 of 1

Version	Date	Author	Comment
2	2016-12-05 18:32:53.745	adminUser1	
1	2016-12-05 10:58:18.447	adminUser1	
0	2016-12-05 10:58:11.787	adminUser2	

Page 1 of 1

Customize display in the Policy window

- The **Show Search** label located below the **Policies** banner opens the **Search** panel. You can enter all or part of a policy name and/or limit the search to policies that are used by a specific type of agent (All or FS). Click **Go** to display only those policies that match the search criteria. Click `Hide Search` to conceal the **Search** panel.
- **Select All**—Selects all the policies that are displayed on the current Web browser page. Select this checkbox to select all the policies on the current page at one time. If you have enabled the **Select** checkbox for many individual policies, a quick way to deselect them is to enable and then disable the **Select All** checkbox.
- **View**—A scroll-list from which to select the maximum number of policies to display on the current page. Up to 200 policies can be displayed on one page. Displays up to the specified number of policies on one Web page, regardless of the display number specified in the preferences.

Navigation buttons are displayed in the **Policies** window. Use these buttons to advance between pages. The buttons are shown in Table 26:

Table 26: Policy Window Panel Navigation Buttons

⏮	First. Display the first page of policies in the *Policy* window.
◀	Previous. Display the previous page of policies in the *Policy* window.
▶	Next. Display the next page of policies in the *Policy* window.
⏭	Last. Display the last page of policies in the *Policy* window.

↵	Jump to. Advance to the specified page of information. Enter the page number in the text-entry box that is next to this button.

Exporting and Importing Policies

GDE Appliance policies can be exported and then imported to the same or another GDE Appliance where you want to replicate the policies you've already created.

You can choose to export all policies from a GDE Appliance or just some specific policies. Policies are exported to a .tar file with the following naming convention; *policy_<YYYY_MM_DD_HHMM>.tar*.

When policies are imported to a domain, all the sets (resource sets, user sets, process sets, and time sets) are imported with the following conditions:

- If a set in the imported policy does not exist in the domain that policy is being imported to, then that set is created.
- If a set in the imported policy exists in the domain to that policy is being imported to, then the existing set is overwritten.
- If a name of a policy being imported conflicts with a name on the domain where it is being imported to, then a number is appended to the name before it is imported. For example, if the imported policy and a policy in the domain where the policy is being imported both contain a policy named 'secure_file_policy' then the policy will be imported as 'secure_file_policy_1'.

Export a policy

If you choose to export only some specific policies, then only those Resource sets, Process sets, User sets, and Time sets, and associated action and effects used by those policies are exported.

1. Log on to the Management Console as an administrator of type Security, Domain and Security, or All.
2. Click **Policies > Import Export Policies** on the Management Console.
3. On the **Export** tab, select the policies that you want to export.
4. Click **Ok**.
5. The policy export file is exported as `policy_`*<YYYY_MM_DD_HHMM>*`.tar`, follow the prompts to save the file to your preferred location.

Import a policy

1. Log on to a GDE Appliance as an administrator of type Security, Domain and Security, or All.
2. Click **Policies > Import Export Policies** on the Management Console.
3. On the **Import** tab, click **Browse** to locate the policy file to import.
4. Click **Import Policy**.

The GDE Appliance performs pre-import checks on the policies to make sure that there are no conflicts or missing items.

- If there are no conflicts or missing keys the import proceeds and the Resource sets, User sets, Process sets, and Time sets are imported. A message confirming that the operation was successful is displayed on the **Import** tab

In the event of conflicts or missing keys are detected any the following could occur:

- If the pre-check process finds that the policy keys are missing, the import is aborted and a message informing you that the operation failed is displayed and the **Messages** text box on the **Import** tab provides the names of the missing key(s).
- If the policy or policies you import contain Resource sets, User sets, Process sets, or Time sets that have names that match existing policies on the GDE Appliance to which they are being imported, or the policy or policies being imported have the same names, the **Messages** text box will contain a message listing the imported sets that conflict with existing sets. You can choose to **Continue** or **Abort** the import operation.

  If you choose to continue, the existing policy will retain it's name and the imported policy will have '_1' or the relevant number in sequence appended to the name. For example, if you are importing policies to GDE Appliance B and it has an existing policy called 'policy1' and the imported policy has the same name, if you choose to continue the import operation, the imported policy will be rename 'policy1_1'.
- If the pre-check operation detects that there unused sets referenced in the policies, you will be prompted to do either of the following:
  - Select **Policies & associated sets**, which means only sets that are used will be imported.
  - Select **Policies & all sets**, which means all sets, regardless of whether they are referenced by the policy or not will be imported.

  You can choose to **Continue** or **Abort** the import operation.
- If you choose **Policies & all sets** and the pre-check finds there are conflicts with exiting sets, you can again choose to continue or abort the operation.

The **Policies & all sets** option is useful when importing policies from earlier versions of the GDE Appliance. Earlier versions of the GDE Appliance always exported all sets regardless of whether they were used by a policy or not.

Configuring Hosts and Host Groups

21

A “protected host” is a computer system on which Agents (VTE/VAE/VTS) are installed. The agent on a host may protect data on that host, or data on other devices connected to that host.

This chapter contains the following sections:

Overview

The *Hosts* page on the Management Console displays all hosts protected by encryption Agents. GDE Appliance Security Administrators manage hosts via this page; hosts can be added, imported, or deleted.

Refer to the *VTE Agent Installation & Configuration Guide* for information about installing and configuring a VTE Agent.

Viewing Hosts

To see all protected hosts registered with a GDE Appliance:

1. Log on to the Management Console as an administrator of type Security, type Domain and Security, or type All.
2. If you log on as type All, click **Domains > Switch Domains**.

   a. In the **Selected** column, click the radio button for the domain you want, then click switch to domain. Skip to step 4.

3. If you log on as a GDE Appliance administrator of type Security or Domain and Security, navigate to **Hosts > Hosts**.
4. Click **Hosts > Hosts**. The *Hosts* page has a table listing names of the protected hosts in the GDE Appliance and the following details about each protected host:

Table 27: Hosts Window Table Details

Column	Description
Select	Select this checkbox to select the host for deletion. Multiple check boxes can be selected at one time.
OS Type	Values may be `Unknown`, `AIX`, `HPUX`, `Linux`, `Solaris`, or `Windows`. `Unknown` indicates that the host has not been registered or is an unsupported type.
Host Name	The name of the host on the GDE Appliance.
VTE/Key Agent	This column consists of child columns of check boxes for the VTE Agent and for VAE: - **Reg. Allowed**—Registration Allowed, indicates that the host can register and be configured to run VTE (File System) Agent software. - **Comm. Enabled**—Communication Enabled, indicates that a policy can be applied to a host. **Reg. Allowed** must be enabled before you can set **Comm. Enabled**. - **Pushing Status**—Status for pushing policy and configuration changes to locally assigned hosts. Status is specific to the local GDE Appliance. Run the Management Console on a failover GDE Appliance to see the push status of the hosts assigned to that server. > **Done**—the host has the latest policy and configuration changes. > **Pending**—an update is in progress or is queued for download to the host. > **N/A**—the local host is disabled or the host is being administered by a different server. This last column is not available for VAE.
One Way Communication	Indicates that the agent was registered with One-Way Communication enabled between the Agent and the GDE Appliance.
Delete Pending	Indicates the status of a request to delete a host.
LDT Enabled	Indicates whether the Live Data Transformation (LDT) feature is enabled on the host. If this feature is enabled, Docker support cannot be enabled.
Docker Enabled	Indicates whether support for Docker feature is enabled on the host. If this feature is enabled, LDT cannot be enabled.
Description	(Optional) Text to help you identify the host.

Column	Description
Sharing	Indicates if the host is shared with another domain. The column may have a value of `Shared`, `External`, or blank. - `Shared` indicates that the host is in the current domain and, if the Security Administrator has the correct roles, it can be fully configured. The shared host is visible only in the domain with which it is being shared. - `External` indicates that host is administered in another domain. You can assign the host a VTE Agent GuardPoint, but you cannot change the host configuration. - A blank value indicates that the host is not shared.

The first time you log in, the list of hosts is empty because you have not yet registered any hosts with the GDE Appliance.

The following tasks can be done from this page:

- **Select All**—Selects all hosts displayed on the current page.

  If you have enabled the **Select** check box for many individual hosts, a quick way to cancel the selection is to enable and then disable the **Select All** check box.

- **View**—Specifies the number of hosts to display on the current page. Up to 200 hosts can be displayed on one page.

- **Search**—The **Show Search** label located below the **Hosts** banner opens the **Search** panel. You can enter a string and/or search for a specific type of agent, and click **Go** to display the hosts that match the search criteria. Click **Hide Search** to conceal the **Search** panel.

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

- **Add**: Click to create a new host record.

- **Delete**: Enable the check box in the **Select** column for one or more hosts and click **Delete** to remove the selected host from the GDE Appliance database. The agent installation is left intact on the host system and needs to be uninstalled from the host if required.

- **Import**: Click **Import** to select a configuration file to add multiple hosts in a batch operation.

Adding Hosts to the GDE Appliance

Hosts can be added to a GDE Appliance manually via the Management Console, or automatically through the *Shared Secret Registration* method. Agents on the host are registered with the GDE Appliance using either the *Fingerprint Registration* method or the *Shared Secret Registration* method. The Shared Secret method is the default.

This section describes the following:

- “Adding hosts using a shared secret”

- "Adding hosts using a certificate fingerprint"
- "Adding hosts using a batch file"

Adding hosts using a shared secret

The Shared Secret method requires a GDE Appliance Administrator to create a registration password for a domain or host group. This password is shared with the Agent Installer, which uses this password to add and register protected hosts with the GDE Appliance in a single step. There is no need to manually add hosts to the GDE Appliance before registering the agent. Adding a host before registering it using the shared secret method, is optional. Multiple protected hosts can be added with a single shared secret password. As of this release, GDE Appliance Administrators can enforce the shared secret registration method for all hosts, by selecting the option on the Web UI.

The GDE Appliance only allows hosts that know the secret to register. The agent in turn, knows that it is registering with the correct GDE Appliance because it has the same secret. Hosts can be added to a domain, or to a host group within a domain, which means that a shared secret can be defined at the domain level or the host group level.

Add a host to a domain using Shared Secret Registration

GDE Appliance Security Administrator Action: Create a registration shared secret:

1. Log on to the Management Console as an administrator of type Security, type Domain and Security, or type All, with Host role permissions.
2. Switch to the domain to which you want to add the host.
3. Select **Hosts > Registration Shared Secret** in the menu bar. The *Registration Shared Secret* window opens.
4. When you use the registration secret feature for the first time, the **Current Registration Secret** section will not have any information. If there is an existing shared secret, a message, **Show Registration Shared Secret** is displayed, select **Yes** to view the secret. The default setting is **No**.

   Enter the following information in the **Create new Registration Shared Secret** section:

   a. **Registration Shared Secret creation method**—The same constraints that apply to password creation, namely uppercase letters, numbers, and special characters required, apply to the shared secret creation.

   - **Manual**—This is the default method. Select this to create the shared secret yourself.
   - **Generate**—Select this option to get an automatically generated password.

   b. **Validity Date**—Enter a date, or select a date by clicking the calendar icon. The date must be in the format MM/DD/YY.

c. **Require that hosts are added first**—Optional. If you select this option, you need to first add the host to the GDE Appliance database with the **Registration Allowed** check box enabled before you install and configure the agent.

d. **Enforce shared secret during host registration**—Optional. If you select this option, hosts *must* register with the GDE Appliance using the shared secret. Any attempt to register a host using the fingerprint method will fail.

5. Click **Ok**.
6. To remove an existing shared secret, click **Expire Registration Shared Secret**. The expiry date turns red to indicate that the shared secret is no longer valid.

The Account Lockout settings defined in **General Preferences > Password > Account Lockout** also apply to the registration shared secret, see "Account Lockout" on page 29 for more information about these settings.

Host Administrator installing the Agent Action: Register the host on the GDE Appliance:

After the agent has been installed, you will be prompted to register the host.

NOTE: The exact sequence of steps may differ from agent to agent, for details about how to install specific agent types, refer to the *VTE Agent Installation & Configuration Guide*.

1. You will be prompted to select a method to register the host. Select the shared secret option to register the host. This is the default option.
2. Enter the following information when prompted:

a. **What is the registration shared secret?**—Enter the shared secret of the domain to which you the host is to be added. Or enter the shared secret of the host group to which the host is to be added.

Warning! Be sure to enter the shared secret correctly, the prompt will not display any entered text, nor does the prompt move until you press enter. If the shared secret was entered incorrectly, an error message is displayed, saying that the certificate signing was unsuccessful. If you exceed the number of tries defined in the **Maximum Number of Login Tries** setting on the *Password Preferences* page, you will be locked out of the system for a period defined in the **User Lockout Time** setting on the same page.

b. **Domain name**—Enter the name of the domain to which the host is to be added.

c. **Host Group**—Optional. If the host is to be added to a host group, enter the name of the host group to which it is to be added, else click enter or next and continue to the next step.

d. **Host description**—Optional. Enter a description of the host to be registered.

3. Confirm the information is correct and proceed with the registration.
4. Open the Management Console on the GDE Appliance, switch to the domain where the host has been added, the host should be listed in the hosts table.

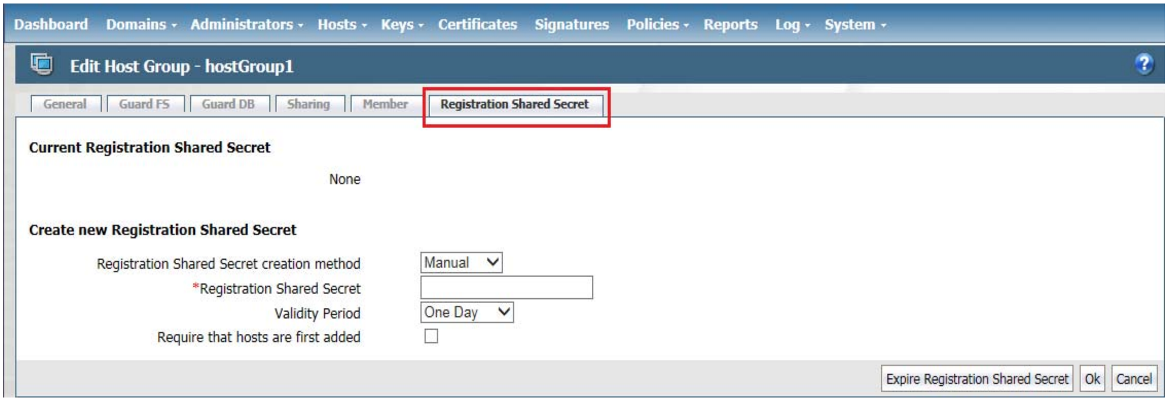
   If the host was added to a host group, select **Hosts > Host Groups** and click the host group where the host has been added, the host should be visible in the table.

Add a host to a host group in a domain, using Shared Secret Registration

GDE Appliance Security Administrator Action: Create a registration shared secret:

1. Log on to the Management Console as an administrator of type Security, type Domain and Security, or type All, with Host role permissions.
2. Switch to the domain to which you want to add the host.
3. Select **Hosts > Host Groups** in the menu bar. The *Host Groups* window opens.
4. Click a host group name or create a host group where the host is to be added and click the host group name. The *Edit Host Group* page is displayed. Click the **Registration Shared Secret** tab.

Figure 43: Host Group Registration Shared Secret window



Edit Host Group - hostGroup1

Current Registration Shared Secret

None

Create new Registration Shared Secret

Registration Shared Secret creation method: Manual

*Registration Shared Secret:

Validity Period: One Day

Require that hosts are first added: □

The remaining steps to create a registration shared secret and register a host are the same as "Add a host to a domain using Shared Secret Registration".

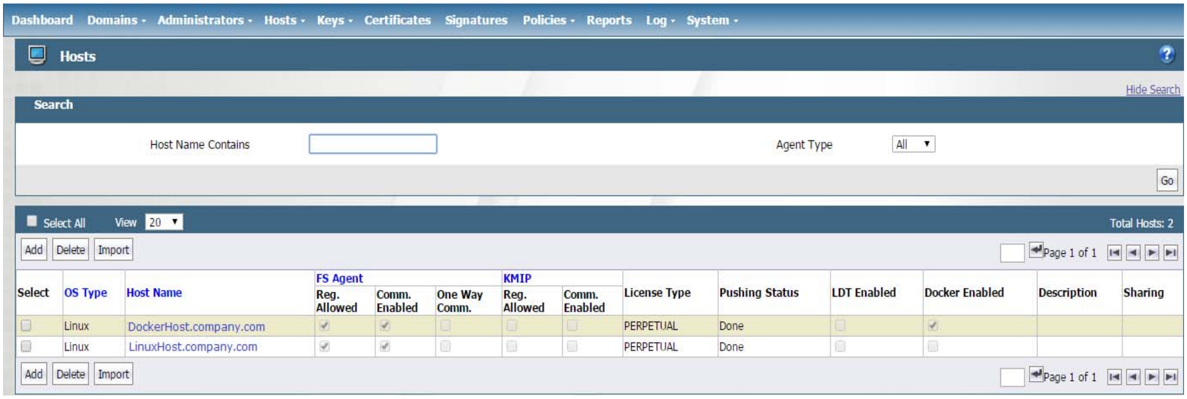
Adding hosts using a certificate fingerprint

The Fingerprint Registration method requires you to first add the host name or its IP address to the GDE Appliance from the Management Console. Once the host is added to the GDE Appliance, you can register the host from the Agent Installer on the host.

To add hosts to the GDE Appliance:

1. Determine the manner in which you want to address the host. That is, FQDN, host name, or IP number.
   - If FQDN, verify that DNS is configured and working on the GDE Appliance.
   - If host name, use the host CLI command to link IP numbers with host names, or edit `/etc/hosts` directly.
2. Log on to the Management Console as an administrator of type Security with `Host` role permissions, type Domain and Security, or type All.
3. Switch to the domain where you will add the host.
4. Select **Hosts > Hosts** in the menu bar. The *Hosts* window opens.

Figure 44: *Hosts* window



Host Name Contains

Agent Type All

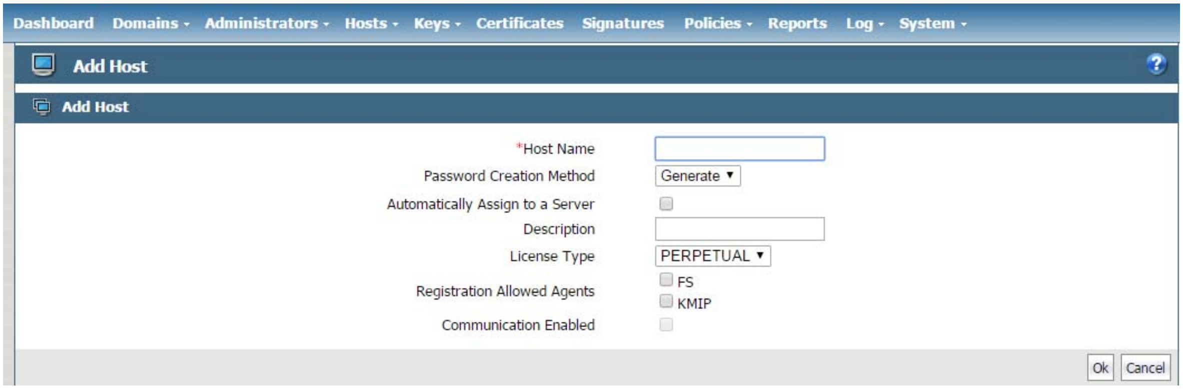
View 20

Total Hosts: 2

Select	OS Type	Host Name	FS Agent Reg. Allowed	 Comm. Enabled	 One Way Comm.	KMIP Reg. Allowed	 Comm. Enabled	License Type	Pushing Status	LDT Enabled	Docker Enabled	Description	Sharing
☐	Linux	DockerHost.company.com	☑	☑	☐	☐	☐	PERPETUAL	Done	☐	☑		
☐	Linux	LinuxHost.company.com	☑	☑	☐	☐	☐	PERPETUAL	Done	☐	☐		

5. Click **Add**. The *Add Host* window opens.

Figure 45: *Add Host* window



*Host Name	
Password Creation Method	Generate
Automatically Assign to a Server	☐
Description	
License Type	PERPETUAL
Registration Allowed Agents	☐ FS ☐ KMIP
Communication Enabled	☐

6. Enter the following information:

a. **Host Name**—Enter the IP address, host name or FQDN (253 characters max.).

NOTE: Host names that include an underscore are rejected by the Management Console. Host names that have a dot (‘.’) appended to them, prevents the agent configuration log files from being uploaded to the GDE Appliance. However, if your hostname does contain a dot appended to it, then you must re-register that host using the host IP address and then upload the log files.

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

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

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

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

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

f. **Registration Allowed Agents**—Select the agents that will run on the host system. Depending on your license, your choices are **FS** (VTE), and **Key** (VAE). The agent must be selected here before you can register that agent with the GDE Appliance. Only the agents you have a license for will display here.

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

7. Click **Ok**.

8. The host administrator (with root access) installs the agent software on the host, as described in the VTE Agent Installation and Configuration Guide.

   You can manually configure agent certificates later if the certificate generation and exchange phase of agent software installation fails.

Adding hosts using a batch file

You can add multiple hosts to the GDE Appliance simultaneously. After they are added to the GDE Appliance, you can install and register the agents that run on those hosts.

NOTE: This batch process does not reduce the time it takes to add individual hosts to the GDE Appliance. It only makes it easier to add many hosts by reducing key strokes and permitting unattended operation.

NOTE: The batch input file is not verified as it is read. If there are errors in the batch input file, such as malformed passwords or inappropriate characters, this operation can fail and hang and no hosts will be added.

The lines in a batch file are individual host definitions that follow an identical format. Each line is a comma-separated list consisting of six fields. If you want to include a comma as part of the field value, enclose the whole field in double-quotes (“). Do not enclose other special characters, such as the colon (:), in double-quotes.

The format of a batch file line is:

hostname,description,password,allow_fs_agent

where:

- **hostname**—An alphanumeric string that represents the host name or FQDN of the host being added. This is the network identity of the host.

NOTE: Do not enter a host name that contains the underscore character (_). Host names that include the underscore character are rejected by the Management Console.

- **description**—A text string that describes the host.
- **password**—This is not a regular login or user password. This is the host password to be used by the host system to decrypt cached keys when the GDE Appliance is not accessible. The host must also be configured with **Cached on Host** keys.
- **allow_fs_agent**—A boolean string that is either “yes” or “no” to enable or disable VTE Agent registration.

  An example batch file is shown below:

```
host1,This is host 1,onlyMe78,yes,yes

host2,This is host 2,bobsNum1,yes,yes

host3,This is host 3,goOd4U678,no,yes
```

```
host4,This is host 4,some1Else,yes,no
host5,This is host 5,qwerty123,no,yes
host6,This is host 6,ooPB2AUoo,no,yes
```

To add hosts using a batch file:

1. Create the batch file as described above.
2. Log on to the Management Console as an administrator of type Security with `Host` role permissions, type Domain and Security, or type All.
3. Select **Hosts > Hosts** in the menu bar. The **Hosts** window opens.
4. Click **Import**. The *Import Hosts* window opens.
5. Click **Browse** next to the **Import Hosts File** text-entry box.
6. Navigate to, and select, the batch file from the *Choose File to Upload* window.
7. Click **Open**.
8. Click **Ok** in the *Import Hosts* window.

   Wait until the following message is displayed: `The operation is successful.`
9. Click **Hosts** on the Management Console menu bar to display the *Hosts* window and the newly added hosts.

Agent software can now be installed on these systems and the agents can be registered with the GDE Appliance.

Configuring Hosts

After adding and registering hosts with the GDE Appliance, you need to configure the new host.

1. Select **Hosts > Hosts** in the menu bar. The *Hosts* window opens.
2. Click the link in the **Host Name** column of the host you want to modify. The *Edit Host* window opens to the **General** tab.

   NOTE: If the *Edit Host* window displays only two tabs, **General** and **Guard FS**, it means you are working with a shared host. Check the host status in the **Sharing** column of the *Hosts* window. If you want to do more than add or remove GuardPoints, switch to the domain in which the host was created.

   The following host attributes are displayed, some of the fields can be modified:

   a. **Name**—the FQDN of the host

   b. **Description**—Add or modify a description of the host.

c. **OS Type**—the operating system on the host

d. **Communication Port**—You can change the port number used to exchange policy enforcement data between the GDE Appliance and the VTE (FS) Agent. Generally, you change the port number only when the default port number is already in use or if your firewall requires a different port number.

If you change the port number, click **Ok**. The configuration change is downloaded to the VTE Agent host after the interval set by the **Update Host Frequency** parameter.

After the update is downloaded, you must manually restart the VTE Agent. Execute one of the following commands on the VTE Agent host to restart the VTE Agent:

- On Linux, Solaris, and AIX:

```
# /etc/init.d/secfs restart
```

- On Redhat 7.2:

```
# /etc/vormetric/secfs restart
```

- On HP-UX:

```
# /sbin/init.d/secfs restart
```

e. Information about UNIX agents applies to earlier versions of those agents, since as of v6.0, UNIX agents are EOL. **FS Agent Locked**—Locks the contents of the VTE Agent directories on the host. See “Setting Host Locks” for about this setting.

f. **System Locked**—Applies an internal policy to the host to lock host system directories, like `/var`, `/bin`, `/etc.` This can be selected only if **FS Agent Locked** is enabled.

g. **Support Challenge & Response**—this check box indicates whether this feature is enabled on the host. It becomes enabled when the VTE Agent running on the host registers with the GDE Appliance.

h. **Password Creation Method**—**Generate** (dynamic) or **Manual** (static)

If you switch the password method from **Manual** to **Generate**, regenerate the password. Select **Regenerate Password** and click **Apply**. A new generated password is downloaded to the host.

If you switch the password method from **Generate** to **Manual**, enter a new password in the **Password** and **Confirm Password** boxes.

By default, the **Password** and **Confirm Password** text-entry boxes display dots. The dots are just graphic placeholders and do not indicate that a password had been entered. You must enter a password in both text-entry boxes or the **Manual** password method will not be applied to the host.

NOTE: If you select the generate password creation method for an agent that does not support the challenge-response feature, an ERROR-level audit message is generated and entered in the log after the agent registers with the GDE Appliance, plus a red warning message is displayed on the *Edit Host* window for the host. In effect, a randomly generated password is created and downloaded to the host system; however, the `vmsec challenge` command is not available on the host system so a user cannot display a challenge string. The solution is to change the host configuration from **Generate** to **Manual** and manually enter the host password.

i. **Regenerate Password**—this is the password method to use to unlock the agent. The host user may be prompted to supply a password to decrypt encrypted data when there is no network connection between the host and the GDE Appliance. The methods are **Generate** (challenge-response) and **Manual** (static password). When **Generate** is selected, the host user must request a new password from a GDE Appliance administrator each time a host password is required.

Password/Confirm Password—Displayed when **Password Creation Method** is set to **Manual**, enter and re-enter the password to use to unlock a GuardPoint when there is no server connection.

j. **Docker Enabled**—Select this check box to enable docker support.

NOTE: If you selected the option to enable Docker support during the agent registration procedure, this check box will display as selected, indicating that this feature has been enabled. Refer to the *VTE Agent Installation and Configuration Guide* for more information.

Once Docker support is enabled, it cannot be disabled. The **Docker Enabled** check box is selectable only if your VTE agent license includes this feature. If your VTE Agent (FS Agent) license includes Live Data Transformation (LDT) and you choose to enable Docker support on a host, then the LDT check box is disabled, as the two features cannot coexist. Similarly if a host has the **Live Data Transformation** check box enabled then the **Docker Enabled** check box is disabled. See “Enabling Docker Support” for steps to enable this feature.

k. **Live Data Transformation**—Select this check box to enable Live Data Transformation (LDT) on the host.

NOTE: If you selected the option to enable LDT support during the agent registration procedure, this check box will display as selected, indicating that this feature has already been enabled. Refer to the *VTE Agent Installation and Configuration Guide* for more information.

Once LDT support is enabled, it cannot be disabled. The **Live Data Transformation** check box is selectable only if your VTE Agent (FS Agent) license includes this feature. If your VTE license includes Docker support and you choose to enable LDT, then the **Docker Enabled** check box is disabled as the two features cannot coexist. Similarly, if a host has the **Docker Enabled** check box enabled then the **Live Data Transformation** check box is disabled. See “Enabling Live Data Transformation” for steps to enable this feature.

l. **Secure Start GuardPoint**—Select this option if you want to create a Secure Start GuardPoint for Active Directory or MSSQL directories. This feature is only supported on hosts running Windows OS. Refer to the *VTE Agent Installation & Configuration Guide* for more information about using Secure Start GuardPoints.

NOTE: The **Docker** and **Live Data Transformation** options are only displayed if you have the relevant license.

3. Once your host is registered with the GDE Appliance, you can start protecting your data by creating GuardPoints, see "Managing GuardPoints" for more about creating and managing GuardPoints.
4. The **Sharing** tab lets you share the GuardPoints on the host with Security Administrators in other domains, see "Sharing a Host" on page 274.
5. Use the **Host Settings** tab to set authentication options for applications running on the host. See "Host Settings" for more information.
6. The **Challenge Response** tab allows a GDE Appliance Security Administrator to generate a temporary passphrase to give to a host administrator to decrypt data on the host when there is no connection to the GDE Appliance. Use the agent log tabs (FS Agent Log, Key Agent Log, Docker Log) to define log settings. See "Agent Log Settings" for more information.
7. You can optionally add the host to a host group using the **Member** tab, see "Configuring Host Groups".

Enabling Docker Support

Data protection policies can be set up for Docker images and Docker containers. In addition to data encryption, the GDE Appliance also provides Docker container-level access control and container-level audit logging. GDE Appliance Security Administrators can create GuardPoints on Docker images and containers via the Management Console.

Docker support is available on the following platforms:

- Docker Host: RHEL 7.0, 7.1, and 7.2
- Docker containers: heterogeneous container support, including but not limited to, RHEL, CentOS, Ubuntu, SUSE
- Docker storage driver: devicemapper

In order to use the Docker support feature on a host, you must have the following:

- VTE Agent 6.0 license with Docker support
- A host with Docker configured and running
- VTE Agent version 6.0 installed on the Docker host

Refer to the *VTE Agent Installation & Configuration Guide* for information about installing and configuring a VTE Agent.

After installing the VTE Agent on the Docker host and registering it with GDE Appliance, you must enable Docker support on the GDE Appliance:

1. Log on to the Management Console as an administrator of type *All*, *Domain and Security*, or *Security*.
2. On the main menu bar of the Management Console, click **Hosts**.
3. On the *Hosts* page, click the name of the Docker host in the **Host Name** column, the *Edit Host* page opens.
4. In the **Host Information** panel of the *Edit Host* page, select the **Docker Enabled** check box.

Once you have enabled Docker on a host, you cannot disable it. To disable the feature, you must first unregister and then delete the host and then re-register the host, without enabling the feature. This will let you reclaim the license for use on another host.

Next, edit the **Host Settings**:

1. Log on to the Management Console as an administrator of type *All*, *Domain and Security*, or *Security*.
2. On the main menu bar of the Management Console, click **Hosts**.
3. On the *Hosts* page, click the name of the Docker host in the **Host Name** column, the *Edit Host* page opens.
4. Click the **Host Settings** tab.
   - If you are using a Docker engine version earlier than version 1.12.1, add the following entry to the **Host Settings** text box:

     ```
     |authenticator|/usr/bin/docker
     ```
   - If you are using a Docker engine version 1.12.1 or later, add the following entry to the **Host Settings** text box

     ```
     |authenticator|/usr/bin/dockerd
     ```

For details about creating Docker GuardPoints, see Chapter 22 “Managing GuardPoints”.

Enabling Live Data Transformation

The Live Data Transformation (LDT) feature, enables GDE Appliance Security Administrators to encrypt or rekey GuardPoint data without blocking user or application access to that data.

In standard VTE deployments, access to data is blocked during initial encryption or rekeying of data. With Live Data Transformation (LDT), encryption and rekeying of data takes place in the background, without disrupting user or application access.

In order to use LDT you must have the following:

- VTE Agent 6.0 license with LDT.

- VTE Agent version 6.0 installed on a host. Refer to the *VTE Agent Installation & Configuration Guide* for information about installing and configuring a VTE Agent.

Refer to the *Live Data Transformation Guide* and the *VDS Compatibility Matrix* for information about implementing LDT and the supported platforms.

NOTE: The LDT feature uses ‘versioned keys', which automatically expire and rotate, as defined by the key's settings. The key rotation and key expiration occur in the background, and it is possible that a GDE Appliance backup may not contain the latest versions of the rotated keys. In the event of a GDE Appliance failure, all keys that were automatically rotated after the last backup would be lost, making all data encrypted with those keys unusable or unrecoverable. Therefore, we recommend that the LDT feature be used in a high availability deployment.

