



BeyondTrust

U-Series Appliance 4.1 Getting Started Guide

Table of Contents

Get Started with Your U-Series Appliance	3
Overview	3
U-Series Appliance Warranty, Specifications, and Requirements	4
Perform Initial Setup of Physical U-Series Appliance	10
Perform Initial Setup of Virtual U-Series Appliance	13
Perform Initial Setup of U-Series Appliance Cloud Instance	16
Run the U-Series Appliance Deployment & Configuration Wizard	26
Update Running Instances for the Amazon U-Series Appliance Deployment	34
Connect to a Cloud Database	37

Get Started with Your U-Series Appliance

Overview

This guide is intended for experienced network security administrators who want to start using a U-Series Appliance in their network to assist with protecting their organization's computing assets. U-Series is a self-contained physical or virtual appliance that contains the operating system, the database, the BeyondTrust BeyondInsight platform, and the BeyondTrust Password Safe solution. This guide provides the necessary details to assist you in getting familiar with your appliance and getting it deployed and set up for use in your network or cloud environment.

The U-Series v20 is the virtual version of the U-Series 20 appliance and is available for VM Ware and Microsoft Hyper V hypervisors for local hosting, and also for AWS and Azure cloud marketplaces.

Both physical and virtual appliances can be deployed in your network as standalone systems or configured for high availability with or without redundancy.

High Level Deployment and Configuration Steps For U-Series Appliances

Getting started with your appliance involves an initial setup to prepare your appliance for access from a web browser in your network. Once you have completed the initial setup of your U-Series Appliance, you must run the U-Series Appliance Deployment & Configuration Wizard to complete the deployment of the appliance in your environment. High level deployment and configuration steps are outlined below.

Initial Setup to Prepare your appliance for First Time Access

- Power on the physical appliance, or download and import the virtual appliance, or launch a cloud instance
- Obtain the pre-assigned IP Address or configure a new IP address for the appliance so you can access it from a web browser

Run the U-Series Appliance Deployment & Configuration Wizard

- License Windows
- Create an Admin account
- Name the appliance
- Configure networking settings such as, IP settings, internet connection, time zone, and SMTP
- Configure your appliance for its intended use by licensing your BeyondTrust solutions, selecting a solution, selecting features for the system, setting up how to receive updates from BeyondTrust

Detailed instructions for each of the above steps are covered in subsequent sections of this guide.

U-Series Appliance Warranty, Specifications, and Requirements

Certification and Warranty Information for Physical Appliances

FCC Certification

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications.

Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

Limited Hardware U-Series Appliance Warranty

This hardware U-Series Appliance is accompanied by a three-year manufacturer's warranty based on the invoice date. (Extended warranties available on request.) The warranty covers all hardware, including internal components supplied in this shipment. The warranty does not cover additional items, such as keyboards, monitors, and mice, not included in this shipment. During the warranty period, the U-Series Appliance will be repaired or replaced at no cost under the warranty terms.

Due to continuing changes in the computer industry, if a replacement is necessary, the U-Series Appliance manufacturer reserves the right to make product substitutions of equal or greater value.

Do not ship any U-Series Appliance without first contacting BeyondTrust Technical Support to coordinate any repairs or replacements. Do not try to repair the U-Series Appliance yourself.

Please back up all data before having the U-Series Appliance serviced or repaired. Neither BeyondTrust nor the U-Series Appliance manufacturer warrants that operation of the U-Series Appliance will be uninterrupted or error-free. In no event will BeyondTrust or the U-Series Appliance manufacturer be responsible or liable for loss or integrity of any data on the U-Series Appliance or any storage media.

Warranty Invalidation

This warranty is void in the event that:

- The U-Series Appliance is damaged due to accident, abuse, misuse, problems with electrical power, modifications or servicing not authorized by BeyondTrust or the U-Series Appliance manufacturer, or failure to operate in accordance with the U-Series Appliance instructions.
- Serial tags, receiving numbers, product stickers, or manufacturer seals have been removed, altered, or tampered with.
- The U-Series Appliance is opened for any reason.
- The U-Series Appliance is damaged due to improper or inadequate packaging when returned for repair or replacement.
- The U-Series Appliance has been tampered with, such as overclocking.

Labor and services performed on items or systems that are found not to be defective may be subject to a separate charge. In addition, the U-Series Appliance manufacturer reserves the right to charge a ten percent restocking fee for items returned which are found not to be defective.


IMPORTANT!

Do not log on to the Console or Remote Desktop to the Virtual U-Series Appliance unless directed to do so by BeyondTrust Technical Support. Installing any software or changing any additional settings may void your warranty.

Physical U-Series Appliance Specifications

U-Series 20 Specifications

Specification	Description
AC Input Voltage	110 to 240 VAC
Rated Input Frequency	50 to 60Hz
Cooling	5 Standard Fans; 1 Standard 1U Heatsink.
Chassis	Chassis with up to 8, 3.5in. Hard Drives
Dimensions	1U rack-mountable server H: 1.68in. (4.28cm) (10.75in. shipping) W: 18.97in. (48.18cm) (24in. shipping) D: 26.89in. (68.30cm) (35.75in. shipping) Weight: approx 45lbs. (48lbs. shipping)
Microprocessor	Intel Xeon Silver 4112, 2.6GHz, 4-Core, 8-Thread, 8.25M Cache, Turbo, HT
Hard Drive	2 × 2TB 7.2 RPM NLAS 12Gbps 512n 2.5in Hot-plug
RAM	128GB
RAID Configuration	RAID 1
RAID Controller	PERC H730P, 2GB NV Cache
NIC	Broadcom 57416 2 Port 10Gb Base-T + 5720 2 Port 1Gb Base-T, rNDC
Power Supply	Dual, hot-plug, Redundant Power Supply (1+1), 495W
Power Cords	2 × NEMA 5-15P to C13 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m)
Rack Rails	ReadyRails™ Sliding Rails with Cable Management Arm
PCIe Riser	Risers with up to 4, x8 PCIe Slots + 2, x16 PCIe Slots
Operating System	Embedded Windows Server 2016 Standard
Database	Microsoft SQL Server 2016 Standard

U-Series 20 SQL Free

Specification	Description
AC Input Voltage	110 to 240 VAC
Rated Input Frequency	50 to 60Hz
Cooling	5 Standard Fans; 1 Standard 1U Heatsink.

Specification	Description
Chassis	Chassis with up to 8, 3.5in. Hard Drives
Dimensions	1U rack-mountable server H: 1.68in. (4.28cm) (10.75in. shipping) W: 18.97in. (48.18cm) (24in. shipping) D: 26.89in. (68.30cm) (35.75in. shipping) Weight: approx 45lbs. (48lbs. shipping)
Microprocessor	Intel Xeon Silver 4112, 2.6GHz, 4-Core, 8-Thread, 8.25M Cache, Turbo, HT
Hard Drive	2 × 2TB 7.2 RPM NLAS 12Gbps 512n 2.5in Hot-plug
RAM	128GB
RAID Configuration	RAID 1
RAID Controller	PERC H730P, 2GB NV Cache
NIC	Broadcom 57416 2 Port 10Gb Base-T + 5720 2 Port 1Gb Base-T, rNDC
Power Supply	Dual, hot-plug, Redundant Power Supply (1+1), 495W
Power Cords	2 × NEMA 5-15P to C13 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m)
Rack Rails	ReadyRails™ Sliding Rails with Cable Management Arm
PCIe Riser	Risers with up to 4, x8 PCIe Slots + 2, x16 PCIe Slots
Operating System	Embedded Windows Server 2016 Standard

Virtual U-Series Appliance Specifications

U-Series v20 and U-Series v20 SQL Free

Requirement	Description
Hard Disk	300GB
RAM	32GB <div style="border: 1px solid black; padding: 5px; background-color: #e6f2ff;">  Note: For a BeyondInsight deployment with a local SQL Server instance, the minimum requirement is 32GB. As the appliance and BeyondInsight Software versions increase, we provide more features and options which consume more RAM. 32GB of RAM is required at the minimum to support all features of the product. If you have below 32GB of RAM, you may experience slowness. </div>
OS	Microsoft Windows Server 2022 Standard
Database	Microsoft SQL Server 2019 Standard <div style="border: 1px solid black; padding: 5px; background-color: #e6f2ff;">  Note: The database information does not apply to the U-Series v20 SQL Free. The U-Series v20 SQL Free does not include a database. </div>
Form Factor	Virtual machines are available in two formats: VMware OVA (vSphere ESX 7.0), and Microsoft VHDX (VM hardware version 17, Hyper-V / Windows Server 2016)
CPU	A typical installation requires 2 CPU / 4 cores. Processor requirements may vary depending on the clock frequency of the processor, available RAM, and database size.



