BeyondTrust

U-Series Appliance 4.0
Cloud Deployment Guide

TC:11/1/2022

Table of Contents

U-Series Appliance Cloud Deployment

Deploy your U-Series Appliance instance in the cloud using an Amazon or Azure server.

Amazon U-Series Appliance Deployments

Introduction

This guide provides important information to help you get started with your U-Series 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 when you go through the Configuration Wizard on the U-Series Appliance instance.

U-Series Appliance Instances

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 at https://aws.amazon.com/ec2/instance-types/.

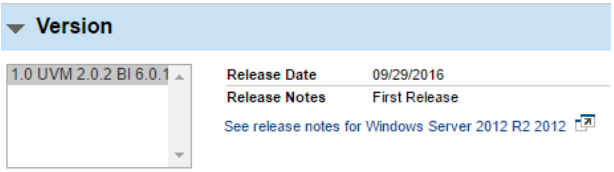
Run an Instance for the Amazon U-Series Appliance Deployment

Log on to the AWS MarketPlace, and search for BeyondTrust or BeyondInsight.

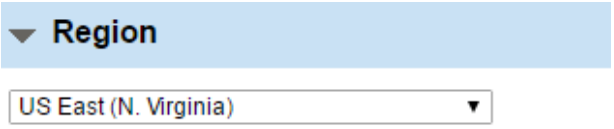
1-Click Launch

1. On the BeyondTrust marketplace website, click **Continue**.
2. Click the **1-Click Launch** tab.
3. Configure the following settings if you want to use the 1-Click Launch option.

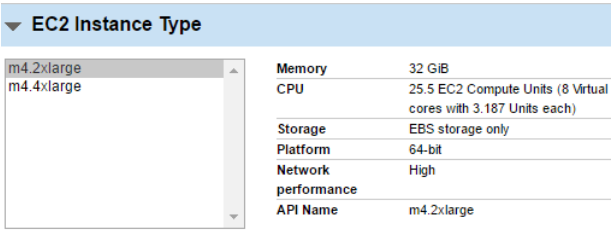
- **Version**



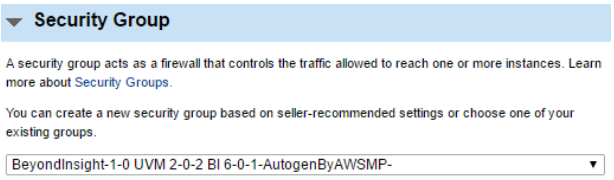
- **Region**



- **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 U-Series Appliance version is selected by default.
4. Select the region and then click **Launch with EC2 Console**.

> *For more information on 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.*

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 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 at https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html#DeleteSecurityGroup.*

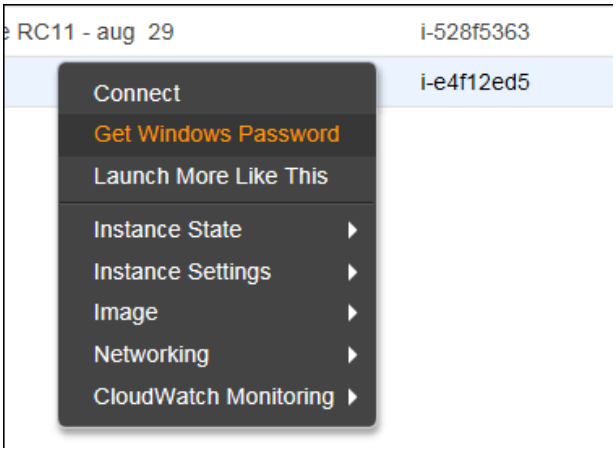
Retrieve a Windows Password

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 the AWS account.

You need this password when you run through the U-Series Appliance Configuration Wizard.

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



> *For more information, please see How do I retrieve my Windows administrator password after launching an instance? at https://aws.amazon.com/premiumsupport/knowledge-center/retrieve-windows-admin-password/.*

VPN Access

We recommend you use a VPN connection when you use your U-Series Appliance instance or access your assets.

> *For more information, please see What Is Amazon VPC? at https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html.*

U-Series Appliance Configuration Wizard for the Amazon Deployment

You must configure your U-Series Appliance using the U-Series Appliance **Configuration Wizard**.

1. Click **Start the Configuration Wizard**.
2. On the **Welcome** page, enter the machine name, or host name, of the U-Series Appliance. Once entered, do not change the U-Series Appliance name.

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 re-deploy the image.

