TREND MICRO™

TippingPoint™

Security Management System (SMS)

H4/H4 XL Appliance Guide

Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that the Security Management System collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Legal Notice

Publication: November 2021

Getting started

The Security Management System (SMS) H4 and H4 XL appliance is the latest hardware platform. It includes servers from the Dell PowerEdge family of servers and the HPE ProLiant Gen-10 family of servers:

- **H4 Servers –** Both the Dell PowerEdge R640 and the HPE DL360 Gen-10 SMS H4 rack servers are deployed with two 800 GB drives arranged in a RAID 1 (mirrored) configuration for a total of 800 GB available storage.
- **H4 XL Servers –** Both the Dell PowerEdge R640 and the HPE DL360 Gen-10 SMS H4 XL rack servers are deployed with six 800 GB drives arranged in a RAID 1+0 (mirrored with stripe) configuration for a total of 2.4 TB available storage.

This document includes configuration and feature information about the 800 GB SSD SAS 2.5-inch drive that ships with each Security Management System (SMS) H4 and H4 XL appliance. It is intended for users who install, administer, and troubleshoot servers and storage systems.

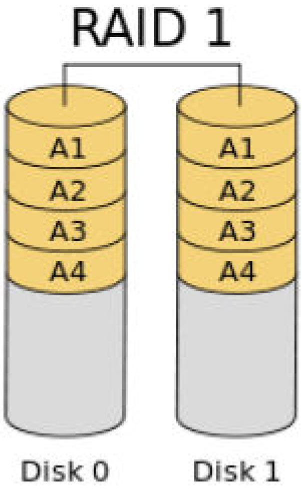
For comprehensive installation information, refer to the Read Me First.

Features	SMS H4	SMS H4 XL
Models	Dell PowerEdge R640 H4 (TPNN0334) HPE DL360 Gen-10 H4 (TPNN0364)	Dell PowerEdge R640 H4 XL (TPNN0335) HPE DL360 Gen-10 H4 XL (TPNN0365)
Physical Characteristics	**Form factor**: Rack (1 U) **Height**: 42.8 mm (1.69”) **Width***: *Dell*: 482.0 mm (18.98”) *HPE*: 434.59 mm (17.11") **Depth***: *Dell*: 743.97 mm (29.29”) *HPE*: 706.88 mm (27.83") **Weight**: *Dell*: 21.9 kg (48.3 lbs) *HPE*: 16.8 kg (37 lbs)	
Memory and Storage	64 GB RAM 800 GB storage (2 x 800 GB disks, RAID 1)	96 GB RAM 2.4 TB storage (6 x 800 GB, RAID 1+0)
AC Power Support	100 ~ 240 VAC, 50 ~ 60 Hz	
Power Supply	*Dell*: Dual 495 W *HPE*: Dual 500 W	*Dell*: Dual 750 W *HPE*: Dual 800 W
	(1+1 redundant, hot-swappable)	
Remote Management Support	*Dell*: Dell iDRAC9 Enterprise *HPE*: HPE iLO 5 Advanced	
Dell PowerEdge R640 LED indicators	Refer to the Dell EMC PowerEdge R640 Installation and Service Manual	

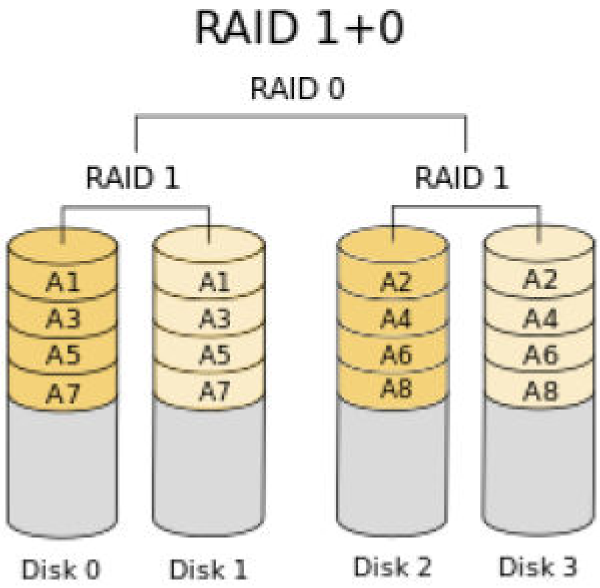
Features	**SMS H4**	**SMS H4 XL**
HPE DL360 Gen-10 LED indicators	Refer to the HPE ProLiant DL360 Gen10 Server - LED Indicators	
*****Note:** Dimensions include bezel.		

