TippingPoint™
Security Management System (SMS)

H3 and H3 XL ProLiant Gen9 RAID 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

Getting started

This document includes feature, installation, and configuration information about the HP SmartDrive shipping with the Security Management System (SMS) H3 and H3 XL appliance. It is intended for the person who installs, administers, and troubleshoots servers and storage systems.

What's new with the SMS

The Security management System (SMS) is now being delivered on a new hardware platform which are part of the HP ProLiant DL Gen9 family of servers:

* The SMS H3 is based on the HP-DL360-G9 rack server and is deployed with two 600 GB drives arranged in a RAID 1 (mirrored) configuration for a total of 600 GB available storage.

* The SMS H3 XL (shown in the following image) is based on the HP-DL380-G9 rack servers and is deployed with six 600 GB drives arranged in a RAID 1+0 (mirrored with stripe) configuration for a total of 1.8 TB available storage.
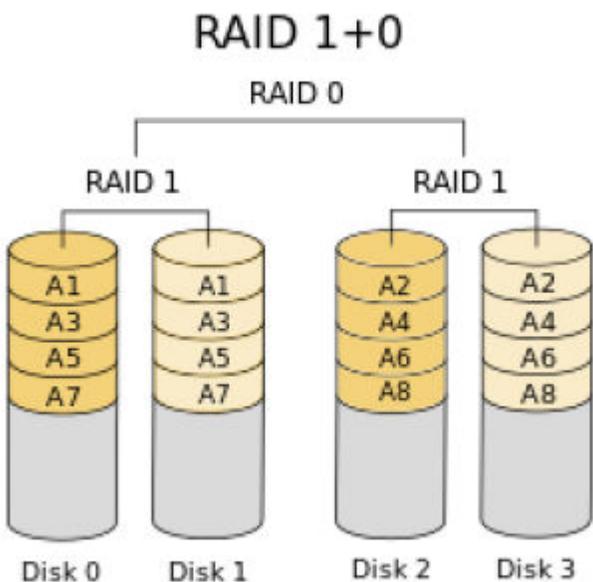
RAID levels

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

A1 A1
A2 A2
A3 A3
A4 A4

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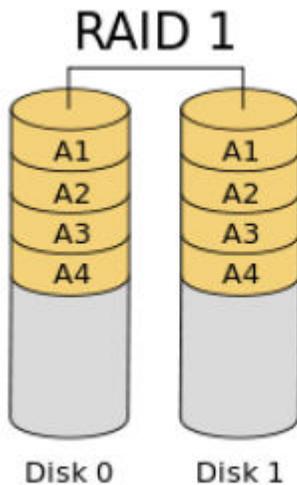
RAID 1+0, also called RAID 10, combines disk mirroring and disk striping to protect data. A RAID 10 configuration requires a minimum of four disks and stripes data across mirrored pairs. As long as one disk in each mirrored pair is functional, data can be retrieved. If two disks in the same mirrored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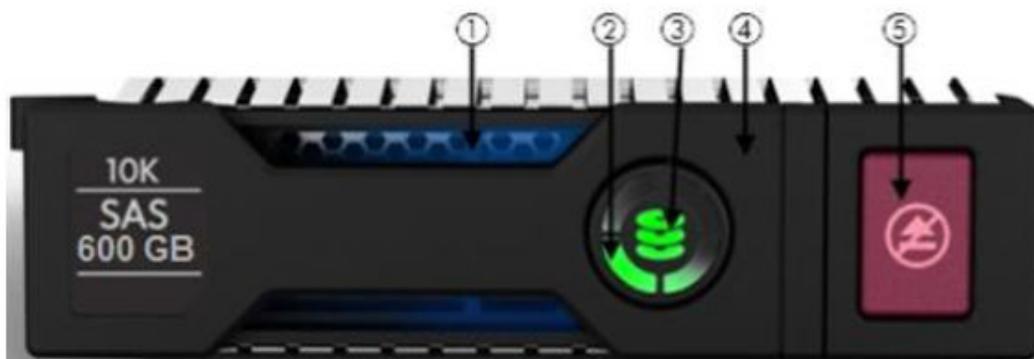
RAID 1+0

RAID 0

RAID 1   RAID 1

A1 A1   A2 A2
A3 A3   A4 A4
A5 A5   A6 A6
A7 A7   A8 A8

Disk 0   Disk 1   Disk 2   Disk 3

TippingPoint Security Management System specifications

Features	Security Management System H3 (TPNN0044)	Security Management System H3 XL (TPNN0046)
Physical Characteristics		
Dimensions	43.47 x 69.85 x 4.32 cm (17.11 x 27.5 x 1.7 in.)	44.55 x 67.94 x 8.73 cm (17.54 x 26.75 x 3.44 in.)
Form Factor	1 U rack mount	2 U rack mount
Weight	16.78 kg (36.99 lbs)	23.6 kg (51.5 lbs)
Memory and Storage	64 GB RAM 600 GB storage (2 x 600 GB disks, RAID 1)	96 GB RAM 1.8 TB storage (6 x 600 GB, RAID 1+0)
Environment		
Operating Temperature	10 to 35°C (50 to 95°F)	
Electrical Characteristics		
Voltage	100 to 120 VAC, 200 to 240 VAC	
Frequency	50/60 Hz	
Current	2.78 A (100 V) to 1.15 A (240 V)	4.58 A (100 V) to 1.88 A (240 V)
Power Supply	Redundant 500W (Hot swappable)	Redundant 800W (hot swappable)
Capacity	200 million historical events	600 million historical events
Lights-Out Management Support	HPE iLO 4 support with dedicated 10/100/1000BASE-T RJ45 iLO port	