If LDT must be used in a single GDE Appliance configuration, we recommend that you specify ‘Cached On Host’ for all keys that are created, and to set the password creation method to ‘Manual’ for all hosts. In the event that the standalone GDE Appliance fails and is unavailable, access to the data on the host is still available by entering the known passphrase, and the data is available as the encryption keys are cached on the host.

After installing the VTE Agent on a host and registering it with GDE Appliance, you must enable LDT support:

1. Log on to the Management Console as an administrator of type *All*, *Domain and Security*, or *Security*.
2. On the main menu bar of the Management Console, click **Hosts**.
3. On the *Hosts* page, click the name of the host on which you want to enable the feature in the **Host Name** column, the *Edit Host* page displays.
4. In the **Host Information** panel of the *Edit Host* page, select the **Live Data Transformation Enabled** check box.

Once Live Data Transformation has been enabled, it cannot be disabled. To remove the feature, you must migrate existing data protected under LDT policies, unregister and delete the host and then re-register the host, without enabling feature. This will let you reclaim the license for use on another host. See “Deleting Hosts” for more information.

For details about creating LDT GuardPoints see, Chapter 22 “Managing GuardPoints”.

For details about how LDT works, guidelines and best practices for using the feature, refer to the *Live Data Transformation Guide*.

Setting Host Locks

FS Agent Locked and **System Locked** are two options used to protect the VTE Agent and certain system files. VTE Agent protection includes preventing some changes to the VTE Agent installation directory and preventing the unauthorized termination of VTE Agent processes. These options appear in **General** tab of the *Edit Host* and *Edit Host Group* windows and are disabled by default.

NOTE: You might not be able to upgrade or delete agent software if you do not disable the locks first.
- Disable **FS Agent Locked** before updating or deleting agent software on the host system.
- Disable **FS Agent Locked** before deleting the host record from the Management Console.
- Disable **System Locked** before updating, deleting, or modifying protected system files.

To apply locks:

1. Check that no one is currently in or accessing the Agent installation directories; otherwise, the GDE Appliance may be unable to lock the Agent software.

2. Log on to the Management Console as an administrator of type Security with Host role permissions, type Domain and Security, or type All.

3. To set the locks on an individual host:

   a. Select **Hosts > Hosts** in the menu bar.

   The *Hosts* window opens.

   b. Click a host name in the **Host Name** column.

   The *Edit Host* window opens to the **General** tab.

   c. To protect VTE Agent files from modification and deletion, enable the **FS Agent Locked** check box.

   d. To protect a set of system files from modification and deletion, enable the **Host > System Locked** check box.

   System Locked is automatically enabled when **FS Agent Locked** is enabled. You can enable and disable **System Locked** only when **FS Agent Locked** is enabled.

   e. Select **Ok** to finalize the changes.

To set locks on hosts in a host group:

1. Select **Hosts > Host Groups** in the menu bar.

   The *Host Groups* window opens.

2. Click a host group in the **Name** column.

   The **Edit Host Group** window opens to the **General** tab.

3. To protect VTE Agent files from modification and deletion, enable the **FS Agent Locked** check box.
4. To protect a set of system files from modification and deletion, select **Host > System Locked**.

   System Locked is automatically enabled when **FS Agent Locked** is enabled. You can enable and disable **System Locked** only when **FS Agent Locked** is enabled.
5. Select **Ok** to finalize the changes.
6. (Optional) As a host administrator with root permissions, verify that the locks have been applied to the agent.

   a. Log onto the host (agent) system.

   b. Execute the `secfsd` command with the `lockstat` argument:

```
# secfsd -status lockstat

  FS Agent Lock: true

  System Lock: true

#
```

NOTE: Sometimes there is a discrepancy between what the GDE Appliance reports as the VTE Agent configuration and the actual VTE Agent configuration. This may be due to the time delay between log uploads to the GDE Appliance, or because a GuardPoint is in use when the lock is applied.

If the locks are enabled and the GDE Appliance cannot administer the host, such as can occur after changing authentication credentials or removing the certificate fingerprint, the host administrator must unlock the host manually. The certificate fingerprint can be removed if the **Registration Allowed** check box on the **General** tab of the *Edit Host* page, is not selected

To unlock the host manually, boot the host into single-user mode and edit the `./secfs/.sec/conf/configuration/secfs_config` file.
Set both `coreguard_locked` and `system_locked` to `false`. Save the file. Boot the system into multi-user mode. You should now be able to administer the host again.
On Windows systems, boot in safe mode, rename `C:\Windows\system32\drivers\vmmgmt.sys and .\drivers\vmfiltr.sys` to something else, then boot in regular mode.

The host administrator must inform the Security Administrator of changes to the system hierarchy.

- **Example 1:** The host system administrator can request to have the locks temporarily disabled to do some administrative functions.
- **Example 2:** The host system administrator can remove directories and files, then, later when the lock is reapplied, the GDE Appliance is protecting non-existent data.

Another common administrative issue pertains to mounted GuardPoints. The host system administrator can remove or unmount an unlocked, non-automounted GuardPoint. The GDE Appliance Management Console interface is not aware of this change and does not issue a warning when you reapply the lock to the now non-existent mounted GuardPoint.

- **To recover an unmounted GuardPoint:**
  - Disable the GuardPoint for the file system in the Management Console.
  - Mount the file system on the host.
  - Enable the GuardPoint for the file system.

FS Agent locked

FS Agent Locked locks the contents of the VTE Agent directories on the host. These directories are `/<install root>/agent/secfs` and `/<install root>/agent/vmd`.

Files in these directories cannot be modified or removed when **FS Agent Locked** is enabled; however, the GDE Appliance can still propagate updates to the host system.

When **FS Agent Locked** is enabled:

- **System Locked** is automatically enabled
- Certificates are exchanged and the host is bound to the GDE Appliance
- The VTE Agent installation directory cannot be deleted or overwritten
- The VTE Agent services cannot be stopped
- The VTE Agent GuardPoints cannot be forcefully unmounted

When **FS Agent Locked** is disabled:

- **System Locked** is automatically disabled
- The VTE Agent software on the host is not protected

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

On Linux systems, all operations are permitted in the following directory when **FS Agent Locked** is enabled.

- `/<install root>/agent/secfs/tmp`

On Linux systems, the following directories cannot be removed or renamed, and directory and file creation will fail when **FS Agent Locked** is enabled.

- `/<install root>/agent/secfs/bin`
- `/<install root>/agent/vmd`

On Linux systems, file creations and other operations will work for the following directory, but the directory cannot be removed or renamed when **FS Agent Locked** is enabled.

- `/<install root>/agent/secfs/`

On AIX systems, the contents of the following directories cannot be changed or moved when **FS Agent Locked** is enabled.

- `/<install root>/agent/vmd`

On AIX systems, the contents of the following files and directories can be modified, but not removed or renamed when **FS Agent Locked** is enabled.

- `/<install root>/agent/secfs/`
- `/<install root>/agent/secfs/tmp`

Information about UNIX agents applies to earlier versions of those agents, since as of v6.0, UNIX agents are EOL. On Windows systems, when **FS Agent Locked** is enabled, the following folder cannot be moved and its contents cannot be modified:

```
C:\Program Files\Vormetric\DataSecurityExpert\Agent\secfs\sec
```

Also, the VTE Agent entries in the registry cannot be modified or deleted when **FS Agent Locked** is enabled on a Windows system.

System locked

System Locked applies an internal policy to the host to lock host system directories, such as `/var`, `/bin`, `/etc`, and so on. When you enable **FS Agent Locked**, **System Locked** is automatically enabled.

NOTE: To upgrade or install third-party software, add new applications, open an SSH session remotely, or modify system directories, you must disable **System Locked**.

NOTE: (Windows only) Verify that the volume letter and the path for the Windows system are correct before proceeding. When Windows VTE Agent software is installed, the volume letter defaults to “`C:`” The executables in the **Host Settings** tab may be on a different volume or in a different folder. If the volume or path information is incorrect, the GDE Appliance cannot sign the applications, and it will be unable to apply **FS Agent Locked** and **System Locked**.

When **System Locked** is enabled:

- Operating system directories on the host are protected.
- Microsoft Update cannot be run on Windows systems to protect the host. Microsoft update and other installation-related executables are specifically blocked. Executables like `wuacuclt.exe` and `msiexec.exe` cannot be run.

- The installation utility checks if **System Locked** is enabled on the host system. If it is, the utility aborts installation and displays a message telling you to "`unlock system before running install/update program`". Other third-party installation utilities do not check if **System Locked** is enabled and are not prevented from installing software.
- New file or directory creation inside a protected directory is not allowed.

When **System Locked** is disabled:

- The internal policy is disabled.
- **FS Agent Locked** remains enabled.
- You can install or update system software.

The following files, directories, and subdirectories are, by default, automatically protected when **System Locked** is enabled. NB: Asterisks (*) indicate pattern matching.

On Linux systems, the following files and the contents of the following directories cannot be changed or moved when **System Locked** is enabled.

- `/etc/pam.d`
- `/etc/rc*`
- `/etc/security`
- `/usr/lib/security`

On Linux systems, the contents of the following files and directories can be modified, but not removed or renamed when **System Locked** is enabled.

- `/etc`
- `/etc/init.d/secfs`
- `/usr`
- `/usr/bin/vmd`
- `/usr/bin/vmsec`
- `/usr/bin/secfsd`
- `/usr/bin/dataxform`
- `/usr/lib`
- `/usr/lib/*pam*`
- `/usr/lib/security`
- `/var/log/vormetric`

On Solaris systems, the following files and directories cannot be created, edited, or deleted, when **System Locked** is applied.

- `/usr/lib/fs*`
- `/usr/ker*`
- `/usr/pla*`
- `/usr/lib/securi*`
- `/etc/rc*`

- `/etc/ns*`
- `/etc/vfs*`
- `/etc/init.d/secfs`
- `/etc/system`
- `/ker*`
- `/pl*`
- `/sbin`

On AIX systems, the following files and the contents of the following directories cannot be changed or moved when **System Locked** is enabled.

- `/etc/rc.d`
- `/etc/security`
- `/usr/lib/security`
- `/sbin/helpers/mount_secfs`

On AIX systems, the contents of the following files and directories can be modified, but not removed or renamed when **System Locked** is enabled.

- `/var/log/vormetric`

On HP-UX systems, the following files and the contents of the following directories cannot be changed or moved when **System Locked** is enabled:

- `/sbin/rc[0-4].d`
- `/sbin/init.d`
- `/usr/lib/security`
- `/etc/pam.conf`
- `/etc`
- `/usr`
- `/sbin`
- `/sbin/rc`
- `/etc/inittab`
- `/usr/lib`

On HP-UX systems, the contents of the following files and directories should not be modified when **System Locked** is enabled:

- `/sbin/fs/secfs2`
- `/usr/bin/secfs`
- `/usr/bin/vmd`
- `/usr/bin/vmsec`
- `/usr/bin/secfsd`
- `/usr/bin/dataxform`

NOTE: Information about UNIX agents applies to earlier versions of those agents, since as of v6.0, UNIX agents are EOL.

When **System Locked** is applied, a protected file or path cannot be renamed or deleted; however, if it is a directory, other files may be added to it. For example, `/etc` cannot be deleted nor renamed, though you can add files to it. A file that cannot be modified cannot be opened and edited in any way.

On Windows systems, files with the following extensions in the Windows OS installation folder (for instance: \Windows, \WinNT, and so on) cannot be moved or modified when **System Locked** is enabled:

- `.exe`
- `.dll`
- `.sys`
- `.cmd`
- `.com`

Setting locks on Docker hosts

The **FS Agent Locked** and **System Locked** options are applicable to Docker host systems but, they are not applicable to Docker images and containers. Files and directories that are locked on the Docker host using these options remain locked, even if they are indirectly accessed through a Docker image or container.

Sharing a Host

Security Administrators in other domains may administer GuardPoints on a locally configured host if sharing is enabled. This feature is used to allow Security Administrators in other domains to manage a host or host group in that domain. The domains that are allowed to administer the local host are set and displayed in the **Sharing** tab of the *Hosts* window.

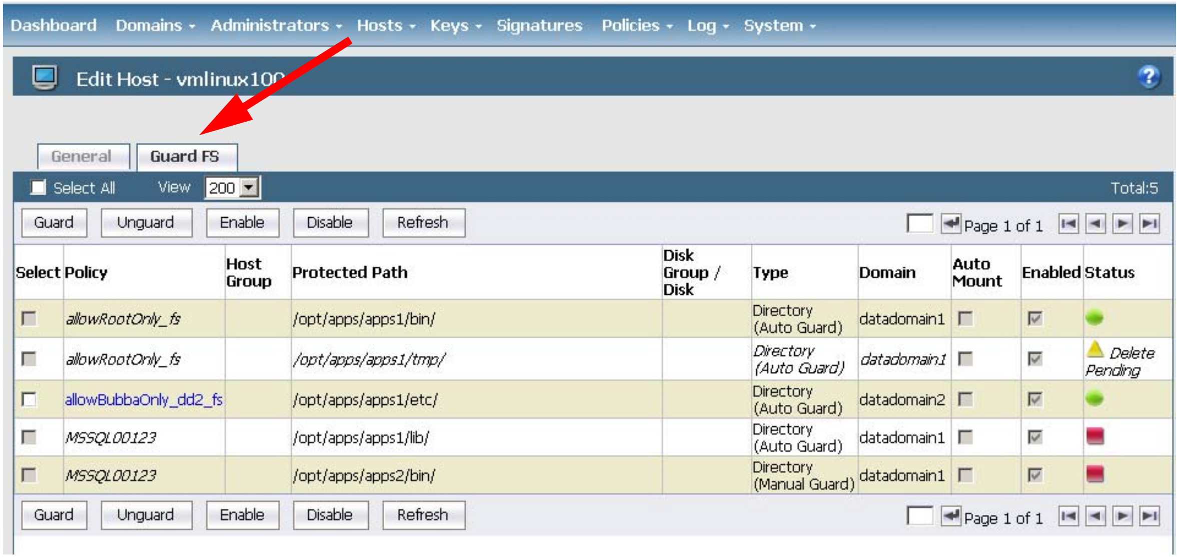
The shared/not shared status of a host is indicated on several Management Console windows:

- *Hosts* and *Host Groups* windows
- *Edit Hosts* window, **Sharing** tab
- *Edit Hosts* window, **Guard FS** tab—indicated by an obscured **Select** check box and italicized host policy name
- A host that is not configured for sharing displays a blank in the **Sharing** status field in the *Hosts* window.

- A shared host that is being accessed in the same domain in which it was created has a fully functional interface and displays *Sharing* in the **Sharing** status field. All the tabs in the *Edit Host* window are displayed and can be used to configure the host.
- A shared host that is being accessed by a Security Administrator in a different domain than the domain in which it was created has a partially functional interface and displays a sharing status of External. Only the **General** and **Guard FS** tabs in the *Edit Host* window are displayed and they are used to add and remove GuardPoints.

The *Edit Host* window in the Management Console normally displays tabs that are used to configure VTE Agents, agent logs, and set other host parameters. The *Edit Host* window for a shared host displays only the **General** and **Guard FS** tabs as shown in Figure 46.

Figure 46: Host shared across domains (note the restricted number [2] of tabs in the Edit Hosts window)



Select	Policy	Host Group	Protected Path	Disk Group / Disk	Type	Domain	Auto Mount	Enabled	Status
☐	*allowRootOnly_fs*		/opt/apps/apps1/bin/		Directory (Auto Guard)	datadomain1	☐	☑	🟢
☐	*allowRootOnly_fs*		*/opt/apps/apps1/tmp/*		*Directory (Auto Guard)*	*datadomain1*	☐	☑	⚠ *Delete Pending*
☐	allowBubbaOnly_dd2_fs		/opt/apps/apps1/etc/		Directory (Auto Guard)	datadomain2	☐	☑	🟢
☐	*MSSQL00123*		/opt/apps/apps1/lib/		Directory (Auto Guard)	datadomain1	☐	☑	🟥
☐	*MSSQL00123*		/opt/apps/apps2/bin/		Directory (Manual Guard)	datadomain1	☐	☑	🟥

The current Security Administrator domain will be displayed in the top-right corner of the Management Console window. The domain of a shared VTE Agent is displayed in the **Guard FS** tab of the *Hosts* and *Edit Hosts* windows. Figure 46 shows a shared host, *vmlinux100*, with five GuardPoints applied. Three GuardPoints were applied in datadomain1 and the other in datadomain2. The **Select** check boxes for GuardPoints in datadomain1 are disabled, but enabled for datadomain2, indicating that the Security Administrator is logged into datadomain2. Therefore, the current Security Administrator can delete the GuardPoint made in datadomain2 but not the one made in datadomain1. The current Security Administrator can also add additional GuardPoints.

Configuration attributes are local to the domain in which the Security Administrator is currently working. Primarily, the keys and policies that are in the local domain are used to configure GuardPoints.

The shared host is indicated in the **Sharing** column of the *Hosts* window. A state of *External* indicates that the host you are accessing is a remote, shared host, and only a limited set of VTE Agent features are available for configuring it. A state of *Shared* indicates that the local host is being shared in one or more other domains.

A grayed-out **Select** checkbox and an italicized **Policy** name in the **Guard FS** tab indicates a GuardPoint that is configured on the same system but in another domain. You cannot determine specifically which domain, other than by switching to each domain and checking configured hosts.

Sharing a Local Host with Another Domain

1. Log on to the Management Console as an administrator of type Security with `Host` role permissions, type Domain and Security, or type All.
2. Change to the desired domain, if you are not already in it.

   a. Select **Domains > Switch Domains**.

      The **Domains** window opens. All the domains in which the current Domain Administrator is a member are displayed. The current domain is not selectable.

   b. Enable the radio button of the desired domain.

      If the desired domain is not listed, ask the Domain Administrator for that domain to add you to it.

   c. Click **Switch to domain**.

      The *Domains* window is redisplayed.
3. Select **Hosts > Hosts** or **Hosts > Host Groups**.
4. Select the host or host group to be shared from the **Host Name** column of the *Hosts* window or the **Name** column of the *Host Groups* window.

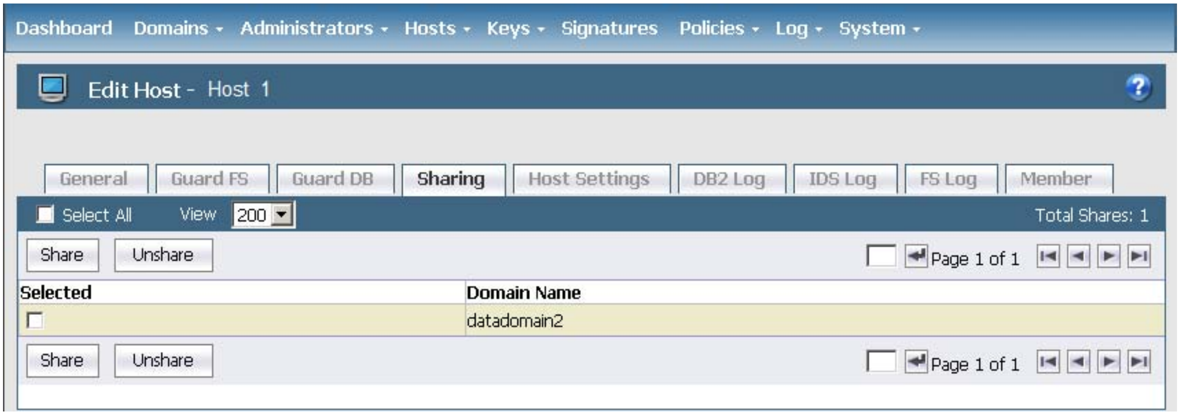
   The *Edit Host* or *Edit Host Group* window opens.
5. Select the **Sharing** tab.
6. Click **Share**.

   The **Sharing** window opens.
7. Enter the name of the domain to be given shared access to the current host in the **Domain Name** text-entry box.

   All configured domains are available, even domains the current Security Administrator is not configured to access. Available domain names are not displayed and a domain browser is not provided. Domain name handling is case-sensitive. Enter the name exactly as it is configured. The Management Console will tell you if you enter an incorrect or non-existent domain name.

8. Click **Ok**.

Figure 47: Sharing hosts



Selected	Domain Name
□	datadomain2

Shared Host Logging

Shared hosts and shared host groups are administered in the domain in which they were created. All of the VTE Agent log data generated on a shared host is displayed only in the domain in which the host was created. You must be in the domain in which the host was created to view GuardPoint activity in the logs.

Only server-generated messages are displayed in the log of the domain that is being granted shared access. That is, only log messages that indicate that the GDE Appliance performed an action are displayed. Host acknowledgment is not displayed. You must enter the domain in which the host or host group was originally created as an administrator of type Security Administrator or All to view host acknowledgment and GuardPoint access activity. If the VTE Agent is assigned to a failover GDE Appliance, agent activity is logged on the failover GDE Appliance.

Host Settings

The *Host Settings* tab allows you to set authentication options for the applications running on the host. Applications such as `su`, `sshd`, and `login` that authenticate a user's identity by requesting a user name and an associated password, are signed applications that identify and authenticate before a child process executes.

GuardPoints may have an associated policy that restricts access to the data contained in those GuardPoints. For a process to be able to access the data, the user's associated identity must be authorized. This authorization can be done by adding an entry in the host settings table that specifies a program, such as mentioned above, along with a keyword that indicates the type of authorization that is applied.

Host Settings on the GDE Appliance are pushed to the hosts periodically. In an HA deployment, you can also click **Notify All Hosts** in the High Availability Servers window to push the latest host configurations directly from the primary GDE Appliance to every host in the HA cluster, regardless if the hosts are assigned to failover GDE Appliances or not. See “Pushing Configuration Changes to Hosts” for more about pushing configuration changes to hosts.

NOTE: Do not click **Notify All Hosts** more than once. Each time you click this button you spawn a new process and each new process slows the GDE Appliance.

Applications in the *Host Settings* tab used to be automatically signed when new settings were pushed from the GDE Appliance. Therefore you could apply host settings after any of the following tasks:

- Installing VTE Agent software
- Installing VTE Agent software with Docker enabled
- Upgrading VTE Agent software
- Changing any of the files listed in the *Host Settings* tab

The signatures of the newly added process or processes are compared against the signatures of the existing settings and, if they differ, an error message is generated. See section “Re-Sign Settings” for how to configure this setting, and refer to the VTE *Agent Installation and Configuration Guide* for details about this feature.

For specific information about HDFS hosts settings information, refer to the *VTE Installation and Configuration Guide*.

Host Settings can also be configured at the host group level, see “Host Group Host Settings” for details.

Host settings for Linux

The text entry box on the *Host Settings* tab is where you specify what authentication mechanisms are in place for certain binaries on the host machine. Each line has the format

```
|behavior|/path/to/binary
```

Default settings for Linux

Linux

```
|authenticator|/usr/sbin/sshd
|authenticator|/usr/sbin/in.rlogind
|authenticator|/bin/login
|authenticator|/usr/bin/gdm-binary
|authenticator|/usr/bin/kdm
|authenticator_euid|/usr/sbin/vsftpd
```

Host settings for Windows

For applications running under Wow64 that require some form of user authentication, create entries in the *Host Settings* tab for Windows. The syswow64 paths are created by default during Windows file agent installation. `\Windows` is for Windows XP and Windows Itanium operating systems.

In Wow64, all file-access to `C:\Windows\System32` is redirected to `C:\Windows\syswow64`, and is implemented using the File System. Redirected syswow64 paths are effective only for 64-bit Windows file agents. This is the path where programs compiled for 32-bits are stored in order to run on a 64-bit system.

Verify that the volume letter and the path for the Windows system are correct before proceeding. When Windows VTE Agent software is installed, the volume letter defaults to “`C:`” It is possible that the executables in the *Host Settings* tab are on a different volume or in a different folder. If the volume or path information is incorrect, the GDE Appliance cannot sign the applications, and it cannot apply **FS Agent Locked** and **System Locked**.

Default settings for Windows

```
C:\WINDOWS\system32\winlogon.exe
|lock|C:\WINDOWS\system32\msiexec.exe
|lock|C:\WINDOWS\system32\wuauclt.exe
|lock|C:\WINDOWS\system32\wupdmgr.exe
|lock|C:\Program
Files\Vormetric\DataSecurityExpert\agent\secfs\sec\bin\vminstall.exe
|exempt|C:\WINDOWS\explorer.exe
|exempt|C:\WINDOWS\regedit.exe
|exempt|C:\WINDOWS\system32\regedt32.exe
|exempt|C:\WINDOWS\system32\svchost.exe
```

```
|exempt|C:\WINDOWS\system32\services.exe
|exempt|C:\WINDOWS\system32\smss.exe
```

Host settings for a Docker enabled host

1. Log on to the Management Console as an administrator of type All, or Domain and Security.
2. On the main menu of the Management Console, click **Hosts**.
3. Click the host in the **Host Name** column, the *Edit Host* page opens
4. Click the **Host Settings** tab.
   - If you are using a Docker engine earlier than version 1.12.1, add the following entry to the **Host Settings** text box:

     ```
     |authenticator|/usr/bin/docker
     ```

   - If you are using a Docker engine version 1.12.1 or later, add the following entry to the **Host Settings** text box:

     ```
     |authenticator|/usr/bin/dockerd
     ```

You can also define host settings for docker containers. It allows all tags for example, `authenticator`, `su`, `protect` etc for containers as well. If you want to tag specific containers, you need to add them as follows:

```
|<tag name><+arg=<+cid=<container ID>>>| path_to_binary
```

For example if you want to add `sshd` authenticator for a Docker container:

1. Log on to your GDE Appliance.
2. On the main menu of the Management Console, click **Hosts**.
3. Click the host in the **Host Name** column, the *Edit Host* page opens
4. Click the **Host Settings** tab and add the following entry:

   ```
   |authenticator+arg=+cid=b4c6a9ca8ce4|/usr/sbin/sshd
   ```

   where `cid` is the 12 character container ID.

Oracle database in a guarded NFS mount on AIX

If you plan to locate your Oracle database in a guarded NFS mount, add the following entries to host settings.

```
|vfsnumber|<path to>/oracle
|vfsnumber|<path to>/dbca
```

Example:

```
|vfsnumber|/u01/app/oracle/dbhome_1/bin/oracle
|vfsnumber|/u01/app/oracle/dbhome_1/bin/dbca
```

NOTE: Information about UNIX agents applies to earlier versions of those agents, since as of v6.0, UNIX agents are EOL.

Host setting keywords

Table 28 lists the keywords that you can enter in the *Host Settings* tab that override different authentication requirements:

Table 28: Host Settings tab keywords

Keyword	Description
|authenticator|	(UNIX only) This keyword means that the given binary is trusted to authenticate users. For example, the `sshd` process on UNIX is a good `|authenticator|` because it takes incoming network connections and authenticates the user that is attempting to log in to the system. All child processes from this session will be trusted as the original user.
|authenticator_euid|	(UNIX only) The `|authenticator|` keyword authenticates based upon the real user ID (ruid) credentials of a process. The `|authenticator_euid|` keyword authenticates based upon the effective user ID (euid) credentials of a process. The |authenticator_euid| keyword is used when you want to authenticate the credentials of a setuid process with the euid value rather than the ruid value.
|vfsnumber|	(AIX [all supported]/Oracle 10gR2) Use this host setting in the case that Oracle RMAN backups fail on NFS as a result of not receiving underlying file system identifiers. Apply |vfsnumber| to the Oracle binaries directory.
|realfsid|	(AIX[All supported], HPUX [All supported]) On AIX, use this host setting if the cp operation fails while copying files with extent attributes on guarded Veritas file systems. The failure is due to the underlying file system identifier not being received. The same host setting should also be used on HPUX environments when using the Veritas `vxresize` utility.
|lock|	(Windows only) Specifies an application that cannot be executed on the host. An application defined with `lock` does not go through an internal policy check. It is not allowed to run at all. A default set of applications is locked on the Windows host to prevent their execution and causing potential failure during bootup. The same effect can be achieved by configuring the **Resource** and **Process** security rule attributes in a policy; however, certain default applications are automatically locked in the *Host Settings* tab as a precautionary measure for when you fail to include these applications in the policy. Sometimes problems occur when installing software on a locked host, such as installation failure or application lockup. Specific processes can be identified where, when they are locked, they cannot be started and the failure goes away. For example: |lock|c:\winnt\system32\msiexec.exe

Keyword	Description
|exempt|	(Windows only) When processes or applications are started, the internal policy and regular policies are checked locally or by the Security Server. When a policy check is performed and exempt is applied to the process, a 6 second timeout is imposed on the check. Without exempt, an application can wait indefinitely for a policy access check to complete, as when the Security Server is required but is not accessible. If the check times-out because the Security Server is unavailable for any reason, access is denied. Exempt host processes are also “exempt” from pop-up messages that describe the occurrence of access violations. An example of what causes such pop-ups is an application that tries to memory map a file for which it does not have encryption permission (for instance, memory map with no view ability key on Windows). The only reasons to include exempt in the configuration are shorter wait periods and blocked pop-ups.

NOTE: |trust| and |trustfrom| have been deprecated. Please re-evaluate host settings and replace with |authenticator| or |authenticator_euid| as appropriate. These settings will continue to be supported.

The different results you get when using `authenticator` or `authenticator_euid` to verify user identities is shown in Table 29.

Table 29: Results from authenticator to verify user identity

Product	Application	Host Setting	User
Oracle	oracle	authenticator_euid	“oracle”
Oracle	oracle	authenticator	*

* indicates the real uid of the user who starts the application. This means that if the policy is configured to check user ID, a security rule must be generated for every possible user.

NOTE: Apply the |`authenticator_euid`| keyword to the `oracle` binary in the *Host Settings* tab to authenticate the `oracle` user because regardless of who starts the `oracle` process, the EUID is always `oracle`.

Configuring Application Authentication Credentials

1. Log on to the Management Console as an administrator of type Security, or type Domain and Security with `Host` role permissions, or type All (administrators of type All are assigned all the roles by default).
2. Select **Hosts > Hosts** in the menu bar. The *Hosts* window opens.

3. Click the host in the **Host Name** column. The *Edit Host* window opens.
4. Select the *Host Settings* tab. This tab displays a default set of system applications that may require authentication entries.
5. Add, modify, or delete entries to control their access permissions. When you add more processes, you must include the entire path.

NOTE: You must use a keyword such as `|authenticator|` in front of a process or it will be ignored by the Management Console.

6. Click **Ok**.
7. Any users who are currently logged on to the system must log off, and then log on again to refresh their user authentication credentials.
8. Verify the change by logging on to the host and accessing a GuardPoint, then check the user information in the Message Log.

Re-Sign Settings

If you add another process to the set of trusted applications on the *Host Settings* tab, check the **Re-Sign Settings** check box to ensure that the new process is signed and authenticated by the host.

The next time host settings are pushed to the VTE Agent, the updated host settings are re-signed and the **Re-Sign Settings** check box on the Management Console is cleared (or reset).

To ensure that the new process is signed and authenticated by the host, do the following:

1. Navigate to the **Hosts > Hosts** option on the Management Console menu.
2. Click the host on which you want to update the host settings.
3. Click the *Host Settings* tab.
4. Make changes to the settings.
5. Select the **Re-Sign Settings** option. Selecting this option will force a signature update. The next time host settings are pushed to the VTE Agent, the updated host settings are re-signed and the **Re-Sign Settings** check box on the GDE Appliance Console is cleared (or reset).

If you do not select this option after adding a new process, the host will ignore the newly added process.

Agent Log Settings

Configure log viewing settings for the various agents from the specific tabs—VTE (FS) Agent on the FS Agent Log tab, Key Agent (VAE/VKM) settings from the Key Agent tab, or Docker settings from the Docker Log tab. If you are outside of a domain, i.e., at the 'system' level, then these configuration settings are applied globally. All host systems added after this change inherit the log settings attributes, but all current hosts configurations remain intact. To configure log settings attributes for a specific host, you need to log into a domain and make the changes on that host. The host level settings take precedence over the system level settings.

FS Agent Log

This section describes VTE (FS) agent log configuration.

The table at the top of the page displays the Message Type and log message destination i.e., where the log files will be stored.

Message Type

- **Management Service**: Logs messages that are related to the agent and VMD process server interaction in the agent logs. Log to File and Upload to Server are enabled by default. The default log message level is INFO.
- **Policy Evaluation**: Logs messages that are related to policy evaluation in the agent log. Set the log message level to desired setting. The default log message level is ERROR.
- **System Administration**: Logs messages that are related to system level events. The default log message level is ERROR.
- **Security Administration**: Logs messages that are related to security related events. The default log message level is INFO.

