UVM Appliance
Cloud Deployment Guide
# Table of Contents

Amazon UVM Deployments ................................................................. 4  
   Introduction ........................................................................... 4  
   Prerequisites ......................................................................... 4  
   License Keys .......................................................................... 4  
   UVM Instances ....................................................................... 4  
   Run an Instance ...................................................................... 5  
      Configure Firewall and AWS Security Groups ..................... 6  
      Retrieve a Windows Password ........................................... 6  
      VPN Access ....................................................................... 6  
   UVM Appliance Configuration Wizard ....................................... 8  
   Take a Snapshot/Back up Your AWS Instance ......................... 10  
   Update Running Instances ..................................................... 11  

Azure UVM Deployments ................................................................. 14  
   Introduction ........................................................................... 14  
   Prerequisites ......................................................................... 14  
      License Keys ...................................................................... 14  
   UVM Instances ....................................................................... 14  
   Run an Azure Virtual Machine ............................................... 14  
      Configure Azure ................................................................. 14  
      Configure the Firewall ....................................................... 16  
      VPN Access ....................................................................... 16  
   UVM Appliance Configuration Wizard ....................................... 16  

Google UVM Deployments ............................................................... 19  
   Introduction ........................................................................... 19  
   Prerequisites ......................................................................... 19  
      License Keys ...................................................................... 19  
   UVM Instances ....................................................................... 19  
   Run an Instance ...................................................................... 19  
      Create an Instance ............................................................. 19  
      Retrieve a Windows Password ........................................... 20  
      VPN Access ....................................................................... 21
Amazon UVM Deployments

Introduction

This guide provides important information that will help you get started with your UVM appliance instance, available from the AWS MarketPlace.

Prerequisites

License Keys

You must already have license keys for the BeyondTrust solutions that you want to use.

Contact BeyondTrust Sales to get the license keys. You will use the keys later when you go through the configuration wizard on the UVM instance.

UVM Instances

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>vCPU</th>
<th>Memory</th>
<th>Storage</th>
<th>EBS Bandwidth (Mbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>m4.2xlarge</td>
<td>8</td>
<td>32 GB</td>
<td>EBS-Only</td>
<td>1,000</td>
</tr>
<tr>
<td>m4.4xlarge</td>
<td>16</td>
<td>64 GB</td>
<td>EBS-Only</td>
<td>2,000</td>
</tr>
<tr>
<td>m5.2xlarge</td>
<td>8</td>
<td>32 GB</td>
<td>EBS-Only</td>
<td>Up to 4,750</td>
</tr>
<tr>
<td>m5.4xlarge</td>
<td>16</td>
<td>64 GB</td>
<td>EBS-Only</td>
<td>4,750</td>
</tr>
<tr>
<td>m5a.2xlarge</td>
<td>8</td>
<td>32 GB</td>
<td>EBS-Only</td>
<td>Up to 2,120</td>
</tr>
<tr>
<td>m5a.4xlarge</td>
<td>16</td>
<td>64 GB</td>
<td>EBS-Only</td>
<td>2,120</td>
</tr>
<tr>
<td>r5.xlarge</td>
<td>4</td>
<td>32 GB</td>
<td>EBS-Only</td>
<td>Up to 4,750</td>
</tr>
<tr>
<td>r5.2xlarge</td>
<td>8</td>
<td>64 GB</td>
<td>EBS-Only</td>
<td>Up to 4,750</td>
</tr>
<tr>
<td>r5.4xlarge</td>
<td>16</td>
<td>128 GB</td>
<td>EBS-Only</td>
<td>4,750</td>
</tr>
</tbody>
</table>

For more information, please see Amazon EC2 Instance Types at https://aws.amazon.com/ec2-instance-types/.
Run an Instance

For more information about how to run an AMI instance, please see Launching an Instance Using the Launch Instance Wizard at https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/launching-instance.html.

