RSA NETWITNESS® SUITE

Series 5 Appliances Setup Guide

Contact Information

RSA Link at https://community.rsa.com contains a knowledgebase that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.

License Agreement

This software and the associated documentation are proprietary and confidential to EMC, are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by EMC.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on RSA Link. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Contents

About this Document

This document is a step-by-step guide for installing the RSA Series 5 (S5) NetWitness Suite appliances (hosts) and connecting them to your network.

The hardware setup instructions in this document are for hardware only; they do not apply to a specific release of NetWitness Suite software. After completing the hardware setup, please continue setup and configuration of the NetWitness Suite appliances as described in the NetWitness Suite online documentation at RSA Link (https://community.rsa.com/docs/DOC-40370).

This document is not a replacement for the original manufacturer's documentation; it contains information specifically for the NetWitness Suite appliances.

> **Note:** When viewing a printed guide, be aware that a newer version of the guide may be available online at RSA Link in RSA NetWitness Suite under Hardware Setup Guides: https://community.rsa.com/community/products/netwitness/hardware-setup-guides

S5 R630 Appliances Hardware Description

All but one of the RSA Series 5 (S5) NetWitness Suite appliances are based on the Dell PowerEdge R630 chassis. The exception is the Hybrid appliance, which is based on the Dell PowerEdge R730xd chassis. The Series 5 appliances are shipped with NetWitness Suite software installed.

This topic describes the Series 5 appliances that are based on the Dell PowerEdge R630 chassis:

- Decoder and Log Decoder

- Concentrator

- Broker

- Archiver

- NetWitness Server

- Malware Analysis

- Event Stream Analysis (ESA)

Except for the ESA appliance, all Dell PowerEdge R630-based appliances have the same components and physical specifications. The ESA appliance has additional hard drives, memory, and a different CPU. NetWitness Suite ESA Appliance Specifications provides details.

The initial setup of a Series 5 appliance in your network involves these steps:

1. Review site requirements and safety information in the *Deployment Guide* for your NetWitness Suite software version.

2. Mount or place the appliance hardware securely in accordance with your site requirements.

3. Connect the appliance (host) to your network: Connect the Appliance to the Network

4. Finish the appliance (host) setup in one of the following sections, depending on your NetWitness Suite version:

    - Additional 10.6 and Earlier Installation Tasks

    - Additional 11.0 and Later Installation Tasks

> **Caution:** To avoid damaging NetWitness servers and appliances, remove them from the rack and dismantle the rack before transporting them to another location. Follow the recommendations of the server manufacturer and rack manufacturer for packaging, transport, and installation.
> RSA does not support re-shipping of racked servers. The customer assumes all risk and liability for transporting NetWitness servers and appliances mounted in a rack.

Package Contents

Verify the contents of the packing box to ensure that you have received all items necessary to install and configure the appliance.

- Series 5 NetWitness Suite appliance (Decoder, Concentrator, Broker, Archiver, NetWitness Server, Malware Analysis, or ESA)

- Static Ready Rails (1 set)

- Left Rail Adapter for EMC deep rack

- RSA Bezel (1) - Keys are taped to the bezel.

- Power Cord (2)

- Dell Product Information Guide book (1)

- RSA Documentation Folder (1)

- RSA EULA (1)

Customer Supplied Materials

To complete the setup procedure, you will need:

- One Ethernet network cable

- Cables to connect a monitor or KVM adapter to the VGA port and a keyboard or KVM adapter to the USB port

- Standard tools

Front View of the Series 5 Appliances (Except Hybrid)
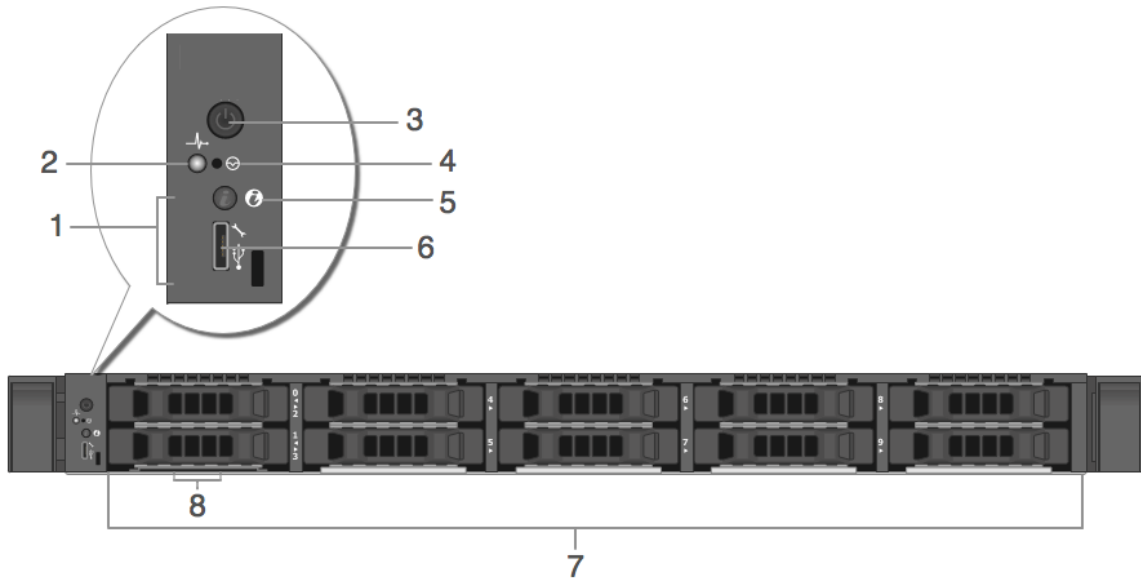
Key	Description
1	Diagnostic indicator location. The diagnostic indicators appear and show the status if there are any errors.
2	System health indicator. This blinks amber when a system fault is detected.
3	Power On/Off
4	Recessed non-maskable interrupt (NMI) button
5	System identification button
6	Micro USB port / iDRAC Direct
7	Ten 2.5-inch hard drive bays (field replaceable). The specifications below identify the number and types of hard drives installed on the appliances.
8	Information tag location

