Vormetric Data Security Manager

Release Notes for Vormetric Data Security Manager (DSM)

Release 6, Version 6.0

Date: February 21, 2018

Document Version History

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

Table 1: Documentation Changes

Documentation Version	Date	Changes
Version 1	01/09/2017	6.0 G.A release.
Version 2	03/24/2017	Updated resolved issues with SRV-16247
Version 3	2/21/2018	Separated VTE and VAE/VKM compatibility tables for clarity

New Features

The DSM v6.0 release introduces the following new features:

- **Remote HSM Management**—Remote HSM management for the V6100 hardware appliance provides operational simplicity and efficiency. With the introduction of this feature, administrators do not have to be physically present in the data center to administer the DSM, smart cards can be presented remotely from a laptop or PC. See the *DSM Installation and Configuration Guide* for details about this feature.
- **Live Data Transformation (LDT)**—the Live Data Transformation feature enables encryption and rekeying of GuardPoint data without blocking user or application access to that data. This feature allows users to define policies with key selection rules that specify transformation

keys, and can schedule when to run LDT processes. See the *DSM Administrators Guide* for details about this feature.

- **Docker Support**—DSM administrators can now create GuardPoints on Docker images and containers via the Management Console. In addition to data encryption, the DSM also provides Docker container level access control and container level audit logging. See the *DSM Administrators Guide* for details about this feature.
- **Concise Logging**—the Concise Logging feature allows DSM administrators to limit the number of messages that are generated by the VTE agent on a host and sent to the DSM. Concise logging lets you focus on actionable messages such as warnings or errors, eliminates repetitive messages, and improves DSM performance. See the *VTE Installation and Configuration Guide* and the *DSM Administrators Guide* for details about this feature.
- **KMIP High Availability**—The DSM supports high availability (HA) deployment for KMIP clients. KMIP keys can be read from a failover DSM in an HA configuration. See the *DSM Administrators Guide* for details about this feature.

Improvements

- **Policy Import/Export**—the Policy Import/Export feature has been enhanced to only export those resource sets, user sets, process sets, time sets, and action sets that are used by the policy being exported. See the *DSM Administrators Guide* for details about this feature.
- **DSM RESTful API**—The DSM RESTful API has been updated to support searching for hosts by description and searching for GuardPoints by guard path.

Resolved Issues

- (SRV-13117) The following error displayed when trying to edit an existing key or create a new key with ‘Stored on Server’ option selected; “Key Refreshing Period is between 1 and 10080 inclusively.”

  This issue is now resolved and any edits or new keys created with the ‘Stored on Server’ option selected are saved without any error messages.
- (SRV-13864) - File ownership belongs non-existent user groups

  Certain files used by the DSM were owned by non-existent user groups creating a security concern.

  This issue has now been resolved and file ownership belongs to existing user groups.

- (SRV-14224) - Changes to permissions on the directory /home causes errors with certain operations

  Changing permissions on the directory /home caused errors when performing certain on the GDE appliance. This issue has been resolved and users are warned not to make any configuration changes on the system where the GDE appliance is installed, this warning is in the installer and in the documentation.

- (SRV-14408) The DSM RESTful API did not allow searching for hosts by description.

  The DSM RESTful API has been enhanced, and a new endpoint is now available to provide this functionality.

- (SRV-14413) Large number of host update requests generated by one-way communication agents caused replication failure.

  The failure occurred when a large number of host status update requests were being generated by the agents in a one-way communication configuration and the primary DSM was replicating these host status updates to the secondary DSMs.

  This issue is now resolved and the status of one-way communication enabled hosts is not replicated to the failover DSM. Updated host information will no longer be available from the failover node. High latency failover nodes that fall behind for more than 7 days, stop replicating and need to be reconfigured. You need to run the Cleanup Replication, convert2failover, and Config Replication utilities.

- (SRV-14416) The DSM RESTful API did not allow searching for GuardPoints by guard paths.

  The DSM RESTful API has been enhanced and a new endpoint is now available to provide this functionality.

- (SRV-14568) DSM GUI: Insecure caching behavior on the Switch Domains page

  The HTTP Cache-Control header and Pragma header were incorrectly set for the Switch Domains page on the DSM Management Console GUI. This resulted in the page, which contained user information, being cached by web browsers, causing a potential security vulnerability.