Note: The license included with the U-Series v20 and U-Series v20 SQL Free for Microsoft Windows Server 2022 covers up to 16 cores on the physical virtualization (host) server.

U-Series Appliance Cloud Instance Specifications

Azure

The below table lists the two recommended U-Series Appliance instances available through the Azure marketplace, along with their specifications.

Instance Type	vCPU	Memory	SSD Storage	Dedicated EBS Bandwidth (Mbps)
DS4_V2	8	28 GB	56 GB	1000
DS5_V2	16	56 GB	112 GB	2000



Note: If you use an Azure SQL Database instance instead of an appliance, you must install the following database services to support BeyondTrust Analytics & Reporting:

- Microsoft SQL Server Reporting Services
- Microsoft SQL Server Analysis Services
- Microsoft SQL Server Integration Services

Amazon

The below table lists the recommended U-Series Appliance instances available through the Amazon marketplace, along with their specifications.

Instance Size	vCPU	Memory (GiB)	Instance Storage (GiB)	EBS Bandwidth (Mbps)
m4.2xlarge	8	32GB	EBS-Only	1,000
m4.4xlarge	16	64GB	EBS-Only	2,000
m5.2xlarge	8	32GB	EBS-Only	Up to 4,750
m5.4xlarge	16	64GB	EBS-Only	4,750
m5a.2xlarge	8	32GB	EBS-Only	Up to 2,880
m5a.4xlarge	16	64GB	EBS-Only	2,880
r5.xlarge	4	32GB	EBS-Only	Up to 4,750
r5.2xlarge	8	64GB	EBS-Only	Up to 4,750
r5.4xlarge	16	128GB	EBS-Only	4,750



For more information, please see [Amazon EC2 Instance Types](https://aws.amazon.com/ec2/instance-types/) at <https://aws.amazon.com/ec2/instance-types/>.

U-Series Appliance Networking and Port Requirements

The U-Series Appliance is designed to be configured and used with a web browser. The browsers that are supported for accessing the appliance, as well as the network connections, firewall settings, and ports required for accessing the appliance are detailed below.

Client Requirements

Supported browsers:

- Microsoft Edge
- Firefox
- Google Chrome
- Safari

U-Series Appliance Requirements

- Rack Mount
- 10/100/1000MB Ethernet Connection
- TCP/IP v4



Note: TCP/IP v6 is not currently supported.

Firewall Settings

- All outgoing ports are allowed.
- Incoming ports are limited to the default Windows rules (includes allowing DCOM), plus the following:

TCP Ports

Port	Purpose	Target Program/System Resource	Initial Status
80	HTTP	System	Enabled
443	HTTPS	System	Enabled
445	SMB	System	Disabled
1433	SQL Server	sqlservr.exe	Enabled
2000	App Bus	C:\Program Files(x86)\Common Files\eye Digital Security\Application Bus\leeyeevnt.exe	Disabled
2383	SQL Analysis Services	msmdsrv.exe	Enabled
3389	RDP	C:\Windows\System32\svchost.exe	Enabled
4422	Session Monitoring SSH	C:\Program Files(x86)\eye Digital Security\Retina CS\pbsmd.exe	Enabled
4489	Session Monitoring RDP	C:\Program Files(x86)\eye Digital Security\Retina CS\pbsmd.exe	Enabled

Port	Purpose	Target Program/System Resource	Initial Status
5022	SQL Server Mirroring	Binn\sqlservr.exe	Enabled
5985	WinRM (AWS Images Only)	System; Restricted to 10.0.0.0-16	Enabled
8530	WSUS HTTP	System	Disabled
8531	WSUS HTTPS	System	Disabled
10001	Central Policy v1	C:\Program Files(x86)\eEye Digital Security\Retina CS\REMCentralPolicyService.exe	Enabled
21690	App Bus	(C:\Program Files(x86)\Common Files\eEye Digital Security\Application Bus\leeyeevnt.exe	Enabled
21690	Event Server	C:\Program Files(x86)\Common Files\eEye Digital Security\Event Server\REMEventsSvc.exe	Enabled

UDP Port

Port	Purpose	Target Program/System Resource	Initial Status
4609	Appliance Discovery	C:\Program Files(x86)\Common Files\eEye Digital Security\Scheduler\leeyeschedulervc.exe	Enabled

ICMPv4 Protocol

Port	Purpose	Target Program/System Resource	Protocol	Initial Status
Any	ICMP Type 3, Code 4- Destination Unreachable Fragmentation Needed	Any	ICMPv4	Enabled
Any	ICMP Type 8- Echo	Any	ICMPv4	Enabled

Perform Initial Setup of Physical U-Series Appliance

The below sections walk you through powering on your appliance for the first time and using the LCD display panel to access and change settings.

The physical U-Series Appliance package consists of the items listed below. Please verify all materials listed are present and free from visible damage or defects before proceeding. If any item appears to be missing or damaged, please contact BeyondTrust Technical Support.

- U-Series Appliance hardware
- Two Power Cords
- Getting Started Guide
- Rack Mount Kit

Once you have completed the initial setup of your U-Series Appliance, you must run the U-Series Appliance Deployment & Configuration Wizard to complete the deployment of the appliance in your environment.



- For physical appliance specifications, please see ["Physical U-Series Appliance Specifications" on page 5.](#)
- For steps to run the U-Series Appliance Deployment & Configuration Wizard, please see ["Run the U-Series Appliance Deployment & Configuration Wizard" on page 26.](#)

Power on the U-Series Appliance

1. Plug the power cables for the U-Series Appliance into a safe power source. The U-Series Appliance's power supplies automatically switch between 120V and 240V, as needed.
2. Plug a network cable into the network interface port.
3. Press and release the power button on the front of the U-Series Appliance. The power LED immediately to the right of the reset button illuminates, and the HDD activity LED (immediately to the right of the power LED) begins to flash. Initialization of the U-Series Appliance completes in about 60 seconds.



Note: The NIC1 and NIC2 LEDs may illuminate and show activity even when the U-Series Appliance is not powered on; therefore, it is important to check the power and HDD LEDs to confirm that the U-Series Appliance is on.

4. The LCD panel displays *Please wait*. Once the U-Series Appliance completes the powering procedures, the U-Series Appliance LCD panel displays the actions you can press to view and change settings, as detailed below. To access the settings:

LCD Panel Functionality

LCD Panel	Description
	Press the check to enter or accept the setting.
	Press the up or down arrow to navigate through the menus.

	Press the right or left arrow to access settings in the menu.
	Press the X to cancel the setting.

Perform Initial Network Configuration

The U-Series Appliance is configured to use DHCP and receives an assigned IP address. You'll need the appliance's IP address to access the appliance from a client or device within your network. You can find the IP Address using the appliance's LED display panel. From the LED panel, you can also configure the appliance to automatically update the IP address or manually configure the IP settings. Obtain or configure your appliance's IP address as follows:

Display IP Address

To display the IP address:

1. Press the check  to enter **Settings / Show IP**.
2. Press check . The IP address of the U-Series Appliance displays.

Automatically Enter IP Address

On the LCD panel, select **Config IP** with the check , then select **Auto DHCP**. The U-Series Appliance automatically updates the IP address to the DHCP protocol.

Manually Enter IP Address

On the LCD panel, select **Config IP** with the check , then select **Manual**. Enter the **IP Address, Subnet Mask, Gateway, DNS 1** and **DNS 2**.