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:

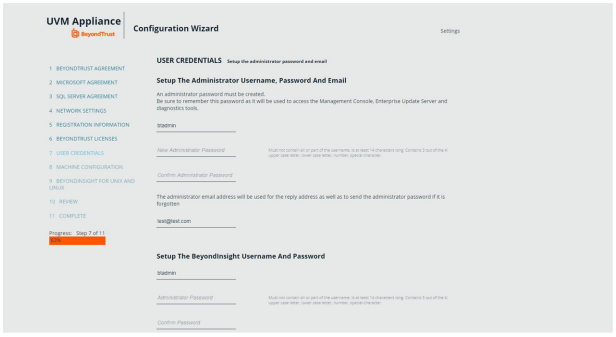
   ### Network State:

   - **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 use a proxy server.
   - **No Internet connection. Requires performing manual updates:** Select if the U-Series Appliance does not have an Internet connection.

   ### SMTP Settings:

   - Enter the SMTP server IP address and port.
   - Check the **SMTP Server requires authentication** 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.
   - **Client Portal Login:** You can choose to retrieve license keys automatically from the BeyondTrust client portal. Enter your username 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:



IMPORTANT!

While the Administrator Name field is editable, you are not allowed to use "Administrator" as a name in this field.

   - **Administrator password:** This password enables you to access the U-Series Appliance. The email address receives U-Series Appliance reports, alerts, and alerts on hardware events.
   - **BeyondInsight username 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.
10. Click **Next**. On the **Review** page, verify the information. Click **Change** to adjust settings.
11. To save the settings to a configuration file, click **Download Configuration File**. If you need to go through the configuration for the U-Series Appliance again, you can upload the configuration file to apply your settings.
12. Click **Next**, and then click **Finish** to restart the U-Series Appliance.

Restarting the U-Series Appliance can take a few minutes. Proceed after the U-Series Appliance restarts.

> *For information on how to retrieve the administrator password, please see "Retrieve a Windows Password" on page 6.*

Take a Snapshot / Back up Your AWS Instance

BeyondTrust provides a way to back up application data on a U-Series 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. Using RDP, connect to your U-Series 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 U-Series Appliance.
3. Right-click your U-Series Appliance instance and select **Connect**. Click **Download Remote Desktop File** to connect to the U-Series Appliance. Use your U-Series Appliance 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 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 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.*

5. After the image is created, restart your U-Series Appliance. Right-click the instance, select **Instance State**, and then select **Start**.

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

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 might 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.

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

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" on page 9 below) and the NVMe drivers ("AWS NVMe Drivers" on page 10 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:

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.
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 file, 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.

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

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.
3. Download the latest driver to the instance.
4. Extract the files from 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.

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

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.
3. If you need to update, download the latest driver package to the instance.
4. Install the driver by running **dpinst.exe**.
5. 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:*
>
> - *"Take a Snapshot / Back up Your AWS Instance" on page 8*
> - *AWS PV Driver Package History at https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/xen-drivers-overview.html#pv-driver-history*
> - *Amazon ENA Driver Versions at https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/enhanced-networking-ena.html*
> - *AWS NVMe Driver Version History at https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/aws-nvme-drivers.html*

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 extract 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 U-Series Appliance Deployments

Introduction

This guide provides important information that will help you get started with your U-Series 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 U-Series Appliance instance.

U-Series Appliance Instances

There are two recommended U-Series Appliance instances available through the Azure marketplace.

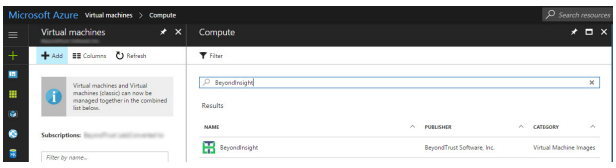
Instance Type	vCPU	Memory	SSD Storage	Dedicated EBS Bandwidth (Mpbs)	Assets
DS4_V2	8	28 GB	56 GB	1000	1 to 10, 000
DS5_V2	16	56 GB	112 GB	2000	10,000 to 20,000

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

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

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

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 Configuration Wizard.

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

IMPORTANT!

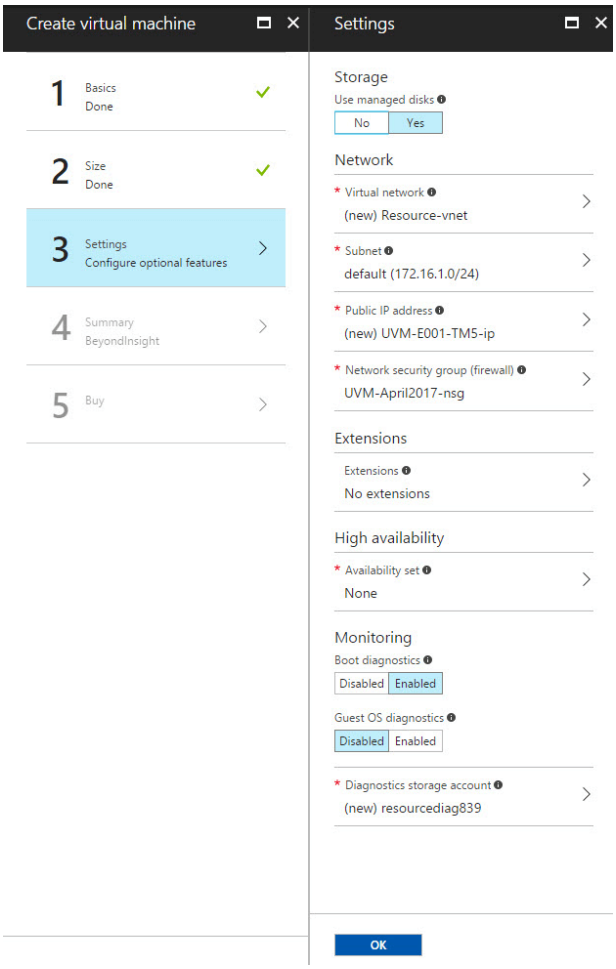
*The username must be **btadmin** during install.*