  The detail and extent of information to be logged by the current agent is determined by the selected error level. The agent supports five log levels. These logs can be logged to a local file, a Syslog server or uploaded to the GDE Appliance.

  In sequence they are:

- **DEBUG**: Designates fine-grained informational events that are targeted towards support engineers and developers.
- **INFO**: Designates informational messages that highlight the progress of the application at coarse-grained level.
- **WARN**: Designates potentially harmful situations.
- **ERROR**: Designates error events that might still allow the application to continue running.

- **FATAL**: The 'FATAL' level designates very severe error events that will presumably lead the application to abort.

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

Message Destination

Log Messages can be stored in several locations.

- **Log to File**: Send log messages to the /var/log/vormetric/vorvmd_root.log file of a UNIX host, or a Windows equivalent, such as \Documents and Settings\All Users or WINDOWS\Application\ Data\Vormetric\DataSecurityExpert\agent\log\vorvmd.log.
- **Log to Syslog**: Send log messages to the syslog server for a UNIX host. If a syslog server is not configured, it is sent to the host 'messages' file, such as /var/adm/messages. On a Windows host, the messages are sent to the Event Viewer (Application events).
- **Upload to Server**: Upload to the GDE Appliance and display in the Management Console Logs window.
- **Level**: Sets the level of error messages to be sent.
- **Duplicates**:
  - **Allow**: All duplicate messages of the corresponding Message Type are captured and displayed in the log.
  - **Suppress**: Messages of the corresponding Message Type will follow the configured Threshold as to how many times duplicate messages are sent to the GDE Appliance during the given Interval.

File Logging Settings

Maximum File Size (bytes): The agent starts a new, empty log file when the specified limit is exceeded. The default is 1000000 bytes.

Delete Old Log Files: Select this check box to delete old FS agent logs. This check box works in conjunction with the Number of Old Log Files to Keep text-entry box. For example, Select this check box and enter 3 as the Number of Old Log Files to Keep value. After 3 logs are generated, the first log, log1, is deleted and a new log, log4, is created. If you do not Select this check box, log files will continue to accumulate in the server database and you will have to remove them manually.

Syslog Settings

Local: Send Syslog messages to the local machine.

Server (1, 2, 3, 4): Enter the hostname of the Syslog server.

Protocol: Select the protocol to connect to the syslog server; UDP or TCP

Message Format: Specifies the format of the message; Plain Message, CEF, or RFC5424.

Upload Logging Settings

Maximum Number of Messages to Upload At Once: Limits the number of messages sent to the GDE Appliance at one time. When the specified number of log entries is reached, those entries are uploaded to the GDE Appliance. The default is 1000.

Upload Messages At Least Every (seconds): The maximum interval to wait before the agent is to upload messages to the GDE Appliance. Use this attribute to update the log viewer even when the Maximum Number of Messages to Upload At Once has not been reached. You can lower the interval if there is little agent activity. The default is 10 seconds.

Upload Messages At Most Every (seconds): The minimum interval to wait before the agent is to upload messages to the GDE Appliance. You can increase the interval if there is considerable agent activity, so the agents do not flood the network with log messages. The default is 1.

Normal Time Out (seconds): The maximum interval of time the agent is to wait for the GDE Appliance to acknowledge a backup or restore request and upload related message data. If the agent cannot connect to the GDE Appliance within the specified interval, the agent will try again after the interval configured by the Upload Messages At Least Every attribute. The default is 2 seconds.

Shutdown Time Out (seconds): The maximum interval of time the agent is to wait for the GDE Appliance to acknowledge job completion and upload related message data. If the agent is unable to upload the log messages within the specified interval, they are left on the agent system. The agent will resend the messages at the beginning of the next job. The default is 30 seconds.

Drop If Busy: Select to slow log message generation and drop log files during periods of extreme logging.

Duplicate Message Suppression Settings

Enable Concise Logging: When enabled, audit log messages are reduced. This option is disabled by default. Instead of logging messages for each file system operation, only the following types of audit messages are logged;

- only one audit message for each read or write activity is logged at the start of that activity.
- audit messages for reading file status information and setting file attributes (and extended attributes) are not logged.
- audit messages for directory open, close and read attributes are not logged.

Threshold (1-100): Used when the Duplicates value is set to Suppress. Specifies the maximum number of duplicate messages the agent is to send to the GDE Appliance within the amount of time specified by the Interval parameter. The default is 5 messages and the maximum is 100 messages.

Interval (seconds) 1-1000: Used when the Duplicates value is set to Suppress. Specifies the time period in which the number of duplicate messages, specified by Threshold, can be uploaded to the GDE Appliance. Once Interval is exceeded, the count specified by the Threshold parameter starts again. The default is 600 seconds (10 minutes). The maximum is 3600.

Maximum Space for Caching Log Files (MB): This setting indicates the space available for caching agent log files. Log files are copied from the agent to the GDE Appliance soon aster they are created, assuming a good network connection. If the network is a little slow, a backlog will build up and the log files are cached. If the space for caching files fills up, the system slows down and new log messages are dropped. The agent sends warning messages to that effect, which can be viewed on the Logs page on the Management Console.

Maximum Number of Cached Log Files: This setting indicates the number of files that can be stored in the space for caching log files pending upload to the GDE Appliance. If the limit is reached, the agent will drop any new log messages and send warning to the GDE Appliance which can be viewed on the Logs page of the Management Console.

NOTE: The default values for **Maximum Space for Caching Log Files (MB)** and **Maximum Number of Cached Log Files** are the recommended values. If these values are changed, they should be kept in the same ratio, since each log file can be about 500Kbytes in size. Additionally, users should ensure that the underlying file system can accommodate a larger backlog of files.

Key Agent Log

Configure log viewing settings for the Key Agent on the Key Agent Log tab. If you are outside of a domain i.e., at the 'system' level, these configuration settings are applied globally. All Key Agent host systems added after this change inherit the log settings attributes, but all current hosts configurations remain intact. To configure log settings attributes for a specific host, you need to log into a domain and make the changes on that host. The host level settings take precedence over the system level settings.This section describes global Key agent log configuration.

The table at the top of the page displays the Message Type and log message destination i.e., where the log files will be stored.

Message Type

Key Operation: Enters messages that are related to the key operation. Log to File and Upload to Server are enabled by default. The default log message level is INFO.

Message Destination

- **Log to File**: Send log messages to the /var/log/vormetric/vorvmd_root.log file of a UNIX host, or a Windows equivalent, such as \Documents and Settings\All Users.WINDOWS\Application\Data\Vormetric\DataSecurityExpert\agent\log\vorvmd.log.
- **Log to Syslog**: Send log messages to the syslog server for a UNIX host. If a syslog server is not configured, it is sent to the host 'messages' file, such as /var/adm/messages. On a Windows host, the messages are sent to the Event Viewer (Application events).
- **Upload to Server**: Upload to the GDE Appliance and display in the Management Console Logs window.
- **Level**: Sets the level of error messages to be sent.
- **Duplicates**:
  - **Allow**: All duplicate messages of the corresponding Message Type are captured and displayed in the log.
  - **Suppress**: Messages of the corresponding Message Type will follow the configured Threshold as to how many times duplicate messages are sent to the GDE Appliance during the given Interval.

  The rest of the settings; File Log Settings, Syslog Settings, Upload Log Settings, and Duplicate Message Suppression Settings are the same as for the FS(VTE) Agent, see “FS Agent Log” for details.

Docker Log

The *Docker Log* tab lets you configure log settings for a docker image or container. The docker logs record events related to the policy applied to the selected images or containers. If no log settings are defined on this tab, the settings defined on the *FS Agent Log* tab will apply. However if policy evaluation log settings are defined on the *Docker Log* tab, they take precedence over any policy evaluation settings defined on the *FS Agent Log* tab.

To configure Docker Logs:

1. Log on to the Management Console and switch to a domain or log on as a local domain administrator of type Security with a Host role.
2. Navigate to the *Hosts* page.
3. Click the name of your Docker host in the **Host Name** column, the *Edit Host* page opens.

   Enter the following information in the **Configure Docker Log Setting** panel:

   - **Docker Image/Container**: Click **Browse** to select an image or container from the Docker host. If you select an image the **Docker Image ID** field displays the image ID. If you select a container, the **Docker Image ID** field displays the image from which the container was spawned and the **Docker Container ID** displays the container ID. You can use these IDs to search for Docker specific logs on the *Logs* page later.

- **Policy Evaluation Level**: Select a log message level.
- **Policy Evaluation Duplicated**: You can choose to suppress or allow duplicate messages. Select SUPPRESS or ALLOW, the default is SUPPRESS.

4. Click **Ok**. The Policy Evaluation settings are saved in a tabular format under the **Configure Docker Log Setting** panel.

Docker log messages are displayed on the *Logs* page.

To search for Docker specific log messages:

1. Navigate to the *Logs* page.
2. Enter the following information in the **Search** panel:
   - **Log Type**: Select whether you want to display logs from both the GDE Appliance and the agents, only the GDE Appliance, or only the agents. The default is All, which means from both GDE Appliance and agents.
   - **Source**: Enter the hostname of the GDE Appliance or agent for which you want to return log files.
   - **Last Refreshed**: Displays the date and time of when the displayed log files were last refreshed. Format is YYYY-MM-DD HH:MM:SS
   - **Message Contains**: Type in text string that you want to search for in the log messages.
   - **Docker Host**: Click **Browse** to select the Docker Host for which you want to return log files.
   - **Docker Image/Container**: Click **Browse** to select an image or container for which you want to display logs.
   - **Docker Image ID**: Displays the ID for the selected Docker image.
   - **Docker Container ID**: Displays the ID of the selected Docker container.
   - Click **Go**. The relevant logs are displayed in the table under the **Search** panel.

Automatic Renewal of Host Certificates

Certificates are used to verify the identity of a remote peer when agents communicate with the GDE Appliance. The current lifespan of these certificates is 365 days. For the automatic agent certificate renewal process to work, you must have the following:

- Agent version 5.2.2 or later.
- Current (not expired) and valid host certificates installed

- Access to the Management Console as a GDE Appliance administrator of type Security, type Domain and Security, or All with `Host` role permissions.

The system prompts the administrator and automatically renews any certificate that is 60 days or closer to expiration. The renewal process is transparent and requires no intervention by the administrator. If multiple host agents require renewal at the same time, the server staggers the renewal process to avoid network congestion. This staggering could introduce a delay of up to 48 hours in the renewal process.

Certificate renewal notification

The GDE Appliance automatically renews certificates for the VTE (FS) agent.

Certificate renewal may cause the agent to restart. When an agent restarts or certificate is renewed, the agent sends a system notification and log entry.

VMD restart sends the following notification for all installed products:

- Certificates for the <`agentname`> agent expire in <`number`> days

Certificate renewal causes the agent to report the following message on restart:

- The new certificate set has been activated

For information about the Key Agent, refer to the relevant Key Agent documentation.

Updating host certificates

You must regenerate host certificates when you:

- Configure an agent to access a new primary GDE Appliance
- Update agent certificates as part of a scheduled update process
- Delete and reinstall agent software
- Regenerate the CA signer certificate of the GDE Appliance

NOTE: The default host registration timeout is 10 minutes. If the host is unable to reach the GDE Appliance within the allotted period because of an extremely slow network connection, set the `REGISTER_HOST_TIMEOUT` environment variable to extend the registration timeout. The variable value is an integer expressed in seconds. You may also have to extend the default TCP timeout. See also "RFC 5482 - TCP User Timeout Option".

Since you are updating host certificates, the host already has certificates and the host is already registered with a primary GDE Appliance. The certificates on the local host will be deleted and regenerated automatically. However, you must unregister the host on the GDE Appliance before proceeding. This is described below.

If you are upgrading agent certificates with the same primary GDE Appliance, there is no need to disable GuardPoints.

If you are upgrading the agent certificates with a different primary GDE Appliance, disable all configured GuardPoints for the host before proceeding. After certificate upgrade completes, assign the GuardPoints from the new GDE Appliance.

To update host certificates:

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions, type Domain and Security, or type All.
2. Click **Hosts > Hosts**. The **Hosts** window opens.
3. Click the host in the **Host Name** column. The **Edit Host** window opens to the **General** tab.
4. Disable the **Registration Allowed** check box for the agent whose certificate you want to change.

   A dialog box opens warning you that the agent certificates will be removed and GDE Appliance-agent communication will be disabled. You will have to re-register the agents. Note that the agent configuration stays in place so you do not have to reconfigure policies, keys, and so on.
5. Click **OK** in the dialog box.
6. Click **Apply** in the *Edit Hosts* page to finalize the configuration change.

   The **Certificate Fingerprint** for the agents should be gone.
7. Re-enable the **Registration Allowed** and **Communication Enabled** check boxes.
8. Click **OK**.

   The GDE Appliance is now ready to re-register the host.

Log on to hosts that needs to be re-registered. Refer to the *VTE Installation and Configuration Guide* for procedures to re-register the host.

Modifying Host Configuration

To modify a host configuration:

1. Select **Hosts > Hosts** in the menu bar. The *Hosts* window opens.
2. Click the link in the **Host Name** column of the host you want to modify. The *Edit Host* window opens to the **General** tab.

NOTE: If the *Edit Host* page displays only two tabs, **General** and **Guard FS**, you are working with a shared host. Check the host status in the **Sharing** column of the **Hosts** window. If you want to do more than add or remove GuardPoints, switch to the domain in which the host was created.

3. In the **Host Information Panel** you can modify the following:

   a. **FS Agent Locked**—Locks the contents of the VTE Agent directories on the host.

   b. **Password Creation Method**—`Generate` (dynamic) or `Manual` (static)

   - If you switch the password method from `Manual` to `Generate`, regenerate the password. Select **Regenerate Password** and click **Apply**. A new generated password is downloaded to the host.
   - If you switch the password method from `Generate` to `Manual`, enter a new password in the **Password** and **Confirm Password** boxes.

NOTE: If you configure a dynamic password for an agent that does not support the challenge-response feature, an ERROR-level audit message is generated and entered in the log after the agent registers with the GDE Appliance, plus a red warning message is displayed on the *Edit Host* window for the host. In effect, a randomly generated password is created and downloaded to the host system; however, the `vmsec challenge` command is not available on the host system so a user cannot display a challenge string. The solution is to change the host configuration from `Generate` to `Manual` and manually enter the host password.

NOTE: By default, the **Password** and **Confirm Password** text-entry boxes display dots. The dots are just graphic placeholders and do not indicate that a password had been entered. You must enter a password in both text-entry boxes or the `Manual` password method will not be applied to the host.

   c. **Description**—Add or modify a description of the host.

   d. **Communication Port**—You can change the port number used to exchange policy enforcement data between the GDE Appliance and the VTE Agent. Generally, you only change the port number when the default port number is already in use or if your firewall requires a different port number.

   If you change the port number, click **Ok**. The configuration change is downloaded to the VTE Agent host after the interval set by the **Update Host Frequency** parameter.

   e. After the update is downloaded, the VTE Agent must be manually restarted. The “host administrator”, must execute one of the following commands on the VTE Agent host to restart the VTE Agent:

   - On Linux, Solaris, and AIX:

```
# /etc/init.d/secfs restart
```

   - On HP-UX:

```
# /sbin/init.d/secfs restart
```

   - On RedHat 7.2:

```
# /etc/vormetric/secfs restart
```

f. **System Locked**—Applies an internal policy to the host to lock host system directories, like `/var`, `/bin`, `/etc`. This can be selected only if **FS Agent Locked** is enabled.

g. The **Support Challenge & Response** check box indicates whether this feature is enabled on the host. It becomes enabled when the VTE Agent running on the host registers with the GDE Appliance.

h. Enable the **Registration Allowed** check boxes for **FS**.

Successfully registered agents display a hash value in the **Certificate Fingerprint** column. The **Registration Allowed** check box must be enabled before you can enable the **Communication Enabled** check box. An agent must be registered and the **Communication Enabled** check box enabled before you can apply policies to that agent.

Configure keys and policies before enabling the host. You can optionally configure the host in a host group.

4. Click **Ok** to finalize the changes.

Changing the VTE Agent host password

The offline password feature is designed to protect the data on a laptop or similar portable system from being accessed by unauthorized users. You must provide a password when there is no connection between the VTE Agent and the GDE Appliance in order to decrypt/encrypt files that are encrypted with an offline key (`Cached on Host`). The offline password feature controls access to encryption keys that are stored locally on a particular machine as a way to keep data secure when the GDE Appliance is not accessible. Provide the password and the VTE Agent will encrypt/decrypt guarded data per the applied policy.

The host password is initially set when the host is added to the GDE Appliance. Passwords can be set on a host-by-host or host group basis.

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions, type Domain and Security Administrator, or type All.
2. Select **Hosts > Hosts** in the menu bar.

   The *Hosts* window opens.
3. Click the host in the **Host Name** column.

   The *Edit Host* page opens to the *General* tab.
4. Select either `Generate` or `Manual` in the **Password Creation Method** scroll-list.
5. If you selected `Manual`, enter the new password in the **Password** and **Confirm Password** text-entry boxes.

   By default, the **Password** and **Confirm Password** text-entry boxes display dots, which makes you think that a password had already been entered or a default password is being used. The dots are just graphic placeholders and do not indicate that a password had been entered. You must enter a password in both text-entry boxes or the `Manual` password method will not be applied to the host group.

6. If you selected `Generate`, enable the **Regenerate Password** check box.

   You must enable the check box or the `Generate` password method will not be applied to the host group.

7. Click **Apply** or **Ok**.

8. When changing a static password, or changing a host from a dynamic password to a static password, tell the host user(s) the new static password or they will be unable to access encrypted data when there is no network connection between the host and GDE Appliance. When changing a host from a static password to a dynamic password, tell the host user(s) that challenge-response authentication has been enabled and that they need to run `vmsec challenge` on UNIX/Linux hosts, or select **Password...** on the Windows etray, when the host cannot connect to the GDE Appliance.

Deleting Hosts

When a host is deleted from the Management Console, the host record and configuration are deleted from the GDE Appliance only. The agent installations on the host continue to run, complete with the applied policies. To completely remove an agent host, run the software removal utility on the host system after you delete the host from the Management Console.

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

When a host record is deleted from the GDE Appliance, it pushes the configuration change to the VTE Agent running on that host. This change deletes VTE Agent certificates from the host and it deletes the “URL” line from the `agent.conf` file. The GuardPoints are removed, the host is no longer recognized by the GDE Appliance. If the agent tries to communicate with the GDE Appliance, the connection is refused.

Indications that a host has been deleted

If there are missing certificates in the `./agent/pem` directory and no URL line in the VTE Agent `agent.conf` file, that is an indication that the host has been deleted. However, if the host is offline when it is deleted from the GDE Appliance, and the host identity is changed before the host comes back online, the GuardPoints will not be removed, the certificates will remain intact in the `./agent/pem` directory and the `agent.conf` file will be unchanged, but the agent and server still will not be able to communicate with each other.

The GDE Appliance URL is deleted from the VTE Agent `agent.conf` file when the host record is deleted from the Management Console.

Logging for the VTE Agent on the GDE Appliance is also affected. If you delete a host from the GDE Appliance while the host is offline, when the host comes back online, log messages concerning the denied connection can be viewed only by GDE Appliance administrators of type System or All (when not in a domain). This is because the GDE Appliance, no longer has the host record, and does not know which domain the host belonged to, and cannot send messages to the appropriate log service.

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

Deleting a host

If a host has active GuardPoints, you will be prevented from deleting the host. A warning message is displayed telling you to unguard or disable the GuardPoints associated with the policy before you can delete the host. Make sure your data is accessible before you disable or unguard GuardPoints. This applies to LDT enabled hosts as well. Refer to the *Live Data Transformation Guide* for more information about data recovery and changing data from encrypted data to clear data on GuardPoints and for information about recovering data from LDT GuardPoints.

Deleting hosts with System or FS Agent Locks

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

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

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

   A dialog box opens that asks if you are sure you want to proceed with the operation.
8. Click **Ok**.

The host administrator with root permissions must log on to the host system and delete the agent software.

Deleting One Way communication hosts

In the case of one-way communication hosts, the host is deleted when the host receives the next status push from the GDE Appliance. If, for any reason the host cannot communicate with the GDE Appliance, a one- way communication host can be deleted manually as follows:

1. Select **Hosts > Hosts** from the Management Console menu bar. The *Hosts* window displays.
2. Select the host to be deleted. The **Delete Pending** column indicates the host as marked for deletion with a check mark.
3. Click on the host name to view the *Edit Host* page.
4. Clear the **Registration Allowed** checkbox, click **Ok** to return to the *Host* page.
5. Select the host again and click **Delete**. The host is removed from the GDE Appliance.

Configuring Host Groups

A Host Group is used to group one or more hosts to simplify configuration and administration. GuardPoints created on a host group are applied to all members of the group. Additionally, you can choose to apply host group configuration settings (except for password, FS Agent Lock, System Lock, Registration Allowed, and Communication Enabled settings), to all hosts that are members of that host group. It is important to keep this in mind when adding hosts to a host group. For example if you create an LDT policy in a host group, and then add a Docker enabled host to that host group, the Docker host will not be protected by that GuardPoint. Similarly, if you create a Linux file system GuardPoint in a host group, and then you add a Windows host to that host group, the Windows host will not be protected by that GuardPoint. See Chapter 22 “Managing GuardPoints” for more about creating GuardPoints on host groups.

The GDE Appliance supports two types of host groups; non-cluster and cluster. GDE Appliance cluster groups contain hosts that are members of a cluster with a cluster file system.

A host can be a member of more than one host group. However, membership in a cluster group is exclusive, so a host that belongs to a cluster, cannot join another cluster group, or host group.

Creating a host group

1. Select **Hosts > Host Groups** in the menu bar. The *Host Groups* window opens.
2. Click **Add**. The *Add Host Groups* window opens.
3. In **Host Group Name** field, enter a name for the new host group. This field is mandatory. The maximum number of characters is 64.
4. Select the host group type from the **Cluster Type** drop-down list. The options are *Non-Cluster*, *GPFS* or *HDFS*. If the host group is not a cluster group, select *Non-Cluster*. See “Creating a cluster host group” for how to create a cluster group.
5. (Optional) Enter a phrase or string in the **Description** text-entry box that helps you to identify this host group. This field is optional. The maximum number of characters is 256.
6. Click **Ok**. The *Host Groups* page opens. The newly created host group is visible in the host group table.

Adding hosts to a host group

Add hosts to the host group using either the registration shared secret or the fingerprint method.

1. If using the shared secret method, create the host group and the shared secret to be used by hosts that will be added to that host group.

2. If hosts were added to the GDE Appliance using the fingerprint method, create a host group and add the hosts to the host group (we recommend that these steps be scripted for large scale deployments).

Creating a Registration Shared Secret for a host group

You can create a registration shared secret at the same time that you create a host group or, you can create a registration secret later once you have planned your host group creation.

1. Create the host group, click the *Registration Shared Secret* tab, or if you have already created a host group and you want to register hosts using the a shared secret, click the name of the host group on the *Host Groups* page and on the *Edit Host Groups* page, click the *Registration Shared Secret* tab.
2. When you use the registration secret feature for the first time, the **Current Registration Secret** section will not have any information. If there is an existing shared secret, a message, **Show Registration Shared Secret** is displayed, select **Yes** to view the secret. The default setting is No.
3. Enter the following information in the **Create New Registration Shared Secret** section:

   a. **Registration Shared Secret creation method**—The same constraints that apply to password creation, namely uppercase letters, numbers, and special characters required, apply to the shared secret creation.

   - **Manual**—This is the default method. Select this to create the shared secret yourself.
   - **Generate**—Select this option to get an automatically generated password.

   b. **Validity period**—Select the period for which the shared secret will be valid. Click the calendar icon to select the dates.

   c. **Require that hosts are added first**—(Optional) If you select this option, you need to first add the host to the GDE Appliance database with the **Registration Allowed** check box enabled before you install and configure the agent.
4. Click **Ok**.

   To remove an existing shared secret, click **Expire Registration Shared Secret**. The expiry date turns red to indicate that the shared secret is no longer valid.

Adding Hosts to a Host Group using Fingerprint method

1. Select the *Member* tab and then click **Add**. The *Add Host* window displays all configured hosts, with the exception of current host group members.
2. Select the hosts to add to the group.

   Select the hosts to add to the host group based on the policies to be applied. For example, if you want to apply file system protection, then the hosts you select should run the VTE Agent.
3. Indicate if the host is to maintain its current host configuration or if the host group configuration is to be applied to the host.

At “`Do you want to apply the selected host(s) settings to host group settings?`”

Select **Yes** to apply the host group settings for **System Locked**, **FS Agent Locked**, communication enabling, and so on to the hosts.

Select **No** to add the hosts as they are and retain their individual configurations. This choice is not recommended. There is little reason to add a host to a host group and leave the host configuration intact. If you choose this option, you must be especially careful not to introduce configuration conflicts.

The default is **Yes**.

Click **Ok**. The *Member* tab displays the new host group members.

Refer to the *VTE Agent Installation Guide* for procedures to install and register the VTE Agent.

Creating a cluster host group

A cluster host group is a group of hosts that form a cluster.

1. Select **Hosts > Host Groups** in the menu bar. The *Host Groups* window opens.
2. Click **Add**. The *Add Host Groups* window opens.
3. In **Host Group Name**, enter the name of the new cluster host group. This field is mandatory. The maximum number of characters is 64.
4. Select the cluster group type from **Cluster Type** drop-down-list. The options are *Non-Cluster*, *GPFS* or *HDFS*. Select GPFS or HDFS depending on the type of file system on the host.

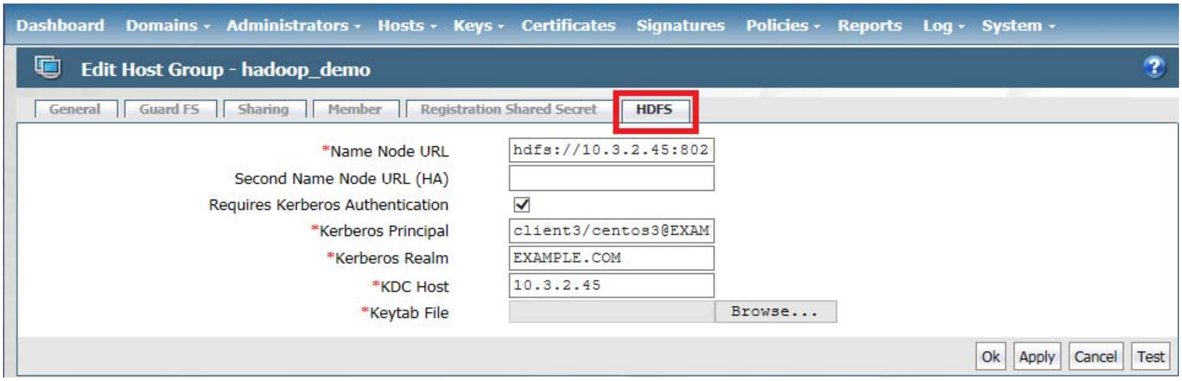
   Add the cluster nodes to the host group.

   GPFS is only supported on VTE Agent versions 5.x. See VTE Agent Release Notes for more information.

5. (Optional) Enter a phrase or string in the **Description** text field that helps you to identify this host group. The maximum number of characters is 256.
6. Click **Ok**. The *Host Groups* window opens. The newly created host group is visible in the host group table.
7. Click the host group in the **Name** column.
8. The *Edit Host Group* window opens. It has the following tabs: General, Guard FS, Guard Docker (if you have a license for it), Sharing, Member, and Registration Shared Secret.

   If the group is an HDFS cluster group, you will see a tab labeled **HDFS**.

Figure 48: HDFS tab in Edit Host groups window



*Name Node URL: hdfs://10.3.2.45:802

Second Name Node URL (HA):

Requires Kerberos Authentication: ☑

*Kerberos Principal: client3/centos3@EXAM

*Kerberos Realm: EXAMPLE.COM

*KDC Host: 10.3.2.45

*Keytab File:

9. Click the **HDFS** tab to complete the HDFS cluster group configuration. Enter the following information:

   a: **Name Node URL**: Enter the URL of the Name Node. If Hadoop authentication is configured as Simple mode, only the NameNode URL information is needed in the URL format `hdfs://<host>:<port>`. By default the port number is 8020, but check the HDFS configuration to make sure this is so. For HDFS HA cluster, the URLs for both active and standby are required.

   b: **Second Name Node URL (HA)**: If this is a high availability configuration, enter the name of the failover Name Node.

   c: **Required Kerberos Authentication**: Select this check box if Kerberos authentication is required for the HDFS cluster.

   > Kerberos Principal: Enter the name of the Kerberos principal

   > Kerberos Realm: Enter the name of the Kerberos realm

   > KDC Host: Enter the FQDN or IP address of the Kerberos Key Distribution Center (KDC)

   > Keytab File: Enter the name of the keytab file to be used for authenticating HDFS cluster hosts. Click **Browse** to navigate to the file.

   For more information about protecting data on HDFS configurations, see the *VTE Installation and Configuration Guide*.

10. Click **Ok** or **Apply** to save the configuration to the GDE Appliance database and then click **Test** to test the connection of the HDFS host to the Kerberos authentication server. The result of the test is displayed in the space above the tabs, if the test is successful, it displays ‘Successful’.

Displaying host groups

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions or type All.

2. Select **Hosts > Host Groups** in the menu bar. The *Host Groups* window opens. All configured host groups are displayed.

Editing host groups

Once you create a host group and add hosts to the group, you can configure the host groups. The following can be modified or configured from the *Edit Host Group* page:

- Change a group description, enabling agent communication, locking VTE agent files on the host
- Change the VTE Agent password for the hosts in the host group
- Enable policy enforcement, editing policies, applying policies
- Define GuardPoints
- Add hosts to a host group

The *General* tab allows you to enable agent communication for the host group, or enable System Lock or FS Agent Lock to control access to agent or system files.

- **Name**: Name of the host group.
- **Description**: Optional. Enter a description for the Host Group.
- **Enable FS Agent Communication**: Select to enable/disable interactive communications of File System Agents installed on members of the host group.
- **Enable Key Agent Communication**: Select to enable/disable interactive communications of key agents installed on members of the host group.
- **System Locked**: Select to lock down the key operating system files of the hosts of members of the host group. (If this is enabled, patches to the operating system of the host will fail due to the protection of these files)
- **FS Agent Locked**: Select to lock down the configuration of the File System Agent on the members of the host group. This will prevent updates to any policies on the members of the host group.
- **System Locked**: This check box is automatically selected when FS Agent Locked option is selected. It locks down the key operating system files of the host. If this is enabled, patches to the operating system of the host will fail.
- **Password Creation Method**: Select the password method to use to unlock the agent. The host user may be prompted to supply a password to decrypt encrypted data when there is no network connection between the host and the GDE Appliance. The methods are **Generate** (challenge-response) and **Manual** (static password).

  When you select **Generate**, the host user must request a new password from a GDE Appliance administrator each time a host password is required. If you select **Generate**, an additional option is displayed; **Regenerate Password**. Enable this toggle to download a new randomly generated password to all hosts in the group.

When you select **Manual**, the host user must request a new password from a GDE Appliance administrator each time a host password is required. Enter the password to apply to the hosts in the host group. The password is applied to each host in the host group and remains in effect when the hosts are removed from the host group or the host group is deleted. If you do not enter a password, the individual host password for each host in the host group remains unchanged. Enter the same password in the **Confirm Password** field to ensure that it had been typed correctly.

Host group password management

The GDE Appliance allows for host password management using host groups. For large-scale deployments where the GDE Appliance must manage several hundreds or thousands of agents, administering passwords on a per-host basis becomes untenable and administratively burdensome. Using a common password across all the hosts in a host group mitigates the administrative burden.

This feature is also useful for offline agent recovery. If a remote agent reboots (planned or unplanned) and cannot communicate with the GDE Appliance in the central office, it will prompt the administrator at the remote site to enter the host password. The remote site administrator typically calls the corporate help desk for the password. Using the password provided by the help desk personnel, the remote site administrator enables offline agent recovery and the resumption of services. Since the password is now known to the remote site administrator and the help desk personnel, it may result in a breach of security and/or render the IT operations to be non-compliant with respect to guaranteeing data privacy. To remedy the compromised situation, the security administrators should change the password—rotate the password—according to existing security practices. The host group password management feature allows changing the password on all the hosts in the host group when the password is compromised.

The use cases for host group password feature can be summarized as follows:

1. Set a common password for all hosts in a host group
2. Reset the common password for all hosts in a host group. If the password is provided to a remote agent administrator for offline agent recovery.

This feature is best used for deployments of scale when many agents are under the management of a GDE Appliance cluster.