  This issue is now resolved so that browsers no longer cache the page.

- (SRV-14247) After converting a failover DSM to a primary DSM, the KMIP server needed to be restarted manually.

  This issue has now been resolved and the KMIP server on a failover DSM restarts automatically after the DSM is converted to a primary server.

- (SRV-14254) The high availability convert2failover command fails on a V6100 appliance during certificate generation, if process aborted mid-way.

  If the convert2failover command on a V6100 appliance is aborted mid-process, say due to insufficient smart cards, the HSM gets stuck in an Uninitialized state and convert2failover fails. This has been resolved and convert2failover is successful even after interrupting HSM initialization. A warning message is displayed to the effect that users should ensure that they have a set of smart cards available for the procedure to continue, and the HSM initialization process can be resumed.

- (SRV-14554) Failover DSM tries to perform auto backup and fails

  A primary DSM with auto backup configured was converted to a failover. The failover DSM continued to have the auto backup configuration and kept trying to run the task and failed.

  This issue has been resolved by removing auto backup setting when convert2failover is run.

- (SRV-14549) Host re-registration, altering license type, or attempted removal of particular hosts results in licensing error

  Issue with updating license on a host that was upgraded from a 4.4.1 agent to a 5.2.4 agent. That host previously had a DB2 agent license. Since this agent is no longer supported, only the FS agent is visible in the GUI. Attempts to re-register the host triggered a licensing error message.

  This has been resolved and licenses for older supported agents no longer trigger a licensing error.

- (SRV-14716) Special character ‘%’ not allowed for resource set name.

  Using the special character % for a resource set name triggered a ‘file name illegal’ error message. This issue has been resolved and the ‘%’ character is allowed.

- (SRV-14740) Wrong CA fingerprint shown in CLI when show command is run from HA when suiteb mode is enabled.

  This issue has been resolved, the correct CA fingerprint is displayed.

- (SRV-14880) Shared secret validity period can be set by a user

  The shared secret validity period used to be restricted to selectable options: 1 day, 1 week or 1 month. This has been changed, users can now select the an expiry date for the shared secret.

- (SRV-14925) The DSM did not allow short hostnames that started with a number

  This hotfix resolves the issue. The DSM now allows adding of hosts configured with short hostnames that begin with a number.

- (SRV-15249) Importing a KMIP certificate fails when client hostname is greater than 54 characters.

  This issue has been resolved. The client hostname can be less than or equal to 255 characters.

- (SRV-15269) In a DSM high availability configuration, KMIP keys were not retrievable from the failover DSM.

  The issue is now resolved. KMIP clients can retrieve keys from a failover DSM.

- (SRV-15310) Browser page does not refresh after a DSM Restore operation

  This has been resolved, after selecting the backup file and clicking and clicking OK to start the restore operation, the following message is displayed, "The browser may need manual refresh if it did not refresh itself after 30 minutes".

- (SRV-15321) Recover from SSH session termination during gencert process

Aborting the ‘gencert’ process midway by e.g., terminating a putty session abruptly, prevents the ‘gencert’ process from restoring the master key from a backup file, after the original master key has been deleted, but before a new master key has been created. A ‘genca’ command was run to access the web console, but then most pages, which contained encrypted data, returned an error since the original master key was deleted.

This issue has been resolved, terminating an SSH session midway through the ‘gencert’ process does not trigger this error.

- (SRV-16247) Upgrade from v5.3.1 to v6.0 fails on a DSM v5800 (non-HSM) appliance

  This issue has now been resolved and the upgrade is successful.

Known Issues

- (SRV-9268) - DSM does not return key information in KMIP response payload.

  The KMIP specification supports a partial name structure for key names, however Vormetric DSM does not, and therefore when the key name value does not match the value in the KMIP table, the query fails.

  There is no workaround for this issue as partial key names are not supported.

- (SRV-15082) - Failover nodes display as red on the primary HA page until synchronization is complete.

  HA replication status for failover DSM nodes is displayed as red while they are waiting to catch up with the primary DSM.

- (SRV-15269) - DSM high availability with KMIP is now supported however, there is currently no UI support for this feature.