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



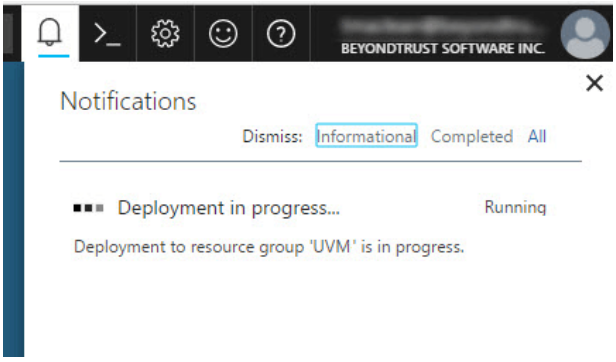
- **Managed Disks:** Click **Yes** to automatically manage the availability of disks to provide data redundancy and fault tolerance without creating and managing storage accounts on your own. Managed disks might not be available in all regions.
- **Virtual Network:** Virtual networks are logically isolated 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.



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

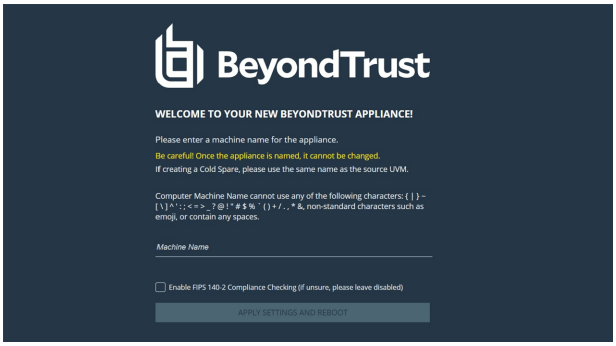
We recommend that you use a VPN connection when you use the U-Series Appliance instance or access your assets.

> *For more information about configuring the VPN tunnel in Azure, please see Create a Site-to-Site connection in the Azure portal at https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal.*

U-Series Appliance Configuration Wizard for the Azure Deployment

You must configure your U-Series Appliance using the U-Series Appliance Configuration Wizard.

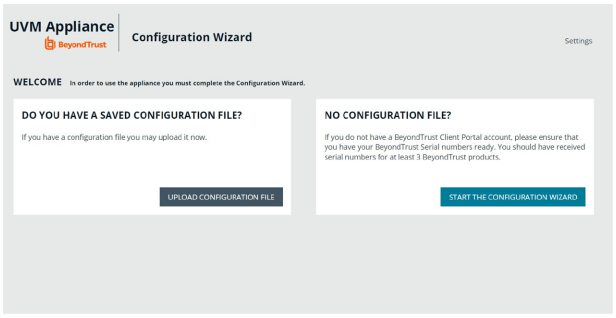
1. On the **Welcome** page, enter the U-Series Appliance machine name. This must be the same name you specified when you created a virtual machine in Azure.



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 re-deploy the image.

2. Choose to upload a configuration file 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 U-Series Appliance does not have an Internet connection.

SMTP Settings:

- Enter the SMTP server IP address and port.
- Check the **SMTP Server requires authentication** 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.
   - **Client Portal Login:** You can choose to retrieve license keys automatically from the BeyondTrust client portal. Enter your username 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:

IMPORTANT!

While the Administrator Name field is editable, you are not allowed to use "Administrator" as a name in this field.

   - **Administrator password:** This password enables you to access the U-Series Appliance. The email address will receive U-Series Appliance reports, alerts, and alerts on hardware events.
   - **BeyondInsight username and password**.
   - **BeyondTrust Updater username 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.
10. Click **Next**. On the **Review** page, verify the information. Click **Change** to adjust settings.
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 U-Series 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. 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 U-Series Appliance after configuration so the scanner can start.

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.

ARM Template

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

> *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.*

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.

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]"
          }
        }
      }
    }
  ]
}
```