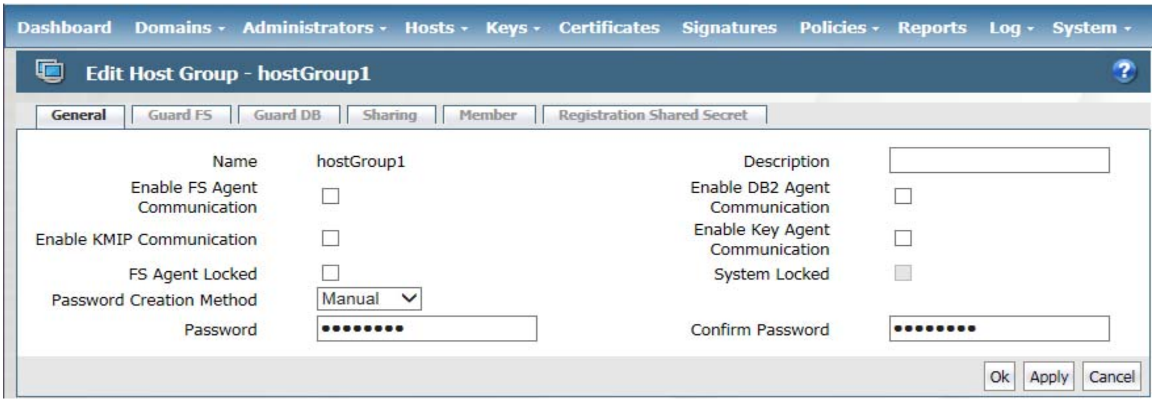
Resetting a host group password

1. Select the host group whose password must be changed.
2. Apply the new password.

When the new password is applied, the server pushes the password to all the hosts in the host group. Hosts that are removed from the host group retain the password set for the host group; hosts added to the host group later do not receive the new password.

Pushing the host group password to thousands of agents is demanding on the GDE Appliance. Initiating other transactions while the password push is in progress may result in the server returning the following message: “Server busy please retry”.

Figure 49: Host group password text boxes



Edit Host Group - hostGroup1

Name hostGroup1
Description
Enable FS Agent Communication □
Enable DB2 Agent Communication □
Enable KMIP Communication □
Enable Key Agent Communication □
FS Agent Locked □
System Locked □
Password Creation Method Manual
Password ••••••••
Confirm Password ••••••••

Protecting a host group

There are two ways to apply host protection. You can apply protection on a host-by-host basis or you can configure multiple hosts into a group and apply the same protection to all hosts in the group. Host groups are a convenient way to assign policies and keys simultaneously to a collection of hosts, rather than configuring each host individually.

You can configure hosts either before or after configuring host groups; however, creating hosts before creating host groups is quicker and requires fewer steps.

Before you apply GuardPoints:

- Create the initial host configuration in the Management Console for each host to be added the host group. See “Configuring Hosts”.
- Install the VTE Agent software on each host system, as described in the VTE Agent Installation and Configuration Guide.
- Create encryption keys. See “Adding Agent Keys”.
- Configure the policies using the encryption keys your just created, to apply to the hosts in the host group. See “Creating and Configuring VTE Policies”.

To create and apply protection to a group of hosts running VTE Agents:

1. Create a host group, see “Creating a host group”.

2. On the *Host Groups* page, click the host group in the **Name** column.

3. The *Edit Host Group* window opens. It has five tabs: *General*, *Guard FS*, *Sharing*, and *Member*.

4. Add hosts to the host group.

   a. Select the *Member* tab and then click **Add**. The *Add Host* window displays all configured hosts, with the exception of current host group members.

   b. Select the hosts to add to the group.

   Select the hosts to add to the host group based on the policies to be applied. For example, if you want to apply file system protection, then the hosts you select should run the VTE Agent.

   c. Indicate if the host is to maintain its current host configuration or if the host group configuration is to be applied to the host.

   At "`Do you want to apply the selected host(s) settings to host group settings?`" Select **Yes** to apply the host group settings for **System Locked**, **FS Agent Locked**, communication enabling, and so on to the hosts.

   Select **No** to add the hosts as they are and retain their individual configurations. This choice is not recommended. There is little reason to add a host to a host group and leave the host configuration intact. If you choose this option, you must be especially careful not to introduce configuration conflicts.

   The default is **Yes**.

   d. Click **Ok**. The *Member* tab displays the new host group members.

5. Apply GuardPoints.

   a. Select the *Guard FS* tab.

   This tab displays the applied policies, the host groups to which the policies are being applied, and their enforcement status. Nothing is displayed if this is a new installation or no policies are applied.

   b. Click **Guard**. The *Guard Host Group File System* window opens to display all VTE Agent policies.

   c. Complete the policy application process.

   For more about creating GuardPoints on a host group, see "Creating GuardPoints on a Host Group". If a host group contains LDT enabled hosts, see "Creating LDT GuardPoints". If the host group contains Docker hosts, see "Creating Docker GuardPoints".

   a. Select the *Guard Docker* tab

   This tab displays the applied policies, the host groups to which the policies are being applied, and their enforcement status. Nothing is displayed if this is a new installation or no policies are applied.

   b. Click **Guard**. The *Guard Host Group File System* window displays.

   c. Complete the policy application process.

6. Select the *General* tab. The *General* tab displays the host group name and its description. It is also used to enable the GDE Appliance to begin administering the host group members.

a. Enable the **Enable FS Agent Communication** check box.

b. The member hosts are administered as a group when you enable these check boxes.

c. (Optional) Enable the **FS Agent Locked** and **System Locked** check boxes to apply protection—prevent the deletion or modification of VTE Agent installation files—to system files and VTE Agent files that reside on the host.

d. (Optional) Set the password method for unlocking GuardPoints when the host cannot communicate with the GDE Appliance.

The password method is applied to each host that is currently a member of the host group. The password method remains in effect until it is changed in the *Edit Host Group* window or the *Edit Host* window. If a host is removed from the group, or the group is deleted, the host retains the current password method. You can use the *Edit Host* window to change the password or password method of an individual host at any time.

Select either **Generate** or **Manual** from the **Password Creation Method** scroll-list. **Generate** enables the challenge-response feature where the user displays a string on the host system, gives the string to the GDE Appliance administrator, and the GDE Appliance administrator returns a response string for the host user to enter. The response string is a single-use password that expires within 15 minutes. **Manual** is used to assign a static password to the host. The static password does not expire and can be used repeatedly until the GDE Appliance administrator changes it. The default method is **Generate** for non-cluster host groups and HDFS host groups, for GPFS cluster groups the only option is **Manual**.

NOTE: If you select **Generate**, all the hosts in the host group must support the challenge-response feature. Hosts that do not support the challenge-response feature will still receive the randomly generated password; however, they will be unable to create the challenge string.

The **Support Challenge & Response** field displays the dynamic password generation status of the host. The **Support Challenge & Response** field is not displayed in the *Edit Host Group* window. To determine if a host supports dynamic passwords, open the *Edit Host* window for the host to the *General* tab to display the **Support Challenge & Response** field on that tab.

The **Password Creation Method** drop-down is used to apply a password creation method to the members of a host group only. It does not indicate the current password method for the host group. By default, the *Edit Host Group* window always displays the **Generate** password method when it is opened. Also, when the **Manual** password method is displayed, the dots in the password text-entry boxes do not indicate that a default password is provided or that a password had been entered.

7. If you switch the password method from `Manual` to `Generate`, regenerate the password.

   The **Regenerate Password** check box is displayed on the *General* tab when you change **Password Creation Method** from **Manual** to **Generate**. Select the **Regenerate Password** check box and click **Apply**. A new randomly generated password is created and downloaded to the hosts in the host group.

8. If you switch the password method from **Generate** to **Manual**, enter a new password.

The **Password** and **Confirm Password** text-entry boxes are displayed. Enter the password to assign the hosts in the **Password** and **Confirm Password** text-entry boxes.

Ignore the dots in the **Password** and **Confirm Password** text-entry boxes when you open the *Edit Host Group* window. They do not indicate a default password or that a password had already been entered.

If you do not enter a password, the hosts in a host group retain their original passwords.

NOTE: The host group password is not applied when a host is added to a host group. The `Do you want to apply the host group configuration to the selected host(s)?` field does not include the host group password. New host group members retain their original host password. To apply the host group password to the hosts in the group, change the password fields the `Edit Host Group` window and click **Apply**.

9. Click **Ok** to finalize the changes and close the window.

10. Check the configuration of each host in the host group.

    We recommend that you open each host in the *Edit Host* (not *Edit Host Group*) window to double-check that no configuration conflicts were introduced by adding the host to the host group. Also, check the status of GuardPoints to ensure that the GuardPoints and policies were applied as expected.

11. For VTE Agents, try accessing a GuardPoint to verify that the GDE Appliance and the host in the host group can communicate, as well as to verify the policy itself.

12. Display the GDE Appliance log to monitor the backup process.

Protecting a Docker host group

You can manage a group of Docker hosts by adding them to a host group and applying security policies to the host group.

Before you apply GuardPoints:

- Create the initial host configuration in the Management Console for each host to be added the host group. See “Configuring Hosts”.
- Install the VTE Agent software on each host system, as described in the VTE Agent Installation and Configuration Guide.
- Create encryption keys. See “Creating symmetric keys”.
- Configure the policies using the encryption keys your just created, to apply to the hosts in the host group. See “Creating and Configuring VTE Policies”

Apply a Docker GuardPoint:

a. Select the *Guard Docker* tab

This tab displays the applied policies, the host groups to which the policies are being applied, and their enforcement status. Nothing is displayed if this is a new installation or no policies are applied.

b. Click **Guard**. The *Guard Host Group File System* window displays.

c. Complete the policy application process; select the Docker host, the policy, the Docker image or container on which you want to apply the GuardPoint, and the path to the image directory or container volume on which to apply the GuardPoint.

If you are creating a Docker Image based GuardPoint, your Docker container stores the data in a Docker volume. You need to enter the path of the folder to be protected manually. This path should match the path that will be seen from inside the Docker container.

Sharing host groups

You can share the members of the host group with other domains. Sharing allows remote Security Administrators in other domains to administer GuardPoints on the local host. Only GuardPoints guarded by File System agents can be shared.

Host sharing example:

Hostgroup_1 in domain_1 is configured with two GuardPoints; gp_A, a manual guard set to /home/manual, and gp_B, an autoguard set to /home/autoguard. Hostgroup_1 has one member; host_1. If hostgroup_1 is now shared with domain_2, it means domain_2 imports hostgroup_1 and any hosts in domain_2 can be added as members of hostgroup_1. GuardPoint configurations defined in hostgroup_1 will now apply to any hosts from domain_2 that are added to that host group.

Share a host group:

1. Select the *Sharing* tab.
2. Click **Share**.
3. Enter the name of the domain with which to share the members of the host group in the **Domain Name** text-entry box.
4. Click **Ok**.

Remove sharing:

Click **Unshare** to remove sharing and return GuardPoints to the domain in which the host was configured.

Host Group Host Settings

Host Settings can be applied at the Host Group level. The Host Settings tab allows you to set authentication options for the applications running on the hosts in this host group. For a detailed explanation of Host Settings options, see “Host Settings” on page 277.

Caution: Care must be taken while defining host settings at the host group level. If a host group contains member hosts with different operating systems (e.g., Linux and Windows), or host with Docker and non-Docker hosts, that inherit host settings from the host group, this may result in conflicts and affect file and user access permissions.

A host that joins a host group has the option to inherit host group configuration, this includes host settings. If host settings have not been defined at the host group level i.e., left blank, then the host retains its own settings. If host settings at the host group level are modified later, then those settings will apply to all members of the group that are set to inherit configuration from that host group. Individual members of that host group will have host settings overwritten by the host group host settings. For example;

- `hostA` has host settings defined and then joins `hostGroup1` and inherits `hostGroup1` configuration. `hostB` also joins `hostGroup1` but, is not set to inherit the host group configuration. `hostGroup1` does not have any Host Settings defined, `hostA` retains it’s own Host Settings and so does `hostB`.
- `hostGroup1` modifies its Host Settings, all members set to inherit host group settings will now have their individual settings overwritten by the host group Host Settings. `hostA` inherits the host group Host Settings but, `hostB` does not, as it does not inherit host group configuration.
- `hostB` then changes it’s inheritance settings from the Host Settings tab to inherit settings from `hostGroup1`. The next time `hostGroup1` updates Host Settings, the changes will apply to both `hostA` and `hostB`.

A host can be a member of more than one host group. If the host is set to inherit host group configuration from the first host group it joins, and the next group it joins, it inherits the Host Settings of the last host group that it joins. For example;

- `hostC` joins `hostGroup2` and inherits the host group configuration, `hostC` now has `hostGroup2` Host Settings. `hostC` is then added to `hostGroup1` and is set to inherit host group configuration and so it gets `hostGroup1` host settings.

If a host group empties its Host Settings, any member hosts that inherit, retain the last Host Settings that were defined. For example;

- hostGroup1 then deletes its Host Settings. All member hosts (hostA, hostB, and hostC) retain the last Host Settings defined for hostGgroup1—blank Host Settings are not passed on to members of the group. hostB leaves hostGroup1, and it retains the Host Settings it last inherited from hostGroup1.

If the Host Settings of a member of a host group are modified, that host no longer inherits Host Settings from the host group. For example;

- Host Settings on hostB are modified. Then the Host Settings for hostGroup1 are modified, all members except hostB will inherit the changes made to the Host Settings for hostGroup1.

Configure Host Group Host Settings

1. Navigate to **Hosts > Host Groups**, click the host group for which to modify Host Settings, the *Edit Host Group* windows displays.
2. Click the *Host Settings* tab of the *Edit Host Group* window.
3. In the **Host Group Settings** text box, add |authenticator| before the path of the binary. (e.g., |authenticator|/bin/su to allow su to be a trusted method of authentication). For further consideration of authentication options, refer to "Host Settings" on page 277.
4. If you add another process to the set of trusted applications in the Host Settings, check the **Re-Sign Settings** check box to ensure that the new process is signed and authenticated by the host. The next time host settings are pushed to the VTE Agent host, the updated host settings are re-signed and the **Re-Sign Settings** check box on the GDE Appliance Console is cleared (or reset). If you do not select this option after adding a new process, the host will ignore the newly added process. See "Re-Sign Settings" for more information about this setting.
5. Select one of the available choices from the **Apply Settings to Hosts** option:
   - **Only Hosts which currently inherit from this Host Group**: this will propagate changes only to the hosts that have chosen to apply Host group configuration.
   - **All hosts in this host group**: this will apply changes to all hosts that are members of this host group.
6. Click **Apply** after making changes to the host settings.

Change Host Group Host Settings inheritance

Hosts that are members of more than one host group inherit host group configuration (including host settings) from the last host group that they joined with inheritance set to 'Yes'.
To change the host group from which to inherit Host Settings:

1. Navigate to **Hosts > Hosts** and click the host for which the host group host settings inheritance is to be changed, the *Edit Host* window displays.

The **Host Settings from** field displays the host group from which the shared host inherits Host Settings.

2. From the **Make Host Settings inherit from** drop-down list, select the host group whose Host Settings you want to apply to this host.
3. Check the **Re-Sign Settings** check box to ensure that the new process is signed and authenticated by the host. The next time host settings are pushed to the VTE Agent host, the updated host settings are re-signed and the **Re-Sign Settings** check box on the GDE Appliance Console is cleared (or reset). If you do not select this option after adding a new process, the host will ignore the newly added process.

The *Member* tab of the *Edit Host Group* window displays where the host inherits its Host Settings, see “Adding hosts to a host group”.

Adding hosts to a host group

The *Member* tab on the *Edit Host Group* window displays the following information about members of the host group:

- **OS Type**: Indicates the host operating system type, e.g., Linux, Windows.
- **Host Name**: The fully qualified domain name of the member host.
- **FS Agent**: Indicates whether a VTE (FS) Agent is installed on the member host.
- **Key Agent**: Indicates whether a Key (VAE/VKM) Agent is installed on the member host.
- **One Way Comm**: Indicates whether the installed agent is configured to use one way communication.
- **FS Agent Lock**: If checked, indicates that the VTE (FS) Agent configuration on that host are locked.
- **System Lock**: If checked, indicates that the key operating system files on the host are locked. If this is enabled, software patches applied to the operating system will fail.
- **LDT Enabled**: Indicates whether this feature has been enabled or not.
- **Docker Enabled**: Indicates whether this feature has been enabled or not.
- **Secure Start**: Indicates whether this feature has been enabled or not.
- **Host Settings From**: Indicates how the host gets its Host Settings. The following are possible:
  - This host - which means the host does not inherit host settings from any host group, they are set on the host.
  - This host group - which means the member host inherits its host settings from the current host group.
  - <<*Name of host group*>> - which means that the member host inherits Host Settings from another host group of which it is a member.

Add hosts to a host group from the *Member* tab on the *Edit Host Group* page.

1. On the *Member* tab page, click **Add**. The *Add Host* window displays all configured hosts, with the exception of current host group members.
2. Select the hosts to add to the group based on the policies to be applied. For example, if you want to apply file system protection policies, then the hosts you select should run the VTE Agent.
3. Indicate if the host is to maintain its current host configuration or if the host group configuration is to be applied to the host.
4. The following message is displayed under the table listing the available hosts; “Do you want to apply the host group configuration to the selected host(s)?”

   a: Select **Yes**, to apply the complete host group configuration (except for the host group password) will be applied to this host including:

   - Host Settings from the selected host group
   - File System Agent Lock
   - System Lock
   - Registration Allowed
   - Communication Enabled

   b: Select **No** to add the hosts as they are and retain their individual configurations. This choice is not recommended. There is little reason to add a host to a host group and leave the host configuration intact. If you choose this option, you must take care not to introduce configuration conflicts.

   The default is Yes.
5. Click **Ok**. The *Member* tab displays the new host group members.

Deleting host groups

As part of GDE Appliance maintenance, you occasionally must remove host groups from the GDE Appliance. Deleting a host group removes only the group; the individual hosts that are members of that group remain intact. You cannot delete host groups that are configured with a policy. You must delete the host group GuardPoints from the host group before you can delete the host group itself. If you configured a host group password, the individual hosts retain the host group password.

To remove a host group:

1. Log on to the Management Console as an administrator of type Security with `Host` role permissions, type Domain and Security, or type All.
2. Select **Hosts > Host Groups** in the menu bar.

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

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

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

4. Click **Delete**.

   You are prompted to verify the deletion.

5. Click **Ok**.

Managing GuardPoints

22

GuardPoints are directories protected by VTE Agent security policies. Access to files and encryption of files in protected directories is controlled by security policies.

This chapter contains the following sections:

Overview

Before you apply GuardPoints you must do the following:

- Add a host to the GDE Appliance, see "Configuring Hosts and Host Groups".
- Install and register the VTE Agent on the host system, as described in the VTE Agent Installation and Configuration Guide.
- Create encryption keys, see "Managing Keys".
- Configure policies using the encryption keys you created, see "Configuring Policies".
- Create a GuardPoint. Check that no one is using the directory to be guarded before making it a GuardPoint.

  If users are working in the directory when it is made into a GuardPoint, users can continue to use data in memory rather than use the actual data in the GuardPoint. Tell users to save their work, to close applications that are running in the directory, and to exit the directory before applying the GuardPoint. When they re-enter the directory they will use protected data and the VTE Agent will work appropriately.

This chapter describes how to create LDT GuardPoints on LDT enabled hosts, and on container images and containers on hosts, Secure Start GuardPoints, as well as creating GuardPoints on host groups.

See “Creating GuardPoints on a Host” for how to create GuardPoints on a host and “Creating GuardPoints on a Host Group” for how to create GuardPoints on a host group.

Secure Start GuardPoints

Secure Start offers a new type of GuardPoint that offers data protection for applications which start earlier in the boot sequence than VMD (VTE agent daemon). This feature is only supported on hosts running Windows OS. For example, an AD (Active Directory), or SQL Server service starts very early. A Secure Start GuardPoint starts before the AD and SQL services, and can, therefore, encrypt those services. For more information about protecting such applications using Secure Start, refer to the Secure Start chapter in the *VTE Installation & Configuration Guide*. To determine if another application qualifies for Secure Start, contact Thales technical support.

Considerations before creating a GuardPoint

1. If a host is to be added to a host group, do not apply a GuardPoint at the host level, rather, apply the GuardPoint at the host group level. You can do both, but it is harder to keep track of GuardPoints applied at the host group level and custom GuardPoints applied at the host level.

2. Certain directories are protected against guarding, plan your GuardPoints accordingly:

   a. The top-level "Program Data" folder on Windows Vista and Windows 2008, and the top-level "Documents and Settings" folder on all other Windows platforms, cannot be guarded because a GuardPoint cannot be applied to a folder that contains open files. The same is true for the “Users” folder. The VTE Agent opens and continually maintains log files in subfolders under "ProgramData" and "Documents and Settings". Other subfolders below "ProgramData" and "Documents and Settings" can be guarded as long as there are no open files in any subfolder at the time the GuardPoint is applied.

   Be especially careful when specifying paths for Windows agents. Cross-guarding the same folder with different policies and encryption keys will give unexpected results and will corrupt the files in that folder.

   GuardPoint paths must use standard Windows path notation and delimiters. Incorrect notation and delimiters are ignored and discarded by the Windows agent. Therefore, it is possible to enter two paths that resolve to the same Windows folder and successfully guard both of them. The GDE Appliance reports that it is guarding two unique folders when, in fact, it is guarding the same folder twice.

   Do not use any of the following characters as path delimiters: `|?<>:*"/,` For example, both `C:\gp\` and `C:\gp/\` are allowed by the GDE Appliance. When the second GuardPoint is applied, the extraneous "/" is discarded by the Windows VTE Agent and the Windows VTE Agent applies a GuardPoint to `C:\gp\` a second time.

b. On Linux, the following directories cannot be guarded:

- `<secfs install root>/agent/secfs/`
- `<install root>/agent/secfs/bin` and everything beneath it
- `<secfs install root>/agent/vmd` and everything beneath it
- `/etc/vormetric` and everything beneath it
- `/etc`
- `/etc/pam.d` and everything beneath it
- `/etc/security` and everything beneath it
- `/usr`
- `/usr/lib`
- `/usr/lib/pam`
- `/usr/lib/security` and everything beneath it
- `/etc/rc*` and everything beneath it
- `/var/log/vormetric`

c. You cannot apply VTE Agent protection to already mounted and guarded directories, nor can you nest GuardPoints.
The `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec` directory is automatically mounted and guarded by `secfs` when the VTE Agent process starts on the host. You cannot apply a GuardPoint to `/opt` because it contains the existing GuardPoint, `/opt/vormetric/DataSecurityExpert/agent/secfs/.sec`; however, you can guard a directory like `/opt/myapps` because it is in a different hierarchy and has no impact on `/opt/vormetric`.

Display mounted and guarded directories using the `df` command.

3. As of the v3.x release, both GDE Appliance and VTE support a new enhanced encryption mode (CBC-CS1). If your host groups contain v6.1.0 VTE hosts and other hosts with earlier versions of VTE, you ***cannot*** apply policies containing keys that use this new encryption mode. The action fails with an error message informing you that all hosts in the host group do not support the key's encryption mode. Only hosts with VTE v6.1.0 support the new encryption mode. Refer to "Enhanced Encryption Mode" on page 205 and to the *VTE Agent Guide* for more about the new encryption mode.

Changing a policy or rekeying a GuardPoint

To change a policy or rekey a GuardPoint, be prepared to temporarily stop access to the GuardPoint. Changing policies for a GuardPoint requires an interruption of service because the transition process entails disabling one policy and then enabling another policy. The

GuardPoint must be inactive during the transition period to ensure GuardPoint integrity. The same rule applies to moving a host between host groups when it includes a change in policies. Coordinate policy changes during a maintenance outage window.

If Live Data Transformation (LDT) is enabled on your hosts, encryption and rekeying of GuardPoint data is done without blocking user or application access to the data. LDT is a separately licensed feature, refer to "Enabling Live Data Transformation" and the *Live Data Transformation Guide* for more information about implementing LDT.

Creating GuardPoints on a Host

This section describes how to create a GuardPoint on a host.

NOTE: Information about UNIX agents applies to earlier versions of those agents, since as of v6.0, UNIX agents are EOL.

Create a host GuardPoint

1. Log on to the Management Console as an administrator of type Security with Host role permissions, type Domain and Security, or type All.

2. Select **Hosts > Hosts** on the menu bar.

   The *Hosts* window opens.

3. Click the target host in the **Host Name** column. The *Edit Host* window opens to the *General* tab for the selected host.

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

   To create LDT GuardPoints, the **Live Data Transformation** check box must be selected, see "Creating LDT GuardPoints".

   To create Docker GuardPoints, the **Docker Enable**d check box must be selected, see "Creating Docker GuardPoints".

   To create a Secure Start GuardPoint, the **Secure Start GuardPoint** checkbox must be enabled. This feature is only supported on Windows hosts. Refer to the *VTE Installation & Configuration Guide* for details and procedures to create these GuardPoints.

4. Select the *Guard FS* tab.

   The panel displays applied policies in a tabular format. Each policy line in the table consists of:

- Select check box: select the GuardPoints that you want to **Unguard**, **Enable**, or **Disable**

  You can also do any of the following from this tab:

  - **Refresh**: Update the *Edit Host* page.
  - **Suspend Rekey**: Click to suspend rekey or data transformation operations, for all GuardPoints on the selected host.
  - **Re-Push Policies**: Click to push a policy update to a host. For example, if a rekey operation is underway on your host and you rotate the encryption key, the agent will not accept the policy push. You can re-push the policy until the agent accepts it and performs the rekey operation again.
  - **Transform Sparse Regions:** This is only applicable for LDT policies. If you selected this option while creating a GuardPoint, it means that sparse file regions will be transformed. Once selected, this option cannot be disabled. If you did not select this option while creating a GuardPoint, sparse regions will not be transformed. You have one opportunity to disable this option from the Guard FS tab. Once you change the setting, you cannot roll it back. It is a one-time change.
  - **Secure Start On:** This button is displayed only if the Secure Start feature has been enabled on the host. Select this option to create a Secure Start GuardPoint.
  - **Secure Start Off:** This button is displayed only if the Secure Start feature has been enabled on the host. Select this option to turn off Secure Start for the GuardPoint.
- **Policy**: the name of the policy applied to the GuardPoint.
- **Host group**: name of the host group of which the current host is a member
- **Protected Path**: the GuardPoint path that is protected
- **Disk/Disk Group**: If a raw partition is a member of an Oracle ASM disk group, it is displayed in the form, group_name/disk_name.
- **Type**: the type of GuardPoint being applied on a UNIX host.
  - Directory (Auto Guard)
  - Directory (Manual Guard)
  - Raw or Block Device (Auto Guard)
  - Raw or Block Device (Manual Guard)
- the type of GuardPoint being applied on a Windows host
  - Directory (Auto Guard)
  - Raw or Block Device (Auto Guard)
- **Domain**: the domain in which the host is administered
- **Auto Mount**: an indicator of the file system mount type, whether a regular mount or an automount

- **Enabled**: displays the policy enforcement status, can be either enabled or disabled.
- **Secure Start**: indicates whether the GuardPoint is a Secure Start GuardPoint. This can be enabled or disabled by selecting the GuardPoint and clicking **Secure Start On**, or **Secure Start Off** as applicable.
- **Transform Sparse Regions**: indicates whether transform sparse regions is enabled or not. If this was set when creating the GuardPoint, you can disable it by unchecking the option in the column. Once disabled, it cannot be re-enabled. This column is displayed only if LDT is enabled for that host.
- **Status**: connection status to the host
- **Rekey Status**: indicates the transformation status of the data rekey operation.

  See the *Live Data Transformation Guide* for more information about LDT GuardPoints.

The policy table is empty if this is a new host configuration or if no policies are applied.

LDT Quality of Service

If you have a Live Data Transformation (LDT) license and the LDT feature enabled on your host, this tab displays **Quality of Service** in the top panel of the Guard FS tab. The QoS feature allows administrators to maintain operational efficiencies in their systems in conjunction with LDT operations. QoS lets administrators specify CPU usage and schedules for LDT operations. See the *Live Data Transformation Guide* for best practices about using LDT and QoS. The following options are available:

- **Schedule**: Select a schedule to run LDT. The options are; ANY_TIME, WEEKENDS, and WEEKNIGHTS. If you select ANY_TIME, LDT will run any day at any time of the week. If you select WEEKENDS, LDT will run between 9:00 PM Friday to 11:59 PM Saturday, and from midnight on Sunday to 7:00 AM on Monday. If you select WEEKNIGHTS, LDT will run between midnight to 7:00 AM from Monday to Friday.

  You can also create custom QoS schedules:

a. Navigate to **Hosts > QoS Schedules**, click **Add**.

b. The *Add/Edit QoS Schedule* page displays. Enter a name for the schedule and a description (this is optional). Click **Add** again.

c. The scheduling options are displayed. You can make the following selections:

  - **Starting Day**: day of the week to start the LDT process
  - **Ending Day**: day of the week to end the LSDT process
  - **Start Time**: Time at which to start the LDT process.
  - **Ending Time**: Time at which to stop the LDT process

d. Click **OK**, then click **OK** again, to go back to the *QoS Schedules* page.

  The new schedule is listed ion the table and will also be available in the **Schedule** drop down list in the LDT Quality of Service panel on the *Guard FS* tab.

- **Set % of available CPU usage for rekey**: Define what percentage of the host servers CPU should be reserved for LDT rekey operations. Refer to the LDT Guide for more information about rekey operations.
- **Cap CPU Allocation**: Select this option to cap CPU usage to the percentage defined in Set % of available CPU usage for rekey. If you do not select this option, LDT operations will utilize all of the available CPU memory.

Create a GuardPoint

NOTE: Information about UNIX agents applies to earlier versions of those agents, since as of v6.0 UNIX agents are EOL.

1. Click **Guard**.

   The *Guard File System* window opens.

2. Select the type of policy to apply from the **Policy** drop-down menu.

   If LDT is enabled on your host, then the Live Data Transformation policy type will also be available, see “Enabling Live Data Transformation” for more information. You must select a policy before you can browse the agent file system.

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

3. Select the type of GuardPoint to apply in the **Type** drop-down menu.

   UNIX choices are **Directory (Auto Guard)**, **Directory (Manual Guard)**, **Raw or Block Device (Auto Guard)**, or **Raw or Block Device (Manual Guard)**.

   Windows choices are **Directory (Auto Guard)** or **Raw or Block Device (Auto Guard)**.Select **Directory (Auto Guard)** or **Directory (Manual Guard)** for file system directories.

   If your host is a Docker host, then only **Directory (Auto Guard)** and **Directory (Manual Guard)** are available.

   Select **Raw or Block Device (Auto Guard)** or **Raw or Block Device (Manual Guard)** for raw or block devices.

   Select **Directory (Manual Guard)** for file system directories that are to be manually guarded and unguarded in order to failover to a different node in a cluster.

   Select **Raw or Block Device (Manual Guard)** for raw devices that are to be manually guarded and unguarded in order to failover to a different node in a cluster.

   Directory (Manual Guard) and **Raw or Block Device (Manual Guard)** are guarded and unguarded (for example, mounted and unmounted) using the `secfsd -guard` and `secfsd -unguard` commands. Do not use the `mount` and `umount` commands to swap GuardPoint nodes in a cluster configuration.

4. In the **Path** text box:

- Enter the full paths of one or more directories in the **Path** text-entry box and click **Ok** to apply the policy to the target GuardPoint. Enter one path per line in the **Path** text-entry box.
- Enter part of a directory path in the **Path** text-entry box and click **Browse** to jump to the specified point. From there, you can use the browser to descend further into the directory hierarchy and select one or more directories to be guarded.
- Click **Browse** to locate and select entire paths. Use the browser to locate the target GuardPoint, to avoid typographical errors, and to verify host availability.

  If multiple paths are entered, they will all be protected by the same policy.
- Click the **Browse** button to locate the host directory to guard. The Remote File Browser window opens.

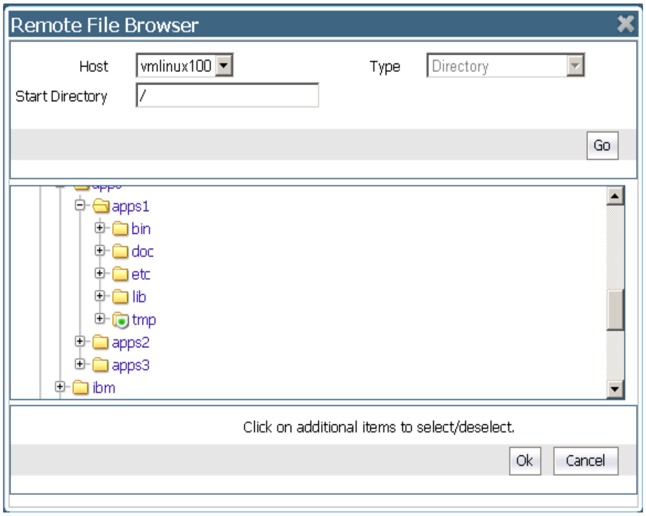
  If a target GuardPoint exists, use the browser to select the GuardPoint path. If it does not exist, be sure to enter the GuardPoint path correctly. The GDE Appliance does not parse manually entered paths for correct syntax.