  You can configure high availability (HA) for a DSM with KMIP clients in the same way that you configure HA but, you need to restart the failover DSM node after replication between the primary and failover node is complete so that the KMIP clients can read relevant data from the failover node.

- (SRV-15542) - Failover DSM node must be restarted when replication is complete.

  In a DSM HA configuration with KMIP, the failover DSM node must be restarted once replication is complete to ensure that the KMIP client can read the data from the failover node. To restart the server;

1. Start a CLI session on the failover node, and restart the server as follows:

2. At the CLI prompt, type the following;

```
0001:vormetric$ system
0002:system$ server restart
```

3. Confirm the restart when prompted to do so.

- (SRV-15374) - Bringing down a DSM IP link configured with an IPv6 address, removes that address.

  When an IPv6 configured DSM Ethernet interface link is brought down using the CLI command

  ```
  ip link set {eth0|eth1} down
  ```

  the IPv6 address is lost. You will need to reconfigure the IPv6 address for that Ethernet interface when you bring it back up.

- (SRV-15592) Cannot use a custom IPMI Web SSL port.

  The IPMI remote console cannot launch the Java application for the remote console if the web port is changed from the default 443 to a custom value.

  To fix this issue: In addition to changing the web port from the IPMI console Configuration settings, you must also edit the .jnlp file that launches the Java console.

1. In the IPMI management console, click **Configuration > Port**
2. Change the Web SSL port from 443 and click **Save**. You will lose connectivity to the IPMI console when you change the port number. Enter the URL to log in again with the new port number as; https://<*IP address or host name*>:<*Port number*>
3. Navigate to **Remote Control > Console Redirection** and click **Launch Console**. Download the resulting .jnlp file. You need to edit the web port information in this .jnlp file. The first line in the file that contains the URL, needs to be edited to change the default port from 443 to the new port number.
4. Save the file and then double-click the .jnlp file to launch the remote Java console.

Upgrade to Release 6, Version 6.0

DSM software version 5.3.1 is the minimum supported version that can be upgraded to DSM software version 6.0. Refer to the *DSM Installation and Configuration Guide* for details about how to upgrade your software.

Vormetric recommends that you backup your DSM configuration *before* you upgrade your DSM software

DSM 6.0 Browser Support

The following browsers are supported:

- Internet Explorer 10, 11
- Firefox

- Chrome

DSM and Agent Compatibility

DSM version 6.0 supports VTE version 5.2.2 onwards and

DSM and VTE Compatibility

The following table shows compatibility between the DSM software versions and VTE (FS) versions:

Table 2: DSM and Agent software compatibility

DSM SW Version	Agent Version				
	5.2.2	5.2.3	5.2.4	5.2.5	6.0
5.2.3	Compatible	Compatible	Compatible	Compatible	Compatible
5.3.0	Compatible	Compatible	Compatible	Compatible	Compatible
5.3.1	Compatible	Compatible	Compatible	Compatible	Compatible
6.0	Compatible	Compatible	Compatible	Compatible	Compatible

NOTE: If a 64-bit database is installed, you must install the 64-bit key agent. Installing the 32-bit key agent with 64-bit database is not supported.

DSM and VAE/VKM Compatibility

The following table shows compatibility between the DSM and VAE/VKM agent versions.

Table 3: DSM and VAE/VKM Compatibility

DSM SW Version	Agent Version		
	5.2.3	5.2.4	5.2.5
5.2.3	Compatible	Compatible	Compatible
5.3.0	Compatible	Compatible	Compatible
5.3.1	Compatible	Compatible	Compatible
6.0	Compatible	Compatible	Compatible

DSM and KMIP agent software version compatibility

The following table shows compatibility between the DSM software versions and KMIP protocol versions.

Table 4: DSM Software and KMIP support

DSM SW Version	KMIP Protocol Version Supported		
	1.0	1.1	1.2
5.2.3	Compatible	Compatible	Compatible
5.3.0	Compatible	Compatible	Compatible
5.3.1	Compatible	Compatible	Compatible
6.0	Compatible	Compatible	Compatible

How to Get Help

For support and troubleshooting issues:

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

For Vormetric Sales:

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

Notices and License

Vormetric Data Security Platform
Vormetric Data Security Manager 6.0
Release Notes v1