To access your U-Series Appliance for the first time:

1. Open a browser on a device on the same network subnet as the U-Series Appliance.
2. Enter the U-Series Appliance's IP address, preceded by **https://**, for example, **https://10.10.123.456**.

Other Actions Available from the LCD Display Panel

Enable RDP

From the LCD panel, start where *U-Series 20 Ready* is displayed.

1. Press the check  to enter **Settings / Show IP**.
2. Press check . The IP address of the U-Series Appliance displays.

3. Hold both the up  and down  buttons for four seconds. Do not do anything else between the previous step and this one.

Reset Administrator Password

1. Check the **Allow LCD Panel to Reset Administrator Password** box.
2. If needed, go to the U-Series Appliance to reset the administrator password.
3. Select **Show IP** to view the IP address.
4. Hold the up  and down  buttons simultaneously on the U-Series Appliance LCD panel. A random password is generated.
5. Press the check  to accept the changed password.

On a U-Series Appliance with Windows Server 2016, you cannot reset an administrator account from the LCD panel. A locked administrator account is unlocked after 20 minutes. Try logging on again after the 20-minute timeout period. If the account remains locked, contact BeyondTrust Technical Support.

View the U-Series Appliance Version

1. On the LCD panel, select **Versions** with the check  .
2. Scroll through with the left  or right  arrows to see the version for the U-Series Appliance, BeyondInsight, Discovery Scanner, and audits.

Power Off The U-Series Appliance

You can power off the U-Series Appliance using the LCD panel. To power off, on the LCD panel, select **Power Off**. The U-Series Appliance powers off.

Hardware Notes

The integrated Dell Remote Access Controller (iDRAC) is configured to use the primary interface (LAN1). The iDRAC shares the interface with Windows. By default, iDRAC is not configured.

The U-Series Appliance has more than one adapter. If all adapters are used, the adapter chosen during scan time is determined by the route associated with it.

Perform Initial Setup of Virtual U-Series Appliance

U-Series v20 is BeyondTrust's virtual U-Series Appliance. You can download U-Series v20 VMware or Hyper-V images from the [BeyondTrust Customer Support Portal](#) and import them as virtual machines in your network. Virtual U-Series Appliances are based on Windows Server 2022.



Note: Image download speed and time may vary due to the large file sizes of these images and your internet connectivity.

The below sections walk you through importing the U-Series v20 appliance as a virtual machine in your environment and configuring it with an IP address so that you can access the appliance from a client web browser within the same network subnet.

Once you have completed the initial setup of your U-Series Appliance, you must run the U-Series Appliance Deployment & Configuration Wizard to complete the deployment of the appliance in your environment.



- For virtual machine requirements, please see "[Virtual U-Series Appliance Specifications](#)" on page 6.
- For steps to run the U-Series Appliance Deployment & Configuration Wizard, please see "[Run the U-Series Appliance Deployment & Configuration Wizard](#)" on page 26.

Deploy / Import the Virtual Machine



IMPORTANT!

We recommend that you do NOT join the Virtual U-Series Appliance to a domain. Local policy is set on the appliance and if the appliance belongs to a domain, it is possible that domain policy is pushed to the appliance overwriting the local policy. This has the potential to negatively impact appliance hardening and usage. If joining the appliance to a domain is a requirement, please contact BeyondTrust Services for assistance.

Before you can configure the Virtual U-Series Appliance, you must deploy / import the virtual image package as a virtual machine into your environment using the following steps.

Deploy the Virtual Machine into VMware using vSphere Client

1. In vSphere Client, select **File > Deploy OVF Template**.
2. In the **Deploy OVF Template** window, click **Browse**.
3. Browse to the folder containing the .ova package you had downloaded, select it and click **Open**.
4. Click **Next** and complete the wizard to deploy the virtual machine image.

Import the Virtual Machine into Microsoft Hyper-V using Hyper-V Manager



Note: The following procedure is a guide only. For more detailed information about Hyper-V features, please refer to [Hyper-V product documentation](#).

1. In **Hyper-V Manager**, select the host machine, then select **Action > Import Virtual Machine**. If the **Before You Begin** page appears, click **Next**. Otherwise, go to step 4.
2. On the **Locate Folder** page, browse to the folder containing the image, and select the name.
3. Click the **Select Folder** button at the bottom.

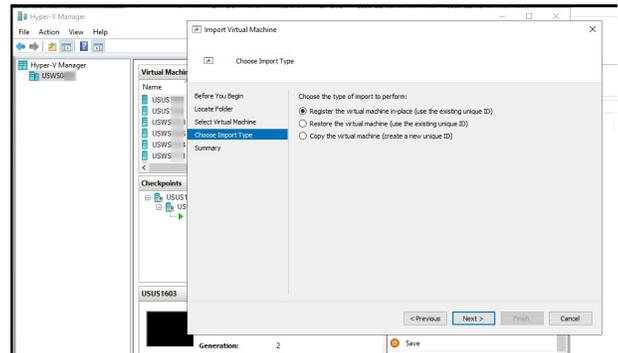


Note: The folder you want to select contains three other folders (*Virtual Machine*, *Virtual Hard Drive*, *Snapshots*). Do not import the VHD directly.

4. On the **Select Virtual Machine** page, verify that the machine appears in the list and click **Next**.
5. On the **Choose Import Type** page, select **Register the virtual machine in-place (use the existing unique ID)** and click **Next**.



Note: If the virtual machine is already registered with Hyper-V, you must delete it before the import works.



6. The default behavior is to import the files to the default Hyper-V folders set by your server configuration. If there are any issues with the import, additional steps will appear.

For example, a Virtual U-Series Appliance is configured to use a minimum of 32GB of RAM. If your server does not support this much RAM or have enough RAM available, the message *Memory virtual quantity above maximum* appears.

7. Review the import settings.
8. Click **Finish** to import the U-Series Appliance.



Note: After importing the image, wait 30 minutes before continuing setup or otherwise interacting with the virtual appliance. This allows time for initialization scripts to run. Interrupting this process can cause the deployment to fail.

Configure the U-Series v20's IP Address



Note: If you already know the IP for the appliance and it is accessible, the below steps are not required. The IP is configured when deploying the appliance using the U-Series Appliance Deployment & Configuration Wizard. Please see "[Run Part 1: New Appliance Deployment Using the Deployment Wizard](#)" on page 27.

You can use the following account to set your IP address.

Account Name: btadmin

Password: ch@ngeM3now#!#!



Note: *If you completed the Deployment & Configuration Wizard, you have already changed the password. If the image has just been deployed, please allow for at least 10 minutes to pass before logging in, to allow post deployment scripts to complete.*

1. Log on to the virtual machine using the **btadmin** account.
2. Double-click the **Local Area Connection** on the desktop.
3. Click the **Properties** button.
4. From the list, select **Internet Protocol Version 4**.
5. Click the **Properties** button.
6. Enter the IP address and DNS server fields, as needed.

Perform Initial Setup of U-Series Appliance Cloud Instance

The below sections provide steps to get you started with running a U-Series Appliance cloud instance, available from the AWS and Azure MarketPlaces.

Once you have completed the initial setup of your U-Series Appliance, you must run the U-Series Appliance Deployment & Configuration Wizard to complete the deployment of the appliance in your environment.



- For cloud instance requirements, please see ["Virtual U-Series Appliance Specifications" on page 6](#).
- For steps to run the U-Series Appliance Deployment & Configuration Wizard, please see ["Run the U-Series Appliance Deployment & Configuration Wizard" on page 26](#).

Launch an Instance from AWS Marketplace

Log in to AWS Marketplace, and search for BeyondTrust or BeyondInsight. From the BeyondTrust marketplace website, click **Continue** and follow the below steps for using the **1-Click Launch** or the **Manual Launch** options to launch an Amazon Machine Image (AMI) instance in the EC2 Console.