  See, “Considerations before creating a GuardPoint” for what to be aware of before creating a GuardPoint.

NOTE: When browsing a Docker image on a host, volumes created on a container run off that image are not visible if that container has been removed. If you want to create a GuardPoint on a container volume that container must exist (e.g. running or stopped), in order for the volume to be visible. Or, you can manually enter a path for a volume you want to guard, and then when a container instance is run off that image, you must remember to create those volumes in order for the GuardPoint to apply.

- Find target GuardPoints. Click the plus symbol (+) next to a folder to display the next level of the directory hierarchy. Click the minus symbol (-) to collapse the hierarchy. Click a folder or file name to select that directory or file.

Figure 1: Browsing for GuardPoints



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

To quickly traverse different directory hierarchies, you can enter part of the path to the GuardPoint in the **Start Directory** text-entry box and click **Go**, or press <`Enter`>, to display and select the rest of the path.

5. Select one or more directories to be configured as GuardPoints.

   Single-click a directory in the scroll-list to select an individual directory. Hold the <`Ctrl`> key down to select multiple directories. Hold the <`Ctrl`> and <`Shift`> keys down to select a range of directories.

   You should check that no file or directory below a selected GuardPoint is being accessed. If something under a GuardPoint is being used or accessed, the GDE Appliance may not be able to take control of the directory and apply protection.

   Keep the following in mind while selecting a GuardPoint path:

   a. The maximum number of characters allowed in a GuardPoint path is determined by your operating system. You can specify a GuardPoint path up to the restriction imposed by the host operating system. However, we recommend that you keep it below 1,000. Beyond 1,000 characters, the path information for the **Resource** field in the Message Log and host messages file (for instance, `/var/log/messages`) is truncated, and the Key and Effect fields that normally follow the **Resource** field are not displayed.

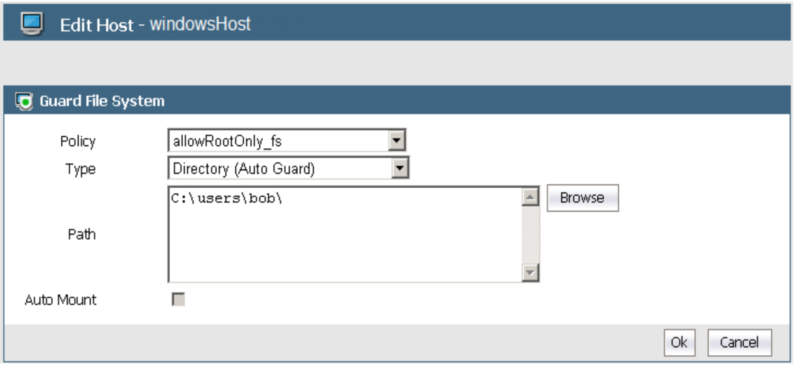
b. The directory (or directory path) specified in a resource set is appended to the GuardPoint. This means if the GuardPoint is `/mnt/remote2` and the resource set directory path is `/remoteDir`, then the policy is applied to the files and directories in `/mnt/remote2/remoteDir`.

6. The **Auto Mount** check box disappears when **Directory (Manual Guard)** or **Raw or Block Device (Manual Guard)** is selected because only regular mounts are supported by these types.

NOTE: The **Auto Mount** option is also disabled for GuardPoints on Docker hosts.

7. Select **Secure Start** to create a Secure Start GuardPoint.
8. Click **OK**.

Figure 2: Completed GuardPoint selection



Edit Host - windowsHost

Guard File System

Policy: allowRootOnly_fs

Type: Directory (Auto Guard)

Path: C:\users\bob\

Auto Mount: □

9. Click **OK**.

   The *Edit Host* page is updated to display the new GuardPoint or GuardPoints.

   Note the GuardPoint status:

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

10. Wait a moment then click the **Refresh** button to update the display.

    The red square should change to a green circle.

    It may be easier to execute the `df` command repeatedly on the host system until you notice a `secfs` mount for the new GuardPoint, or, execute `tail -f /var/log/vormetric/vorvmd_root.log` and wait until a message like the following is displayed:

```
Successfully received and implemented a new security configuration.
```

11. Redisplay the *Guard FS* tab.

Creating LDT GuardPoints

To create an LDT GuardPoint:

1. Create an LDT policy
2. Set the Quality of Service, see "LDT Quality of Service".
3. Click **Guard** on the *Guard FS* tab to apply an LDT policy to a directory or file and create a GuardPoint.

See the *Live Data Transformation Guide* for more information about creating policies, creating QoS schedules, and creating LDT GuardPoints. See "Creating and Configuring VTE Policies" for procedures to create LDT policies.

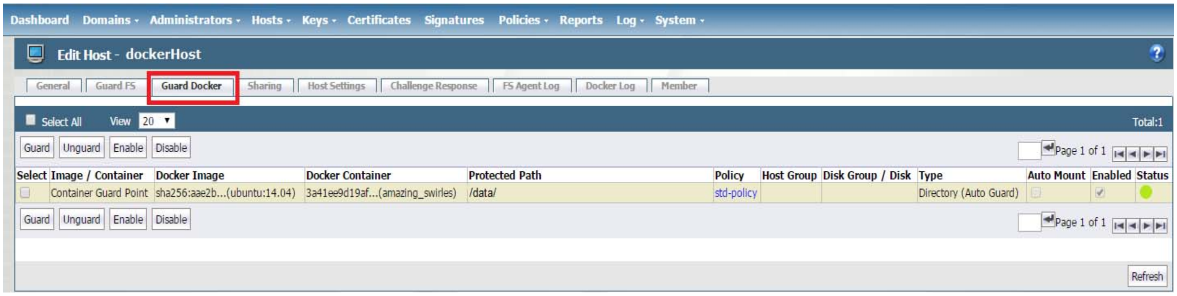
Creating Docker GuardPoints

GuardPoints can be created for Docker images or for docker containers. Before creating GuardPoints on Docker images and containers, the following must be taken into consideration:

- In order to use Vormetric data security protection, you must add the Docker engine process to the Host Settings, see "Host settings for a Docker enabled host".
- When applying GuardPoint policies to Docker containers, users must ensure that the root user has at least 'permit' effect on the GuardPoint, or else the GuardPoint will be completely inaccessible to all users, even for users with ‘apply_key’, and ‘permit’ effects.
- If you create a Docker image-based GuardPoint, that GuardPoint is pushed to any container that is run off that image. A Docker container started from that protected image, stores data in a Docker volume. To protect volumes used by the container, you need to enter the path of the folder to be protected manually. This path should match the path that will be seen from inside the Docker container.

1. Log on to your GDE Appliance as an administrator of type Security, Domain and Security, or All.
2. Navigate to **Hosts**.

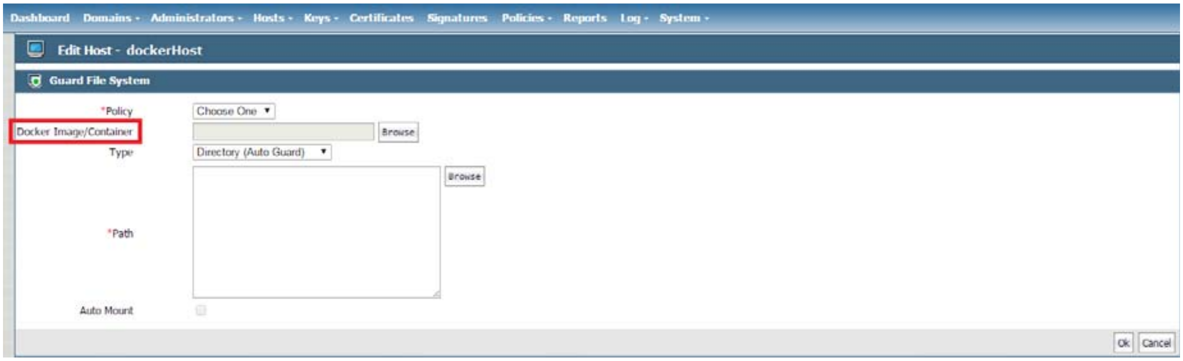
Figure 3: Guard Docker tab



Select	Image / Container	Docker Image	Docker Container	Protected Path	Policy	Host Group	Disk Group / Disk	Type	Auto Mount	Enabled	Status
□	Container Guard Point	sha256:aae2b...(ubuntu:14.04)	3a41ee9d19af...(amazing_swirles)	/data/	std-policy			Directory (Auto Guard)	□	☑	●

3. On the *Hosts* page, click the name of the host in the **Host Name** column, the *Edit Host* page opens.
4. Click the **Guard Docker** tab.
5. Click **Guard** to open the *Guard File System* page, from where you can select a policy to apply to a Docker image or container on your docker host.
6. Select a policy to apply to the GuardPoint you are about to create.
7. Click **Browse** next to the **Docker Image/Container** field to browse the Docker host for an image or container to which to apply the policy.
8. Select the type of directory to guard.
9. Click **Browse** next to the **Path** text box to browse the image or container for a file path to add the GuardPoint.

Figure 4: Guard File System - select a Docker image or container



*Policy	Choose One
Docker Image/Container	
Type	Directory (Auto Guard)
*Path	
Auto Mount	□

10. Click **Ok**, the *Edit Host* page opens with the newly created GuardPoint listed in the table.

NOTE: Auto Mount is not supported in a Docker environment.

Refer to the *Data Transformation Guide* for details about transforming data on Docker image and container GuardPoints.

Creating Secure Start GuardPoints

Access to a Secure Start GuardPoint is only permitted during the boot sequence and for a short period of time. Once the VMD is up and running, it performs the normal agent initialization and communicates with the GDE Appliance to access files within a GuardPoint location.

To apply Secure Start GuardPoints:

1. Click **Hosts > Hosts > <hostName>** on the Management Console.
2. In the **General** host information section, select the option: **Secure Start GuardPoint**.
3. Click **Guard FS**.
4. Select the directory and click **Guard**.
5. In the **Policy** field, select an LDT or Standard Production policy.
6. Set **Type** to Directory (Auto Guard).
7. Click **Browse** and navigate to the folder that you just created for the AD or SQL directory.
8. Select the option: **Secure Start**.
9. Click **OK**.
10. Select the GuardPoint and click **Secure Start On**.

For details about using this feature, refer to the *VTE Installation & Configuration Guide*.

Creating GuardPoints on a Host Group

GuardPoints created on a host group are applied to all members of the group. Additionally, you can choose to apply host group configuration settings (except for password, FS Agent Lock, System Lock, Registration Allowed, and Communication Enabled settings), to all hosts that are members of that host group. It is important to keep this in mind when adding hosts to a host group. For example if you create an LDT policy in a host group, and then add a Docker enabled host to that host group, the Docker host will not be protected by that GuardPoint. Similarly, if you create a Linux file system GuardPoint in a host group, and then you add a Windows host to that host group, the Windows host will not be protected by that GuardPoint.

If you create a host group and add a host to that group that does not have LDT enabled but you create LDT GuardPoints on the host group, those GuardPoints will not be propagated to that host. However if you subsequently enable LDT on that host in that host group (assuming you have a license for this feature), the LDT GuardPoint is now propagated to the LDT enabled host.

Similarly in the case of a Docker enabled host, if you later enable Docker on a host and the host contains the same Docker image as the host group GuardPoint, then that Docker GuardPoint is propagated to the Docker enabled host.

Create a host group GuardPoint

1. Log on to the Management Console as an administrator of type Security with Host role permissions, type Domain and Security, or type All.
2. Select **Hosts > Host Groups** on the menu bar.

   The *Host Groups* page opens.
3. Click the target host in the **Host Name** column. The *Edit Host Group* window opens to the *General* tab for the selected host. The following host group is displayed:
   - **Name**: Name of the host group. This cannot be modified once the host group has been created.
   - **Description**: Optional. Enter a description for the Host Group. This file can be modified.
   - **Enable FS (VTE) Agent Communication**: Select to enable or disable interactive communications of VTE Agents installed on members of the host group.
   - **Enable Key Agent Communication**: Select to enable or disable interactive communications of key agents installed on members of the host group.
   - **System Locked**: Select to lock down the key operating system files of the hosts of members of the host group. (If this is enabled, patches to the operating system of the host will fail due to the protection of these files)
   - **FS (VTE) Agent Locked**: Select to lock down the configuration of the VTE Agent on the members of the host group. This will prevent updates to any policies on the members of the host group.
   - **System Locked**: This check box is automatically selected when VTE Agent Locked option is selected. It locks down the key operating system files of the host. If this is enabled, patches to the operating system of the host will fail.
   - **Password Creation Method**: Select the password method to use to unlock the agent. The host user may be prompted to supply a password to decrypt encrypted data when there is no

network connection between the host and the GDE Appliance. The methods are **Generate** (challenge-response) and **Manual** (static password).

When you select **Generate**, the host user must request a new password from a GDE Appliance administrator each time a host password is required. The additional field for **Generate**, **Regenerate Password**, is displayed when **Password Creation Method** is set to **Generate**. Enable this toggle to download a new randomly generated password to all hosts in the group.

When you select **Manual**, the host user must request a new password from a GDE Appliance administrator each time a host password is required. The additional fields displayed when **Password Creation Method** is set to **Manual** are; **Password**: Enter the password to apply to the hosts in the host group. The password is applied to each host in the host group and remains in effect when the hosts are removed from the host group or the host group is deleted. If you do not enter a password, the individual host password for each host in the host group remains unchanged. **Confirm Password**: Enter the same password to ensure that it had been typed correctly.

4. Select the *Guard FS* tab. This tab displays the group GuardPoints in the host group. The panel displays applied policies in a tabular format. Each policy line in the table consists of:

   - **Select**: select the GuardPoints that you want to Unguard, Enable, or Disable.
   - **Policy**: Name of the policy applied to the GuardPoint.
   - **Protected Path**: The path of the protected directory.
   - **Type**: the type of GuardPoint applied to the host group.
   - **Auto Mount**: Indicates whether or not Auto Mount is enabled for the GuardPoint. Auto Mount is not available for Docker hosts.
   - **Enabled**: Indicates whether the GuardPoint is enabled or not.
   - **Transform Sparse Regions**: Indicates whether this option is enabled or not.
   - **Secure Start**: Indicates whether this feature is enabled or not.

   You can also do any of the following from this tab:

   - **Guard**: Click to add a shared GuardPoint to all members within the host group.
   - **Unguard**: Click to remove a shared GuardPoint from all members within the host group.
   - **Enable**: Click to enable an existing disabled GuardPoint.
   - **Disable**: Click to disable an existing enabled GuardPoint.
   - **Transform Sparse Regions**: If you selected this option while creating a GuardPoint, it means that sparse file regions will be transformed. Once selected, this option cannot be disabled. If you did not select this option while creating a GuardPoint, sparse regions will not be transformed. You have one opportunity to disable this option from the Guard FS tab. Once you change the setting, you cannot roll it back. It is a one-time change.
   - **Secure Start On**: Click to enable this feature on a GuardPoint. You must first select the GuardPoint and then click Secure Start On.

- **Secure Start Off**: Click to disable this feature on a GuardPoint. You must first select the GuardPoint and then click Secure Start Off.

5. Click **Guard** to add a shared GuardPoint to all members within the host group.

   The *Guard Host Group File System* page displays.

6. Select a host in the **Host to Browse** field to apply the GuardPoint. It is important to note that for this GuardPoint to be applicable to all hosts in the host group, they must all have the same file system type as the host selected here.

7. Select the type of policy to apply from the **Policy** drop-down menu. All available policies are listed here, you must ensure that you select a policy that is applicable to the file system on the selected host, as there is no restriction on the type of hosts that can be added to a host group.

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

   UNIX choices are Directory (Auto Guard), Directory (Manual Guard), Raw or Block Device (Auto Guard), or Raw or Block Device (Manual Guard).

   NOTE: Information about UNIX agents applies to earlier versions of those agents, since as of v6.0, UNIX agents are EOL.

   Windows choices are Directory (Auto Guard) or Raw or Block Device (Auto Guard).[10557, 10521, 10948] Select Directory (Auto Guard) or Directory (Manual Guard) for file system directories.

   - Select Raw or Block Device (Auto Guard) or Raw or Block Device (Manual Guard) for raw or block devices.
   - Select Directory (Manual Guard) for file system directories that are to be manually guarded and unguarded in order to failover to a different node in a cluster.
   - Select Raw or Block Device (Manual Guard) for raw devices that are to be manually guarded and unguarded in order to failover to a different node in a cluster.
   - Directory (Manual Guard) and Raw or Block Device (Manual Guard) are guarded and unguarded (for example, mounted and unmounted) using the secfsd -guard and secfsd -unguard commands. Do not use the mount and umount commands to swap GuardPoint nodes in a cluster configuration.

9. In the **Path** text box, you can any of the following:

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

- Click **Browse** to locate and select entire paths. Use the browser to locate the target GuardPoint, to avoid typographical errors, and to verify host availability.
- If multiple paths are entered, they will all be protected by the same policy.
- Click the **Browse** button to locate the host directory to guard. The Remote File Browser opens.

See, "Creating GuardPoints on a Host" for more information about these options for browsing for file locations.

10. If applicable, select the check box to indicate that the GuardPoint is a Windows network drive or a UNIX auto mount by enabling the Network Drive or Auto Mount toggle.

    The Auto Mount check box disappears when Directory (Manual Guard) or Raw or Block Device (Manual Guard) is selected because only regular mounts are supported by these types.

NOTE: The Auto Mount option is also disabled for GuardPoints on Docker hosts.

Information about UNIX agents applies to earlier versions of those agents, since as of v6.0, UNIX agents are EOL.

11. Click Ok to create the GuardPoint and go back to the Edit Host Group page. The new GuardPoint will be listed in the table.

Creating LDT GuardPoints on a host group

The steps to create a an host group LDT GuardPoint are the same as for a creating a host group GuardPoint except that you must select an LDT policy to apply to the GuardPoint.

To create an LDT GuardPoint on a host group:

1. Create an LDT policy.
2. Set the Quality of Service, see "LDT Quality of Service".
3. Click **Guard** on the Guard FS tab to apply an LDT policy to a directory or file and create a GuardPoint. See "Creating GuardPoints on a Host Group" for procedures.

See the *Live Data Transformation Guide* for more information about LDT policies, QoS schedules, and LDT GuardPoints. See "Creating and Configuring VTE Policies" for procedures to create LDT policies.

Creating Docker GuardPoints on a host group

The steps to create a an host group LDT GuardPoint are the same as for a creating a host group GuardPoint except that select the Guard Docker tab and select a Docker host on which to apply the GuardPoint. When you a create a GuardPoint on a Docker image, for a Docker image-based

GuardPoint to apply to all the Docker hosts in a Docker host group, that same Docker image must also be available on all the Docker hosts.

To create a Docker GuardPoint on a host group:

1. Create a policy.
2. Click Guard on the Guard Docker tab to apply a policy to a Docker image or container. See "Creating GuardPoints on a Host Group" and for Docker specific information see, "Creating Docker GuardPoints".

Automatic and Manual GuardPoints

NOTE: Manual GuardPoints can be applied to UNIX platforms only.

Information about UNIX agents applies to earlier versions of those agents, since as of v6.0, UNIX agents are EOL.

A GuardPoint is usually applied immediately after it is configured in the Management Console; however, it can be applied later on the host system.

When would you want to apply the GuardPoint later? Consider the case of a 2-node cluster configured as active/passive in a cluster environment, such VCS, HACMP, or MSCS. There are two nodes, one which is currently active and the other that is currently inactive. Both nodes are locked. Apply GuardPoint protection to active nodes only. You should never apply a GuardPoint to a passive node. If the active node develops a problem and tries to switch over to the inactive node, the cluster process will fail to switch over because the mirror directory on the inactive node is currently mounted on the active node. The solution is for the cluster process to unmount (for example, unguard) the currently active node, place it in an inactive state, place the old inactive node in an active state, and then mount (for example, guard) the mirror directory on the newly active node.

Generally, when you get error messages, check that only active nodes are properly guarded.

Automatic and manual GuardPoint application is set in the *Edit Host* window, *Guard File System* sub-window.

The GuardPoint type is usually set to `Directory (Auto Guard)` for file-system based directories and to `Raw or Block Device (Auto Guard)` when applying GuardPoint protection to raw or block devices. When an auto GuardPoint is applied, regardless if it is a file system directory or a raw device, the change is pushed to the host system, and the GuardPoint is applied immediately.

Use the df command to display secfs mounts (for example, GuardPoints) or secfsd to display the GuardPoints themselves. The secfsd output shows a guard type of local for directories configured with Directory (Auto Guard).

For example:

```
# df
Filesystem           1K-blocks      Used Available Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
                      40123784  11352236  26733380  30% /
/dev/sda1               101086     14590     81277  16% /boot
none                    254492         0    254492   0% /dev/shm
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec
                      40123784  11352236  26733380  30%
/opt/vormetric/DataSecurityExpert/agent/secfs/.sec
/opt/apps/apps1/tmp   40123784  11352236  26733380  30% /opt/apps/apps1/tmp
/opt/apps/apps1/lib   40123784  11352236  26733380  30% /opt/apps/apps1/lib
/opt/apps/apps1/doc   40123784  11352236  26733380  30% /opt/apps/apps1/doc


# secfsd -status guard
GuardPoint           Policy                    Type    ConfigState  Status
Reason
----------          ------                   ----    --------    ------     ---
/opt/apps/apps1/tmp  allowAllOps_fs           local   guarded     guarded    N/A
/opt/apps/apps1/lib  allowAllRootUsers_fs     local   guarded     guarded    N/A
/opt/apps/apps1/doc  allowAllOps-winusers1_fs local   guarded     guarded
N/A
#
```

When a manual GuardPoint is applied, regardless if it is a file system directory or a raw device, the change is pushed to the host system only. The host is aware of the GuardPoint but the host does not mount it. This is indicated in the Type column of the “secfsd -status guard” output. For example, the GuardPoint /opt/apps/apps2/bin has been configured with Directory (Manual Guard) so the guard type is set to “manual”.

```
# secfsd -status guard
GuardPoint           Policy                    Type    ConfigState  Status
Reason
----------          ------                   ----    --------    ------     ---
/opt/apps/apps1/tmp  allowAllOps_fs           local   guarded     guarded    N/A
/opt/apps/apps1/lib  allowAllRootUsers_fs     local   guarded     guarded    N/A
```

```
/opt/apps/apps1/doc  allowAllOps-winusers1_fs local   guarded    guarded
N/A
/opt/apps/apps2/bin  HR_policy01              manual  unguarded  not guarded
Inactive
#
```

Note the Type value. A Type of manual indicates a manual GuardPoint. A Type of local indicates an automatic GuardPoint.

A manually applied GuardPoint retains a yellow triangle status (Pending) until the GuardPoint is applied on the host. After the GuardPoint is applied on the host, and the host communicates the change to the server, the status changes to a green ball (Normal). It returns to the yellow triangle when the GuardPoint is manually unguarded.

Use the secfsd command to guard and unguard Directory (Manual Guard) and Raw or Block Device (Manual Guard) GuardPoints. The secfsd syntax is:

```
secfsd -guard path
secfsd -unguard path
```

NOTE: In zone-based VTE Agent deployments, such as Solaris Zones, always specify paths relative to the global zone, never the local zone. Also, you must guard and unguard manual GuardPoints in the global zone.

For example, to manually guard and unguard a file system directory:

1. Configure a GuardPoint with the type Directory (Manual Guard).
2. The host administrator with root permissions must log on to the agent system as a root user.
3. Wait until the configuration change is downloaded to the agent system.

   The status command is run until the manual GuardPoint displays.

   For example:

```
# secfsd -status guard
GuardPoint        Policy          Type   ConfigState  Status    Reason
----------        ------          ----   -----------  ------    ------
/opt/apps/etc     allowAllOps_fs  manual unguarded    not guarded N/A
/opt/apps/lib/dx3 allowAllOps_fs  local  guarded      guarded     N/A
#
```

4. Enable the GuardPoint.

```
# secfsd -guard /opt/apps/apps2/bin
  secfsd: Guard initiated
#
```

The GuardPoint is active and the policy is enforced.

5. Disable the GuardPoint.

```
# secfsd -unguard /opt/apps/apps2/bin
  secfsd: Unguard initiated
#
```

Selecting a GuardPoint mount type

- Under random circumstances, NFS file systems can be mounted before the VTE Agent drivers are loaded. When this occurs, the VTE Agent is unable to protect GuardPoints on the file system. The **Auto Mount** feature prevents this from occurring. Select the **Auto Mount** toggle in the *Edit Host* window when the GuardPoint is in an automounted file system.
- When applying file system protection to an automounted file system, do not apply the GuardPoint to the link-target directory. Rather, apply the GuardPoint to the full path to the directory underneath it. For example, if the automounted directory "`/Auto`" mounts a link-target directory named "`/documents`", do not set the GuardPoint to "`/documents`". Instead, set the GuardPoint to "`/Auto/documents`".
- Do not configure Linux 64-bit hosts to automount directories with the "`/net`" option. The automounter uses the automount map associated with each mount point to locate each file system as it is accessed. The VTE Agent cannot resolve file system selections for GuardPoints, including any directories below a GuardPoint, that are configured with the "`/net`" option.

Displaying VTE Agent GuardPoint Status

The VTE Agent GuardPoint status can be displayed on the GDE Appliance and on the host running the VTE Agent. The agent status displayed in the Management Console shows the status as it is configured on the GDE Appliance. It is not a real-time indication of the actual status.

For actual status, the host administrator with root permissions must log on to the agent system and run VTE Agent utilities. Compare the two to ensure that the GuardPoint status on the GDE Appliance and Encryption Agent match. If the two do not match, go with what you see on the host (agent) system.

Viewing VTE Agent GuardPoint status

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions or type All.

2. Select **Hosts > Hosts** in the menu bar.

   The *Hosts* window opens.

3. Click the host in the **Host Name** column.

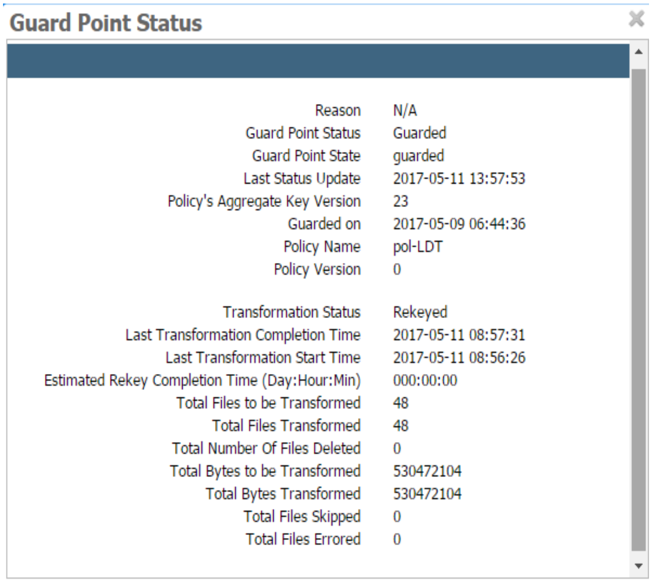
   The *Edit Host* window opens to the *General* tab.

4. Click *Guard FS* tab to view GuardPoints on the host. Click the status indicator of a GuardPoint.

   The status indicator is a green circle, a yellow triangle, or a red square in the **Status** column.

   The *GuardPoint Status* pop-up displays.

Figure 5: GuardPoint Status summary



Guard Point Status

Reason	N/A
Guard Point Status	Guarded
Guard Point State	guarded
Last Status Update	2017-05-11 13:57:53
Policy's Aggregate Key Version	23
Guarded on	2017-05-09 06:44:36
Policy Name	pol-LDT
Policy Version	0
Transformation Status	Rekeyed
Last Transformation Completion Time	2017-05-11 08:57:31
Last Transformation Start Time	2017-05-11 08:56:26
Estimated Rekey Completion Time (Day:Hour:Min)	000:00:00
Total Files to be Transformed	48
Total Files Transformed	48
Total Number Of Files Deleted	0
Total Bytes to be Transformed	530472104
Total Bytes Transformed	530472104
Total Files Skipped	0
Total Files Errored	0

   Do not click a GuardPoint with a red square status indicator. The *Guard Point Status* window will not display any configuration or status data when a red square is displayed.

   The window is not automatically updated. You must close and reopen the window after the GDE Appliance and VTE Agent synchronize and the status indicator turns green.

5. Click the “**X**” on the *Guard Point Status* window to close it.

Viewing Docker GuardPoint Status

To view Docker GuardPoint status information:

1. Log on to the Management Console as an administrator of type Security Administrator with `Host` role permissions or type All.

2. Select **Hosts > Hosts** in the menu bar.

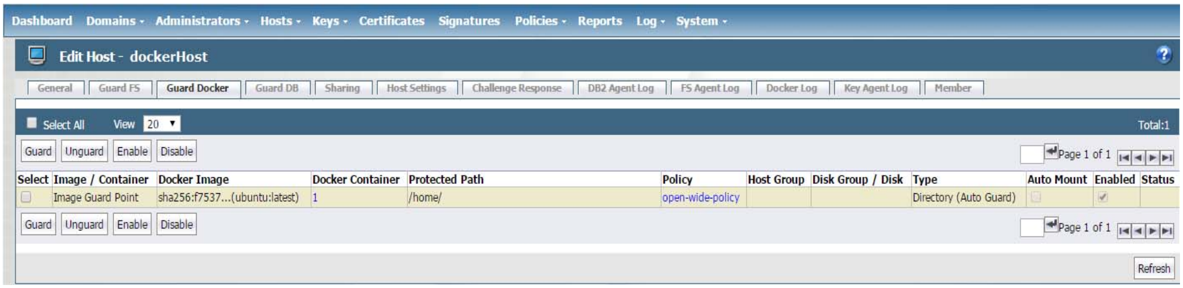
The *Hosts* window opens.

3. Click the host in the **Host Name** column.

   The *Edit Host* window opens to the *General* tab.

4. Click *Guard Docker* tab to view GuardPoints on a Docker host.

Figure 6: Docker GuardPoints

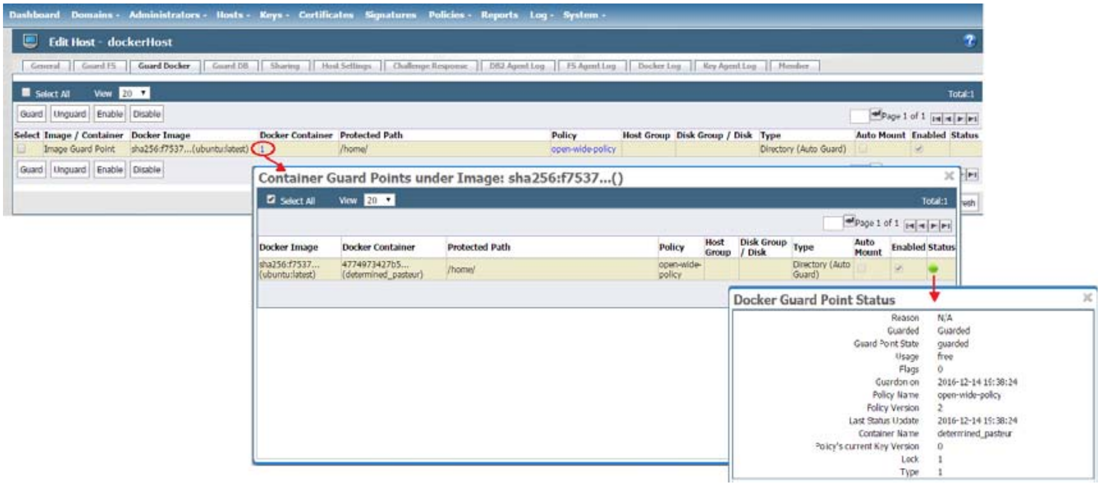


Select	Image / Container	Docker Image	Docker Container	Protected Path	Policy	Host Group	Disk Group / Disk	Type	Auto Mount	Enabled	Status
□	Image Guard Point	sha256:f7537...(ubuntu:latest)	1	/home/	open-wide-policy			Directory (Auto Guard)	□	✓	

A Docker image-based GuardPoint does not display any information in the **Status** column of the table. However, if there are containers running off that image, then the image-based GuardPoint applies to those containers and the **Docker Container** column displays the number of containers that are running.

5. Click the number in the **Docker Container** column, a pop-up dialog displays the Docker container GuardPoints. Click the status indicator in the **Status** column to view Docker GuardPoint Status.