1-Click Launch

1. Log on to the AWS MarketPlace, and search for BeyondTrust or BeyondInsight.
2. On the BeyondTrust marketplace website, click Continue.
3. Click the 1-Click Launch tab.
4. Configure the following settings if you want to use the 1-Click Launch option.
   - **Version**
   - **Region**
   - **EC2 Instance Type:** m4.2xlarge or m4.4xlarge
   - **VPC settings**
     - **Security Group:** Select the default BeyondTrust security group.
   - **Select the Key Pair**
5. Click Launch 1-Click Launch.

Manual Launch

1. On the BeyondTrust marketplace website, click Continue.
2. Click Manual Launch.
3. The UVM version is selected by default.
4. Select the region and then click **Launch with EC2 Console**.

### Configure Firewall and AWS Security Groups

When you run the instance, be sure to configure the AWS firewall. When you initially run the instance, the 3389 port is open to all IP addresses. Change the firewall settings to reflect your IP address only. For security purposes, limit your internet exposure to only your IP address.

Additionally, you can create an AWS security group that provides similar security protection as the firewall settings.

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

### Retrieve a Windows Password

You must retrieve a Windows password through the Amazon Marketplace website. Amazon assigns a random default password to the administrator account.

You must know the key pair to retrieve a password. The key pair was created when you created your AWS account.

- For more information, 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/).

You need this password when you run through the UVM appliance configuration wizard.

1. Right-click the instance and select **Get Windows Password**.

### VPN Access

We recommend you use a VPN connection when you use your UVM appliance instance or access your assets.
For more information, please see What Is Amazon VPC? at
UVM Appliance Configuration Wizard

You must configure your UVM appliance using the UVM Configuration Wizard.

1. Click Start the Configuration Wizard.
2. Read the license agreement and click I Agree.
   You must accept the licensing agreement for the installation to continue.
3. On the Network Settings page, provide the following details:

   **Network State:**
   - Connect to the Internet for licensing and updates. No proxy required: Select if there is an Internet connection and no proxy server.
   - Connect to the Internet for licensing and updates through a proxy server: Select if you are using a proxy server.
   - No Internet connection. Requires performing manual updates: Select if the appliance does not have an Internet connection.

4. Click Next. On the Registration Information page, enter the name, organization, and address information.
5. Click Next. On the BeyondTrust Licenses page, enter the license keys.

   If you selected No internet connection in step 3, see Offline Licensing.

   - **Client Portal Login:** You can choose to retrieve license keys automatically from the BeyondTrust client portal. Enter your user name and password, and then click Retrieve Serial Numbers.
   - **Serial Numbers:** Enter the serial number provided when you purchased the product. To access your serial number, log on to the client portal, and select Product Licensing > Managing Your Serial Numbers. Click Get Offline License and follow the instructions on obtaining the license key offline. When received, manually enter the license key.

6. On the User Credentials page, enter the following passwords:

   - **Administrator password:** This password enables you to access the appliance. The email address will receive UVM reports, alerts, and alerts on hardware events.

   Retrieve the administrator password as described in Retrieve a Windows Password.

   - **BeyondInsight user name and password.

7. Click Next.
8. On the Machine Configuration page:

   - Enter the name of the appliance (host name), time zone information, and date and time.

   **Note:** Once entered here, do not change the appliance name.

   - Select an auto synchronization setting.

10. To save the settings to a configuration file, click **Download Configuration File**. If you need to go through the configuration for the appliance again, you can upload the configuration file to apply your settings.

11. Click **Next**, and then click **Finish** to restart the appliance.

Restarting the appliance can take a few minutes. Proceed after the appliance restarts.
Take a Snapshot/Back up Your AWS Instance

BeyondTrust provides a way to back up application data on a UVM appliance. 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.

1. RDP into your appliance to shut it down gracefully. Enable RDP using your Maintenance application.


2. Open the Amazon EC2 console and in the navigation pane, select **Instances**. Find the instance that represents your UVM Appliance.

3. Right-click your appliance instance and select **Connect**. Click **Download Remote Desktop File** to RDP into the UVM. Use your UVM credentials to log in, and from the Windows **Start** menu, click the **Power Options** button in the upper-left corner of the screen. Select **Shut down** from the context menu that appears.