Use the 1-Click Launch Option

1. Click the **1-Click Launch** tab.
2. Configure the following settings:
 - **Version:** Select the desired UVM version from the list.
 - **Region:** Select the applicable region from the list.
 - **EC2 Instance Type:** Select **m4.2xlarge** or **m4.4xlarge** from the list.
 - **VPC Settings:** Select a Virtual Private Cloud (VPC) and Subnet from the lists.
 - **Security Group:** Select the default BeyondTrust security group from the list.
 - Select the **Key Pair**.



Note: The key pair is required to retrieve Windows passwords for your instance. Please see [How do I retrieve my Windows administrator password after launching an instance?](https://aws.amazon.com/premiumsupport/knowledge-center/retrieve-windows-admin-password/) at <https://aws.amazon.com/premiumsupport/knowledge-center/retrieve-windows-admin-password/>.

3. Click **Launch 1-Click Launch**.



Note: Initially, port 3389 is open to all IP addresses. We recommend changing firewall settings to reflect your IP address only. Additionally, you can create an AWS security group that provides similar security protection as the firewall settings.



For more information on AWS security groups, please see [Security Groups for Your VPC](https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#DeleteSecurityGroup) at https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#DeleteSecurityGroup.

Use the Manual Launch Option

1. Click **Manual Launch**.
2. The U-Series Appliance version is selected by default.
3. Select the region and then click **Launch with EC2 Console**.

- i**
- For more information on how to run an AMI instance, please see [Launching an Instance Using the Launch Instance Wizard](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html) at <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html>.
 - We recommend you use an AWS VPN connection when you use your instance or access your assets. For more information, please see [What Is Amazon VPC?](https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html) at <https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html>.

Run an Azure Virtual Machine for the U-Series Appliance Deployment

To run an azure virtual machine, log in to Azure MarketPlace, and follow the below steps:

1. Select **Virtual Machines > Add** from the menu on the left.
2. Enter **BeyondInsight** in the search box.
3. Select a deployment model and click **Create**.

The five steps to complete your purchase are detailed below.

Step 1: Basics

1. Enter a virtual machine name and VM disc type.

The VM name must be the name you want to use as the machine name for the U-Series Appliance. The name must be 15 characters or less, or it will violate the requirement below. The U-Series Appliance name is entered when you run the U-Series Appliance Deployment & Configuration Wizard.

2. Add **btadmin** as the username and enter a password. Minimum password length is 14 characters.

! IMPORTANT!

*The username must be **btadmin** during install.*

3. You can create a new resource group or choose an existing one.
4. Select a location and click **OK**.

Step 2: Size

Choose a size. We recommend that you select a U-Series Appliance size from the recommended systems.

Step 3: Configure Optional Features

- **Managed Disks:** Click **Yes** to automatically manage the availability of disks to provide data redundancy and fault tolerance without creating and managing storage accounts on your own. Managed disks might not be available in all regions.
- **Virtual Network:** Virtual networks are logically isolated from each other in Azure. You can configure their IP address ranges, subnets, route tables, gateways and security settings, much like a traditional network in your data center. Virtual machines on the same virtual network can access each other by default.
- **Subnet:** A subnet is a range of IP addresses in your virtual network, which can be used to isolate virtual machines from each other or from the Internet.
- **Public IP Address:** Use a public IP address to communicate with the virtual machine from outside the virtual network. Choose **Dynamic** or **Static** and give it a name.
- **Extensions:** Extensions are not currently supported.
- **High Availability:** Select **None**.
- **Monitoring:** Enable this feature to capture serial console output and screenshots of the virtual machine running on a host to help diagnose startup issues.
- Click **OK**.

Step 4: Summary

A summary of the configuration settings is displayed. Click **OK** to confirm.

Step 5: Buy

- Click **Purchase** to complete your order.
- It takes several minutes for the machine to deploy. After the machine deploys, select **Informational** from the options under the **Notifications** tab.



Note: Initially, port 3389 is open to all IP addresses. We recommend changing firewall settings to reflect your IP address only. For security purposes, limit your Internet exposure to only your IP address.



For more information on how to run an Azure virtual machine, please see [Windows Virtual Machine Pricing](https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/) at <https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/>.



- For more information on how to run an Azure virtual machine, please see [Windows Virtual Machine Pricing](https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/) at <https://azure.microsoft.com/en-us/pricing/details/virtual-machines/windows/>.
- We recommend you use a VPN connection when you use your instance or access your assets. For more information on configuring the VPN Tunnel in Azure, please see [Create a Site-to-Site connection in the Azure portal](https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal) at <https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal>.

Deploy the Azure U-Series Appliance Using ARM Template

You can use the Azure Resource Manager (ARM) template to help automate creating your U-Series Appliance. You can use the template in the following ways:

- Use the template and JSON parameters provided in the code block below to create two separate JSON files and use PowerShell or Azure CLI scripting to execute them.
- You can use the template in the Azure portal with the **Create with Template** option and upload the JSON file to the portal. This gives the user minimal parameters, assuming defaults to some of the Azure Resource properties.

You can add your new U-Series Appliance to an existing virtual network (V-Net) or create a V-Net.

Key points to consider:

- Licensing is applied after the U-Series Appliance is created and is not part of the ARM template.
- When using this ARM template using Azure Portal with the **Create with custom Template** option, use the same resource group for both the virtual machine and virtual network.

This section assumes you have knowledge about Azure ARM templates and Microsoft Azure Cloud.

i For more information on Azure templates, please see [Tutorial: Deploy a local ARM template at https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-tutorial-local-template?tabs=azure-powershell](https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/deployment-tutorial-local-template?tabs=azure-powershell).

Arm Template Parameters

The following parameters are part of the ARM template. There are different areas to can enter the parameters depending on how you launch the ARM template.

- **vmName**: This is the name for the VM and is usually the same as the U-Series Appliance name configured during setup.
- **vmSize**: Azure sizing for the virtual machine. The default is **Standard_D2s_v3**.
- **Admin Username**: The credential for the administrator account.
- **Admin Password**: The password for the administrator account.
- **vNet New or Existing**: Specify whether to create a new or existing virtual network for the VM.
- **Virtual Network Name**: The name of the new or existing virtual network.
- **Virtual Network Resource Group**: The name of the new or existing resource group for the virtual network.
- **Subnet name**: Name of the subnet in the virtual network you want to use.
- **DNS Name**: Unique DNS Name for the Public IP used to access the virtual machine.
- **Network Security Group Name ('nsgName')**: Name of the new or existing NSG.

Deploy SQL Free Image

To deploy the SQL Free image, you must change a couple of lines in the JSON file.

From:

```
"imageReference": {  
  "publisher": "beyondtrust",  
  "offer": "beyondinsight",  
  "sku": "u-series",  
  "version": "latest"
```

To:

```
"imageReference": {  
  "publisher": "beyondtrust",  
  "offer": "uvm-sf",  
  "sku": "u-series_sf",  
  "version": "latest"
```