Rear View of the Series 5 Appliances (Except Hybrid)

Key	Description
1	System identification button
2	LP PCIe expansion slots 1 and 2. The 10G Decoder may use an LP PCIe slot for an optional Intel X540 Optical network interface card.
3	PERC H830 RAID controller. It is shown in LP PCIe slot 3, but it may be installed in another LP PCIe slot. The PERC H830 is the the RAID controller for the storage expansion DAC. It requires a cable with a Mini-SAS port to connect to the DAC.
4	System identification connector
5	iDRAC port
6	RS232 Serial Port (serial connection to laptop via DB9 or serial server)
7	VGA Video Port (monitor)
8	USB Ports (Keyboard, mouse, USB thumb drive, and so on)
9	10GBASE-T ethernet ports em3 and em4
10	Primary Network 1000BASE-T management port: em1
11	Secondary Network 1000BASE-T port: em2
12	Hot Swappable Power Supply 1 and 2 (field replaceable)

Note: The PERC H830 RAID controller requires a cable with a Mini-SAS port to connect to the DAC.

Series 5 Appliance Specifications (Except Hybrid and ESA)

Item	Description
Form Factor	1U, full depth
Weight (approximate)	18.4 kg (40.5 lbs)
Dimensions (approximate)	With bezel: 482.43 mm (18.99 in) [w] x 808.59 mm (31.83 in) [d] x 42.80 mm (1.69 in) [h] Without bezel: 482.43 mm (18.99 in) [w] x 776.16 mm (30.56 in) [d] x 42.80 mm (1.69 in) [h]
Power supplies	Dual, Hot-plug, Redundant Power Supply (1+1), 1100W
Processors	2 * E5-2667v3
RAM	16 * 8GB 2133MT/s RDIMMs (128GB)
Hard drives (field replaceable)	2 * 1TB 7.2K RPM NLSAS 6Gbps 2.5 in Hot-plug Hard Drive 2 * 2TB 7.2K RPM NLSAS 12Gbps 512e 2.5 in Hot-plug Hard Drive
RAID Controller	External: PERC H830 RAID Internal: PERC H730P
Network Interface Card	Intel Ethernet X540 10Gb BT DP + I350 1Gb BT DP Network Daughter Card

NetWitness Suite ESA Appliance Specifications

Item	Description
Form Factor	1U, full depth
Weight (approximate)	18.4 kg (40.5 lbs)

Item	Description
Dimensions (approximate)	With bezel: 482.43 mm (18.99 in) [w] x 808.59 mm (31.83 in) [d] x 42.80 mm (1.69 in) [h] Without bezel: 482.43 mm (18.99 in) [w] x 776.16 mm (30.56 in) [d] x 42.80 mm (1.69 in) [h]
Power supplies	Dual, Hot-plug, Redundant Power Supply (1+1), 1100W
Processors	2 * E5-2680v3
RAM	8 * 32GB 2133MT/s RDIMMs (256GB)
Hard drives (field replaceable)	2 * 1TB 7.2K RPM NLSAS 6Gbps 2.5 in Hot-plug Hard Drive 4 * 2TB 7.2K RPM NLSAS 12Gbps 512e 2.5 in Hot-plug Hard Drive
RAID Controller	External: PERC H830 RAID Internal: PERC H730P
Network Interface Card	Intel Ethernet X540 10Gb BT DP + I350 1Gb BT DP Network Daughter Card

Caution: Opening the appliance chassis will void the warranty unless you are specifically instructed to do so by RSA Customer Care. The hard drives and power supplies are replaceable in the field by a qualified technician.

Install a Deep-Rack Adapter for an R630 Appliance

Note: This procedure is only applicable if you are installing the S5 R630 appliance in the EMC Titan D Ultra Rack.