4. Refresh your EC2 console periodically until the **Instance State** column changes to **Stopped**. Right-click the instance, select **Image**, and then select **Create Image**. Provide an image name and description.

   **Note:** There may 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.

5. After the image is created, restart your UVM. Right-click the instance, select **Instance State**, and then select **Start**.
Update Running Instances

The UVM 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 UVM, and notifying you of the need to update (which will require a reboot of your Appliance). Until that update method is available, we fully support manually updating these drivers as per the AWS guidance.

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

For more information, please see "Take a Snapshot/Back up Your AWS Instance" on page 10.

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 (AWS ENA Drivers below) and the NVMe drivers (AWS NVMe Drivers 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 deployed an Appliance to one of these three instance types.

We recommend updating the following drivers:

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, select Programs and Features, and in the list of installed programs, look for AWS PV Drivers. 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

3. 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.

   For more information, please see AWS PV Driver Package History. To download the latest driver package, click https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/Latest/AWSPVDriver.zip

4. 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

5. Extract the contents of the folder and then run AWSPVDriverSetup.msi.
6. After running the MSI, the instance automatically reboots and then upgrades the driver. The instance will not be available for up to 15 minutes.
7. 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.
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. Under Network Adapters, right-click Amazon Elastic Network Adapter and select Properties. On the Driver tab, verify the Driver Version that is installed. Verify the version installed against the Amazon ENA Driver Versions list.

For more information, please see Amazon ENA Driver Versions. To download the latest driver package, click https://s3.amazonaws.com/ec2-windows-drivers-downloads/ENA/Latest/AwsEnaNetworkDriver.zip

3. Download the latest driver to the instance.
4. Extract the zip archive.
5. Install the driver by running the install.ps1 PowerShell script as administrator.
6. If the installer does not reboot your instance for you, restart the instance.

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. Under Storage Controllers, right-click AWS NVMe Elastic Block Storage Adapter and select Properties. On the Driver tab, verify the Driver Version that is installed. Verify the version installed against the AWS NVMe Driver Version History list.

For more information, please see AWS NVMe Driver Version History. To download the latest driver package, click https://s3.amazonaws.com/ec2-windows-drivers-downloads/NVMe/Latest/AWSNVMe.zip

1. If you need to update, download the latest driver package to the instance.
2. Install the driver by running dpinst.exe.
3. You may get disconnected from RDP when the update runs and the instance reboots.
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, and in the list of installed programs, look for Ec2ConfigService. The version number appears in the Version column. Consult the EC2Config Version History to determine if you need to update.
3. To update, download and unzip the EC2Config installer.
4. Run EC2Install.exe and follow the prompts.

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 specific need to use or upgrade EC2Launch, please contact BeyondTrust Technical Support.
Azure UVM Deployments

Introduction

This guide provides important information that will help you get started with your UVM appliance instance, available from the Azure Marketplace.

Prerequisites

License Keys

You must already have license keys for the BeyondTrust solutions that you want to use.

Contact BeyondTrust Sales to get the license keys. You will use the keys later when you go through the configuration wizard on the UVM instance.

UVM Instances

There are two recommended UVM instances available through the Azure marketplace.

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>vCPU</th>
<th>Memory</th>
<th>SSD Storage</th>
<th>Dedicated EBS Bandwidth (Mpbs)</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS4_V2</td>
<td>8</td>
<td>28 GB</td>
<td>56 GB</td>
<td>1000</td>
<td>1 to 10,000</td>
</tr>
<tr>
<td>DS5_V2</td>
<td>16</td>
<td>56 GB</td>
<td>112 GB</td>
<td>2000</td>
<td>10,000 to 20,000</td>
</tr>
</tbody>
</table>

Run an Azure Virtual Machine


Configure Azure

1. Select Virtual Machines from the menu on the left.
2. Select Add. Enter BeyondInsight in the search box.

3. Select a deployment model and click Create. The following section goes through the five steps to complete your purchase.