JSON Template Code Block

Template JSON

```
"$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",  
"contentVersion": "1.0.0.0",  
"parameters": {  
  "vmName": {  
    "type": "string",  
    "defaultValue": "btuseries",  
    "metadata": {  
      "description": "Name of the VM"  
    }  
  },  
  "vmSize": {  
    "type": "string",  
    "defaultValue": "Standard_DS4_v2",  
    "metadata": {  
      "description": "Size of the VM"  
    }  
  },  
  "adminUsername": {  
    "type": "string",  
    "metadata": {  
      "description": "VM Admin User Name"  
    }  
  },  
  "adminPassword": {  
    "type": "string",  
    "metadata": {  
      "description": "VM Admin Password"  
    }  
  },  
  "vNetNewOrExisting": {
```

```
"type": "string",
"defaultValue": "new",
"allowedValues": [
  "new",
  "existing"
],
"metadata": {
  "description": "Specify whether to create a new or existing virtual network for the VM."
},
},
"virtualNetworkName": {
  "type": "string",
  "defaultValue": "",
  "metadata": {
    "description": "Name of the new/existing VNET"
  }
},
"virtualNetworkResourceGroup": {
  "type": "string",
  "defaultValue": "",
  "metadata": {
    "description": "Name of the new/existing VNET resource group"
  }
},
"subnetName": {
  "type": "string",
  "defaultValue": "",
  "metadata": {
    "description": "Name of the subnet in the virtual network you want to use"
  }
},
"dnsNameForPublicIP": {
  "type": "string",
  "defaultValue": "",
  "metadata": {
    "description": "Unique DNS Name for the Public IP used to access the Virtual Machine."
  }
},
"nsgName": {
  "defaultValue": "",
  "type": "string",
  "metadata": {
    "description": "Network Security Group"
  }
},
"osDiskType": {
  "type": "string",
  "defaultValue": "Premium_LRS",
  "metadata": {
    "description": "OS Disk Type"
  }
},
"location": {
  "type": "string",
  "defaultValue": "eastus",
```

```
    "metadata": {
      "description": "Location for all resources."
    }
  },
  "variables": {
    "diagStorageAccountName": "[concat(uniquestring(resourceGroup().id), 'specvm')]",
    "subnetRef": "[resourceId(parameters('virtualNetworkResourceGroup'),
'Microsoft.Network/virtualNetworks/subnets', parameters('virtualNetworkName'), parameters
('subnetName'))]",
    "nicName": "nic",
    "publicIPAddressName": "publicIp"
  },
  "resources": [
    {
      "condition": "[equals(parameters('vNetNewOrExisting'), 'new')]",
      "type": "Microsoft.Network/networkSecurityGroups",
      "apiVersion": "2020-11-01",
      "name": "[parameters('nsgName')]",
      "location": "eastus",
      "properties": {
        "securityRules": []
      }
    },
    {
      "condition": "[equals(parameters('vNetNewOrExisting'), 'new')]",
      "apiVersion": "2018-10-01",
      "type": "Microsoft.Network/virtualNetworks",
      "name": "[parameters('virtualNetworkName')]",
      "location": "[parameters('location')]",
      "properties": {
        "addressSpace": {
          "addressPrefixes": [
            "10.0.0.0/16"
          ]
        },
        "subnets": [
          {
            "name": "[parameters('subnetName')]",
            "properties": {
              "addressPrefix": "10.0.0.0/24"
            }
          }
        ]
      }
    },
    {
      "type": "Microsoft.Storage/storageAccounts",
      "name": "[variables('diagStorageAccountName')]",
      "apiVersion": "2018-07-01",
      "location": "[parameters('location')]",
      "sku": {
        "name": "Standard_LRS"
      },
      "kind": "Storage",
    }
  ]
}
```

```
"properties": {}
},
{
  "apiVersion": "2018-10-01",
  "type": "Microsoft.Network/publicIPAddresses",
  "name": "[variables('publicIPAddressName')]",
  "location": "[parameters('location')]",
  "tags": {
    "displayName": "PublicIPAddress"
  },
  "properties": {
    "publicIPAllocationMethod": "Dynamic",
    "dnsSettings": {
      "domainNameLabel": "[parameters('dnsNameForPublicIP')]"
    }
  }
},
{
  "apiVersion": "2018-10-01",
  "type": "Microsoft.Network/networkInterfaces",
  "name": "[variables('nicName')]",
  "location": "[parameters('location')]",
  "dependsOn": [
    "[variables('publicIPAddressName')]",
    "[resourceId('Microsoft.Network/networkSecurityGroups', parameters('nsgName'))]"
  ],
  "tags": {
    "displayName": "NetworkInterface"
  },
  "properties": {
    "ipConfigurations": [
      {
        "name": "ipconfig1",
        "properties": {
          "privateIPAllocationMethod": "Dynamic",
          "publicIPAddress": {
            "id": "[resourceId('Microsoft.Network/publicIPAddresses', variables('publicIPAddressName'))]"
          },
          "subnet": {
            "id": "[variables('subnetRef')]"
          }
        }
      }
    ],
    "networkSecurityGroup": {
      "id": "[resourceId('Microsoft.Network/networkSecurityGroups', parameters('nsgName'))]"
    }
  }
},
{
  "apiVersion": "2018-10-01",
  "type": "Microsoft.Compute/virtualMachines",
  "name": "[parameters('vmName')]",
  "location": "[parameters('location')]",
```

```
"tags": {
  "displayName": "VirtualMachine"
},
"dependsOn": [
  "[variables('nicName')]"
],
"plan": {
  "name": "u-series",
  "publisher": "beyondtrust",
  "product": "beyondinsight"
},
"properties": {
  "hardwareProfile": {
    "vmSize": "[parameters('vmSize')]"
  },
  "storageProfile": {
    "osDisk": {
      "createOption": "FromImage",
      "managedDisk": {
        "storageAccountType": "[parameters('osDiskType')]"
      }
    },
    "imageReference": {
      "publisher": "beyondtrust",
      "offer": "beyondinsight",
      "sku": "u-series",
      "version": "latest"
    }
  },
  "networkProfile": {
    "networkInterfaces": [
      {
        "id": "[resourceId('Microsoft.Network/networkInterfaces', variables('nicName'))]"
      }
    ]
  },
  "osProfile": {
    "computerName": "[parameters('vmName')]",
    "adminUsername": "[parameters('adminUsername')]",
    "adminPassword": "[parameters('adminPassword')]",
    "windowsConfiguration": {
      "enableAutomaticUpdates": true,
      "provisionVmAgent": true
    }
  },
  "diagnosticsProfile": {
    "bootDiagnostics": {
      "enabled": true,
      "storageUri": "[reference(variables('diagStorageAccountName')).primaryEndpoints.blob]"
    }
  }
}
]
```

}

Run the U-Series Appliance Deployment & Configuration Wizard

Once you have completed the initial setup of your U-Series Appliance, you must run the U-Series Appliance Deployment & Configuration Wizard to complete the deployment of the appliance in your environment. There are two distinct and separate components of the wizard to allow infrastructure teams to handle the initial deployment in the network, while leaving the feature configuration to your network security administrator, outlined as follows:

- **Part 1: Appliance Deployment** - Intended for infrastructure teams, and includes the following:
 - Licensing Windows
 - Creating the appliance admin account
 - Naming the appliance
 - Setting up networking details, such as IP address settings, internet connection, timezone and time settings, and SMTP settings
- **Part 2: Appliance Configuration** - Intended for security administrators, and includes the following:
 - Licensing your BeyondTrust solutions
 - Selecting your BeyondTrust solution
 - Selecting and configuring appliance features
 - Configuring user credentials for BeyondInsight, Central Policy, and BeyondTrust Updater
 - Configuring appliance backup and restore location and schedule
 - Setting up how to receive updates from BeyondTrust



Note: Once part 1 is complete, you may complete part 2 now or at a later time. There are no time restrictions on completing the configuration.



IMPORTANT!

If you purchased Professional Services, schedule your engagement with your Professional Services representative before starting configuring your appliance.

Access your Appliance from Web Browser for the First Time

To access your appliance, open a web browser from a device within the same network subnet as the appliance, and enter the IP address for the U-Series Appliance, **[https://\[U-Series Appliance IP address\]](https://[U-Series Appliance IP address])**.

When accessing your appliance for the first time, you are presented with a message advising you of the SSL certificate that is automatically created for the administration of the appliance to ensure encrypted communications.

Because this HTTPS SSL certificate is self-generated and not registered with a public certificate authority, your browser displays a warning message when connecting to the appliance via SSL. To avoid these warnings, install the certificate through a web browser or obtain a custom certificate from a public certificate authority.

Browser warnings are displayed until the SSL certificate is installed or a valid certificate is obtained. Check the box next to **Do not show this message again** if you don't want this message to display each time you access the appliance.

Click **Accept** to continue to the U-Series Appliance Deployment & Configuration Wizard.



PLEASE ACCEPT TO CONTINUE

SSL Certificate

The HTTPS SSL certificate automatically created for the administration of this appliance ensures encrypted communications. However, because the certificate is self-generated and not registered with a public certificate authority, your browser will display a warning message when connecting to the appliance via SSL. [Example Warning Messages](#)

To avoid these warnings, install the certificate through the web browser or obtain a certificate from a public certificate authority.