Figure 7: Docker GuardPoint Status



Select	Image / Container	Docker Image	Docker Container	Protected Path	Policy	Host Group	Disk Group / Disk	Type	Auto Mount	Enabled	Status
□	Image Guard Point	sha256:f7537...(ubuntu:latest)	1	/home/	open-wide-policy			Directory (Auto Guard)	□	✓	

Container Guard Points under Image: sha256:f7537...()

Docker Image	Docker Container	Protected Path	Policy	Host Group	Disk Group / Disk	Type	Auto Mount	Enabled	Status
sha256:f7537... (ubuntu:latest)	4774973427b5... (determined_pasteur)	/home/	open-wide-policy			Directory (Auto Guard)	□	✓	●

Docker Guard Point Status

Reason	N/A
Guarded	Guarded
Guard Point State	guarded
Usage	free
Flags	0
Guardon on	2016-12-14 15:38:24
Policy Name	open-wide-policy
Policy Version	2
Last Status Update	2016-12-14 15:38:24
Container Name	determined_pasteur
Policy's current Key Version	0
Lock	1
Type	1

If there are no containers running off the Docker image, the **Docker Container** column displays ‘0’ and no pop-up is available.

Configuring Windows Network Drives

Windows network drives may need user credentials and domain information for the GDE Appliance to configure GuardPoints and to push configuration changes to the VTE Agent. The *Remote File Browser* window enables you to automatically supply the user credentials.

Guard network mapped drives on a Windows host using the complete Universal Naming Convention (UNC) name for each file path. For example:

- `\\1.2.3.4\ShareName\dirpath`
- `\\ServerName.DomainName.com\ShareName\dirpath`
- `\\ServerName\ShareName\dirpath`

We recommend that you use the GDE Appliance IP address instead of the DNS name. GuaardPoint protection is still enforced even when the GDE Appliance name is used.

NOTE: The **Auto Mount** check box is displayed but not selectable for Windows platforms. Auto Mount is for UNIX platforms only.

To configure a network drive:

1. Open *Guard File System* window.
2. Click **Browse**.

   The *Remote File Browser* window opens.
3. Enable **Network Drive**.

   Three text-entry boxes are displayed. They are **Username**, **Password**, and **Windows Domain**.
4. Enter the network name of the user who has access permission to the network drive in the **Username** text-entry box.
5. Enter the password for the specified user in the **Password** text-entry box.
6. Enter the domain name of the system hosting the network drive in the **Windows Domain** text-entry box.
7. Select the GuardPoint and apply the policy as you would a non-network resource.

Deleting GuardPoints

The following preliminary steps need to be taken before deleting a GuardPoint:

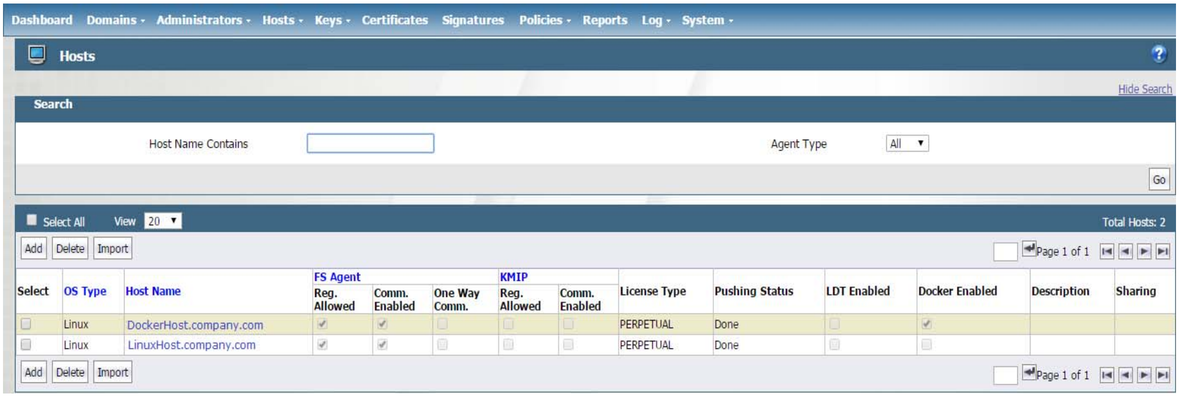
- Encrypted data in a GuardPoint will still be encrypted when the GuardPoint is removed. If you are not going to reuse the GuardPoint for any reason, such as uninstalling the VTE Agent software from a host, either copy the encrypted files out of the GuardPoint so that they are saved as unencrypted files or rekey the encrypted files while the GuardPoint is still applied.

- If the GuardPoint is an LDT GuardPoint, make sure you run through the procedures described in the *Live Data Transformation Guide* to ensure that the data in those GuardPoints remains available.
- Take the GuardPoint out of service so that no user or application is accessing the directories and files in the GuardPoint. A GuardPoint is a mounted file system. Removing a GuardPoint involves unmounting the file system. File systems cannot be unmounted when in use.
- Delete all the GuardPoints and disable the locks for a host before deleting the host from the GDE Appliance. This ensures that there are no residual GuardPoints in effect on the host.

1. Log on to the Management Console as an administrator of type Security with `Host` role permissions, type Domain and Security, or type All.
2. Select **Hosts > Hosts** in the menu bar.

   The *Hosts* window opens (Figure 8).

Figure 8: *Hosts* window



Host Name Contains

Agent Type: All

View: 20

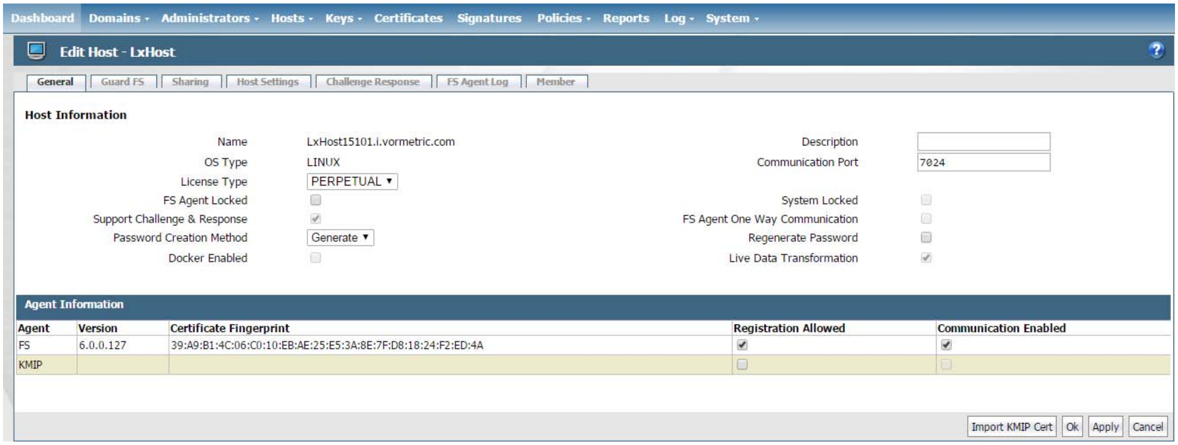
Total Hosts: 2

Select	OS Type	Host Name	FS Agent Reg. Allowed	FS Agent Comm. Enabled	FS Agent One Way Comm.	KMIP Reg. Allowed	KMIP Comm. Enabled	License Type	Pushing Status	LDT Enabled	Docker Enabled	Description	Sharing
□	Linux	DockerHost.company.com	☑	☑	□	□	□	PERPETUAL	Done	□	☑		
□	Linux	LinuxHost.company.com	☑	☑	□	□	□	PERPETUAL	Done	□	□		

3. Select a host in the **Host Name** column of the *Hosts* page.

   The *Edit Host* page opens (Figure).

Figure 9: *Edit Host* window



Host Information

Name	LxHost15101.i.vormetric.com	Description	
OS Type	LINUX	Communication Port	7024
License Type	PERPETUAL ▾		
FS Agent Locked	□	System Locked	□
Support Challenge & Response	☑	FS Agent One Way Communication	□
Password Creation Method	Generate ▾	Regenerate Password	□
Docker Enabled	□	Live Data Transformation	☑

Agent Information

Agent	Version	Certificate Fingerprint	Registration Allowed	Communication Enabled
FS	6.0.0.127	39:A9:B1:4C:06:C0:10:EB:AE:25:E5:3A:8E:7F:D8:18:24:F2:ED:4A	☑	☑
KMIP			□	□

4. Select the *Guard FS* tab.

   The GuardPoints are displayed.

5. Select the radio button in the **Select** column for the GuardPoint to be deleted.

   Only one GuardPoint at a time can be selected at a time.

6. Click **Unguard**.

7. Note the GuardPoint status:

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

8. Click **Refresh** to update the tab.

   After the VTE Agent acknowledges that the GuardPoint has been removed from the host, it is removed from the Management Console **Guard FS** tab.

9. Check the mount points on the VTE Agent host to ensure that the GuardPoint has been removed.

   On UNIX, you can run the `df` command or the `secfsd -status guard` command. On Windows, you can select the Vormetric icon and **View > File System > Guardpoints**.

Security Administrator Preferences & Logs

23

Viewing Preferences

Although most preferences for viewing the various windows and panels on the GDE Appliance Management Console are set by the GDE Appliance System Administrator, as a GDE Appliance Security Administrator you can still set certain viewing preferences within the domains you are authorized to access. From the **System > General Preference** window, you can set parameters for the following pages:

- Domain Page
- Administrator Page
- Host Page
- Policy Page
- Key/Certificate Page
- Signature Page
- Log Page

You can also set the Management Console Timeout limit for your sessions.

From the **System > Log Preferences** window, you can set the following parameters for:

- Server
  - Logging Settings such as Logging Level (DEBUG, INFO, WARN, ERROR, FATAL)
    - Log Upload DB Retry (secs)
    - Log Buffer Size (messages)
    - Log Buffer Flush Time (secs)
  - Communication Settings
    - Update Host Frequency (secs)
    - Default Host Communication Port
- Agent Logs—the available tabs will depend on the agents for which you have a licenses installed.

NOTE: We recommend turning on **Log to File** or **Log to Syslog** instead of **Upload to Server** for INFO and DEBUG levels. For general day-to-day operation, we recommend enabling and setting only ERROR Level (so that only ERROR, WARNING, and FATAL log entries are received). Setting Upload to Server to INFO or DEBUG level for policy evaluation can affect GDE Appliance performance.

Viewing Logs

The entries displayed in the Message Log depend on the GDE Appliance administrator type (System, Domain, Security, All), the domain in which the administrator is working, and, for Security Administrators, the administrator role (Audit, Key, Policy, Host, Challenge & Response, Client Identity).

Security Administrators can see log entries for the management of Security Administrators by Domain Administrator, GuardPoint application, and policy evaluation.

Log entries are displayed in the Management Console based on the current administrator type and the domain in which the administrator is working. The combined list of this log information is available in the `server.log` file on the GDE Appliance.

Part IV:GDE Appliance CLI Administrators

CLI administrators are system users with login accounts. That is, they are entered in `/etc/passwd` and they have directories under `/home`. CLI administrators do the tasks to set up and operate the GDE Appliance installation and any tasks that need to be done from the CLI. GDE Appliance administrators exist only on the GDE Appliance and access only the Management Console.

Table 1: Differences between CLI administrators and Management Console administrators

GDE Appliance CLI Administrators	GDE Appliance Administrators
CLI administrators are created and administered in the CLI only .	GDE Appliance administrators are created and administered in the GDE Appliance Management Console only.
CLI administrators cannot log on to the GDE Appliance Management Console.	GDE Appliance administrators cannot log on to the CLI.
CLI administrators are not included in the backup.	Only GDE Appliance administrators are included in a GDE Appliance backup.
The CLI administrator exists only on the appliance or system on which they were created.	Only GDE Appliance administrators are propagated to failover GDE Appliances. A GDE Appliance administrator can open a Web browser session on both the primary and failovers using the same password.

The password requirements for both CLI and GDE Appliance administrators are set by the password policy in the Management Console.

GDE Appliance Command Line Interface

24

The GDE Appliance Command Line Interface (CLI) enables you to configure the GDE Appliance (represented in the code as a Security Server) network and do other system-level tasks.

Procedures for the GDE Appliance are divided between the Management Console and the CLI. This is usually because the procedures require a mix of network, GDE Appliance database, or system access, such as for GDE Appliance upgrades. The Management Console Web interface (GUI) is used to upload GDE Appliance application upgrade images and GDE Appliance OS upgrade images, because the GDE Appliance CLI does not support file uploading.

The Management Console cannot be used to restart the GDE Appliance and the CLI cannot be used to download files across the net.

A mixture of GDE Appliance CLI and Management Console activities is required for some procedures to reduce the potential for software hacks or other misuse.

This chapter consists of the following sections:

- "Overview"
- "GDE Appliance CLI Navigation"
- "Network Category Commands"
- "System Category Commands"
- "HSM Category Commands"
- "Maintenance Category Commands"
- "High Availability Category Commands"
- "User Category Commands"

Overview

CLI administrators are system users with login accounts. That is, they are entered in `/etc/passwd` and they have directories under `/home`. CLI administrators do the tasks to set up and operate the GDE Appliance installation and any tasks that need to be done from the CLI. GDE Appliance administrators only access the Management Console.

Table 2: Differences between CLI administrators and Management Console administrators

GDE Appliance CLI Administrators	Management Console Administrators
CLI administrators are created and administered in the CLI only.	Administrators are created and administered in the Management Console only.
CLI administrators cannot log on to the GDE Appliance Management Console.	Management Console administrators cannot log on to the CLI.
CLI administrators are not included in the backup.	Included in a GDE Appliance backup.
The CLI administrator exists only on the appliance or system on which they were created.	Only GDE Appliance administrators are propagated to failover GDE Appliances. A GDE Appliance administrator can open a Web browser session on both the primary and failovers using the same password.

The password requirements for both CLI and Management Console administrators are set by the password policy in the Management Console.

GDE Appliance CLI Navigation

These are the CLI command categories:

- `network`
- `system`
- `maintenance`
- HA (High Availability)
- `user`

As a GDE Appliance CLI administrator, log on to the CLI, then enter a command category by typing the category name at the command line prompt. For example, type `system` to enter the `system` category. While in the category, you can execute the commands for that category.

Enter the entire category name, command, or argument, or enter just enough characters to uniquely identify the category, command, or argument. For example, both of these commands achieve the same result:

```
ip address add 10.3.5.100/16 dev eth1
```

```
i a a 10.3.5.100/16 d eth1
```

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

For example:

At the top level, enter `m` and press <Tab>, the CLI expands it to `maintenance`.

Inside the `maintenance` category, you can enter `di`<Tab> and it expands to `diag`. Type `d`<Tab> and it expands to `diskusage`. Note that you must enter `di` because there are other `d` commands in the maintenance category, like `date` and `delver`.

Other supported CLI navigation methods are:

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

Network Category Commands

The `network` category is used to set, modify or delete IP addresses on the system, and set up DNS servers. DHCP is supported and is enabled by default on a fresh installation. DHCP must be enabled on an upgraded appliance.

The `network` category supports the following commands:

Table 3: Network category commands

`ip`	Configures the network interface.
`dns`	Sets one or more DNS servers for the appliance.
`host`	Configures an IP address to a host name.
`ssh`	Enables Secure Shell (SSH) port
`ping`	Pings an IP address, host name, or FQDN.
`traceroute`	Traces route to IP address or host name.
`rping`	Sends an ARP (Address Resolution Protocol) request to a neighbor host.
`arp`	Displays the system ARP cache.
`checkport`	Checks local and remote TCP port status.
`nslookup`	Queries DNS to domain name to IP address mapping.

ip

The `ip` command configures the network interface.

It includes the following elements:

Table 4: Network category `ip` command elements

`address`	Adds, deletes, or initializes the IP address a network interface.
`diag`	TCP/IP interface configuration and routing utility.
`link`	Sets the physical components of the network interface, such as connection speed, mode, set bond mode for bonded NICs, and MTU.
`route`	Configures network routing.
`dhcp`	Manages Dynamic Host Configuration Protocol (DHCP) settings.

ip address

Use the `ip address` command to add, initialize (set to default), delete, or show different addresses on the interface, or to assign an IP address to a bonded NIC. The GDE Appliance also supports IPv6 addresses, examples are included below.

Syntax

```
ip address {init|add|delete} ip_address dev {eth0|eth1|bond0}
[label {diag|this}]

ip address {show|flush} {eth0|eth1|bond0} [label {diag|this}]
```

The `ip address` command takes the following arguments:

Table 5: Network category `ip address` command

`init`	Sets the system interfaces to the original settings from manufacturing.
`add`	Adds an IP address to the specified interface.
`delete`	Deletes an IP address from an interface.
`show`	Displays the current addresses on the interfaces.
`flush`	Removes the IP addresses on the specified interface.

Example 1

The following example assigns an IP address to the bonded NIC interface, bond0:

```
0000: dsm$ network
0001:network$ 0001:network$ ip address init 1.2.3.4/16 dev bond0
```

for IPv6:

```
0001:network$ 0001:network$ ip address init fa01::3:15:130/64 dev bond0
```

Example 2

The following example changes the current `eth0` IP address:

```
0001:vormetric1000$ network

0002:network$ ip address init 1.2.3.4/16 dev eth0
```

for IPv6

```
0002:network$ ip address init fa01::3:15:130/64 dev eth0
```

Example 3

The following example deletes the IP address for the `eth1` network interface and assigns the IP address to `bond0`:

```
0003:network$ ip address delete 1.2.34/16 dev eth1 label diag

WARNING: Changing network ip address requires server software to
be restarted.

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

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

0004:network$ ip address show

   Device           Prefix     Broadcast        Label

   eth0    192.168.10.1/16       192.168.255.255 diag

   Show ip address SUCCESS

0005:network$ ip address add 1.2.3.4/16 dev bond0 label diag

WARNING: Changing network ip address requires server software to
be restarted.

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

SUCCESS: add ip address. Please restart server software to pick
up the changes.
```

To view the IP address changes, use the `show` command:

```
0006:network$ ip address show

   Device Prefix      Broadcast        Label

   eth0 192.168.10.1/16 192.168.255.255     diag

   bond0 1.2.3.4/16        1.2.255.255     diag

   Show ip address SUCCESS
```

ip diag

The `ip diag` command is the equivalent of running the Linux `ip` command. Check the IP man-pages on a Linux system for details.

Syntax

```
ip diag ipcommand
```

Example

```
0050:network$ ip diag -V
ip utility, iproute2-ss061002
ip diag SUCCESS
0051:network$ ip diag maddr show
1:      lo
        inet  224.0.0.1
        inet6 ff02::1
2:      eth0
        link  33:33:00:00:00:fb
        link  01:00:5e:00:00:fb
        link  01:00:5e:00:00:01
        link  33:33:ff:60:f9:3e
        link  33:33:00:00:00:01
        inet  224.0.0.251
        inet  224.0.0.1
        inet6 ff02::fb
        inet6 ff02::1:ff60:f93e
        inet6 ff02::1
ip diag SUCCESS
0052:network$
```

ip link

The `ip link` command establishes how the various interfaces connect to the other nodes in the network. The `ip link` command is used to specify the bandwidth of the `eth0` and `eth1` interfaces and sets the Maximum Transmission Unit (MTU). It is also used to set the mode for the bonded NIC interface `bond0`. See the *Installation & Configuration Guide* for more information about bonded NICs. See below for the different modes that can be set for the `bond0` interface.

Syntax

```
ip link set (eth0|eth1|bond0) [mtu {100..1500}] [{up|down}]
[mode {0..6}]|[speed
{auto|10mb_half|10mb_full|100mb_half|100mb_full|1000mb_half|100
0mb_full}]
```

```
ip link show [eth0|eth1|bond0]
```

NOTE: When an IPv6 configured GDE Appliance Ethernet interface link is brought down using the command,
`ip link set {eth0|eth1|bond0} down`
the IPv6 address is lost. You will need to reconfigure the IPv6 address for that Ethernet interface when you bring it back up

The `ip link` command can take the following arguments:

Table 6: Network category `ip link` command arguments

`eth0`	Network interface card 1.
`eth1`	Network interface card 2.
`bond0`	Bonded NIC device type interface.
`mtu`	Sets the Maximum Transmission Unit value. The default MTU is 1500.
`set`	Enables the parameter settings below for the ip link command.
`show`	Displays information about the IP link connections.
`speed`	Sets the link speed of the interface.

NOTE: Use auto detect to set the data rate of all interfaces and set the MTU value to the default, 1500.

Table 7: 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

Mode	Name	Description	Load-balancing	Fault tolerance
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

Example 1

The following example configures the `eth1` interface to operate at 100 Mb/s, in full-duplex mode, and then activates the interface so that it is network accessible:

```
0002:network$ ip link set eth1 speed 100mb_full

ip link speed SUCCESS

0003:
```

Example 2

The following example sets the `bond0` interface mode to mode 2:

```
0003:network$ ip link set bond0 mode 2
```

ip link show

The `ip link show` command displays the physical link settings on the system. Also use it to verify any changes made to the physical link settings:

```
0003:network$ ip link show


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
0004:network$
```

ip route

Use the `ip route` command to set up IP routes. If the `eth01` and `eth1` interfaces are set on the same subnet, you do not have to include a netmask. If they are on separate subnets, include the netmask for the other subnet.

NOTE: Configure a default route connection outside of the subnet.

The `ip route` command uses the following arguments:

Table 8: Network category `ip route` command arguments

`add`	Adds a static route.
`delete`	Deletes a static route.
`get`	Shows information for a specific route.
`replace`	Changes the table, gateway and/or source of an existing IP route.
`show`	Displays all the currently configured route

Syntax

```
ip roudd|delete|replace} [ip|default]
table main.table [dev {eth0|eth1|bond0} | via {ip}] src ip

ip route get ip

ip route show
```

Example 1

The following example adds a gateway to the `eth1` interface, which has 1.2.3.4 as it’s IP address and then displays the results:

```
0044:network$ ip route add default table main.table dev eth1 via
1.2.6.7
```

NOTE: Ignore the separation of routes into unique tables. All routes are considered members of the main routing table, as reflected in the Management Console. Separate routing tables have been deprecated.

```
ip route SUCCESS

0045:network$ ip route get 1.2.3.4

local 1.2.3.4 dev lo src 1.2.3.4

cache <local>

ip route SUCCESS

0046:network$
```

A default route specifies the gateway to which IP packets are sent when the local routing table is unable to resolve a destination. Always configure a default route. The following example configures a default route on the `eth0` interface:

```
ip route add default table main.table dev eth1 via 1.2.6.7
```

The default interface is `eth0`.

Example 2

The following example adds a default gateway to the bond0 interface:

```
0005:network$ ip route add default table main.table dev bond0
via 1.2.6.7
```

Example 3

The `ip route show` command displays the IP routes that have been assigned to the system. Use the `ip route show` command to verify the changes you made to the IP route tables:

```
0020:network$ ip route show

Main routing table

1.2.0.0/16 dev eth1 proto kernel scope link src 1.2.3.4

192.168.0.0/16 dev eth0 proto kernel scope link src 192.168.10.1

ip route show SUCCESS
```

The following example displays the IP routes that have been assigned with the bond0 interface configured:

```
0000:dsm$ network

0001:network$ ip route show


Main routing table

default via 1.2.6.7 dev bond0

1.2.0.0/16 dev bond0 proto kernel scope link src 1.2.3.4

6.2.0.0/16 dev bond0 scope link metric 1004

6.2.0.0/16 dev bond0 scope link metric 1005

192.168.0.0/16 dev eth0 proto kernel scope link src 192.168.10.1


ip route show SUCCESS

0002:network$
```

ip dhcp

Use the `ip dhcp` command to manage DHCP settings. Note that when DHCP addressing is released, all network configuration is removed, you will have to reconfigure the gateway and DNS information. The current GDE Appliance DHCP implementation does not support IPv6 addresses.

Syntax

```
ip dhcp {enable|release|renew|show} {eth0|eth1|bond0} version
{4|6}
```

Table 9: Network category ip dhcp command arguments

`enable`	Enables DHCP IP address leasing for a specified interface.
`release`	Releases DHCP IP address leasing for a specified interface.
`renew`	Renews DHCP IP address leasing for a specified interface.
`show`	Displays DHCP IP address leasing status for all interfaces, there are no additional parameters for this command.

Example 1

The following example enables DHCP on the `bond0` interface for an IPv4 address:

```
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$
```

Example 2

The following example releases DHCP IP address leasing for the `eth0` interface for an IPv4 address:

```
0000:dsm$ 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$
```

Example 3

The following example renews DHCP IP leasing for the `eth0` interface:

```
0008:network$ ip dhcp renew 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.
```

Example 4

The following example displays the DHCP IP leasing status for all interfaces. In this example, the `bond0` interface has been enabled so the 'Active' column and the `eth0` and `eth1` interfaces are not in use.

```
0000:dsm$ network

0001:network$ ip dhcp show


Device Active? DCHP? DHCP Addr DHCPv6? DHCPv6 Addr

------ ------- ----- --------- ------- -------------

eth0

eth1

bond0     Y       Y 1.3.2.4/16

SUCCESS

0004:network$
```

dns

The DNS command sets the DNS domain servers that the GDE Appliance will use for primary-to-failover and GDE Appliance-to-VTE Agent communication. This is equivalent to editing the `/etc/resolv.conf` file.

Syntax

```
dns [search domainname] [dns1 ip] [dns2 ip] [dns3 ip][clear][show]
```

The `dns` command includes the following elements:

Table 10: Network category `dns` elements

`clear`	Removes all the DNS settings.

`dns1`	Specifies settings for domain server 1.
`dns2`	Specifies settings for domain server 2.
`dns3`	Specifies settings for domain server 3.
`search`	Sets the domain server name.
`domainname`	The name of the domain server.
`ip`	The IP address for the specified domain server.
`show`	Show all the currently configured Domain Name Servers.

You can configure just the DNS server name, just the DNS server IP addresses, or both the DNS server name and IP addresses.

Example

The following example sets the domain to i.`vormetric.com` and the `dns1` lookup IP address to `192.168.2.254`.

```
0027:network$ dns search i.vormetric.com dns1 192.168.2.254
DNS SUCCESS
0028:network$ dns show
search i.vormetric.com
nameserver 192.168.2.254
DNS show SUCCESS
0029:network$
```

To remove all the DNS settings use the `dns clear` command:

```
0004:network$ dns clear
dns SUCCESS
```

host

The `host` GDE Appliance CLI command is used to add and remove static IP addresses to and from the `/etc/hosts` file of an appliance-based GDE Appliance. By default, only hosts with resolvable host names or FQDNs can be configured in the GDE Appliance database. The `host` GDE Appliance CLI command allows the GDE Appliance to communicate with other GDE Appliances and hosts without using DNS.

This feature is provided on appliance-based GDE Appliances only. Administrators on appliance-based GDE Appliances cannot edit system files directly. Administrators on software-only GDE Appliances can edit system files directly and so do not need this feature.

The name of a host in the Management Console and the host's network identity are one and the same.

To name a host with a valid network host name without DNS so that the network host name resolves to a valid IP address, run the `host` command on an appliance-based GDE Appliance or edit the `/etc/hosts` file on a software-only GDE Appliance.

Check that the network host names and FQDNs resolve successfully on the GDE Appliance. Host names cannot contain spaces and IP addresses must be in the standard *`xxx.xxx.xxx.xxx`* format. You cannot assign multiple host names to an IP address like you can if you were editing `/etc/hosts` directly. Also, if an IP address is already assigned multiple names, the `host show` command will display the first name only and the GDE Appliance uses the first entry only.

For example, `/etc/hosts` can contain:

```
    1.3.5.7 deptsys deptsys.domain.com
```

but `host show` will display:

```
    name=deptsys ip=1.3.5.7
```

Syntax

```
    host add name ip

    host delete name

    host show
```

where, *name* is the host name of a failover GDE Appliance or agent system, and *ip* is the IP address to use to contact that failover node or agent system.

The `host` command has the following options:

Table 11: Network category `host` command options

`add`	Inserts a *host*:*IP* pair in `/etc/hosts`.
`delete`	Removes a *host*:*IP* pair from `/etc/hosts`.
`show`	Shows the `/etc/hosts` file except for blank lines, comment lines, and the `localhost` entry. Displayed entries are not sorted.

Example

The following example adds a *host*:*IP* pair to the `/etc/hosts` file and then displays all the configured *host*:*IP* pairs.

```
    0029:network$ host add deptsys 1.3.5.9

    SUCCESS: add host

    0030:network$ host show
```

```
name=vmlinux10 ip=1.3.5.10
name=vmlinux11 ip=1.3.5.11
name=vmlinux12 ip=1.3.5.12
name=vmlinux13 ip=1.3.5.13
name=vmlinux14 ip=1.3.5.14
name=deptsys ip=1.3.5.9
SUCCESS: show host
0031:network$
```

The following example deletes a host from the `/etc/hosts` file:

```
0031:network$ host delete deptsys
SUCCESS: delete host
0032:network$
```

ssh

The `ssh` command enables the secure shell (SSH) port.

Syntax

```
ssh [on|off|show]
```

Table 12: Network category `ssh` command options

`on`	Enables the SSH port.
`off`	Disables the SSH port.
`show`	Shows whether SSH port is enabled or not.

Example

The following example displays the SSH port status:

```
0000:dsm$ network
0001:network$ ssh show
ssh port : on
SUCCESS: ssh port status shown.
0002:network$
```

ping

The `ping` command sends ICMP (Internet Control Message Protocol) echo request packets (ECHO_REQUEST) to a specified network host. The `ping` command uses the ICMP protocol's mandatory echo request datagram to elicit an ICMP echo response (ECHO_RESPONSE) from a host or gateway. The `ping` command sends six packets to the network host and then reports the results.

Syntax

`ping` {*ipaddress* | *FQDN*}

Table 13: Network category `ping` command options

ipaddress	IP address of the host from which you want a response.
FQDN	Fully qualified domain name of the host from which you want a response.

Example

The following example sends a `ping` request to the host `vmlinux04_RH5`:

```
0022:network$ ping deptsys
PING deptsys (1.3.5.9) 56(84) bytes of data.
64 bytes from deptsys (1.3.5.9): icmp_seq=1 ttl=64 time=3.07 ms
64 bytes from deptsys (1.3.5.9): icmp_seq=2 ttl=64 time=0.477 ms
64 bytes from deptsys (1.3.5.9): icmp_seq=3 ttl=64 time=0.121 ms
64 bytes from deptsys (1.3.5.9): icmp_seq=4 ttl=64 time=0.136 ms
64 bytes from deptsys (1.3.5.9): icmp_seq=5 ttl=64 time=0.131 ms
64 bytes from deptsys (1.3.5.9): icmp_seq=6 ttl=64 time=0.214 ms

--- deptsys ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5003ms
rtt min/avg/max/mdev = 0.121/0.691/3.070/1.071 ms
ping SUCCESS
```

traceroute

The `traceroute` command uses the IP-protocol time field to elicit an ICMP time exceeded (`TIME_EXCEEDED`) response from each gateway along the path to a specified host.

Specify the target IP address or FQDN. The `traceroute` command supports a timeout option.

Syntax

```
traceroute (ipaddress|FQDN) {timeout}
```

Table 14: Network category `traceroute` command options

`ipaddress`	IP address of the host for which you want the path information.
`FQDN`	Fully qualified domain name of the host for which you want the path information.
`timeout`	The time period in seconds after which the request is dropped, range is from 1 to 60 seconds.

Example

The following example sends a `traceroute` command request to an IP address:

```
0028:network$ traceroute 192.168.60.7

traceroute to 192.168.60.7 (192.168.60.7), 30 hops max, 40 byte
packets

 1  10.3.244.3  3000.605 ms !H  3000.571 ms !H  3000.548 ms !H

Traceroute Completed

0029:network$
```

rping

The `rping` command sends Address Resolution Protocol (ARP) requests to a neighbor host, pings the address on the device interface by ARP packets and informs how many users are using a particular IP address.

Syntax

```
rping ipaddress {eth0|eth1}
```

Example

```
0024:network$ rping 1.3.5.9 eth0

ARPING 1.3.5.9 from 1.3.5.7 eth0

Unicast reply from 1.3.5.9 [00:0C:29:36:9E:B3]  2.518ms

Unicast reply from 1.3.5.9 [00:0C:29:36:9E:B3]  0.817ms

Unicast reply from 1.3.5.9 [00:0C:29:36:9E:B3]  0.866ms

Sent 3 probes (1 broadcast(s))

Received 3 response(s)

Arping SUCCESS

0025:network$
```

arp

The `arp` command displays the current Address Resolution Protocol (ARP) cache of the GDE Appliance.