   **Step 1: Basics**

   Enter a virtual machine name, VM disc type, create a user name (must be btadmin) and password. You can create a new resource group or choose an existing one. Select a location and click OK.
The VM name must be the name you want to use as the machine name for the UVM. The name must be 15 characters or less, or it will violate the requirement below. The UVM name is entered when you run the UVM Appliance Configuration Wizard. Minimum password length is 14 characters.

**Step 2: Size**

Choose a size. It is recommended that you select a UVM 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 may 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.
- Select 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.
4. It will take several minutes for the machine to deploy. After the machine deploys select **Informational** from the options under the Notifications tab.

**Configure the Firewall**

When you run the instance you want, be sure to configure your firewall. When you initially run the instance, the 3389 port is open to all IP addresses. Change the firewall settings to reflect your IP address only. For security purposes, limit your Internet exposure to only your IP address.

**VPN Access**

It is recommended that you use a VPN connection when you use your UVM appliance instance or access your assets.


**UVM Appliance Configuration Wizard**

You must configure your UVM appliance using the UVM Configuration Wizard.

1. On the **Welcome** page, enter the UVM machine name. This must be the same name you created earlier when you were creating a virtual machine in Azure.
2. Select to upload a configuration or click Start the Configuration Wizard without a configuration file.

3. Read the license agreement and click I Agree. You must accept the licensing agreement for the installation to continue.

4. On the Network Settings page, provide the following details:

   **Network State:**
   - Connect to the Internet for licensing and updates. No proxy required: Select if there is an Internet connection and no proxy server.
   - Connect to the Internet for licensing and updates through a proxy server: Select if you are using a proxy server.
   - No Internet connection. Requires performing manual updates: Select if the appliance does not have an Internet connection.

   **SMTP Settings:**
   - Enter the SMTP server IP address and port.
   - Select the SMTP Server requires authentication check box to use credentials to access the server.

5. Click Next. On the Registration Information page, enter the name, organization, and address information.

6. Click Next. On the BeyondTrust Licenses page, enter the license keys.

   If you selected No internet connection in step 5, see Offline Licensing.

   - **Client Portal Login:** You can choose to retrieve license keys automatically from the BeyondTrust client portal. Enter your user name and password, and then click Retrieve Serial Numbers.
   - **Serial Numbers:** Enter the serial number provided when you purchased the product. To access your serial number, log on to the client portal, and select Product Licensing > Managing Your Serial Numbers. Click Get Offline License and follow the instructions on obtaining the license key offline. When received, manually enter the license key.

7. On the User Credentials page, enter the following passwords:
   - **Administrator password:** This password enables you to access the appliance. The email address will receive UVM reports, alerts, and alerts on hardware events.
   - **BeyondInsight user name and password.**
   - **BeyondTrust Updater user name and password.**

8. Click Next.

9. On the Machine Configuration page:
   - Enter the time zone information, and date and time.
   - Select an auto synchronization setting.


11. To save the settings to a configuration file, click Download Configuration File. If for any reason you need to go through the configuration for the appliance again, you can upload the configuration file to apply your settings.
12. Click **Next**, and then click **Proceed to the Roles Configuration**.

13. If the roles configuration is correct, then click **The Current Roles Configuration Looks Good**, otherwise click **Go to The Roles Editor**.
   - In the **Roles Editor**, change the role settings you need, apply your changes and when complete, click **Close Roles Editor**.

14. If the BeyondInsights license includes Password Safe, then you can configure High Availability now. Otherwise, configure HA on the **High Availability** page later.

15. Click **Start Appliance**. The configuration completes and the browser opens to the **Diagnostics** logon page.

16. Restart the UVM after configuration so the scanner can start.
Google UVM Deployments

Introduction

This guide provides important information that will help you get started with your UVM appliance instance, available from the Google Cloud Platform Marketplace (GCP Marketplace).

Prerequisites

License Keys

You must already have license keys for the BeyondTrust solutions that you want to use. Contact BeyondTrust Sales to get the license keys. You will use the keys later when you go through the configuration wizard on the UVM instance.

UVM Instances

We recommend the following machine types. Choose a machine type that can accommodate the number of assets in your organization.

