



BeyondTrust

Secure Remote Access Virtual Appliance Setup

Table of Contents

SRA Virtual Appliance Installation	4
Review License and Sizing Conditions	4
Deploy the BeyondTrust SRA Virtual Appliance into a VMware Environment	5
Review Prerequisites for VMware	5
Deploy the SRA Virtual Appliance	5
Deploy the BeyondTrust SRA Virtual Appliance into a Hyper-V Environment	12
Review Prerequisites for Hyper-V	12
Configure via Hyper-V Manager	13
Configure via PowerShell	20
Deploy the BeyondTrust SRA Virtual Appliance into a Microsoft Azure Environment ...	23
Review Prerequisites for Microsoft Azure	23
Deploy the SRA Virtual Appliance	23
Deploy the BeyondTrust SRA Virtual Appliance into an Amazon AWS Environment	27
Deploy the BeyondTrust SRA Virtual Appliance into a Nutanix AHV Environment	29
Review Prerequisites for Nutanix	29
Deploy the SRA Virtual Appliance	29
SRA Virtual Appliance First Boot	35
Configure the SRA Virtual Appliance	36
URL reference	37
SRA Virtual Machine Console Administration	38
Configuration Options	38
View SRA Virtual Appliance Health	39
Status Icons	39
Migrate Sites and Licenses to a New BeyondTrust SRA Virtual Appliance	40
Use the Site Migration Tool	40
Manual Site Migration	44
SRA Virtual Appliance Frequently Asked Questions	46
VMware	46
Can I Install VMware Tools Onto My BeyondTrust SRA Virtual Appliance?	46
Can a Time Skew Between My ESXi Host and My BeyondTrust SRA Virtual Appliance Cause Connectivity Issues?	46

What Version of VMware is Supported to Host the BeyondTrust SRA Virtual Appliance? .	46
Does the BeyondTrust SRA Virtual Appliance Require Reserved Resources in VMware?	46
Does BeyondTrust Support Using the VMware Snapshot Functionality?	46
Can I Run the BeyondTrust SRA Virtual Appliance in My Clustered VMware Environment?	47
Can I Specify an Alternate Disk for Recordings?	47
The Virtual Hardware of My BeyondTrust SRA Virtual Appliance is Currently on an Old Version and Needs to be Upgraded. What Are BeyondTrust's Recommendations for Virtual Hardware Version Upgrades?	47
What is the Error: "The OVF certificate file is invalid"?	47
Should the Second Virtual Disk Use Thick or Thin Provisioning?	47
Why Does the Virtual Appliance Download Come as a TAR File?	47
Can the Virtual Hard Disks be Stored in Multiple Datastores?	48
Hyper-V	48
What Version of Hyper-V is Supported to Host the BeyondTrust SRA Virtual Appliance? .	48
Does BeyondTrust Support Using the Hyper-V Snapshot Functionality?	48
Can I Specify an Alternate Disk for Recordings?	48
The Virtual Hardware of My BeyondTrust SRA Virtual Appliance is Currently on an Old Version and Needs to be Upgraded. What Are BeyondTrust's Recommendations for Virtual Hardware Version Upgrades?	48
Microsoft Azure	48
Is the Azure Classic Deployment Model Supported?	48
Do I Need to Configure the Windows PowerShell Script Differently if I Have a Premium Storage Account?	49
Can I Use Any Additional Azure Features Provided by Using Azure Linux Agent with My BeyondTrustSRA Virtual Appliance?	49
Do I Need to Enter My Public IP Anywhere in the BeyondTrust /appliance Interface?	49
Is Failover Needed? Is Failover Supported for Microsoft Azure?	49
Do I Need a Static IP for My BeyondTrust SRA Virtual Appliance?	49
General Issues	49
Can an Evaluation SRA Virtual Appliance be Converted to Production?	49
Can Available Resources be Modified?	49
Can the SRA Virtual Appliance Fail Over to a Slower Storage Tier?	50
Is Cloning SRA Virtual Appliances Supported?	50
Does the SRA Virtual Appliance Support vCenter Site Recovery Manager (SRM)?	50

SRA Virtual Appliance Installation

This guide is designed to walk you through the initial setup and configuration of your BeyondTrust SRA Virtual Appliance. Should you need any assistance, please log into the [Customer Portal](https://beyondtrustcorp.service-now.com/csm) at <https://beyondtrustcorp.service-now.com/csm> to chat with Support.