Syntax

```
arp
```

Example

The following example displays the current ARP cache:

```
0001:network$ arp

1.3.5.25 dev eth0 lladdr 00:08:a1:59:c1:cc REACHABLE

1.3.5.254 dev eth0  FAILED

1.3.11.14 dev eth0 lladdr 00:17:31:6f:58:16 STALE


link info

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue \
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00

2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
pfifo_fast qlen 1000\    link/ether 00:0c:29:60:f9:3e brd
ff:ff:ff:ff:ff:ff

3: sit0: <NOARP> mtu 1480 qdisc noop \    link/sit 0.0.0.0 brd
0.0.0.0

arp SUCCESS


0002:network$
```

If a connection is STALE, ping it and check again. It should change to REACHABLE. If it does not change, or it changes to FAILED, the connection is no longer available.

checkport

The `checkport` command is used to scan a port on a network-accessible system to verify that a TCP connection can be made to the system using the specified port. It does not guarantee that you can log on, just that a communication channel can be opened on the GDE Appliance or on a host. It is typically used to check the status and availability of the ports through which to administrate and run the GDE Appliance. These are ports such as 22, 7024, 8443, 8444, and 8445. The `checkport` command returns the transport layer protocol and the service using that port. The transport layer protocol is always TCP. The service is a system service like ssh, vmsvc, and *.

A "Connection refused" message can be returned for various reasons, such as a port is not assigned and/or is not in a LISTEN state.

NOTE: If a GDE Appliance port refuses a connection, you must troubleshoot the TCP connection.

`checkport` activity is logged in the Management Console, and is displayed when operating outside of a domain. A sample *Logs* window entry is shown below.

```
18713  2010-08-27 13:07:11.944 PDT  I  vmSSA05  CLI0003I:
[cliadmin] network checkport vmlinux101 7024
```

When `checkport` is executed in the Management Console interface, rather than on the command line, the log entry is appended with "`timeout` *x*", where *x* is either the value you entered on the command line or the default timeout.

Syntax

```
checkport host port [timeout x]
```

where, *host* is an IP address, FQDN, hostname, or even "localhost". Typically, it is a valid GDE Appliance or agent host, as configured in the Management Console.

port is a single TCP port number or a range of port numbers. A port number range is a hyphen/dash-separated list and is entered in the form "startnum-endnum". For example, `8440-8449`.

x is an integer between 1 and 600, inclusive. It is the timeout threshold and is expressed in seconds. The default is `180` seconds.

Example

The following example checks the availability of port (`8445`) used to run the Management Console on a failover GDE Appliance node:

```
0004:network$ checkport vmSSA06 8445

Connection to vmSSA06 8445 port [tcp/*] succeeded!

SUCCESS: invoked checkport(nc) command.

0005:network$
```

The following example checks the availability of port (`7024`) used to download configuration data to an agent host:

```
0005:network$ checkport solaris120 7024

Connection to solaris120 7024 port [tcp/vmsvc] succeeded!

SUCCESS: invoked checkport(nc) command.

0006:network$
```

The following example checks the availability of a range of ports on the local system, a GDE Appliance, and includes a 10 second timeout.

```
0081:network$ checkport localhost 8440-8449 timeout 10

nc: connect to localhost port 8440 (tcp) failed: Connection
refused

nc: connect to localhost port 8441 (tcp) failed: Connection
refused

nc: connect to localhost port 8442 (tcp) failed: Connection
refused

nc: connect to localhost port 8446 (tcp) failed: Connection
refused

nc: connect to localhost port 8447 (tcp) failed: Connection
refused

nc: connect to localhost port 8448 (tcp) failed: Connection
refused

nc: connect to localhost port 8449 (tcp) failed: Connection
refused

Connection to localhost 8443 port [tcp/pcsync-https] succeeded!

Connection to localhost 8444 port [tcp/pcsync-http] succeeded!

Connection to localhost 8445 port [tcp/*] succeeded!

SUCCESS: invoked checkport(nc) command.

0082:network$
```

nslookup

The `nslookup` command is used to query the DNS to get hostname to IP address mapping. Specify the FQDN or IP address of the server for which you want the IP address or host name information.

Syntax

```
nslookup HOST_NAME [timeout {1..600} | port {1..65535}]
```

Example

```
0010:network$ nslookup linuxhost.domain.com

Server: <dns server>

Address: <dns server ip address>

Name: linuxhost.domain.com

Address: 1.2.3.4
```

```
SUCCESS: invoked nslookup command.
```

System Category Commands

The `system` configuration category enables you to set the appliance host name, enable/disable the console port, create certificates, restart the GDE appliance, and reboots/shuts down the GDE appliance.

NOTE: These GDE Appliance CLI commands work only on a GDE appliance. Software-only GDE Appliance installations do not support the `console`, `reboot`, `setinfo`, and `shutdown` commands.

Enter the `system` configuration category by typing:

```
0001:dsm$ system
```

The `system` category supports the following commands:

Table 15: System category commands

`setinfo`	Sets the host name or FQDN of the GDE appliance.
`console`	Enables or disables the serial console port.
`security`	Creates the CA signer certificate and the GDE appliance certificate. It also signs the GDE appliance certificate.
`mfauth`	Enables, disables, or displays the configuration status of multi-factor authentication.
`shutdown`	Stops the GDE appliance software and powers off the appliance.
`reboot`	Reboots the GDE appliance and restarts the GDE software.
`server`	Provides the options to restart, start, and stop the GDE appliance as well as the option to check the status of the GDE appliance.

setinfo

The `setinfo` command enables you to set the host name of the GDE appliance and display appliance-related information such as the hardware UUID, serial number, and uptime.

The assigned name is used to identify the appliance and identify the certificate owner. If you change the host name after generating the CA signer and GDE appliance certificates, you must regenerate the certificates because the host name is used in the certificates to identify the GDE appliance.

Syntax

```
setinfo [show | hostname | sshbanner ]
```

The `setinfo` command can take the following arguments:

Table 16: System category setinfo command arguments

`hostname`	Sets the host name for your system. This option takes one argument, the network name to assign the appliance.
`sshbanner`	Defines the `/etc/ssh/ssh-banner` file. Available only on Vormetric-provided physical and virtual GDE Appliances. Edit the banner shown when logging on to the GDE Appliance CLI. The default is “Welcome to the Vormetric Data Security Manager.”
`show`	Shows the current `setinfo` settings.

Example

The following example sets the GDE Appliance host name to `vmSSA001`:

```
0005:system$ setinfo hostname SSA666

SUCCESS: setinfo hostname. If the DSM certificate is already
generated, please re-sign the server certificate to reflect the
hostname changes.

0006:system$
```

setinfo show

The `setinfo show` command displays general appliance information. The following example was taken on an appliance-based GDE Appliance.

```
0017:system$ setinfo show

hostname = SSA666

UUID = 53D19F64-D663-A017-8922-003048C497D4

serial number = 999X9120411

part number = 30-1010002-01

uptime =  10:36:56 up 15:47,  2 users,

          load average: 0.09, 0.05, 0.01


ssh banner = Welcome to the Vormetric Data Security Manager.

Show setinfo SUCCESS

0018:system$
```

console

The `console` option displays the state of the serial console. By default the serial console is always on. If you turn off the serial console port the only access to the appliance will be through the network. We strongly recommend that you leave the serial console on.

- `console on`—This command turns the serial console on. It is on by default.
- `console off` —This command turns the serial console off. You cannot use the serial console to log on when the console is off.

Syntax

```
console [on | off | show]
```

Example

```
0013:system$ console on
Be prepared to wait for a few minutes
0014:system$ console show
console on
```

security

The system category security command creates the SSL credentials used to authenticate GDE Appliances and their agents.

Table 17: System category security command arguments

`genca`	Generates the CA signing certificate on the primary GDE Appliance.
`gencert`	Re-generates the GDE Appliance certificate.
`legacyregistration`	Manually close/open port 8080 for new deployment or backwards compatibility.
`masterkey`	Master key management
`signcert`	Re-signs the GDE Appliance certificate.
`suiteb`	Suite B mode configuration
`cc`	Common Criteria Mode configuration
`tlsha`	Configure TLS for HA replication
`boot-passphrase`	Set a passphrase to unlock the GDE Appliance at system boot time, to maintain the security of the encrypted filesystem. This is feature is available only on a fresh installation of v6.0.2 or later.

genca

The `security genca` command regenerates the Certificate Authority (CA) on the primary GDE Appliance.

The administrator should run this utility in one of the following situations:

- Setting up a new GDE Appliance
- When the signer key is compromised
- When the signer certificate expires
- Any of the fields of the signer certificate has changed
- Restoring a backup configuration to a different GDE Appliance (Recommended)

The command does the following, in the following order:

- Generates a new signer certificate
- Deletes the old signer certificate from the keystore
- Imports the new signer certificate into the keystore
- Generates a new certificate request from the existing GDE Appliance certificate
- Signs the GDE Appliance certificate with new CA
- Imports the new GDE Appliance certificate into the keystore
- Restarts the GDE Appliance

Do the following operations after running the `security genca` command.

- If failover GDE Appliances are configured, there is now a certificate mismatch and the failover GDE Appliance certificates must be re-signed by the primary GDE Appliance. Establish a GDE Appliance CLI connection to each failover GDE Appliance and run the `signcert` command.

Every agent registered with the GDE Appliance must be re-registered. No agent-GDE Appliance communication will occur until the following steps are completed:

1. Disable the agent's registration from the Management Console to remove the agent's certificates.
2. Re-enable that agent's registration on the GDE Appliance.
3. Run register_host on that agent.

The information that you provide is displayed when the signer-certificate is viewed. You are prompted to specify:

- Your organizational unit, which is frequently a department or group name
- Organization name, which is frequently the company name
- City or locality in which the organization is located
- State or province in which the organization is located

- The country in which the organization is located

After you enter this data, the utility creates certificates, completes the installation process, and then starts the GDE Appliance. You are then returned to the CLI prompt.

Syntax

```
security genca
```

Example

```
0001: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

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.

Security Server host name[vmSSA05]:

Please enter the following information for key and certificate
generation. Security Server Certificate Configuration

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

What is the name of your organization? []:Excelsior

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

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

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

Regenerating the CA and server certificates now...

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$
```

gencert

The CLI `security gencert` command generates the GDE Appliance certificate for the current GDE Appliance. This command is run on both the primary and failover nodes.

Regenerate the GDE Appliance certificate when:

- The GDE Appliance key has been compromised
- The GDE Appliance certificate has expired
- When the host name of the GDE Appliance changes
- One of the certificate fields (such as organization, city, and so on) of the certificate has changed
- When the GDE Appliance is restored on another appliance with a different host name

The utility does the following, in the following order:

- Checks for an existing GDE Appliance certificate
- Generates a new key pair in the keystore
- Swaps the master key encryption to use the new key pair
- Deletes the old key pair in the keystore
- Generates a new certificate request based on the new key
- Gets the certificate request signed by the CA (Certificate Authority, located on the primary GDE Appliance)
- Imports the new GDE Appliance certificate back to the keystore

GDE Appliance and VTE Agent communication is not affected by this change. The information that you provide is displayed when the signer-certificate is viewed. You are prompted to specify:

- Your organizational unit, which is frequently a department or group name
- Organization name, which is frequently the company name
- City or locality in which the organization is located
- State or province in which the organization is located
- The country in which the organization is located

After you enter this data, the utility creates certificates, completes the installation process, and then starts the GDE Appliance. After which, you are returned to the GDE Appliance CLI prompt.

Syntax

```
security gencert
```

Example

```
0036:system$ security gencert
```

```
WARNING: The server certificate will be regenerated, and the
security server software will be restarted automatically!

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

Primary Security Server system administrator name:alladmin

Primary Security Server system administrator password:

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[vmSSA06]:

Please enter the following information for key and certificate
generation.

What is the name of your organizational unit? []:Really Fine
Stuff

What is the name of your organization? []:Widgets, Inc.

What is the name of your City or Locality? []:Santa Clara

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

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

Regenerating the server certificates now...

SUCCESS: The security certificates are re-generated and the
Security Server software is restarted.

0037:system$
```

legacyregistration

Port 8080 is no longer used for registration, but you can manually close/open this legacy port for new deployment.

Syntax

```
# security legacyregistration [ on | off | show ]
```

Example

```
# security legacyregistration show
```

masterkey

The `security masterkey` command displays the GDE Appliance master key. It displays the master key identifier and the date on which it was created.

Syntax

```
security masterkey show
```

Example

```
0006:system$ security masterkey show

identifier=4fc24a6b

creation_date=2016-04-08

SUCCESS: showed master key info
```

signcert

This utility signs the GDE Appliance certificate for the primary GDE Appliance. Usually it is used to re-sign expired primary and failover certificates.

The utility does the following, in the following order:

- Generates a new certificate request from the existing key pair in the keystore
- Gets the certificate request signed by the CA (Certificate Authority, located on the primary GDE Appliance)
- Imports the new GDE Appliance certificate back to the keystore

GDE Appliance and VTE Agent communication is not affected by this change.

Syntax

```
security signcert
```

Example

```
0037:system$ security signcert

WARNING: The server certificate will be resigned, and the
security server software will be restarted automatically!

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

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.

Security Server host name[vmlinux03_RH5]:

Please enter the following information for key and certificate
generation. Security Server Certificate Configuration

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

What is the name of your organization? []:Widgets, Inc.

What is the name of your City or Locality? []:Santa Clara

What is the name of your State or Province? []:CA
What is your two-letter country code? [US]:

Regenerating the server certificates now...

Deleting existing key with alias cgss_server_app

Renaming new key with alias cgss_server_app_new to
cgss_server_app

Generating certificate signing request

Signing certificates

Deleting old signer certificate from keystore

Importing new signer certificates into keystore

Importing new server certificates into keystore

DB20000I  The SQL command completed successfully.

Server certificate has been re-signed by the Certificate
Authority successfully.

Starting the Security Server.
```

After you enter this data, the utility creates certificates, completes the installation process, and then starts the GDE Appliance. You are then returned to the GDE Appliance CLI prompt.

suiteb

The `suiteb` command is used to activate or deactivate Suite B mode, Compatible mode, or RSA mode.

Syntax

```
security suiteb [set [suiteb | compatible | rsa] | show]
```

The `suiteb` command can take the following arguments:

Table 18: Security suite B command arguments

`set`	This command is used to activate or deactivate Suite B mode, or compatible mode, or RSA mode `[suiteb	compatible	rsa]`
`show`	Show Suite B mode configuration

The GDE Appliance is in ‘Compatible’ mode by default. The Suite B or RSA modes must be enabled to take effect.

Compatibility mode uses both RSA and ECC certificates—the GDE Appliance uses the ECC certificate by default to communicate with other GDE Appliances, newly installed or upgraded agents, and uses the RSA certificate to communicate with older agents. When the agent negotiates a transaction with the GDE Appliance, the handshake determines which certificate is to be used.

Suite B uses only ECC certificates and older agents that do not support ECC will need to be upgraded or will fail to communicate with the GDE Appliance.

RSA mode uses only RSA certificates. Any agents that already registered when RSA mode is enabled must be re-registered as the ECC port is now closed and in order to communicate with the GDE Appliance, agents will need to re-register with that GDE Appliance.

Examples

The following example activates Suite B mode:

```
0008:system$ security suiteb set suiteb

WARNING: After setting to suiteb mode, the security server
software will be restarted automatically if you have certificate
configured!

Microsoft IE is the only browser to support suiteb mode, please
use latest IE to access management console.

Please make sure the DSM ports 8446-8448 are not blocked by
firewall.

Also if you have HA setup, please make sure all the cluster
server nodes are in suiteb mode.

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

Enter ‘yes’ to enable Suite B mode.

The following example shows whether Suite B is configured:

```
0009:system$ security suiteb show

Current mode is: suiteb

SUCCESS: showed suiteb status
```

The following example activates RSA mode:

```
0004:system$ security suiteb set  rsa

Important!: Ensure DSM ports 8443-8445 are not blocked by
corporate firewall.

           In addition, all other DSMs in this cluster must also
be in rsa mode.

            The Security Server will be restarted.

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

Enter ‘yes’ to enable RSA mode.

cc

The cc command is used to enable or disable Common Criteria mode.

Syntax

```
security cc [on | off | show]
```

The cc command takes the following arguments:

Table 19: Security cc command arguments

on	Enable Common Criteria mode
off	Disable Common Criteria mode
show	Show console port status

Example

The following example enables Common Criteria mode:

```
0001:system$ security cc on

cc (Common Criteria) mode is node specific configuration, and
need to be configured in each cluster node individually. Turning
on cc (Common Criteria) will improve the security level but
limit some functionality, and server will restart automatically,
continue? (yes|no)[no]:
```

The following example shows whether Common Criteria is enabled:

```
0002:system$ security cc show

SUCCESS: Common Criteria mode is off

0003:system$
```

tlsha

The `tlsha` command is used to enable TLS for HA replication. It must be enabled on the primary GDE Appliance as well as on each failover node, *before* setting up HA.

Syntax

```
security tlsha [ on | off | show | status ]
```

The tlsha command takes the following arguments:

Table 20: Security tlsha command arguments

on	Enable TLS for HA replication
off	Disable TLS for HA replication
show	Show whether TLS is enabled or disabled

status	Indicate the status of TLS for HA replication, i.e., is it running or not

Example 1

The following example enables TLS for HA replication:

```
0004:system$ security tlsha on

Enable TLS for HA replication for this DSM? The Security Server
service will restart automatically on failover DSMs.

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

SUCCESS: Turned on TLS for HA replication.

Run this command on every server node in the cluster then run
convert2failover on failover servers.

0005:system$
```

Example 2

The following example shows TLS for HA replication turned on:

```
0006:system$ security tlsha show

TLS for HA replication is enabled

SUCCESS: Showed TLS for HA replication.

0007:system$
```

Example 3

The following example shows TLS status for three different conditions:

```
0013:system$ security tlsha status

No failover servers configured for replication

SUCCESS: Showed TLS for HA replication status.


0014:system$ security tlsha status

TLS HA replication is running

SUCCESS: Showed TLS for HA replication status.


0001:system$ security tlsha status

TLS HA replication has stopped
SUCCESS: Showed TLS for HA replication status.
```

boot-passphrase

The `boot-passphrase` command sets and manages a passphrase required at GDE Appliance system boot time to unlock the system. Refer to the *Installation & Configuration Guide* for more information about this feature.

Syntax

```
security boot-passphrase [ set | clear | show ]

security boot-passphrase recovery [ show [<filename>] | delete
<filename> ]
```

Table 21: Security boot-passphrase command arguments

`set`	Set a boot-passphrase to unlock the GDE Appliance filesystem at system boot up
`clear`	Clears the boot passphrase
`show`	Shows whether a boot-passphrase has been set or not
`recovery show`	Displays the passphrase recovery file and displays the contents—the encrypted passphrase, the public key used to encrypt the passphrase, and a sample command to recover the passphrase using the associated private key
`recovery delete`	Deletes the passphrase recovery file

Example 1

The following example shows how to set a boot passphrase. After setting the passphrase, the GDE Appliance reboots and the SSH console connection is lost. You need to have IPMI Java console access, or if using a virtual appliance, you can connect to the GDE Appliance via the console available from the virtualization application in use. Refer to the Installation & Configuration Guide for details about setting a boot passphrase.

```
0000:dsm$ system

0001:system$ security boot-passphrase set


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-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwYIf0Z04nzne9j78BY7
m

Q9kMTgh8YErtklECnVVhxExob/UvAWOvSBcGDVgixpeMCywWVh8OgTIbj751PVf
a

TI8/C+gP4Rd6cdtO7fGzsYsAZxN9OCssRQlCJfCe6y6fNep3dDOh1noTFyFNTqO
y
```

```
c3WW0gAlJ9ILPwn6uxVRgtXPgLnFfP9zNieyWmHTLw6He8BZAAYkWbESMgnA5Bo
J

mcxdpv/i/8ZODTMMo/6Ji4oYpQPa8i9Ex7qTZinl5hxjIjC8eIcUOMNdAhvslNz
s

T6FZPJ2BEYBU6TAQpxDPLwPAQIEw1x/NzcYUUfgaP1pZIAdhWFJUZkx4FqmEA5o
d

MwIDAQAB

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


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


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...
```

Example 2

The following example shows whether a boot passphrase has been set or not:

```
0008:system$ security boot-passphrase show

Prompt-On-Boot mode - the system disk is encrypted and there is
a custom boot passphrase set.

SUCCESS

0009:system$
```

Example 3

The following example shows the recovery file and the contents of that file

```
0000:dsm$ system

0001:system$ security boot-passphrase recovery show

SUCCESS
```

```
 The following passphrase recovery files are available:

 0. 201710031407


 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-----


 Example command for decrypting the passphrase, given the
 matching private key:

      base64 -d <file-containing-the-ciphertext-above> | openssl
 rsautl -inkey <private-key> -decrypt

 SUCCESS
```

Example 4

The following example clears the boot passphrase. When you clear the passphrase the recovery file is not deleted, you can delete it later, see next example:

```
0004:system$ security boot-passphrase clear

Enter current boot passphrase:

WARNING: After clearing the custom boot passphrase, the system
will be rebooted automatically!
```

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

0005:system$ security boot-passphrase clear

Enter current boot passphrase:

WARNING: After clearing the custom boot passphrase, the system
will be rebooted automatically!

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

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


This operation will take some time, please wait....

SUCCESS: custom boot passphrase has been cleared, unattended
boot enabled.


DSM server is rebooting

0006:system$
```

Example 5

The following example deletes the passphrase recovery file:

```
0003:system$ security boot-passphrase recovery delete
201710031407

SUCCESS: removed passphrase recovery file '201710031407'

0004:system$
```

mfauth

The `mfauth` command enables or disables the multi-factor authentication of GDE Appliance Management Console administrators. When enabled, the Management Console login screen displays the usual **Login** and **Password** boxes.

- GDE Appliance Management Console administrators with multi-factor authentication must enter the value displayed on their RSA SecurID device into the **Password** box.
- GDE Appliance Management Console administrators **without multi-factor authentication should enter the GDE Appliance administrator password in the Password** box.

The `mfauth` command includes a `clean` option to remove all configured administrator:device bindings. To remove the administrator:device bindings of individual Management Console administrators, open the *Edit Administrator* window and delete the value in the **RSA User Name** box.

The `mfauth` command displays the enabled/disabled status of multi-factor authentication. The current `mfauth` status is also indicated in the **System > General Preferences > System** tab. The **Multi-Factor Authentication Status** checkbox is a display indicator only and cannot be set in the Management Console.

Do not enable multi-factor authentication until after the RSA Authentication Agent is configured on the GDE Appliance.

NOTE: Do not run the `mfauth` GDE Appliance CLI command on a failover node. The GDE Appliance CLI is independent of the Management Console database and you can enable or disable multi-factor authentication on a failover node independent of the primary GDE Appliance, resulting in a primary:failover database mismatch. If, for example, you turn off multi-factor authentication on a failover node, RSA-configured administrators will be unable to log on to the Management Console of that failover.

Syntax

```
mfauth on | off | clean | show
```

Example

The following example shows the current multi-factor configuration status of the GDE Appliance. The GDE Appliance is configured for multi-factor authentication. It’s just not enabled.

```
0001:system$ mfauth show

Administrator multiple factor authentication : off

RSA secret file configured : on

SUCCESS: administrator multiple factor authentication status
showed.

0002:system$
```

The following example enables multi-factor authentication for GDE Appliance administrators.

```
0010:system$ mfauth on

WARNING: After enabling the administrator multiple factor
authentication, the security server software will start to
validate the extra one-time password!

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

SUCCESS: administrator multiple factor authentication enabled.

0011:system$
```

The following example deletes the RSA node secret file from the GDE Appliance, effectively breaking all communication between the GDE Appliance and the RSA Authentication Manager, which, in turn, disables multi-factor authentication of GDE Appliance administrators. If you remove the node secret using `mfauth clean`, you must also delete the node secret on the RSA Security Console by running `Clear Node Secret`. A new node secret will be automatically generated the next time any Vormetric administrator logs into the Management Console. To break all GDE Appliance administrator<->device bindings on the GDE Appliance:

```
0001:system$ mfauth clean

WARNING: Cleaning RSA secret file will break the communication
between the security server and RSA server!

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

SUCCESS: RSA secret file is removed.

0002:system$
```

tls1

The `tls1` command enables or disables support for TLS protocols v1.0 and 1.1. This command turns on or turns off support for both v1.0 and v1.1 of the TLS protocol, you cannot select one or the other.

However, if you have host servers protected by VTE Agent versions earlier than v5.2.1, TLS v1.2 is not supported, and you will need to enable support for TLS v1.0/1.1. If you have HA configured, you must enable TLS v1.0/1.1 support on each of the failover nodes as well.

Enabling TLS v1.0/1.1 support restarts the GDE Appliance software.

Syntax

```
tls1 [on | off | show]
```

The `tls1` command takes the following arguments:

Table 22: System tls1 command arguments

`on`	Enable TLS 1.0/1.1 support
`off`	Disable TLS v1.0/1.1 support
`show`	Show status of TLS v1.0/1.1 support (enabled or not)

Example

The following example turns on TLS v1.0/1.1:

```
0002:system$ tls1 on

WARNING: After enabling TLS 1.0/1.1, the security server
software will restart!

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

SUCCESS: TLS 1.0/1.1 enabled and server restarted.
```

```
This change only affected this node. Run the same tls1 command on
all other nodes in the cluster.

0003:system$
```

The following example shows whether TLS v1.0/1.1 is enabled or not:

```
0004:system$ tls1 show

TLS 1.0/1.1 is disabled

SUCCESS: TLS 1.0/1.1 status shown

0005:system$
```

shutdown

The `shutdown` command stops the GDE Appliance software, brings down the appliance operating system, and then powers off the appliance. Configuration changes are automatically saved. Afterwards, the appliance can be safely turned off.

Syntax

```
shutdown
```

Example

The following example shuts the system down:

```
0038:system$ shutdown

Do you want to shutdown the system ? (y/n):y

Shutting down now...

Shutdown SUCCESS

0039:system$
```

The last message displayed on the appliance LCD before it powers down is:

```
Power off or reboot in approx 15 secs
```

You can remove the power cords and power modules after the appliance powers down. Reapply power by reattaching the power cords and pressing the power switch. The power-interrupt alarm may sound. If it does, press the red reset button on the back of the appliance.

reboot

The reboot command reboots the GDE Appliance appliance.

Syntax

```
reboot
```

Example

The following example reboots the system immediately:

```
0001:system$ reboot
Reboot the system y/n?
Rebooting now...
Reboot SUCCESS
system$
Broadcast message from root (Sun Feb 9 02:44:20 2014):
The system is going down for reboot NOW!
```

server

Previous CLI commands limited the GDE Appliance CLI administrator to do a restart of the GDE Appliance. The commands have been enhanced so that GDE Appliance CLI administrators can start and stop the GDE Appliance based on the need for maintenance intervals, test cycles and so on. Available server commands are listed in Table 23:

Table 23: GDE Appliance CLI system category server commands

`restart`	Restarts the GDE Appliance software. Shuts down the GDE Appliance software and then restarts it.
`start`	Starts the GDE Appliance software.
`stop`	Stops the GDE Appliance software.
`status`	Displays the GDE Appliance software running status.

restart

The `restart` command stops and then starts the GDE Appliance software. It does not reboot the appliance. The `reboot` command restarts the GDE Appliance operating system and, in the process of coming up, starts the GDE Appliance software. Use the `reboot` command only if `restart` does not correct a problem.

Syntax

```
restart
```

Example

The following example restarts the GDE Appliance:

```
0033:system$ server restart
Do you want to restart the server software ? (y/n):y
Restarting now...
Stopping Security Server...done.
```

```
    Stopping the data store...done.
    Starting Security Server...done.
    SUCCESS: The security server software is restarted.
    0034:system$
```

status

The status command displays the current running status of the GDE Appliance software.

Syntax

```
    status
```

Example

The following example shows the status display.

```
    0038:system$ server status
    Security Server is running.
    Security Server uptime:  2 days, 09:27:27
    SUCCESS: The security server software status is shown.
```

HSM Category Commands

connect

The `connect` command is used to enable or disable a network HSM for a GDE Appliance appliance that does not have a built-in HSM—DSM V6000 and the virtual appliance.

Syntax

```
    connect [ add nShield Connect IP address RFS IP address | delete
    | show ]
```

where,

nShield Connect IP address is the IP address of the nShield Connect appliance

RFS IP address is the IP address of the computer that has the RFS installed

The connect command is used as follows:

Table 24: HSM Category connect command

`add`	Add a nShield Connect Network HSM
`delete`	Delete a nShield Connect Network HSM
`show`	Show currently configured nShield Connect Network HSMs

Example

```
0001:hsm$ connect add 1.2.3.16 1.2.3.4

This DSM is being connected to a nShield Connect for the first
time(i.e. it is being converted into HSM enabled). A new DSM
master key in the HSM will replace the existing master key in the
Java keystore. Once that is done, this DSM cannot be converted
back to non-HSM enabled without all the data being destroyed
with ‘config load default’ to reset it back to factory
configuration.

An administrator card from the ACS of the Security World the
nShield Connect belongs to is required if the Security World is
FIPS 140-2 level 3 compliant. If you don't have the
administrator card currently, you need to abort now.


Do you want to continue? (yes|no)[no]: yes


Please remove the administrator card from the reader.


Stopping the Security Server

Stopping the data store [ OK ]

Self test in progress: passed

Starting Security Server

Security Server started in compatible mode

nShield Connect HSM with IP address 1.2.3.16 is added
successfully.

SUCCESS: connect command ran successfully

0002:hsm$
```

secworldupdate

The secworldupdate command is used to synchronize the GDE Appliance with the nShield Connect when the Security World on the configured nShield Connect appliance has been upgraded. A Security World update may be triggered for various reasons, for example the ACS has been replaced. If the GDE Appliance is in an HA cluster, the command must be run all cluster nodes.

Syntax

```
secworldupdate
```

Example

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

Maintenance Category Commands

The maintenance category is used to restore the GDE Appliance to factory defaults, upgrade the current GDE Appliance installation, and set operating system attributes, such as date, time, and time zone.

Enter the maintenance category by typing:

```
0009:dsm$ maintenance
0010:maintenance$
```

The maintenance category consists of the following commands:

Table 25: GDE ApplianceCLI maintenance category commands

config	This command restores the appliance image and configuration to the same state and version at which the appliance was shipped from the factory. This command also configures automatic backup and remote archival.
showver	Displays the GDE Appliance versions that are on the system and indicates the version that is currently running.
delver	Deletes a GDE Appliance image from the GDE Appliance.
ntpdate	Configures one or more Network Time Protocol (NTP) servers with which to synchronize the system clock.
date	Sets the system date.

`time`	Sets the system time.
`gmttimezone`	Sets the system time zone.
`diag`	Displays GDE Appliance and system logs, available system disk space, system OS version, and system uptime.
`repair`	Removes ghost DB2 instances and restores the embedded database to its original condition.

config

This section describes using the CLI maintenance category `config` command to delete the GDE Appliance configuration or restore the GDE Appliance to its original factory configuration.

The `config reset` and `config load default` commands restore the GDE Appliance installation to an unconfigured state.

The `config reset` command removes all the configuration data that was added after the current GDE Appliance software was installed. The command preserves the currently installed GDE Appliance software but, removes all configuration data except the network configuration.

NOTE: The config load default command causes a reboot of the GDE Appliance. When the command is issued, wait for the system to fully reboot and restart. ***Do not cycle power***. Critical system files are installed on the reboot following a config load default so it is important to wait until it has completed

The `config load default` command is an extreme form of `config reset`. The `config load default` command deletes everything from the appliance and restores the same GDE Appliance installation with which the appliance was shipped. The partitions that contain GDE Appliance installations are deleted from the appliance, so there is no hope of retrieving any data once this command is executed.

The `config load default` command produces the same result as the Kill switch:

- Execute this CLI command when there is a serial console connection to the appliance, or when there is a terminal window from which to SSH onto the appliance.
- Press the Kill Switch when you do not have console or terminal access, but you do have access to the physical appliance.

The `config reset` and `config load default` commands discard the CA signer certificate. The CA signer certificates must be restored from a backup or regenerated later.

If the system is configured as a primary GDE Appliance, be sure to back up the current configuration before running either of these commands. Configuration data will be restored on a failover GDE Appliance once it rejoins the HA configuration, so there is no need to back up a failover node. However, if agent activity is logged on a failover node, back up the logs on the GDE Appliance before proceeding.

Syntax

The following is the CLI `config` command syntax:

```
config load default

config reset
```

The `config` command supports the following arguments:

Table 26: CLI maintenance category config commands

`load`	Removes the current GDE Appliance installation and restores the manufacturer default GDE Appliance installation. It removes all policies, hosts, keys, and so on from the GDE Appliance.
`reset`	Preserves the currently installed GDE Appliance software but removes all configuration data, except the network configuration.

The following example deletes the partitions that contain GDE Appliance installations. Everything that has been added since the appliance was first started is deleted. The appliance reboots and loads the original GDE Appliance installation.

NOTE: The original GDE Appliance installation will not contain any patches or upgrades.

Example 1

```
0011:maintenance$ config load default

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

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

config load SUCCESS.