Do not show this message again.

ACCEPT

Run Part 1: New Appliance Deployment Using the Deployment Wizard

After accepting the SSL certificate message, the BeyondTrust U-Series Appliance Deployment & Configuration wizard starts. Part 1 of the wizard involves configuring settings related to the deployment of your appliance in your network. Follow the below steps for configuring appliance deployment.



IMPORTANT!

While it is possible to rename administrator accounts later, we recommended choosing account names carefully during deployment and configuration to avoid renaming them later.

1. Enter the Windows 2022 activation key you received from BeyondTrust, and then click **License Windows**.
 - Alternatively, if you have not yet purchased the appliance, click **Skip**, to trial the appliance for 180 days.



Note: SQL Server can be included as part of your U-Series Appliance, or you can use your own SQL Server deployment. If SQL Server is part of your U-Series Appliance package, a SQL Server COA is included along with the Windows Operating System key and the BeyondInsight key.



Note: If you do not activate Windows, once deployment is complete, an evaluation banner displays at the top of the **U-Series Appliance** website indicating you are using the software in evaluation mode and shows the number of days remaining for the evaluation period.

After 180 days, you must activate Windows to continue using the appliance. For more information, please see [Manage Licensing and Admin Accounts in the U-Series Appliance](#).

2. Read through the deployment and configuration details, and then click **Start Deployment**.
3. Enter a username, password, and email address to create an administrator account for the appliance.



Note: This is the Windows admin account used to log in to the appliance. It cannot be named Administrator. U-Series Appliance notifications and reports are sent to this email address.

4. Click **Create Admin**.
5. On the **Appliance Name** screen, enter the name for the U-Series Appliance, following the naming conventions used in your environment, and click **Next**.



IMPORTANT!

Once you have named your U-Series Appliance, it cannot be renamed. If at any point you need to rename the appliance, you must either re-image (if it is a physical appliance) or re-deploy the image (if it is a virtual appliance). The appliance name is stored in the BeyondInsight database and associated to the asset in BeyondInsight, so it is important to name it appropriately during deployment.



Note: If creating a Cold Spare, use the same name as the source appliance.

6. On the **IP Settings** screen, if you wish to keep automatically assigned IP settings, click **Next**. Otherwise, you can manually configure these settings for each network adapter, and then click **Next**.



Note: Physical appliances have 4 ports, so you could potentially see 4 network adapters listed here and they can each be configured separately.

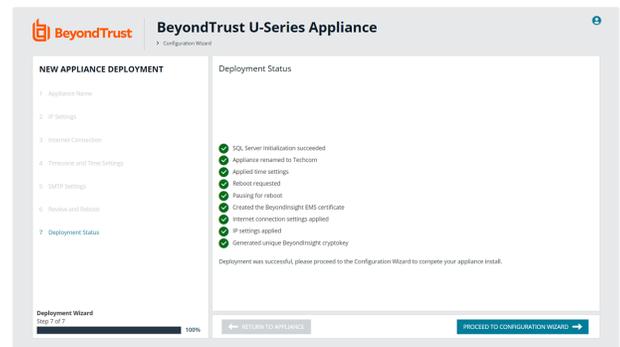
7. On the **Internet Connection** screen:
 - Select one of the following ways to connect to the internet to validate license keys and to receive updates:
 - **Connect to the internet for licensing and updates. (No proxy required):** Select this option if there is an internet connection and no proxy server.
 - **Connect to the Internet for licensing and updates through a proxy server:** Select this option and provide the address and port number for the proxy, to use a proxy server.
 - **No Internet connection. (Perform manual updates):** Select this option if the U-Series Appliance does not have an Internet connection, for example in air gap environments.
 - Click **Test Connection** to verify connectivity.
 - Once the connectivity test shows as succeeded, click **Next**.

8. On the **Timezone and Time Settings** screen:
 - Select a timezone from the dropdown.
 - Select one of the following date and time synchronization options:
 - **Use NTP server for time:** Provide the name of the Network Time Protocol (NTP) server.
 - **Manually Configure Date and Time:** Set the date and optionally set the time.
 - **Enable VMware Tools periodic time synchronization**
 - Click **Next**.
9. On the **SMTP Settings** screen, specify the email server for the appliance software, BeyondInsight, and BT Updater to send notifications to users:
 - Enter the SMTP server address and port. The default port number is **25**.
 - Optionally, select **SSL** to enforce SSL encryption when accessing the server.
 - Optionally, check the **SMTP Server requires authentication** box and enter the username and password to use credentials to access the server.
 - Click **Next**.
10. Review the deployment settings to verify everything is correct. Click **Back** if you need to make changes, otherwise, click **Finish** to reboot the appliance.



Note: It can take several minutes for the deployment settings to apply as the appliance reboots. If any errors occur, you can click the wizard's **Back** button to change settings, if needed.

11. A **Deployment Status** page displays while the appliance is rebooting and settings are being applied.
12. Once deployment is successful, click **Proceed to Configuration Wizard**.



Run Part 2: New Appliance Configuration Using the Configuration Wizard

Part 2 of the wizard involves configuring settings related to how your appliance functions in your network and which application services it provides to your users. Follow the below steps for configuring the appliance.



IMPORTANT!

While it is possible to rename administrator accounts later, we recommended choosing account names carefully during deployment and configuration to avoid renaming them later.

1. On the **BeyondTrust Licenses** screen:
 - Enter the **BeyondInsight Serial Number**, and then click **Get License Key**. The **BeyondInsight License Key** box is populated with the key.
 - Alternatively, if you are working offline, go to <https://licensing.beyondtrust.com> to get the BeyondInsight license key.
 - If you do not currently have serial numbers and would like to evaluate the solution for 30 days, leave the **Evaluate solution** option selected. This option is not available for cloud deployments.
 - Click **Next**.
2. On the **Solution** screen, select one of the following options that represents your implementation for the U-Series Appliance, and then click **Next**:
 - **Single Appliance**: Select this option if this appliance hosts all of your BeyondTrust products and your SQL database.
 - **Database Server in a Multi-Node Deployment**: Select this option if you plan to have multiple appliances and this appliance hosts your SQL database with no failover configured.
 - **High Availability Pair**: Select this option if this appliance hosts your SQL database and stores application data and you plan to use this appliance in a pair with another appliance that also hosts a SQL database. The pair provides failover for the database and application services.
 - **SQL-less Appliance**: Select this option if you have multiple appliances in your environment and this appliance either does not have SQL Server installed or you plan to configure a connection to a remote database as opposed to using the local SQL server. Check the box to enable application service failover with another appliance, if desired.
 - **Cold Spare Appliance**: Select this option if you plan to use this appliance as a backup appliance. This appliance serves as a duplicate of your primary appliance. It actively restores backups of the primary on a schedule. This spare appliance inherits features from the primary. Feature selection and configuration is not required.
3. On the **Feature Options** screen, select one of the following options, and then click **Next**:
 - Select **Use default features with the option to customize** to have features settings enabled based on your chosen solution. You can enable or disable features at any time after your appliance has been deployed and configured.
 - Or, select **Feature Questionnaire** if you aren't sure which features to select for this appliance and need some guidance. The **Feature Questionnaire** guides you through a series of questions to assist you in determining the features best suited for your appliance.
4. On the **Feature Selection** screen, leave the defaults or click the toggles to enable or disable the features on this appliance. Click **Next** to configure your features.
5. On the **Feature Configuration** screen, select the tab for the respective feature to set up that feature, and then click **Next**:
 - **SQL Server Feature**: Check the **Allow incoming remote database connections** option, and then enter the database password and confirm it.
 - **BeyondInsight Database Access**: Select the database server for BeyondInsight to use and enter the database credentials.
 - For a local database, if the provided username doesn't exist, the account is created with least privilege.
 - For a remote database, provide the credentials supplied by your database administrator.
 - Optionally, enter command timeout and connection timeout values.
 - For a SQL cluster deployments, configure the following:
 - Enable the **Multi Subnet Failover** option.