When installing the S5 R630 appliance into the EMC Titan D Ultra Rack, a 1U deep-rack adapter is required. Follow this procedure to install a new bracket on the server rails.

1. Locate the alternate rail bracket in the accessory box in the R630 appliance carton.

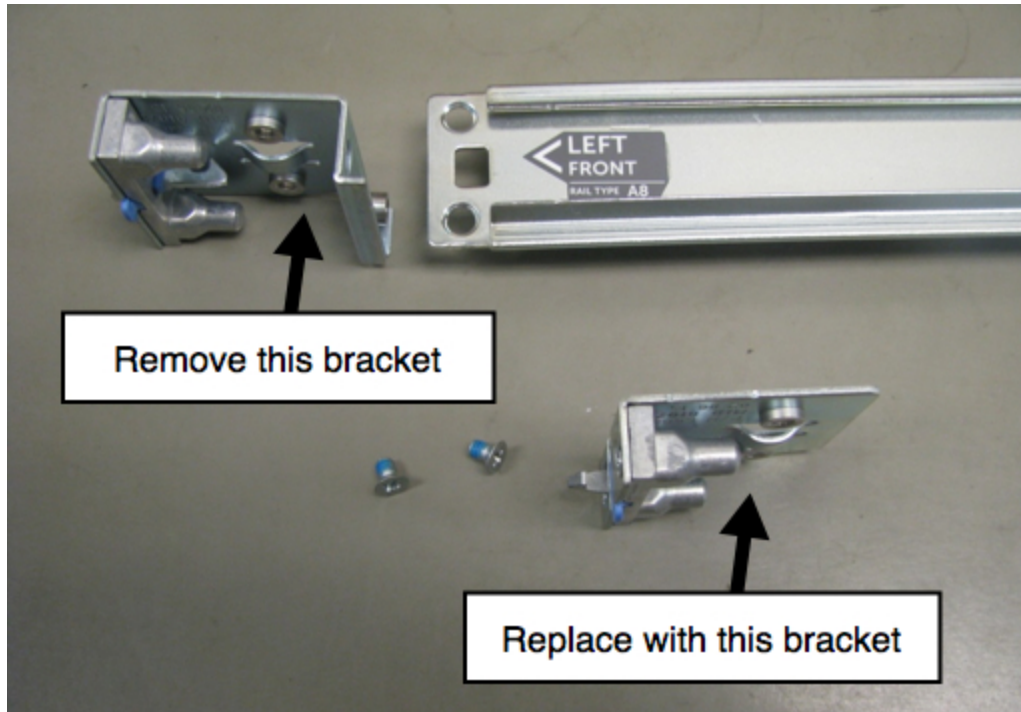2. Remove the left side rail from the rail carton.
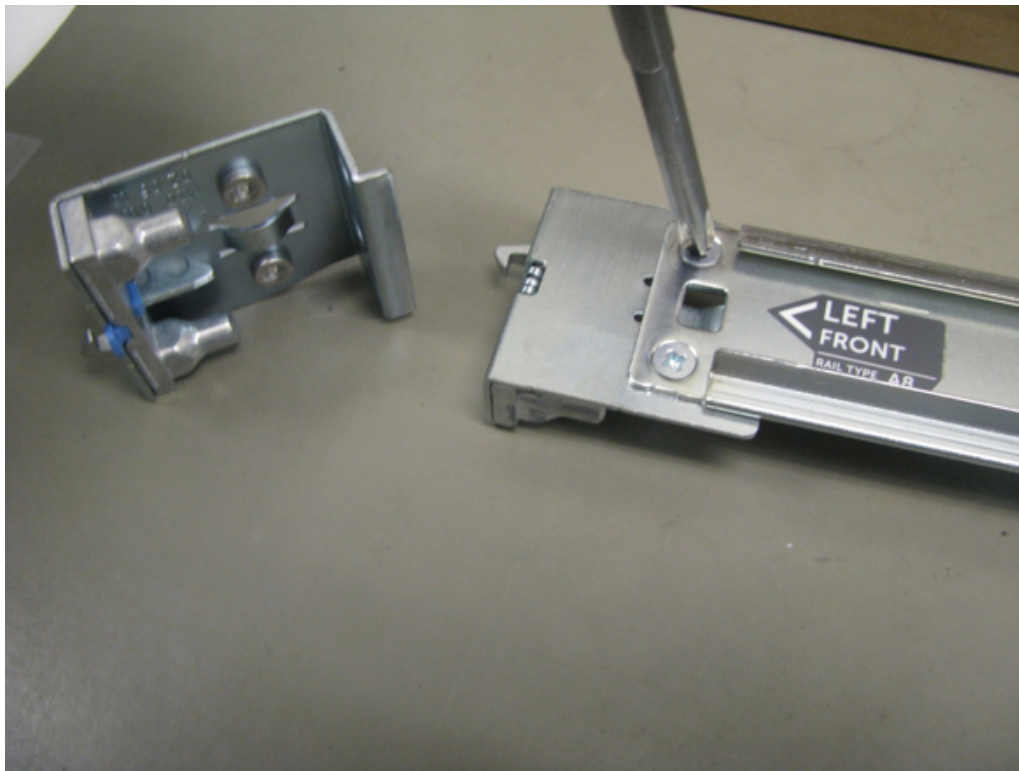

   Each rail is marked.