<table>
<thead>
<tr>
<th>Machine Type</th>
<th>vCPU</th>
<th>Memory</th>
<th>Boot Disk</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>n1-standard-8</td>
<td>8</td>
<td>30 GB</td>
<td>SSD Available</td>
<td>1 to 10,000</td>
</tr>
<tr>
<td>n1-standard-16</td>
<td>16</td>
<td>60 GB</td>
<td>SSD Available</td>
<td>10,000 to 20,000</td>
</tr>
</tbody>
</table>

For more information about Google's machine types, please see Machine Types at https://cloud.google.com/compute/docs/machine-types.

Run an Instance

For more information about how to run an instance, please see Virtual machine instances at https://cloud.google.com/compute/docs/instances/.

Create an Instance

1. Log on to the GCP Marketplace, and search for BeyondTrust or BeyondInsight.
2. On the listing page, click **Launch on Compute Engine**.

3. Configure the following settings.
   - **Zone**: Select the zone for your area.
   - **Machine type**: Recommended types:
     - n1-standard-8
     - n1-standard-16
   - **Service Account**: Select a security group.
     - **Firewall**: Select **Allow HTTPS traffic**.

4. Click **Deploy**.

### Retrieve a Windows Password

You must retrieve a Windows password through the Google Cloud website. Google assigns a random default password to the administrator account.

You need this password when you run through the UVM appliance configuration wizard.
1. On the **Instance Details** page, click the instance and select **Set Windows Password**.

![VM instance details](image)

2. Enter the `btadmin` account for the user name. This is the account that you must use to log on to the UVM later.

![Set new Windows password](image)

3. Click **Set**.

### VPN Access

We recommend you use a VPN connection when you use your UVM appliance instance or access your assets.

For more information, please see [Choosing a VPN option](https://cloud.google.com/vpn/docs/how-to/choosing-a-vpn).

### UVM Appliance Configuration Wizard

You must configure your UVM appliance using the UVM Configuration Wizard.

1. Click **Start the Configuration Wizard**.
2. Read the license agreement and click **I Agree**.

You must accept the licensing agreement for the installation to continue.
3. On the **Network Settings** page, provide the following details:

**Network State:**
- **Connect to the Internet for licensing and updates. No proxy required:** Select if there is an Internet connection and no proxy server.
- **Connect to the Internet for licensing and updates through a proxy server:** Select if you are using a proxy server.
- **No Internet connection. Requires performing manual updates:** Select if the appliance does not have an Internet connection.

**SMTP Settings:**
- Enter the SMTP server IP address and port.
- Select the **SMTP Server requires authentication** check box to use credentials to access the server.

4. Click **Next**. On the **Registration Information** page, enter the name, organization, and address information.

5. Click **Next**. On the **BeyondTrust Licenses** page, enter the license keys.

If you selected **No internet connection** in step 3, see Offline Licensing.

- **Client Portal Login:** You can choose to retrieve license keys automatically from the BeyondTrust client portal. Enter your user name and password, and then click **Retrieve Serial Numbers**.
- **Serial Numbers:** Enter the serial number provided when you purchased the product. To access your serial number, log on to the client portal, and select **Product Licensing > Managing Your Serial Numbers**. Click **Get Offline License** and follow the instructions on obtaining the license key offline. When received, manually enter the license key.

6. On the **User Credentials** page, enter the following passwords:

- **Administrator password:** This password enables you to access the appliance. The email address will receive UVM reports, alerts, and alerts on hardware events.

  Retrieve the administrator password as described in Retrieve a Windows Password.

- **BeyondInsight user name and password.**

7. Click **Next**.

8. On the **Machine Configuration** page:

- Enter the name of the appliance (host name), time zone information, and date and time.

  **Note:** *Once entered here, do not change the appliance name.*

  - Select an auto synchronization setting.

9. Click **Next**. On the **Review** page, verify the information. Click **Change** to adjust settings.

10. To save the settings to a configuration file, click **Download Configuration File**. If you need to go through the configuration for the appliance again, you can upload the configuration file to apply your settings.

11. Click **Next**, and then click **Finish** to restart the appliance.

Restarting the appliance can take a few minutes. Proceed after the appliance restarts.