- If the database does not yet exist on the SQL cluster, check **Create the Remote Database** to have the database created on the remote server. Provide the credentials for the account that has sufficient permissions to create the database. These credentials are used only once during this initial database connection and are not saved. Moving forward, BeyondInsight uses the least privileged credentials you created or provided in the above steps to connect to the database.
- If your primary appliance is already in place, and you are connecting this appliance to the same database, you can export the Crypto Key from the primary appliance and import it here, providing the password. To create and export the Crypto Key zip file from the primary appliance:
 - From the left menu, under **Security and Compliance**, click **Data Encryption Key**.
 - Enter the encryption password and confirm it.
 - Click **Export and Download Crypto Key**.
- **BIUL Setup Feature:**
 - Select **Local** to create a SQL database on the local appliance. If the provided username doesn't exist, the account is created with least privilege.
 - If you select **Remote**, provide the database details to access the remote database, including server name, database name, port number (default is **1433**), and database credentials. The remote database must already exist.
- **Cold Spare Setup Feature:** Set up the **Restore Location** where backups are stored from the production server this cold spare would replace, if that need ever arises. For example, in disaster recovery, failure, and network issue scenarios. The cold spare machine stores those backups and performs a restore on them at the scheduled interval. A temporary name is used to ensure there are no DNS name resolution conflicts, if your network is not segregated. This temporary name is used until the appliance is taken out of *Cold Spare* mode, which happens when you disable the **Cold Spare** feature.
- **Endpoint Privilege Management (EPM):** Select the appropriate option for configuring database settings for EPM and Privileged Management Reporting (PMR), depending on the appliance and database architecture deployed in your environment:
 - **Single Appliance using the Local Database:** Select this option if this is the only appliance in your environment. This option applies the configuration for EPM using the SQL Server configured on this local appliance and the credentials entered on the **SQL Server Feature** tab.
 - **Multi-node deployment using the Local Database:** Select this option if you have more than one appliance deployed in your environment, SQL Server is configured on this local appliance, and you want other appliances to be able to connect to the database on this appliance. This option applies the configuration for EPM using the local SQL Server and the credentials entered on the **SQL Server Feature** tab.
 - You must select this local appliance from the **Server Name** dropdown and it must be the FQDN or IP address of this appliance (not localhost).
 - **Multi-node deployment using Remote Database (first time connecting):** Select this option if you have more than one appliance deployed in your environment, the BeyondInsight and EPM databases are on remote SQL Servers, and no appliances have ever been configured to connect to the EPM database. This option saves the connection details to the remote BeyondInsight database.
 - Enter the FQDN or IP address of the remote server where the EPM database exists.
 - The EPM database must already exist on the destination server.
 - Enter the SQL credentials provided by your database administrator to connect to the EPM Event Collector and PMR Report Reader.
 - Test the connection settings.
 - **Multi-node deployment using Remote Database (load configuration from BeyondInsight):** Select this option if you have more than one appliance deployed in your environment, the BeyondInsight and EPM databases are on

remote SQL Servers, and the EPM configuration has already been saved to the remote BeyondInsight database (as other appliances have previously been configured to connect to the EPM database).

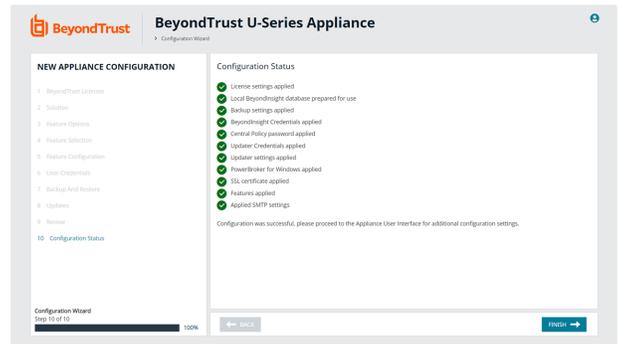
- The remote database must be configured on the **BeyondInsight Database Access** tab.

 **Note:** Only the features that are applicable to the appliance, based on your selection, are enabled here for configuration. After initial deployment and configuration is complete, you can edit the appliance feature configuration by clicking **Appliance Feature Configuration**, under **Features and Services** from the sidebar.

6. On the **User Credentials** screen, enter login credentials for the following user accounts: BeyondInsight, Central Policy, and BeyondTrust Updater.
7. On the **Backup and Restore** screen, set up the location and schedule for backup files. Alternatively, select **I will setup my Appliance later through the Appliance User Interface** to create backups later from the **Business Continuity > Backup and Restore** page. Click **Next**.
8. On the **Updates** page, select to install updates from the BeyondTrust Update Server or from an internal BeyondTrust Updater Enterprise server. Optionally, select **Do not check for updates** to opt out of this feature. Click **Next**.
9. A **Review** page displays a summary the settings you configured. Verify everything is accurate. Click **Back** if you need to make changes, otherwise, click **Next**.
10. A **Configuration Status** page displays while the settings are being applied.
11. Once configuration is successful, click **Finish**. You are directed to the BeyondInsight login page on your appliance.

 **Note:** The BeyondInsight configuration provides the same least privilege SQL Server account during the database configuration.

 For more information about the permissions assigned to that account, please see section "Least Privilege Database User Account Setup" in the [BeyondInsight Installation Guide](https://www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-install.pdf) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-install.pdf>.



Key Management Service Support

After installation and configuration, if your server does not automatically discover the Key Management Service (KMS) server, you may receive a *Windows activation failed* message. Specify the KMS key and IP address again.

You can replace our key with a known Volume License Key and then call into your KMS server to count against your total (number of licenses).

To activate your volume license key:

1. From the left menu, under **Software and Licensing**, click **Product Licensing**.
2. Click the **Microsoft** tab, and select the **KMS (Key Management Service)** option, which displays two fields to complete.
3. Enter your **Volume License Key**.

4. Enter the **KMS (Key Management Service)** that will validate and track the license. This is only valid on appliances created as volume images.
5. Click **Activate Windows**.



For more information, please see [Why did Windows activation fail on my EC2 Windows instance?](https://aws.amazon.com/premiumsupport/knowledge-center/windows-activation-fails/) at <https://aws.amazon.com/premiumsupport/knowledge-center/windows-activation-fails/>.

Update Running Instances for the Amazon U-Series Appliance Deployment

The U-Series Appliance available in the Marketplace is based on an AWS Windows AMI that is configured by BeyondTrust. This includes drivers and configurations that support the AWS instance types available when the AMI was built. Over time, these drivers may require updating, as Amazon does not force an update to running virtual machines. BeyondTrust is working on a method of delivering these drivers directly to your U-Series Appliance, and notifying you of the need to update (which requires a reboot of your U-Series Appliance). Until that update method is available, we fully support manually updating these drivers as per the AWS guidance, as documented in the below sections.

Prior to updating any drivers, we recommend taking a snapshot of your running instance.

Take a Snapshot / Back Up Your AWS Instance

When working in virtual environments, we recommend periodic backups of the virtual machine. We also recommend creating a backup prior to any updates that affect the operating systems of the virtual machine. Back up application data on a U-Series Appliance as follows:

1. From the **Network > RDP and Console Access** page in the U-Series Appliance management console, enable remote desktop and console access.
2. Using RDP, connect to your U-Series Appliance to shut it down gracefully.
3. Open the Amazon EC2 console.
4. From the navigation pane, select **Instances**.
5. Find the instance that represents your U-Series Appliance and right-click it.
6. Select **Connect**.
7. Click **Download Remote Desktop File** to connect to the U-Series Appliance.
8. Use your U-Series Appliance credentials to log in.
9. From the Windows **Start** menu **Power** options, click **Shut down**.
10. Refresh your EC2 console periodically until the **Instance State** column changes to **Stopped**.
11. Right-click the instance, select **Image**, and then select **Create Image**. Provide an image name and description.



Note: There might be costs associated with the storage of the image. BeyondTrust is not responsible for any incurred costs, and it is your responsibility to manage any costs associated with image backups. If a backup is recommended during an upgrade, you can delete the backup after the upgrade is determined to be successful.