Review License and Sizing Conditions

Sizing Guidelines	Users	Endpoints	CPU	Memory	Disk 1	Disk 2
Small	1 - 20	1 - 1,000	2 - 4	4 - 8 GB	8 - 128 GB	64+ GB
Medium	20 - 75	1,000 - 10,000	4 - 8	16 - 32 GB	32 - 256 GB	132+ GB
Large	75 - 150	10,000 - 35,000	8 - 16	64 - 128 GB	128 - 1024 GB	1024+ GB
Enterprise	150 - 300	35,000 - 50,000	16 - 32	128 - 512 GB	512 - 4096 GB	1024+ GB
Atlas	300 - 3,000	50,000 - 250,000	Enterprise	Enterprise	Enterprise	Enterprise



Note:

- For Atlas deployments please work with your solutions engineer for more detailed architecture planning.
- If you are an existing BeyondTrust customer and anticipate increasing to more than 300 concurrent users, please log into the [Customer Portal](https://beyondtrustcorp.service-now.com/csm) at <https://beyondtrustcorp.service-now.com/csm> to chat with Support, to ensure that the resources allocated meet your needs. Most situations over 300 concurrent users require transitioning to an Atlas based architecture.
- The range that your deployment falls into is influenced by variables such as API usage, Console usage, size and number of Jump Groups, recording settings, failover replication frequency, and Jump Client upgrade settings.
- BeyondTrust offers a 150 Jump Clients per concurrent license.
- The above numbers assume one session per concurrent user.
- The resource specifications in this document represent recommendations. For troubleshooting purposes, BeyondTrust Technical Support may require your BeyondTrust SRA Virtual Appliance to be given reserved resources matching those listed here.

Deploy the BeyondTrust SRA Virtual Appliance into a VMware Environment

Review Prerequisites for VMware

You must have a VMware account and environment already configured.

Before beginning the BeyondTrust SRA Virtual Appliance setup, please review the following prerequisites:

- VMware vCenter 6.5+ and virtual hardware versions 13+.
- At least 4GB of memory available.
- At least 140GB of storage available.
- One 32GB partition for the BeyondTrust OS, and at least 100GB available for logs and recordings.
- External IP SANs require a 1Gbit or 10Gbit reserved network with a 10K RPM disk or better.



For more information about sizes, please see ["Review License and Sizing Conditions" on page 4.](#)

- A static IP for your SRA Virtual Appliance.
- A private DNS A-record resolving to the static IP of your SRA Virtual Appliance. A public A-record and a public IP are also required if public clients access the B Series Appliance. The DNS A-record is the fully qualified domain name (FQDN) of your site (access.example.com, for example).



Note: "Public clients" include any client software (browsers, BeyondTrust access consoles, endpoint clients, etc.) which connect from external networks and VPN(s) local to the B Series Appliance's network.

- A valid NTP server that is reachable by the B Series Appliance.
- Ensure that the system time between the host ESXi server and the guest BeyondTrust OS are in sync. Variations by only a few seconds can potentially result in performance or connectivity issues.

Deploy the SRA Virtual Appliance

To deploy the BeyondTrust SRA Virtual Appliance into a VMWare environment, follow the steps below:

1. Open the email you received from BeyondTrust Technical Support and click the link to download the BeyondTrust SRA Virtual Appliance OVA file.

BeyondTrust Download Available

 BeyondTrust Build System <mysupport@beyondtrust.com>
To

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Greetings,

Thank you for choosing BeyondTrust for your Secure Remote Access needs!

Your BeyondTrust Virtual Appliance is registered in our systems for [deploy.beyondtrust.com](#) and is ready for download.