Identifying the status of an HP SmartDrive

HP SmartDrives are the latest HP drive technology and are only supported on the new Gen9 SMS servers. Identify an HP SmartDrive by its carrier, shown in the following illustration. When a drive is configured as a part of an array and connected to a powered-up controller, the drive LEDs indicate the condition of the drive.

Callout number	LED	Status	Definition
1	Locate* Backlight	Solid blue	The drive is being identified by a host application.
		Flashing blue	The drive carrier firmware is being updated or requires an update.
2	Activity Ring	Rotating green	Drive activity.
		Off	No drive activity.
3	Hard Drive Indicator	Off	The drive is not configured by a RAID controller.
		Solid green	The drive is a member of one or more logical drives.
		Flashing green	The drive is rebuilding or performing a RAID migration, strip size migration, capacity expansion, or logical drive extension, or it is erasing.
		Flashing amber/green	The drive is a member of one or more logical drives and predicts the drive will fail.
		Flashing amber	The drive is not configured and predicts the drive will fail.
		Solid amber	The drive has failed.
4	Do not remove	Solid white	Do not remove the drive. Removing the drive causes one or more of the logical drives to fail.
		Off	Removing the drive does not cause a logical drive to fail.
5	Handle	Pull	Drive cage handle comes out when eject button is pressed.
*Note: The blue Locate LED is behind the release lever and is visible when illuminated.			

How do I know if a drive has failed?

- If the drive status LED illuminates solid amber, flashing amber or flashing amber/green

- If the SMS server is rebooted, a POST message lists failed drives when the system is restarted, as long as the controller detects at least one functional drive.

- Access the iLO 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 H3 with RAID 1 will continue to function if one of the drives in the mirrored set fails. Just RMA the failed drive and replace to re-establish the mirror. If both drives should fail, call customer support to request an RMA for the appliance.

*   The SMS H3 XL with RAID 1+0 will continue to function even if all three drives from the mirror set fail. 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.

For systems that support hot-pluggable drives, 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 press the F1 key 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.

When automatic data recovery has finished, the drive status LED changes from flashing green to solid green.

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 (you can change the priority setting by using HP SSA)

*   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 from 200 to 520 GB/h, the system could be unprotected against drive failure for an extended period during data recovery or a drive capacity upgrade. When possible, perform rebuild operations only during periods of minimal system activity.

HP Integrated Lights Out (iLO)

The HP iLO subsystem is a standard component of HP ProLiant servers that simplifies initial server setup, server health monitoring, power and thermal optimization, and remote server administration. The HP iLO subsystem includes an intelligent microprocessor, secure memory, and a dedicated network interface. This design makes HP iLO independent of the host server and its operating system.

HP iLO enables and manages the Active Health System and also features Agentless Management. HP iLO monitors all key internal subsystems. When HP iLO is enabled, SNMP alerts are sent directly by HP iLO, regardless of the host operating system or whether a host operating system is installed. Embedded remote support software is available on HP ProLiant Gen8 and Gen9 servers with iLO 4, regardless of the operating system software and without installing OS agents on the server.

How should iLO connect to the network?

Typically, iLO is connected to the network through one of the following:

- A *corporate network* that both the NIC and the iLO port are connected to. This connection enables access to iLO from anywhere on the network and reduces the amount of networking hardware and infrastructure required to support iLO. However, on a corporate network, traffic can hinder iLO performance.

- A *dedicated management network* with the iLO 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, iLO cannot be accessed directly from the corporate network.

How will iLO acquire an IP address?

To access iLO after connecting it to the network, the iLO 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. iLO obtains the IP address and subnet mask from DNS or DHCP servers. This method is the simplest.

- A *static IP address* is used if DNS or DHCP servers are not available on the network. A static IP address can be configured by using iLO ROM-Based Setup Utility (RBSU) or the iLO 4 Configuration Utility.

What access security is required, and what user accounts and privileges are needed?

iLO provides several options to control user access. Use one of the following methods to prevent unauthorized access:

- **Local accounts** – Up to 12 user accounts can be stored in iLO. This is ideal for small environments, such as labs and small-sized or medium-sized businesses.

- **Directory services** – Use the corporate directory to manage iLO user access. This is ideal for environments with a large number of users. If you plan to use directory services, consider enabling at least one local administrator account for alternate access.

Additional resources

Server remote management with HPE Integrated Lights Out (iLO)

HPE iLO 4 User Guide

Smart Array Controller for Gen9 Servers