3. Use a Phillips screwdriver to remove the two mounting screws.

4. Remove the bracket and replace it with the new bracket.

5. Re-use the screws to fasten the new bracket in place.

The rail is now ready for the R630 appliance installation.

S5 R730xd Hybrid Appliance Hardware Description

The RSA NetWitness Suite Series 5 Hybrid appliance is based on the Dell PowerEdge R730xd chassis. The RSA NetWitness Suite Series 5 Hybrid appliance is shipped with NetWitness Suite Hybrid appliance software installed. Hybrid appliance software includes Concentrator and Decoder (log or packet, not both).

The initial setup of a Series 5 appliance in your network involves these steps:

1. Review site requirements and safety information in the *Deployment Guide* for your NetWitness Suite software version.

2. Mount or place the appliance hardware securely in accordance with your site requirements.

3. Connect the appliance (host) to your network: Connect the Appliance to the Network

4. Finish the appliance (host) setup in one of the following sections, depending on your NetWitness Suite version:

   - Additional 10.6 and Earlier Installation Tasks

   - Additional 11.0 and Later Installation Tasks

> **Caution:** To avoid damaging NetWitness servers and appliances, remove them from the rack and dismantle the rack before transporting them to another location. Follow the recommendations of the server manufacturer and rack manufacturer for packaging, transport, and installation.
> RSA does not support re-shipping of racked servers. The customer assumes all risk and liability for transporting NetWitness servers and appliances mounted in a rack.

Package Contents

Verify the contents of the packing box to ensure that you have received all items necessary to install and configure your Hybrid appliance.

- Series 5 Hybrid appliance

- Static Ready Rails (1 set)

- Left Rail 2U Adapter for EMC deep rack

- 2U RSA Bezel (1) - Keys are taped to the bezel

- Power Cord (2)

- Dell Product Information Guide book (1)

- RSA Documentation Folder (1)

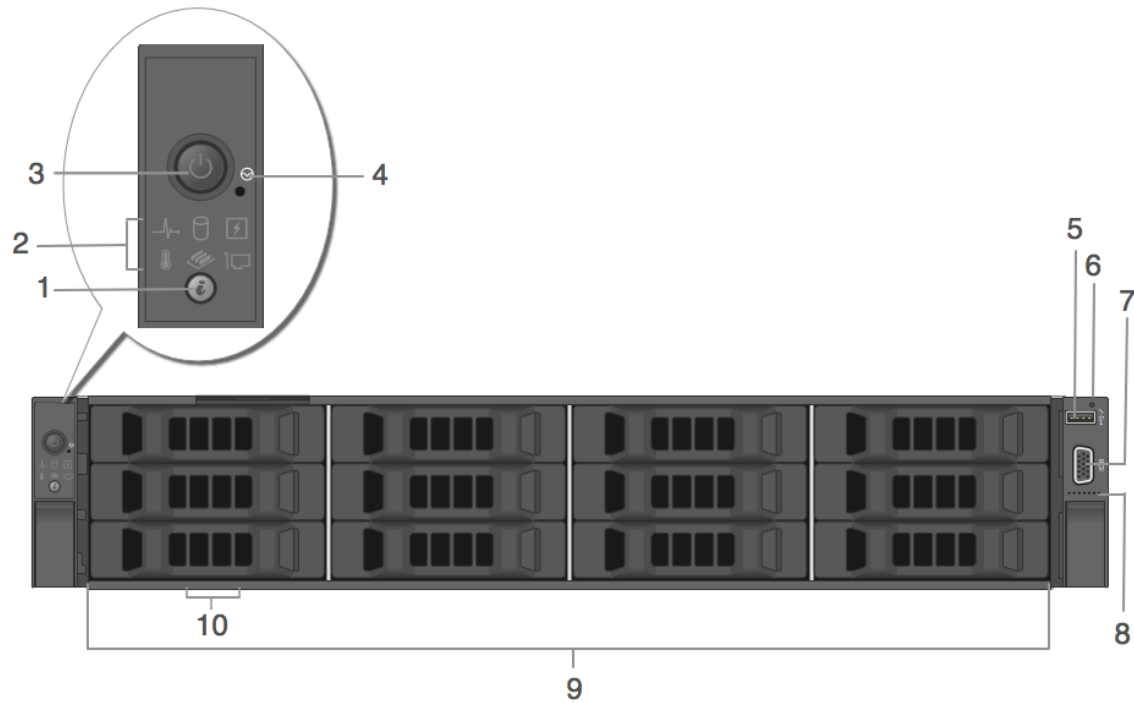- RSA EULA (1)