To install and configure this Virtual Appliance, follow all of the instructions below:

The BeyondTrust Virtual Appliance**Download your BeyondTrust Virtual Appliance**

- [Click here for your BeyondTrust Virtual Appliance \(VMware\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Hyper-V and Azure\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Nutanix AHV\)](#)

Deploy your BeyondTrust Virtual Appliance in AWS

- Link your AWS account(s) by clicking [here](#).

BeyondTrust Virtual Appliance Setup

1. Follow the appropriate installation guide for your product:
 - o [BeyondTrust RS Virtual Appliance Installation guide](#)
 - o [Privileged Remote Access Virtual Appliance Installation guide](#)
2. When prompted for the Appliance License Key (ALK), enter
3. Install any available BeyondTrust updates using 'Check for Updates'

Contacting BeyondTrust

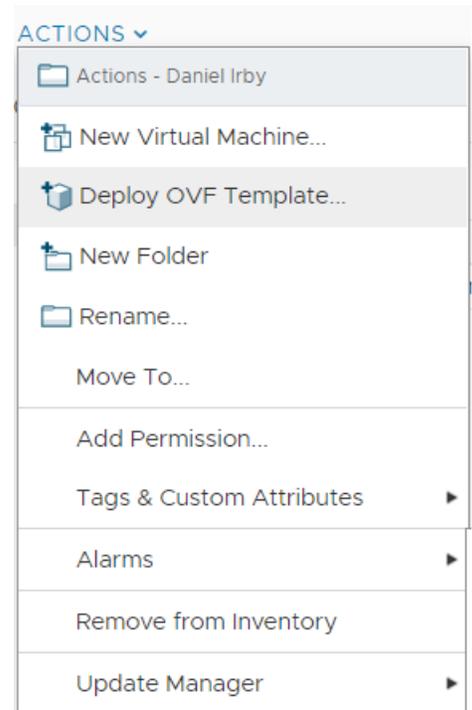
If you need additional assistance, please contact [BeyondTrust Support](#)

We look forward to serving you. If you have any questions, don't hesitate to contact us at mysupport@beyondtrust.com.

Best Regards,

BeyondTrust Support Team

2. Log in to your virtual infrastructure client. You must use an account with permissions to deploy a virtual machine as an OVF template.



3. On the **Select an OVF Template** screen, select the **BeyondTrust.ova** file.

Deploy OVF Template

1 Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

Bomgar.ova

4. Review the OVF template details.

Deploy OVF Template

4 Review details

Review details

Verify the template details.

Publisher	Symantec Class 3 SHA256 Code Signing CA (Trusted certificate)
Product	BeyondTrust Secure Remote Access Appliance
Version	2.0
Vendor	BeyondTrust
Description	BeyondTrust Secure Remote Access Appliance
Download size	653.6 MB
Size on disk	Unknown (thin provisioned)
	1.7 TB (thick provisioned)

5. Read and accept the end user license agreement.

Deploy OVF Template

5 License agreements

License agreements

The end-user license agreement must be accepted.

Read and accept the terms for the license agreement.

I accept all license agreements.

8. Select a resource pool to which you have rights.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select a compute resource
Select the destination compute resource for this operation

Compatibility

✓ Compatibility checks succeeded.

9. Select the datastore on which you want the SRA Virtual Appliance to run. This is where the operating system and session data is stored.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage
Select the storage for the configuration and disk files

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy:

Disable Storage DRS for this virtual machine

Name	Capacity	Provisioned	Free	Type
Bronze_DatastoreCluster	15 TB	11.88 TB	3.12 TB	
PureStorage_Cluster	72.99 TB	62.8 TB	10.19 TB	
Silver_DatastoreCluster	18 TB	13.47 TB	4.53 TB	
Bronze_Datastore_3	4 TB	4.43 TB	630.99 GB	VM
Bronze_Datastore_Cont...	4 TB	2.56 TB	1.77 TB	VM
Bronze_Filetransfer	4 TB	2.01 TB	1.99 TB	VM
Bronze_Replication	4 TB	162 GB	4 TB	VM
Bronze_Zero_Replication	4 TB	3.01 TB	1.28 TB	VM
Bronze_Zero_Replicati...	4 TB	4.72 TB	937.3 GB	VM
Bronze_Zero_Replicati...	4 TB	1.05 TB	3.92 TB	VM
Comple_Cluster_03	2 TB	2.25 TB	713.13 GB	VM

Compatibility

✓ Compatibility checks succeeded.