0012:maintenance$
```

Example 2

The following example resets the current GDE Appliance installation back to its initial unconfigured state. This command returns database and configuration files to their original, fresh installation state without changing or reinstalling the current GDE Appliance version.

```
0003: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.

0004:maintenance$
```

showver

The showver command displays the GDE Appliance software images that have been uploaded and that are available for use. The GDE Appliance comes from the factory with one image pre-installed. Up to two images can be installed and configured at one time. Software patches are not displayed by this or any other command.

Syntax

```
showver
```

Example

Enter the showver command without any arguments to display the current image. For example:

```
0001:maintenance$ showver
ver_count=1
cur_ver=6.0

show version SUCCESS

0002:maintenance$
```

delver

The delver command deletes the inactive GDE Appliance image from the system. Up to two images can be installed on the appliance or system at one time. As image updates become available, you will cycle through the installed images, usually deleting the older of the two images. You cannot delete an active image, nor can you simply stop the GDE Appliance.

Syntax

```
delver
```

You are prompted to continue.

Example

The following example deletes the image from the system.

```
0010:maintenance$ delver

You are deleting the alternative software version.
Continue? (yes|no)[no]:yes

Delete version SUCCESS
```

```
0011:maintenance$
```

ntpdate

The `ntpdate` command:

- Configures one to four Network Time Protocol (NTP) servers for the current GDE Appliance
- Enables and disables NTP on the appliance
- Forces immediate clock synchronization with an NTP server
- Shows the current NTP configuration status

When NTP is configured and enabled, at one hour intervals the CLI daemon synchronizes the system clock of the GDE Appliance with the first available NTP server. If, within one second, the GDE Appliance cannot connect with the NTP server, the CLI daemon tries the next NTP server in the list. The NTP server can reside in any time zone.

Syntax

```
ntpdate sync | add SERVER_ADDRESS | delete SERVER_ADDRESS | on |
off | show
```

The `ntpdate` command takes the following arguments:

Table 27: tntpdate command arguments

`sync`	forces clock synchronization with the first available NTP server.
`add` SERVER_ADDRESS	adds the named NTP server to the list of servers to contact for time synchronization. At least one server must be configured before you can enable (turn on) time synchronization. You may configure up to four NTP servers.
`delete` SERVER_ADDRESS	removes the named NTP server from the list of servers to contact for time synchronization. Time synchronization is disabled (turned off) when the last NTP server is removed from the list.
`on`	enables NTP time synchronization. At least one NTP server must be configured before you can enable synchronization.
`off`	disables time synchronization and leaves the current NTP server list intact. You can re-enable synchronization without having to reconfigure the NTP servers.
`show`	Displays the NTP server configuration and state. The `ntpdate show` command does not sort the output. It displays all the configured NTP servers in the same order that they were added to the GDE Appliance.

`sync`, `add`, `delete`, `on`, `off`, and `show` are literals that are entered as shown or in abbreviated form.

Examples

The following examples:

- displays the default NTP configuration environment
- adds four NTP servers
- enables NTP synchronization
- displays a fully-configured NTP environment
- synchronizes the appliance clock with the first available NTP server clock
- swaps the last two NTP servers in the list to change access order

```
0001:maintenance$ ntpdate show
Total ntpdate server number  : 0
ntpdate is off

ntpdate SUCCESS


0007:maintenance$ ntpdate add 172.16.78.110

ntpdate SUCCESS

0008:maintenance$ ntpdate add search.domain.com

ntpdate SUCCESS

0009:maintenance$ ntpdate add 172.30.45.115

ntpdate SUCCESS

0010:maintenance$ ntpdate add 172.20.244.75

ntpdate SUCCESS


0011:maintenance$ ntpdate on

ntpdate SUCCESS


0012:maintenance$ ntpdate show

Total ntpdate server number  : 4

ntpdate server [1] : 172.16.78.100

ntpdate server [2] : search.domain.com

ntpdate server [3] : 172.30.45.115

ntpdate server [4] : 172.20.244.75

ntpdate is on

ntpdate SUCCESS
```

```
0013:maintenance$ ntpdate sync
ntpdate SUCCESS

0014:maintenance$ ntpdate delete 172.16.78.100
ntpdate SUCCESS
0015:maintenance$ ntpdate add 172.16.78.100
ntpdate SUCCESS

0016:maintenance$ ntpdate show
Total ntpdate server number  : 4
ntpdate server [1] : 172.30.78.100
ntpdate server [2] : search.domain.com
ntpdate server [3] : 172.20.244.75
ntpdate server [4] : 172.16.78.100
ntpdate is on
ntpdate SUCCESS
0017:maintenance$
```

date

The `date` command in the `maintenance` category is used to set or to display the date on the system. The `date` command without any arguments displays the current system date. If a parameter is included with the `date` command it resets the system date to the specified date.

Syntax

The syntax for the `date` command is:

```
date MM/DD/YYYY
date
```

Example

To set the date on the system to December 20th, 2014, enter the following:

```
0001:maintenance$ date 12/20/2014
```

The following example displays the system date:

```
0004:maintenance$ date
month=Dec day=20 year=2014
Show system date SUCCESS
```

```
0005:maintenance$
```

time

The `time` command sets or to displays the time on the system using a 24-hour clock. When no parameters accompany the `time` command, it displays the current system time. If a parameter is included with the time command, it resets the system time to the specified value.

Syntax

The syntax for the `time` command is:

```
time HH:MM:SS

time
```

Example

To set the time on the system enter the following:

```
0001:maintenance$ time 02:23:00
```

This sets the system to 2:23 AM.

The following example uses the time command to display the system time:

```
0003:maintenance$ time

hour=18 min=22 sec=38 zone=PDT

Show system time SUCCESS

0004:maintenance$
```

gmttimezone

The `gmttimezone` command in the maintenance category is used to set the system time zone. If a parameter is included with the `gmttimezone` command, it sets the time to the zone specified. To see a list of supported time zones, enter `gmttimezone list`.

Syntax

The syntax for the `gmttimezone` command is:

```
gmttimezone {list|show|set zonename}

gmttimezone list

gmttimezone show
```

Example

To list and set the `gmttimezone` on the system enter the following:

```
0025:maintenance$ gmttimezone list

...
```

```
(GMT-07:00) America/Phoenix (Mountain Standard Time)
(GMT-07:00) America/Shiprock (Mountain Standard Time)
(GMT-07:00) America/Yellowknife (Mountain Standard Time)
(GMT-08:00) America/Dawson (Pacific Standard Time)
(GMT-08:00) America/Los_Angeles (Pacific Standard Time)
(GMT-08:00) America/Tijuana (Pacific Standard Time)
(GMT-08:00) America/Vancouver (Pacific Standard Time)
(GMT-08:00) America/Whitehorse (Pacific Standard Time)
(GMT-08:00) Pacific/Pitcairn
(GMT-09:00) America/Anchorage
...
0026:maintenance$ gmttimezone show
Timezone is set to : US/Pacific
Show timezone SUCCESS
0030:maintenance$ gmttimezone set America/Tijuana
Set timezone SUCCESS
0031:maintenance$ gmttimezone show
Timezone is set to : America/Tijuana
Show timezone SUCCESS
```

diag

The `diag` command in the `maintenance` category displays OS system information and related log files. This command is available in appliance-based installations only.

Table 28: CLI maintenance category diag command arguments

`diskusage`	Displays system disk space usage.
`hardware`	View RAID and motherboard status.
`log`	Lists and displays system messages and logs.
`osversion`	Displays the system kernel version.
`tlsmon`	Monitor TLS connections and generate audit logs.
`uptime`	Displays how long the system has been running since the last reboot, the current number of administrators logged into the system, and CPU load usage.

vmstat	Displays CPU and memory usage.

diskusage

The diskusage argument to the diag command displays information about the system disk, such as partitions, amount of used and available disk space, percentage of free space, and partition names.

Syntax

```
diag diskusage
```

Example

```
0017:maintenance$ diag diskusage
Filesystem    1M-blocks   Used Available Use% Mounted on
/dev/sda6     9389    4403    4510  50% /
/dev/sda9   254458    939   240594   1% /partitions/large
/dev/sda1      935     22      866   3% /grub
tmpfs         1963      0     1963   0% /dev/shm
/dev/sda2     7511   2307     4823  33% /partitions/std/2
/dev/sda8     7513    155     6977   3% /tmp
SUCCESS: Show disk usage
0018:maintenance$
```

log

The log argument to the diag command is used to list and view system files on the GDE Appliance.

Syntax

```
diag log list
diag log view <file>
```

The diag log command supports three additional arguments, list and view.

The list argument displays the system files that are available for viewing. It takes no additional input. The view argument takes the name of the log file to display. The view argument calls the "more" system command to display the file. Some of the "more" command display options are supported. Active logs are log files that being currently written to and updated by GDE Appliance processes. Inactive logs are logs that have been filled to capacity and then closed. The name of the closed log file is the original name usually appended with the date. For example, the name of the active GDE Appliance log is `cgss.log`. When it reaches the configured capacity, it is made inactive and renamed to `cgss.log.`*YYYY-MM-DD*.

The GDE Appliance log files that you can view are described below:

- The `server.log` file contains details about agent backup and restore requests, connection status, Management Console interaction, Java exceptions, JBoss start and stop processes, and more. This file contains diverse information and it should be the first file you check for problems that are related to GDE Appliance operation.
- The `cgss.log` file contains a record of the events that make up the BEK generation process for an agent requesting to make a backup, as well as the names of uploaded audit files. This file does not contain events that pertain to restore operations. Check this file if the agent fails to back up a database, even though agent/GDE Appliance authentication is correctly configured, and the policy for this agent permits the backup operation.
- The `messages` file is generated by syslog. It contains kernel entries for enabling/disabling the log service, memory usage, CPU usage, system calls, device initialization, and so on. It also contains log entries that would otherwise be displayed in the Message Log but, for some reason, cannot be uploaded to the GDE Appliance. The `messages` file follows the standard naming convention to cycle large files. For example, the active file is `messages`. The cycled files are `messages.1`, `messages.2`, `messages.3`, and so on.

Example 1

To list the files that are available for viewing:

```
0011:maintenance$ diag log list
messages
messages.1
messages.2
messages.3
messages.4
cgss.log
cgss.log.2014-01-08
server.log
server.log.2014-01-15
SUCCESS: list log file
0012:maintenance$
```

Example 2

To display a log file, execute the `diag log view` command followed by the name of the file to view. For example:

```
0018:maintenance$ diag log view cgss.log

...

2014-01-19 19:09:22,025 INFO
[com.vormetric.server.sdk.user.UserManager] Entering createUser

2014-01-19 19:09:22,025 INFO
[com.vormetric.server.sdk.user.UserManager] User is authorized.
Generating password...

2014-01-19 19:09:22,025 INFO
[com.vormetric.server.sdk.user.UserManager] Verifying whether
the password meets the PasswordPolicy conditions...

2014-01-19 19:09:22,027 INFO
[com.vormetric.server.sdk.user.UserManager] Verifying complete:
Password meets all the PasswordPolicy conditions

2014-01-19 19:09:22,032 INFO
[com.vormetric.server.sdk.user.UserManager] Password generation
complete

...

0019:maintenance$
```

osversion

The `osversion` command displays the operating system version and kernel that is running on the GDE Appliance. The `osversion` command is equivalent to the Linux "`uname -a`" command.

Syntax

```
osversion
```

Example

To display the appliance operating system version and kernel:

```
0014:maintenance$ diag osversion

Linux SSA666 2.6.18-128.el5PAE #1 SMP Wed Jan 21 11:19:46 EST
2009 i686 i686 i386 GNU/Linux

SUCCESS: Show version

0015:maintenance$
```

uptime

The `uptime` command displays the amount of time the operating system has been running since the last bootup. It also displays the system load and the number of GDE Appliance CLI administrators that are currently running CLI sessions on the GDE Appliance. Administrators that are configured in the GDE Appliance Management Console GUI are not included in the count because GDE Appliance CLI administrators are actual system users and Management Console administrators exist only in the GDE Appliance database. The uptime command is equivalent to the Linux "`uptime`" command.

Syntax

```
uptime
```

Example

To display the amount of time that the appliance has been running, system load, and the number of current GDE Appliance CLI sessions:

```
0019:maintenance$ diag uptime

 17:02:20 up 3 days, 22:02,  2 users,  load average: 0.14, 0.06,
0.01

SUCCESS: Show uptime

0020:maintenance$
```

vmstat

The `vmstat` argument to the `diag` command displays information about the system disk, such as partitions, amount of used and available disk space, percentage of free space, and partition names.

Syntax

```
diag vmstat
```

Example

```
0001:maintenance$ diag vmstat

procs -----memory- --swap---io---system-----cpu-----

 r  b   swpd   free   buff  cache   si   so    bi    bo   in   cs
us sy id wa st

 1  0      0 4984848 203208 3793404    0    0     0    12   10
2  0  0 99  00

 SUCCESS: Show vmstat result

0002:maintenance$
```

repair

The `repair` command is used to remove database deadlocks. A deadlock occurs when two database instance processes try to place a lock on the same object. Normally, the GDE Appliance automatically aborts one instance process and allows the other to lock the object. If this process is abruptly interrupted while it is doing a GDE Appliance database operation, such as from a power failure, the system remembers the lock when it powers up the next time, and, being unable to place a new lock on the GDE Appliance database object, the GDE Appliance database cannot start and you cannot log into the Management Console.

Deadlocks consume SQL Server resources, especially the CPU, and reduce overall GDE Appliance performance.

The `repair` command automatically stops and restarts the GDE Appliance application.

Syntax

```
repair dblock
```

Example

```
0013:maintenance$ repair dblock
SUCCESS: called db command to repair db lock
0014:maintenance$
```

High Availability Category Commands

High Availability (HA) is the configuration of multiple GDE Appliances such that one acts as the primary GDE Appliance on which all configuration and management occurs, and the other GDE Appliances act as failover nodes that are continually updated with the changes that occur on the primary. In effect, the failover nodes maintain mirror copies of the primary GDE Appliance database. Agents access the failover when the primary GDE Appliance fails or cannot be contacted. A HA configuration always contains one primary and any number of failover nodes. Four is the recommended maximum number of failover GDE Appliances.

HA configuration and maintenance are done in both the GDE Appliance CLI and the Management Console.

Table 29: GDE Appliance CLI HA category commands

`config`	Specifies the primary node that the failover node is to register with.
`cleanup`	Removes failover node replication data from the primary database.
`convert2primary`	Changes a failover node to a primary node.
`convert2failover`	Changes a primary to a failover node or reinitializes a failover node before adding it to the HA cluster.
`show`	Lists all the configured failover GDE Appliances.

config

NOTE: To avoid database corruption, you must do a cleanup replication for every registered failover on the primary GDE Appliance before converting the primary GDE Appliance to a failover node.

The `config` command does the following tasks:

- On an appliance or system that is being configured as a failover, the `config` command is used to specify the host name or FQDN of a primary GDE Appliance. The failover and primary nodes exchange GDE Appliance certificates in order for both nodes to trust each other. This command is used by a failover to identify the primary that the failover GDE Appliance is to connect to during failover node certificate generation and database replication. This command is deprecated in favor of the `convert2failover` command. The `config` function is done by the `convert2failover` command. Using the `convert2failover` command is a less interactive but more complete way to configure a failover GDE Appliance node.
- On the primary GDE Appliance, the `config` command is used to specify the host name or FQDN of a failover node. The primary and failover nodes exchange GDE Appliance certificates in order for both nodes to trust each other. The command then registers the failover with the primary GDE Appliance and configures the failover for replication. Run this command on the primary only if failover certificates have already been generated and the failover is registered. The GDE Appliance CLI `config` command, when executed on the primary GDE Appliance, has the same function as the Management Console **Config Replication** button.

Syntax

The syntax for the `config` command is:

```
config server
```

where, *server* is the host name or FQDN of a primary or failover GDE Appliance.

Example

Assuming you have a primary and a failover GDE Appliance configured, the following is one way to add the failover to the primary GDE Appliance HA cluster, and initiate replication, using the GDE Appliance CLI `config` command:

1. Start a Management Console session on the target primary GDE Appliance.
2. If the failover was previously configured and registered with the primary GDE Appliance:
    a. If there are hosts explicitly assigned to the failover, reassign them to other GDE Appliances in the HA cluster.

   b. Delete the previous failover configuration and registration data from the primary database using the GDE Appliance CLI `cleanup` command or the Management Console **Cleanup Registration** button.

   c. Select the **Selected** radio button for the failover.

   d. Click the **Delete** button.

3. Add the failover node host name or FQDN back onto the primary GDE Appliance.

   This allows the failover to register with the primary GDE Appliance.

4. On the failover , enter the GDE Appliance CLI `config` command followed by the host name or FQDN of the primary GDE Appliance. For example:

   ```
   0029:ha$ config vmSSA05

   WARNING: We will now configure the Security Server on this
   machine for automated replication from an installed Primary
   Security Server. If you already configured a Primary Server, all
   its configuration will be replaced.

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

5. Enter `yes` when prompted to continue.

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

   Warning: This will overwrite all keystores on this failover
   server!

   Primary_Server=vmSSA05
   CAs_Fingerprint=BB:26:3A:21:CB:A0:3E:17:F4:F3:07:6D:21:BE:E6:C6
   :AD:87:CB:99

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

   SUCCESS: config primary server. Please verify the fingerprint
   and generate failover server certificate

   0030:ha$
   ```

6. Generate the failover certificate on the failover using the GDE Appliance CLI `gencert` command.

7. Execute **Config Replication** on the primary GDE Appliance.

The following example shows how to configure a failover that is already registered with the primary GDE Appliance from a GDE Appliance CLI session running on the primary GDE Appliance. This is the equivalent of clicking **Config Replication** in the *High Availability Servers* window. Note that you are not prompted to verify the failover node fingerprint in this example because the failover was previously configured with the primary GDE Appliance and the certificates were not changed or deleted on either GDE Appliance.

```
0004:ha$ config vmSSA06
```

```
WARNING: We will now configure the Security Server on this
machine for automated replication to an installed failover
server. We recommend that you perform a backup of this Security
Server.

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

SUCCESS: config failover server

0005:ha$
```

cleanup

The `cleanup command` removes a configured failover node from the primary GDE Appliance. This command must be run before you can regenerate the failover node certificates and re-register the failover with the primary GDE Appliance. This command has the same function as the **Cleanup Replication** button in the *High Availability Servers* window.

If failover node credentials exist when the Management Console **Config Replication** button is clicked, **Config Replication** will fail because it does not overwrite existing credentials. This command unregisters the failover and removes the failover certificates from the primary GDE Appliance. The actual failover software installation remains intact on the failover.

Syntax

```
cleanup failover
```

Example

To remove a failover GDE Appliance configuration from the primary GDE Appliance database:

1. Display the configured failover GDE Appliances in the GDE Appliance CLI.

   For example:

```
0002:ha$ show

   Failover Server:

   vmSSA05

   vmSSA06

   SUCCESS: show server list

0003:ha$
```

2. Enter the `cleanup command` and the name of the failover GDE Appliance to be deleted in the GDE Appliance CLI.

   For example:

```
0003:ha$ cleanup vmSSA06
```

   A brief message is displayed and you are prompted to proceed.

```
WARNING: We will now cleanup the replication for this
failover server.
Continue? (yes|no)[no]:
```

3. Enter "`yes`" to continue.

```
SUCCESS: cleanup failover server
0004:ha$
```

convert2primary

The `convert2primary` command is used to convert a failover node to a primary GDE Appliance. This command takes no arguments.

During conversion to a primary node, most of the database on the former failover is left intact. The former failover has working copies of the host records, GuardPoints, policies, keys, certificates, preferences, etc. that were on the original primary GDE Appliance. However, the cluster configuration from the original primary node is not carried over to the new primary GDE Appliance. After the failover becomes a primary, you have to configure a new HA cluster from scratch.

You may have to reconfigure agent installations to point to the new primary GDE Appliance if the new primary will administer the same HA configuration in which it was a former failover node. That is, you are using a failover to replace a dead primary GDE Appliance in the same HA cluster.

NOTE: A failover node must be a configured and operational failover GDE Appliance before it can be converted to a primary. A primary can be converted to a failover right out of the box or right after installing the GDE Appliance software.

If a primary GDE Appliance fails, and there is no recent backup to restore the GDE Appliance, you can recover by following these steps:

- If not already offline, take the primary GDE Appliance offline.
- Take a failover node offline.
- Convert the failover to a primary.
- If converting a primary to a failover, add the host name or FQDN of the soon-to-be failover to the new primary GDE Appliance HA configuration.
- If converting the old primary to a failover, convert the old primary to a failover now.
- Configure replication between the primary and failover nodes and wait until after the two have synchronized databases.

Syntax

The syntax for the `convert2primary` command is:

```
convert2primary
```

Example

To convert a failover GDE Appliance to a primary:

1. If the failover node is part of a functioning HA cluster:

    a. Start a Management Console on the current primary GDE Appliance.

    b. Take the failover out of service.

    c. Delete the failover record from the HA configuration.

2. Start a GDE Appliance CLI session on the soon-to-be primary GDE Appliance.
3. Type the GDE Appliance CLI `convert2primary` command.

    ```
    0001:ha$ convert2primary

    WARNING: We will now convert this failover server to primary
    server.

    This may take several minutes.

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

4. Enter `yes` to continue.

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

    SUCCESS: convert server to primary server. the server is
    restarted.

    0002:ha$
    ```

5. Start a Manager Console session on the new primary GDE Appliance.
6. Configure a new HA cluster.

convert2failover

NOTE: To avoid database corruption, you must do a cleanup replication for every registered failover on the primary GDE Appliance before converting the primary to a failover.

The `convert2failover` command is used to convert a primary GDE Appliance to a failover. It is also used after upgrading a failover to wipe the contents of the failover database. You must empty the database of an updated failover GDE Appliance before replacing it in the HA cluster to ensure accurate and complete synchronization with the primary. This command takes no arguments.

Back up the primary node before converting it to a failover. During conversion to a failover , the database on the former primary GDE Appliance is wiped and reconfigured with the database of a new primary. The former primary database no longer exists.

The `convert2failover` command does the following steps:

1. Converts the database from a primary schema to a failover schema. Most of the time required to perform `convert2failover` command is spent on this step. There is no GDE Appliance CLI command equivalent for this step.
2. Specifies the primary GDE Appliance. The GDE Appliance CLI command equivalent of this step is "`config`".
3. The failover node registers with the primary GDE Appliance. Most of unsuccessful registration attempts occur on this step. The GDE Appliance CLI command equivalent is "`gencert`".

You may need to reconfigure agent installations to point to the correct primary GDE Appliance after converting the former primary to a failover node. If an agent cannot access a GDE Appliance, it will try the next GDE Appliance in its configuration. The agent will continue to operate, the GDE Appliance will still evaluate access requests, and the GDE Appliance will still provide keys. However, the agent configuration cannot be modified because the agent is still registered to the former primary GDE Appliance. The new primary cannot administer the agent until after the agent registers with the new primary node.

During the conversion process you will be prompted to enter the primary host name or FQDN, the administrator name and password, and information with which to generate user credentials.

The `convert2failover` command generates a detailed record of the database manipulation and reconstruction that occurred as a result of the conversion process. This log is accessible by clicking **Download Logs** under the **Log** tab in the Management Console.

Syntax

The syntax for the `convert2failover` command is:

```
convert2failover
```

Example

To convert a primary to a failover:

1. If the primary GDE Appliance is part of a functioning HA cluster:

   a. Back up the primary.

   b. Take the primary out of service.

   c. Install and configure a new primary for the other failover nodes in the HA cluster.
2. Add the host name or FQDN of the soon-to-be failover to the HA configuration of a different primary GDE Appliance.
3. Start a GDE Appliance CLI session on the soon-to-be failover.

4. Enter the GDE Appliance CLI `convert2failover` command.

   ```
   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.

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

   If the GDE Appliance is already a failover, the starting prompt is different:

   ```
   WARNING: This server is already a failover server, we will now
   convert this server to failover server again. Please make sure
   the primary server is running and has this server on its failover
   server list. This may take several minutes.

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

5. Enter `yes` to continue.
6. Enter the host name or FQDN of the primary node that is to service the new failover.

   ```
   Primary Security Server host name:vmSSA05
   ```

7. Enter the name and password of a Management Console administrator of type System or All that is configured on the primary GDE Appliance.

   ```
   Primary Security Server system administrator name:alladmin

   Primary Security Server system administrator password:


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

   This Security Server host name[vmSSA06]:
   ```

8. Press the <Enter> key to use the default name for the local host.
9. Enter information to identify the certificate issuer.

   The primary GDE Appliance will be configured as the certificate issuer. The information that you provide is displayed when the signer-certificate is viewed. You are prompted to specify:

   - Your organizational unit, which is frequently a department or group name
   - Organization name, which is frequently the company name
   - City or locality in which the organization is located
   - State or province in which the organization is located
   - The country in which the organization is located

10. Compare the CA fingerprint displayed in the Management Console *Dashboard* window on the primary GDE Appliance with the fingerprint displayed by the GDE Appliance CLI `convert2failover` command.
11. Check the *High Availability Servers* window on the primary GDE Appliance for the new failover.

show

When executed on the primary GDE Appliance, the `show` command displays all the failovers that are configured on that primary GDE Appliance. All the failovers are listed, regardless if they are registered or not. When executed on a failover node, the `show` command displays the primary GDE Appliance configured for that failover and the CA signer fingerprint.

Syntax

```
show
```

Example

To list configured failovers, execute the `show` command on the primary GDE Appliance:

```
0014:ha$ show

Failover Server:

vmlinux04_RH5

vmlinux05_RH5

SUCCESS: show server list

0015:ha$
```

To list the primary GDE Appliance and the CA signer certificate, execute the `show` command on a failover node:

```
0044:ha$ show

Primary_Server=vmSSA05
CAs_Fingerprint=98:9C:FE:2E:D2:A0:FC:C3:7C:7A:9F:4D:32:18:C1:31
:8A:CE:2D:A2

SUCCESS: show server

0045:ha$
```

User Category Commands

The `user` category enables you to add, modify, delete, and display GDE Appliance CLI administrators. When setting up a new appliance, access the appliance or system through the GDE Appliance CLI and do basic appliance configuration, like IP address and host name. After the appliance or system is setup, you can run the Management Console to configure policies, keys, and GuardPoints.

CLI administrators are system users, and are not related to the administrators configured and displayed in the Management Console. GDE Appliance CLI administrators configure the appliance network, configure High Availability, and do general appliance administrative tasks. A GDE Appliance CLI administrator cannot log into the Management Console and a Management Console administrator cannot log into the GDE Appliance CLI.

The `user` category supports the following commands:

Table 30: GDE Appliance CLI user category commands

`add`	Adds a new CLI administrator.
`delete`	Deletes a CLI administrator.
`modify`	Changes a CLI administrator password.
`show`	Lists all configured CLI administrators.

add

The `add` command enables you to add new GDE Appliance CLI administrators.

CLI administrators are system administrators and are not related to the administrators configured and displayed in the Management Console or to the HSM administrator. Administrators created in the Management Console are placed in the GDE Appliance database, and follow the strong password requirements set the Management Console *Password* window. Administrators created via the CLI are also placed in the `/etc/passwd` file on the system, and use a modified set of requirements. If the administrator already exists in `/etc/hosts` as a regular system administrator, the CLI administrator will not add the administrator to the GDE Appliance database.

The default CLI user, `cliadmin` password is `cliadmin123`. The password that you enter can be include a-z, A-Z, 0-9, and the special characters !@#$%^&*(){}[]
Other characters, such as spaces and periods, are not supported.

Password complexity is defined in the *Password* tab in the *General Preferences* window. The password may be from 8 to 31 characters long. The **Password Complexity** group of parameters set requirements for uppercase/lowercase characters, special characters, and integers in the password.

Syntax

```
new name
```

Example

```
0016:user$ new bubba
```

```
   Enter new password  : bubBa!0565
   Enter password again: bubBa!0565
   Add user SUCCESS
0017:user$ show
   user[1]: name=cliadmin
   user[2]: name=bubba
   total: 2
   Show user SUCCESS
0018:user$
```

This is an example only. The password is not actually displayed when it is entered.

If the administrator already exists as a regular system administrator, an error like the following will be returned.

```
0001:user$ show
   user[1]: name=cliadmin
   total: 1
   Show user SUCCESS
0002:user$ add bubba
   Enter new password  :
   Enter password again:
   ERROR: User name bubba already exists
0003:user$
```

Though the user bubba does not exist on the GDE Appliance, user bubba cannot be added to the database because it already exists in `/etc/passwd`. If you want to add the user to the GDE Appliance, delete that user from `/etc/passwd` and then run the GDE Appliance CLI command again.

delete

The `delete` command removes a GDE Appliance CLI administrator from the system.

Syntax

```
delete name
```

Example:

The following example deletes an administrator named bubba:

```
0010:user$ delete bubba
```

```
   Delete user SUCCESS
0011:user$
```

modify

The `modify` command is used to change a GDE Appliance CLI administrator password.

You must know the current password of the administrator to execute this command. The requirements for an acceptable password are set in the Management Console *Password* window.

The password that you enter can include a-z, A-Z, 0-9, and the special characters
!@#$%^&*(){}[]
Other characters such as spaces and periods are not supported.

Password complexity is defined in the *Password* tab in the *General Preferences* window. The password may be from 8 to 31 characters long. The **Password Complexity** group of parameters set requirements for uppercase/lowercase characters, special characters, and integers in the password.

Syntax

```
modify name passwd
```

Example

The following example changes the password of the GDE Appliance CLI administrator `bubba`.

```
0022:user$ modify bubba passwd
   Enter old password  : bubBa!0565
   Enter new password  : 0957#buBba
   Enter password again: 0957#buBba
   Modify user SUCCESS
0023:user$
```

This is an example only. The password is not displayed when it is entered.

show

The `show` command displays configured GDE Appliance CLI administrators.

Syntax

```
show
```

Example

The following example displays information about all currently configured GDE Appliance CLI administrators on the GDE Appliance.

```
0017:user$ show
   user[1]: name=cliadmin
   user[2]: name=bubba
   total: 2
   Show user SUCCESS
0018:user$
```

Part V: Other Administrators

Personnel doing the initial GDE Appliance setup and configuration using the CLI can also be thought of as administrators. They may include any of the following job titles and are system users with login accounts. Note that different companies will have different titles for the roles and responsibilities (and may combine two or more) for these personnel.

Although they may temporarily be granted access to the GDE Appliance through the CLI, they will not have access to the GDE Appliance Management Console unless they have been granted permission as one of the types of GDE Appliance Administrators.

The following personnel will occasionally have need to access and work with the CLI with limited permissions:

- “System Administrators”
- “Data Center Administrators”
- “Database Administrators”
- “Network Administrators”
- “Security Administrators”
- “Web Administrators”
- “Storage Administrators”
- “Computer Operators and Lab Technicians”

Other Data Center Administrative Roles

25

System Administrators

A system administrator is responsible for the upkeep, configuration, and reliable operation of computer systems in a data center. Some system administrators have access to the data on the machines that they administer; however, they don't need this access and it is a security liability.

Data Center Administrators

Data center administrators set up, run, and maintain data centers, and are responsible for the day-to-day operation and interoperability of the sometimes large and complex data centers.

Database Administrators

Database administrators (DBA) maintain a database system, and are responsible for the integrity of the data and the efficiency and performance of the system.

Network Administrators

Network administrators maintain network infrastructure such as hubs, bridges, switches, and routers, and diagnose problems with these or with the behavior of network-attached computers.

Security Administrators

Security administrators are specialists in computer and network security, including the administration of security devices such as firewalls, as well as consulting on general security measures. Security administrators may be part of a company's loss prevention team or as members of a separate group in a company's data center. A specific security administrator (or security administrators) in an organization may or may not have GDE Appliance administrator privileges depending on the organization's separation of duties policies.

Web Administrators

Web administrators maintain web server services (such as Apache or IIS) that allow for internal or external access to web sites. Tasks include managing multiple sites, administering security, and configuring components and software. Web administrator responsibilities may also include software change management.

Storage Administrators

Storage (SAN) Administrators create, provision, add, or remove storage to/from computer systems. Storage can be attached local to the system or from a Storage Area Network (SAN) or Network Attached Storage (NAS). Storage administrators also create file systems from newly added storage.

Computer Operators and Lab Technicians

Computer operators and lab technicians do routine maintenance and upkeep, such as changing backup tapes or replacing failed drives in a RAID. Such tasks usually require physical presence in the room with the computer; and while less skilled than system administrator tasks, require a similar level of trust, since the operator has access to possibly sensitive data.

GLOSSARY

G

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 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.

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 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.

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 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.

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.