Customer Supplied Materials

To complete the setup procedure, you will need:

- One Ethernet network cable

- Cables to connect a monitor or KVM adapter to the VGA port and a keyboard or KVM adapter to the USB port

- Standard tools

Front View of the NetWitness Suite Hybrid Appliance

Key	Description
1	System identification button
2	Diagnostic indicators
3	Power On/Off
4	Recessed non-maskable interrupt (NMI) button
5	USB management port/iDRAC Direct
6	iDRAC Direct LED indicator
7	Video connector
8	Quick Sync (optional)

Key	Description
9	12 3.5-inch hard drives (HDDs) (field replaceable). The NetWitness Suite Hybrid appliance has a total of 14 disks. There are 12 HDDs on the front and 2 solid state disks (SSDs) on the back. See the appliance specifications below for additional details.
10	Information tag location

Rear View of the NetWitness Suite Hybrid Appliance
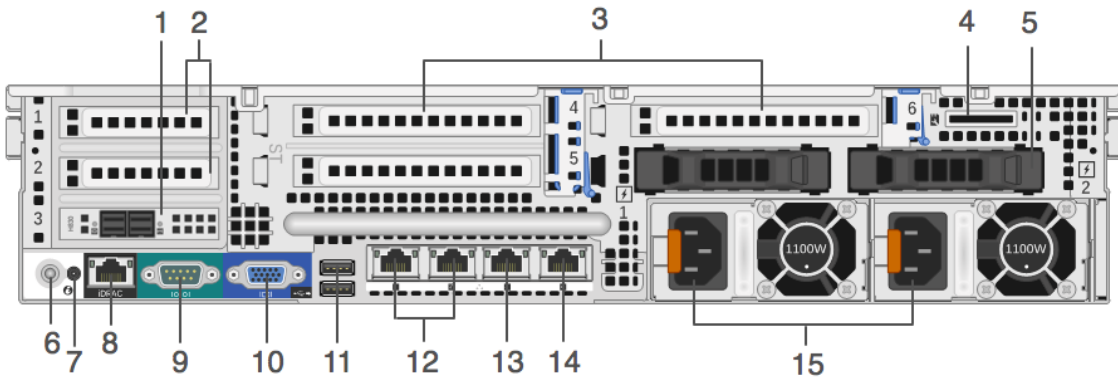
Key	Description
1	PERC H830 RAID controller. It is shown in half-height PCIe card slot 3, but it may be installed in another half-height PCIe slot. The PERC H830 is the RAID controller for the storage expansion DAC. It requires a cable with a Mini-SAS port to connect to the DAC.
2	Half-height PCIe expansion-card slots 1 and 2
3	Full-height PCIe expansion-card slots (3)
4	vFlash media card slot
5	Two 2.5 inch SSDs (hot-swappable)
6	System identification button
7	System identification connector
8	iDRAC8 Enterprise Port
9	RS232 Serial Port (serial connection to laptop via DB9 or serial server)
10	VGA Video Port (monitor)
11	USB Ports (Keyboard, mouse, USB thumb drive, and so on)
12	10GBASE-T Gigabit Ethernet Ports: em3 and em4

Key	Description
13	Primary Network 1000BASE-T Management Port: em1
14	Secondary Network 1000BASE-T Port: em2
15	Hot Swappable Power Supply 1 and 2 (field replaceable)

> **Note:** The PERC H830 RAID controller requires a cable with a Mini-SAS port to connect to the DAC.

NetWitness Suite Hybrid Appliance Specifications

Item	Description
Form Factor	2U, full depth
Weight (approximate)	36.5 kg (80.47 lb)
Dimensions (approximate)	H: 8.73 cm (3.44 in.) x W: 48.2 cm (18.98 in.) x D: 75.58 cm (29.75 in.)
Power supplies	Dual, Hot-plug, Redundant Power Supply (1+1), 1100W
Processors	2 * E5-2680v3
RAM	16 * 8GB 2133MT/s RDIMMs (128GB)
Hard drives	The NetWitness Suite Hybrid appliance has a total of 14 disks. There are 12 HDDs on the front and 2 solid state disks (SSDs) on the back. 2 * 800GB SSD (Back) 4 x 1TB 7.2K RPM NLSAS 6Gbps 8 x 6TB 7.2K RPM NLSAS 6Gbps
RAID Controller	External: PERC H830 RAID Internal: PERC H730P

Item	Description
Network Inter-face Card	Intel Ethernet X540 10Gb BT DP + I350 1Gb BT DP Network Daughter Card

> **Caution:** Opening the appliance chassis will void the warranty unless you are specifically instructed to do so by RSA Customer Care. The hard drives and power supplies are replaceable in the field by a qualified technician.