RAID levels

RAID 1 consists of an exact copy (or mirror) of a set of data on two or more disks; a classic RAID 1 mirrored pair contains two disks. This layout is useful when “read performance” or reliability is more important than the resulting data storage capacity; such an array can only be as big as the smallest member disk.



RAID 1+0, also called RAID 10, combines disk mirroring and disk striping to protect data. A RAID 10 configuration requires a minimum of four disks and stripes data across mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved. If two disks in the same mirrored pair fail, all data will be lost because there is no parity in the striped sets.



Identifying drive status for Dell PowerEdge R640 servers

To identify drive status according to the Dell PowerEdge R640 LEDs, refer to:

- Dell EMC PowerEdge R640 Installation and Service Manual
- Dell Enterprise HDD : What is the meaning of LED on Physical Drives (PD) ?

Identifying drive status for HPE DL360 Gen-10 servers

To identify drive status according to the HPE DL360 Gen-10 LEDs, refer to:

- *Hot-plug drive LED definitions* at HPE ProLiant DL360 Gen10 Server - LED Indicators
- *uFF drive components and LEDs* at HPE ProLiant DL360 Gen10 Server - LED Indicators

How do I know if a drive has failed?

- Refer to the drive status LED information for your server.
- If the SMS server is rebooted, a POST message lists failed drives when the system restarts, as long as the controller detects at least one functional drive.
- For Dell servers, access the *Dell iDRAC* interface to view drive status.
- For HPE servers, access the HPE iLO 5 Advanced interface to view drive status.

Effects of a hard drive failure on logical drives

When a drive fails, all logical drives that are in the same array are affected. Each logical drive in an array might be using a different fault-tolerance method, so each logical drive can be affected differently.

- The SMS H4 with RAID 1 will continue to function if one of the drives in the mirrored set fails. Just return to manufacturing (RMA) the failed drive for replacement to re-establish the mirror. If both drives should fail, call customer support to request an RMA for the appliance.
- The SMS H4 XL with RAID 1+0 will continue to function even if three of the six drives fail, provided they are not all from the same mirror set. Just RMA the failed drives and replace to re-establish the mirror.

Replacing drives

The most common reason for replacing a drive is that it has failed.

If you replace a failed drive that belongs to a fault-tolerant configuration while the system power is on, all drive activity in the array pauses for 1 or 2 seconds while the new drive is initializing. When the drive is ready, data recovery to the replacement drive begins automatically.

If you replace a drive belonging to a fault-tolerant configuration while the system power is off, a POST message is displayed when the system is next powered up. This message prompts you to start automatic data recovery. If you do not enable automatic data recovery, the logical volume remains in a ready-to-recover condition, and the same POST message is displayed whenever the system is restarted.

Automatic data recovery (rebuild)

When you replace a drive in an array, the controller uses the fault-tolerance information on the remaining drives in the array to reconstruct the missing data (the data that was originally on the replaced drive) and then writes the data to the replacement drive. This process is called *automatic data recovery* or *rebuild*. If fault tolerance is compromised, the controller cannot reconstruct the data, and the data is likely lost permanently.

If another drive in the array fails while fault tolerance is unavailable during rebuild, a fatal system error can occur, and all data on the array can be lost. However, failure of another drive does not always lead to a fatal system error in the following exceptional cases:

- Failure after activation of a spare drive
- Failure of a drive that is not mirrored to any other failed drives in either the RAID 1 or RAID 1+0 configurations.

A change in the drive status LED should indicate when automatic data recovery has finished.

If the drive status LED on the replacement drive changes to flashing or solid amber, the rebuild process has terminated abnormally.