10. Select the appropriate network mapping for your environment. Your SRA Virtual Appliance can function anywhere in your network with internet access. If you plan to access systems outside of your network, security practices recommend that you place the SRA Virtual Appliance in a DMZ or outside of your internal firewall. Network location considerations are outlined in the table below.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select networks
Select a destination network for each source network:

Source Network	Destination Network
DMZ Network	

1 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

Network Location Considerations for B Series Appliances	
Network Location	Advantages/Disadvantages
Outside your firewall	Does not require that ports 80 and 443 be open inbound for TCP traffic on your firewall. Simplifies the setup process significantly because both the representative and customer clients are built to resolve to a specific DNS; if your registered DNS resolves to a public IP address directly assigned to your B Series Appliance, no additional setup is required by you to initiate a session.
DMZ	Might require additional setup depending on your router or routers.
Inside your firewall	Requires port forwarding on your firewall and possibly additional setup of your NAT routing and internal DNS.

- Return to the email you received from BeyondTrust Technical Support, and copy the Appliance License Key. In the Deployment Wizard, paste the key into the field.

 **Note:** If for some reason you are unable to provide the Appliance License Key at this time, you can manually enter it later, from the virtual machine console.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template
Customize the deployment properties of this software solution.

✓ All properties have valid values

License	1 settings
Appliance License Key (ALK)	The Appliance License Key will be provided by Bomgar when you purchased your appliance. If you don't have it right now, you may leave this blank and proceed with deployment. Please contact Bomgar Support to obtain your ALK, which can be configured later after you boot the system.

CANCEL

- Review your settings and click **Finish**.
- The SRA Virtual Appliance deploys in the location and with the resources you have specified.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- ✓ 9 Customize template
- 10 Ready to complete**

Ready to complete
Click Finish to start creation.

Provisioning type	Deploy from template
Name	Bomgar
Template name	Bomgar
Download size	594.6 MB
Size on disk	1.7 TB
Folder	...
Resource	...
Storage mapping	1
All disks	Datastore: PureStorage_Cluster; Format: Thick provision lazy zeroed
Network mapping	1
DMZ Network	...
IP allocation settings	
IP protocol	IPv4
IP allocation	Static - Manual

CANCEL



For detailed information about network locations, please see [The BeyondTrust Appliance B Series in the Network](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz) at www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz.

Deploy the BeyondTrust SRA Virtual Appliance into a Hyper-V Environment

Review Prerequisites for Hyper-V

You must have a Hyper-V account and environment already configured.

Before beginning the BeyondTrust SRA Virtual Appliance setup, please review the following prerequisites:

- Hyper-V 2012 R2 (standalone or as a role) and Generation 2 hardware only.
- At least 4GB of memory available.
- At least 140GB of storage available.
- One 32GB partition for the BeyondTrust OS, and at least 100GB available for logs and recordings.
- External IP SANs require a 1Gbit or 10Gbit reserved network with a 10K RPM disk or better.



For more information about sizes, please see "[Review License and Sizing Conditions](#)" on page 4.

- A static IP for your SRA Virtual Appliance.
- A private DNS A-record resolving to the static IP of your SRA Virtual Appliance. A public A-record and a public IP are also required if public clients access the B Series Appliance. The DNS A-record is the fully qualified domain name (FQDN) of your site (access.example.com, for example).



Note: "Public clients" include any client software (browsers, BeyondTrust access consoles, endpoint clients, etc.) which connect from external networks and VPN(s) local to the B Series Appliance's network.

- A valid NTP server that is reachable by the B Series Appliance.
- Ensure that the system time between the host ESXi server and the guest BeyondTrust OS are in sync. Variations by only a few seconds can potentially result in performance or connectivity issues.