Install a Deep-Rack Adapter for an R730xd Hybrid

> **Note:** This procedure is only applicable if you are installing the S5 R730xd Hybrid appliance in the EMC Titan D Ultra Rack.

When installing the S5 R730xd Hybrid appliance into the EMC Titan D Ultra Rack, a 2U deep-rack adapter is required. Follow this procedure to install a new bracket on the server rails.

1. Locate the alternate rail bracket in the accessory box in the R730xd Hybrid appliance carton.
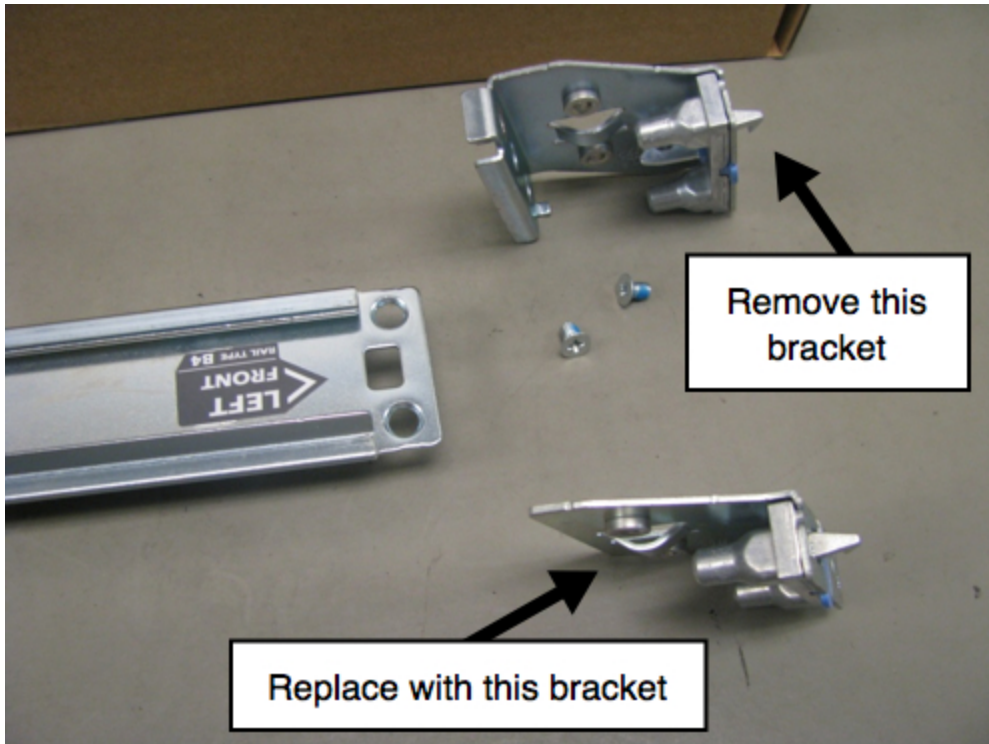

2. Remove the left side rail from the rail carton. Each rail is marked.

3. Use a Phillips screwdriver to remove the two mounting screws.

4. Remove the bracket and replace it with the new bracket.

5. Re-use the screws to fasten the new bracket in place.

The rail is now ready for the R730xd Hybrid appliance installation.

Connect the Appliance to the Network

This topic provides instructions for connecting a NetWitness Suite S5 appliance (host) to your network.

Prerequisites

For each NetWitness Suite Series 5 appliance, obtain and write the information in the following table.

| Configuration	Default	Your Appliance
Login	root	
Password	netwitness	
System IP Address	192.168.1.1*	
System Netmask	255.255.255.0*	
Default Gateway		
Primary DNS Server IP Address		
Secondary DNS Server IP		
Local Domain Name (or None)		
Unqualified Hostname	NWAPPLIANCE<xxxxxx>, where <xxxxxx> is a generated random number.*	
IP Address of NetWitness Server		

* This default applies to 10.6 and earlier.

> **Note:** Before you begin network configuration, mount or place the appliance securely in accordance with site requirements.

Configuring network parameters for an RSA NetWitness Suite S5 appliance consists of setting the default IP address, your DNS servers, the hostname, and the network clock source. To set these parameters, you connect to the appliance console using a keyboard and mouse.
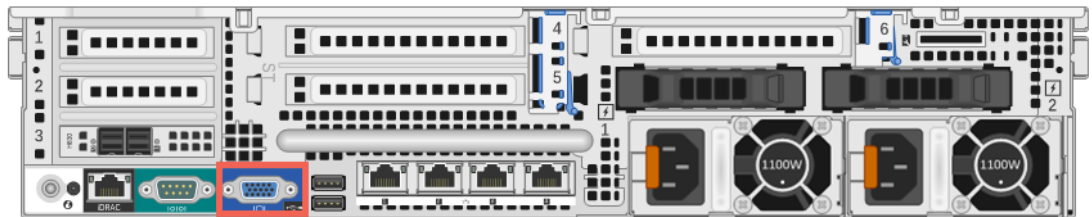
The preferred practice is to provision the NetWitness Server before configuring the other RSA NetWitness Suite appliances (hosts).