Time required for a rebuild

The time required for a rebuild varies, depending on several factors:

- Priority that the rebuild is given over normal I/O operations

- Amount of I/O activity during the rebuild operation
- Average bandwidth capability (MBps) of the drives
- Availability of drive cache
- Brand, model, and age of the drives
- Amount of unused capacity on the drives
- Strip size of the logical volume

⚠ **CAUTION!**

Because data rebuild time ranges vary, the system could be unprotected against drive failure for an extended period during array recovery. When possible, perform rebuild operations only during periods of minimal system activity, or otherwise with the system offline.

Abnormal termination of a rebuild

If the activity LED on the replacement drive permanently ceases to be illuminated even while other drives in the array are active, the rebuild process has terminated abnormally. The following table indicates the three possible causes of abnormal termination of a rebuild.

OBSERVATION	CAUSE OF REBUILD TERMINATION
None of the drives in the array have an illuminated amber drive status LED.	One of the drives in the array has experienced an uncorrectable read error.
The replacement drive has an illuminated amber drive status LED.	The replacement drive has failed.
One of the other drives in the array has an illuminated amber drive status LED.	The drive with the illuminated amber LED has now failed.

Dell iDRAC

The Integrated Dell Remote Access Controller (iDRAC) is designed to make Dell PowerEdge server administrators more productive, and to improve the overall availability of Dell servers. iDRAC alerts administrators to server issues, helps them perform remote server management, and reduces the need for physical access to the server.

iDRAC with Lifecycle Controller technology is part of a larger data center solution that helps keep business critical applications and workloads available always. The technology enables administrators to deploy, monitor, manage, configure, update, troubleshoot, and remediate Dell servers from any location, and without the use of agents. It accomplishes this regardless of operating system or hypervisor presence or state.

Learn more about iDRAC remote management:

- Integrated Dell Remote Access Controller (iDRAC)
- Integrated Dell Remote Access Controller 9 User Guide

How should iDRAC connect to the network?

Typically, you connect iDRAC to the network through one of the following:

- A *corporate network* that both the NIC and the iDRAC port are connected to. This connection enables access to iDRAC from anywhere on the network and reduces the amount of networking hardware and infrastructure required to support iDRAC. However, on a corporate network, traffic can hinder iDRAC performance.
- A *dedicated management network* with the iDRAC port on a separate network. A separate network improves performance and security because you can physically control which workstations are connected to the network. A separate network also provides redundant access to the server if a hardware failure occurs on the corporate network. In this configuration, iDRAC cannot be accessed directly from the corporate network.

How will iDRAC acquire an IP address?

To access iDRAC after connecting it to the network, the iDRAC management processor must acquire an IP address and subnet mask by using either a dynamic or static process.

- A *dynamic IP address* is set by default. iDRAC obtains the IP address and subnet mask from DNS or DHCP servers. This method is the simplest.
- A *static IP address* can be used if DNS or DHCP servers are not available on the network. Static IP address can be configured by pressing <F2> during Power-on Self-test (POST) and selecting iDRAC settings from the System Setup Main Menu page.

Authentication mechanisms

You can use Active Directory to define iDRAC user access using two methods:

- *Standard schema solution*, which uses Microsoft's default Active Directory group objects only.
- *Extended schema solution*, which has customized Active Directory objects. All the access control objects are maintained in Active Directory. It provides maximum flexibility to configure user access on different iDRACs with varying privilege levels.

HPE iLO 5

HPE DL360 Gen-10 servers have the iLO 5 remote server management processor embedded on the system boards. This processor enables administrators to monitor and control servers from remote locations.

Learn more about HPE iLO 5.

Contact TippingPoint Support

TippingPoint Support is available 24 hours per day and seven days per week by telephone, as well as online using the Business Support Portal support request.

Note

For a complete list of phone numbers, visit our Support Contact information page.

Online support request are managed using the Trend Micro TippingPoint Business Support Portal (BSP). The BSP facilitates case management for the Trend Micro TippingPoint customer community. You can access the Business Support Portal at the following URLs:

- Global: https://success.trendmicro.com/sign-in
- Japan: https://success.trendmicro.com/jp/sign-in

Review the BSP registration and usage instructions by clicking here.