Configure via Hyper-V Manager

1. Open the email you received from BeyondTrust Technical Support and click the link to download the **BeyondTrust SRA Virtual Appliance (Hyper-V and Azure)** file.
2. Save the file to an appropriate location to import to your Hyper-V host, and then double-click the ZIP file to extract your SRA Virtual Appliance.

3. Start Hyper-V Manager.
4. Ensure the server you wish to install the SRA Virtual Appliance on is present. Right-click the desired server and select **New > Virtual Machine** to start the **New Virtual Machine Wizard**.

BeyondTrust Download Available

 BeyondTrust Build System <mysupport@beyondtrust.com>
To

 Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Greetings,

Thank you for choosing BeyondTrust for your Secure Remote Access needs!

Your BeyondTrust Virtual Appliance is registered in our systems for deploy.beyondtrust.com and is ready for download.

To install and configure this Virtual Appliance, follow all of the instructions below:

The BeyondTrust Virtual Appliance

Download your BeyondTrust Virtual Appliance

- [Click here for your BeyondTrust Virtual Appliance \(VMware\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Hyper-V and Azure\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Nutanix AHV\)](#)

Deploy your BeyondTrust Virtual Appliance in AWS

- Link your AWS account(s) by clicking [here](#).

BeyondTrust Virtual Appliance Setup

1. Follow the appropriate installation guide for your product:
 - o [BeyondTrust RS Virtual Appliance Installation guide](#)
 - o [Privileged Remote Access Virtual Appliance Installation guide](#)
2. When prompted for the Appliance License Key (ALK), enter
3. Install any available BeyondTrust updates using 'Check for Updates'

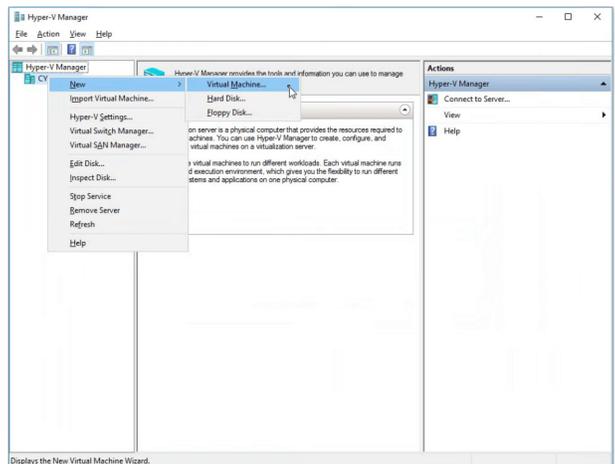
Contacting BeyondTrust

If you need additional assistance, please contact [BeyondTrust Support](#)

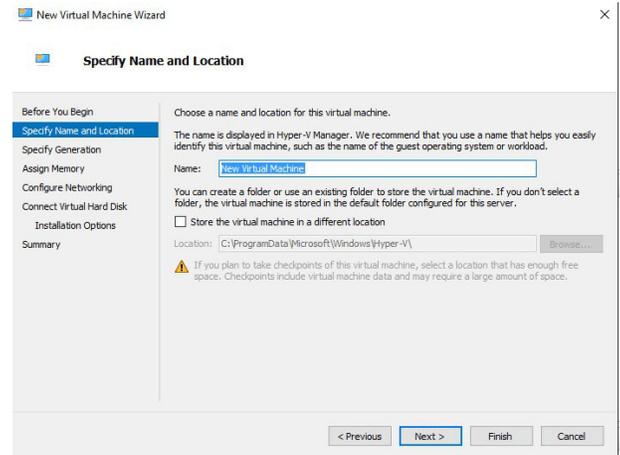
We look forward to serving you. If you have any questions, don't hesitate to contact us at mysupport@beyondtrust.com.