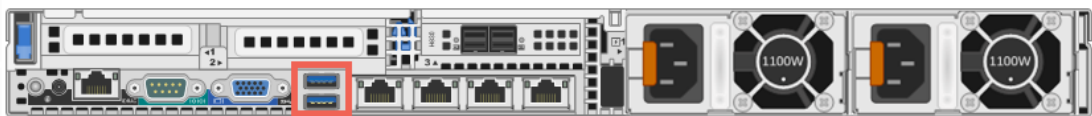# Connect to the Appliance Console

1. Connect a monitor or KVM adapter to the VGA Port on the back of the appliance.
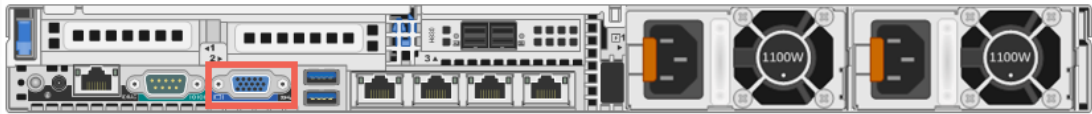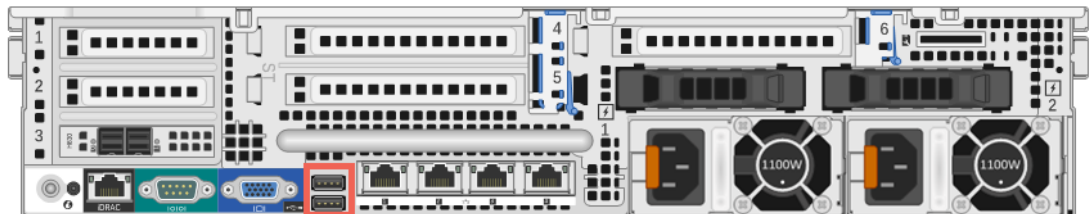
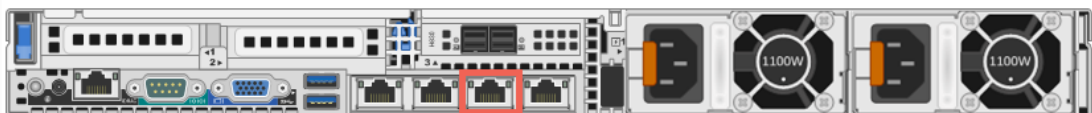The following figure shows the VGA Port location for the Hybrid appliance.

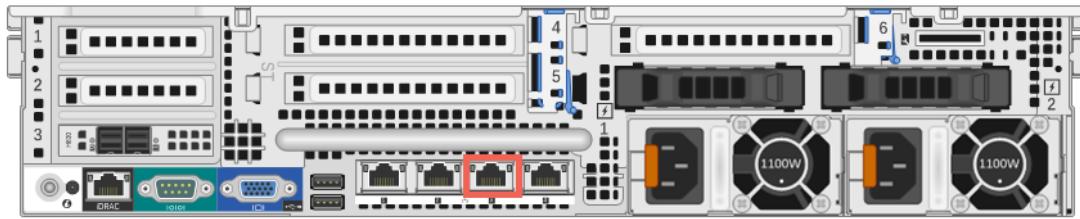2. Connect a keyboard or KVM adapter to one of the USB ports on the back of the appliance.

The following figure shows the USB port location for the Hybrid appliance.

3. Connect an Ethernet cable from the network to the em1 port on the back of the appliance.

The following figure shows the em1 port location for the Hybrid appliance.

4. Connect a power cord to each of the two power supplies on the rear of the appliance. Connect the power cords to a power source. To provide a more robust setup, connect each power supply to a different circuit.

> **Caution:** 5V standby power is active whenever the system is plugged in. To remove power from the system, you must unplug both AC power cords from the power source.

5. Power on the appliance and continue to one of the following sections, depending on your NetWitness Suite version:

   - Additional 10.6 and Earlier Installation Tasks

   - Additional 11.0 and Later Installation Tasks

Additional 10.6 and Earlier Installation Tasks

If you are on NetWitness Suite 10.6 or earlier, follow the steps below to configure the network parameters on the appliance (host) and finish the setup in NetWitness Suite.

Configure Network Parameters

1. At the login prompt, enter the default credentials to gain access to the operating system:

   `NWAPPLIANCE<xxxxxx> login:` **`root`**

   `Password:` **`netwitness`**

   > **Note:** If you do not receive the prompts for configuring network parameters, you can run `#netconfig.sh` from the command line to prompt you to enter the configuration options.