12. After the image is created, right-click the instance, and then select **Instance State > Start** to restart your U-Series Appliance.



For more information, please see [Configure RDP](https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/administration/network-and-rdp.htm#Configure-RDP) at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/administration/network-and-rdp.htm#Configure-RDP>.

At this time, we do not recommend using the AWS Systems Manager console and the SSM Agent for updating instances. BeyondTrust packages and distributes updates using the Security Update Package Installer.

The Elastic Network Adapter (ENA) drivers ("[Update AWS ENA Drivers](#)" on [page 35](#) below) and the NVMe drivers ("[Update AWS NVMe Drivers](#)" on [page 36](#) below) only apply to instance sizes that use the Nitro hypervisor (A1, C5, C5d, C5n, M5, M5a, M5d, p3dn.24xlarge, R5, R5a, R5d, T3, and z1d). Of these, we only recommend using M5, M5a, and R5 instances, so you only need to update these drivers if you deploy a U-Series Appliance to one of these three instance types.

We recommend updating the following drivers:

Update AWS PV Drivers

1. Connect to your instance and log in as the local administrator.
2. To verify the version of the driver, open **Control Panel** and select **Programs and Features**.
3. Look for **AWS PV Drivers** in the list of installed programs. The version number appears in the **Version** column. Alternatively, you can verify the driver version currently installed by running the following PowerShell command:

```
Get-ItemProperty HKLM:\SOFTWARE\Amazon\PVDriver
```

4. Check to see if you have the latest version in the **AWS PV Driver Package History** table. If no value is returned by the above command or if it is not listed in **Programs and Features**, update the driver.
5. Download the latest driver package to the instance, or run the following PowerShell command:

```
PS C:\>invoke-webrequest https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/Latest/AWSPVDriver.zip -outfile $env:USERPROFILE\pv_driver.zip expand-archive $env:userprofile\pv_driver.zip -DestinationPath $env:userprofile\pv_drivers
```

6. Extract the contents of the folder and then run **AWSPVDriverSetup.msi**.
7. After running the MSI file, the instance automatically reboots and then upgrades the driver. The instance will not be available for up to 15 minutes.
8. After the upgrade is complete and the instance passes both health checks in the Amazon EC2 console, you can verify that the new driver was installed by connecting to the instance using Remote Desktop and running the command provided in step 1.



Tip: To download the latest driver package, click <https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/Latest/AWSPVDriver.zip>.

Update AWS ENA Drivers

This procedure applies to M5, M5a, and R5 instances only.

1. Connect to your instance and log in as the local administrator.
2. Click the Windows **Start** menu button, and type **Device Manager (Enter)** to open the Device Manager.
3. Under **Network Adapters**, right-click **Amazon Elastic Network Adapter** and select **Properties**.
4. On the **Driver** tab, verify the driver version that is installed. Verify the version installed against the **Amazon ENA Driver Versions** list.
5. Download the latest driver to the instance.
6. Extract the files from the zip archive.
7. Install the driver by running the **install.ps1** PowerShell script as administrator.
8. If the installer does not reboot your instance for you, restart the instance.



Tip: To download the latest driver package, click <https://s3.amazonaws.com/ec2-windows-drivers-downloads/ENA/Latest/AwsEnaNetworkDriver.zip>.

Update AWS NVMe Drivers

This procedure applies to M5, M5a, and R5 instances only.

1. Connect to your instance and log in as the local administrator.
2. Click the Windows **Start** menu button, and type **Device Manager (Enter)** to open the Device Manager.
3. Under **Storage Controllers**, right-click **AWS NVMe Elastic Block Storage Adapter** and select **Properties**.
4. On the **Driver** tab, verify the driver version that is installed. Verify the version installed against the **AWS NVMe Driver Version History** list.
5. If you need to update, download the latest driver package to the instance.
6. Install the driver by running **dpinst.exe**.
7. You may get disconnected from RDP when the update runs and the instance reboots.



Tip: To download the latest driver package, click <https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/Latest/AWSNVMe.zip>.



For more information, please see the following:

- [AWS PV Driver Package History](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/xen-drivers-overview.html#pv-driver-history) at <https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/xen-drivers-overview.html#pv-driver-history>
- [Amazon ENA Driver Versions](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/enhanced-networking-ena.html) at <https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/enhanced-networking-ena.html>
- [AWS NVMe Driver Version History](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/aws-nvme-drivers.html) at <https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/aws-nvme-drivers.html>

Update the EC2Config Application

1. To verify the version of EC2Config, launch an instance from your AMI and connect to it.
2. In **Control Panel**, select **Programs and Features**.
3. Look for **Ec2ConfigService** in the list of installed programs. The version number appears in the **Version** column.
4. Consult the **EC2Config Version History** to determine if you need to update.
5. To update, download and extract the EC2Config installer.
6. Run **EC2Install.exe** and follow the prompts.

Update the EC2Launch Application

As of the 2020-R1 image, BeyondTrust does not configure or use EC2Launch, but it may be used in future releases. For this reason, we do not recommend manual updates. If you have a need to use or upgrade EC2Launch, please contact BeyondTrust Technical Support.

Connect to a Cloud Database

You can create remote database connections to an Azure SQL database or Amazon RDS database.

Connect to Azure SQL Database

Review the information in this section to learn more about using an Azure SQL database for BeyondInsight.

Prerequisites

- If starting a new BeyondInsight installation, ensure you have already created an empty database in Azure SQL.
- If you are connecting to an existing database server in Azure SQL, ensure the connection string details are available.
- BeyondInsight 22.2 or later release.

Resources

An Azure SQL database must already be created.

i For more information, please see the following:

- [Create and manage servers and single databases in Azure SQL Database at https://docs.microsoft.com/en-us/azure/azure-sql/database/single-database-manage](https://docs.microsoft.com/en-us/azure/azure-sql/database/single-database-manage)
- [Quickstart: Create an Azure SQL Database single database at https://docs.microsoft.com/en-us/azure/azure-sql/database/single-database-create-quickstart?tabs=azure-portal](https://docs.microsoft.com/en-us/azure/azure-sql/database/single-database-create-quickstart?tabs=azure-portal)

Configure Azure SQL

1. Create an empty database in Azure SQL.
 - Ensure a database server is created.
 - Make a note of the connection string information.
 - Make a note of the Azure SQL Server administrator name and password. This is needed during the U-Series Configuration Wizard when you create the database.
2. Ensure firewall rules are set up appropriately to allow your U-Series Appliance to connect to your Azure SQL machine.



Note: Every Azure SQL machine has firewall rules that need to be configured in addition to general Azure firewall rules.

3. When going through the U-Series Appliance Deployment & Configuration Wizard, on the **Feature Configuration** screen, select **Remote** for the BeyondInsight database access.

Although the Azure SQL database is already created, you must select the **Create the Remote Database** option on the first appliance configured to populate the empty Azure SQL database with BeyondInsight SQL Server tables.

For any additional appliances, use the existing database option on the **Feature Configuration** page after the first appliance is configured and the crypto key is exported.

Connect to Amazon RDS Instance

Prerequisites

- BeyondInsight 22.3 or later release
- U-Series Appliance 4.0 or later release

Resources

A database instance must already be created.



For more information, please see *Getting started with Amazon RDS* at https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/CHAP_GettingStarted.html.

Configure Amazon RDS

1. Create an empty database.
 - Ensure a database server is created.
 - Make a note of the connection string information.
 - Make a note of the Amazon RDS administrator name and password. This is needed during the U-Series Configuration Wizard when you create the connection to the service.
2. Ensure firewall rules are set up appropriately to allow your U-Series Appliance to connect to the Amazon RDS machine.
3. When going through the U-Series Appliance Deployment & Configuration Wizard, on the **Feature Configuration** screen, select **Remote** for the BeyondInsight database access.

You must select the **Create the Remote Database** option on the first appliance configured to populate the empty Amazon RDS database with BeyondInsight SQL Server tables.

For any additional appliances, use the existing database option on the **Feature Configuration** page after the first appliance is configured and the crypto key is exported.