2. Enter the following information when prompted:

   a. System IP Address (or **d** for DHCP)

   b. System Netmask

   c. Default Gateway

   d. Primary DNS Server IP Address

   e. Secondary DNS Server IP (or press **Enter** for none)

   f. Local Domain Name (or press **Enter** for none)

   g. Unqualified Hostname

   Upon completion of the initial configuration, you should see a prompt that allows you to save the configuration as shown in the following figure.

```
you entered the following network parameters
IP Address: 192.168.1.20
Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
Primary DNS: 192.168.1.2
Secondary DNS: 192.168.1.3
Local Domain: SampleDomain.com
Host Name: SA-Server
--------------------------------------
enter y to confirm and save
enter q to quit without saving
enter d for don't save or ask me this
enter 1 to re-enter IP address
enter 2 to re-enter netmask
enter 3 to re-enter default gateway
enter 4 to re-enter primary DNS
enter 5 to re-enter secondary DNS
enter 6 to re-enter local domain
enter 7 to re-enter host name
enter a to re-enter all network data
--------------------------------------
?
```

3. Verify the entered information and enter y to save the configuration.

    This sets the network information and restarts the network services.

4. If your appliance is not a NetWitness Server, **wait approximately 15 seconds for a prompt** and then enter the NetWitness Server IP Address at the prompt.

5. Verify network connectivity by pinging your DNS Server.

6. Continue to the *Specify the Network Clock Source* section.

Specify the Network Clock Source

Configuring time synchronization between services and appliances is required. It is highly recommended to use an NTP time source for synchronization. Not only is time crucial for underlying communications between services, but not having appliances in synch can result in mismatched times shown during analysis of data. If the NTP server is not configured or reachable at this time, the network clock source configuration will fail, but can be done from the RSA NetWitness Suite interface later.

Best Practices

RSA recommends the following best practices:

For better data integrity, configure the NetWitness Server as the clock source for all other appliances. All appliances, including Event Stream Analysis (ESA), get their time from the NetWitness Server. Only the NetWitness Server is configured to an external NTP time source.

For the NetWitness Server appliance, use the NwConsole utility to connect to the NTP time source.

If the other appliances have NetWitness Suite 10.5.1 or later, the time is automatically set on all appliances attached to the NetWitness Server appliance. If the other appliances do not have NetWitness Suite 10.5.1 or later, set the time to point to the NetWitness Server manually.

Set Time on the NetWitness Server using the NwConsole Utility

To set the network clock source on the NetWitness Suite using the NwConsole utility:

1. At the root prompt `[root@NwAppliance~]#` enter the following command:

   NwConsole

   NwConsole starts up and the startup message with a version and date displayed:

   `RSA NetWitness Suite Console`

2. In NwConsole, enter the following command:

   login localhost:50006 <username> <password>

   The system administrator account username for NetWitness Suite is **admin** and the default password is **netwitness**.

   You are logged onto the appliance and the following message is displayed:

   `Successfully logged in as session <session #>`

3. At the localhost prompt `[localhost:50006] />` do one of the following:

   a. If you want to use your network clock source, enter the following command:

   appliance setNTP source=<NTP_server_hostname or IP_ address>

   For example: **appliance setNTP source=0.pool.ntp.org**

   b. If you want to use the appliance clock as a clock source, type: **appliance setNTP source=local**

4. When you see an output of `Success` from the command, type **exit** to log out and exit the NwConsole program.

> **Note:** If you specified an NTP clock source of local, the appliance clock serves as the clock source and the time is configured using Set Appliance Built-In Clock as described in NetWitness Suite online documentation.

Finish Appliance Setup in NetWitness Suite

To finish configuration of a Series 5 appliance, you need to log on to NetWitness Suite and use the configuration options available in the NetWitness Suite Administration module. Each type of appliance has a slight variation in configuration steps. This section provides basic information and links to online help documents to guide you through the process.

Log On to NetWitness Suite

RSA NetWitness Suite is a web-based application that you launch in a browser window. Compatible browsers include any browser that supports WebSockets, LocalStorage, and the HTML5 History API: Google Chrome, Apple Safari, Mozilla Firefox, and Internet Explorer 10 and above.

1. Type the following in your web browser:

   `https://<hostname or IP address>/login`

   Where `<hostname or IP address>` is the hostname or IP address of your NetWitness Server.

   The NetWitness Suite login screen is displayed.

2. Type your username and password, and then click **Login**.

   The system administrator account username for NetWitness Suite is **admin** and the default password is **netwitness**.

Open the Online Help

Instructions for configuring individual appliances are provided based on the software version installed on the appliance.

For NetWitness Suite 10.5 or later, read these documents: *Hosts and Services Configuration Guides* and *Licensing Guide*. A good starting point to understand the general configuration process and begin configuration is the *Hosts and Services Getting Started Guide*.

Additional 11.0 and Later Installation Tasks

If you are on NetWitness Suite 11.0 or later, go to the *Physical Host Installation Guide* and follow the steps for installing and configuring your appliance (host).

RSA Part Number: R7153A1