Best Regards,

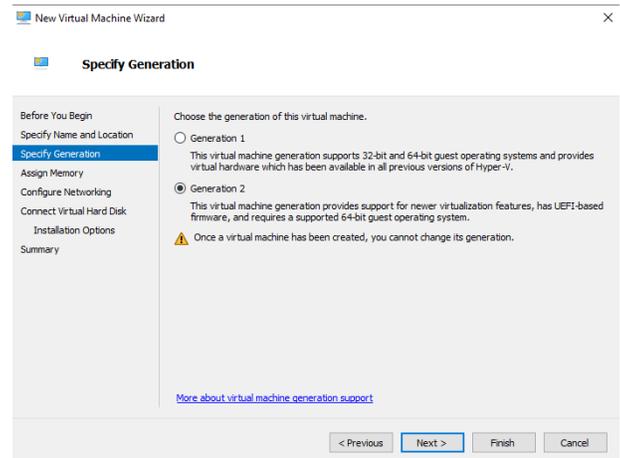
BeyondTrust Support Team



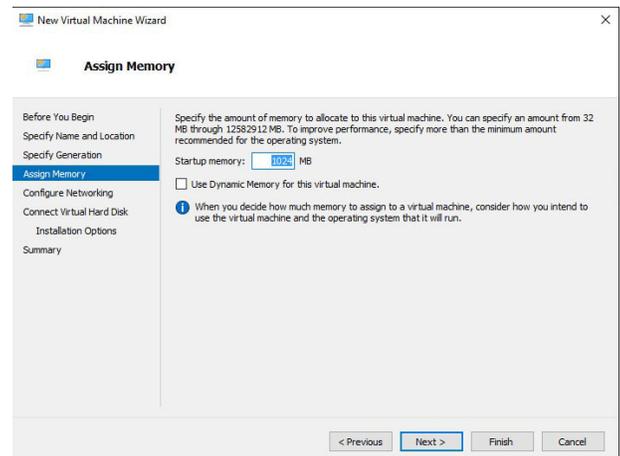
5. Enter a display name to easily identify the virtual machine, and choose a location for the BeyondTrust SRA Virtual Appliance. Then click **Next**.



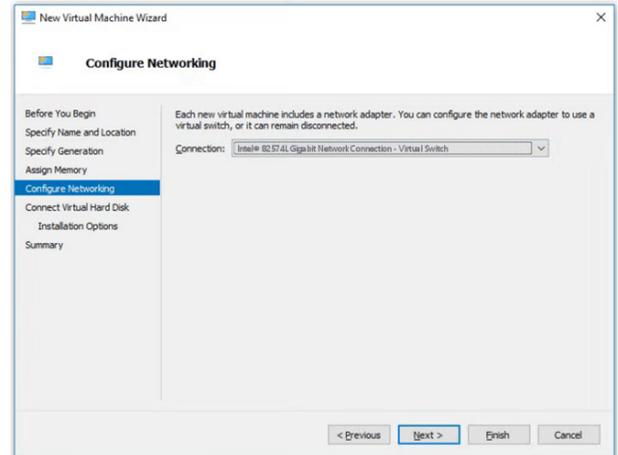
6. Select **Generation 2** and click **Next**.



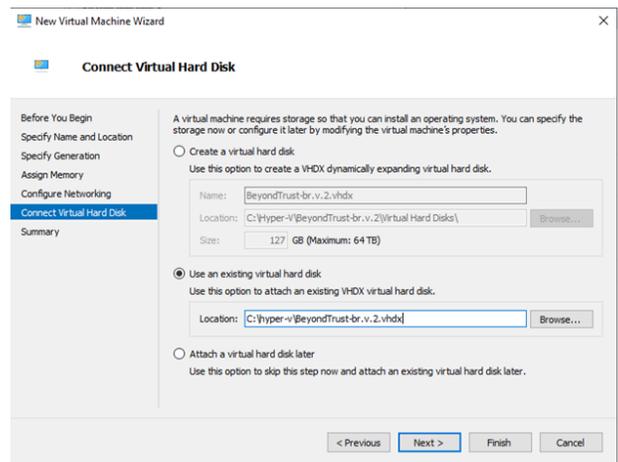
7. Enter **4096 MB** for a small deployment, or **8192 MB** for any other size. Do not use dynamic memory. Click **Next**.



8. From the **Connection** dropdown, select the network interface option that best suits your needs, and then click **Next**.

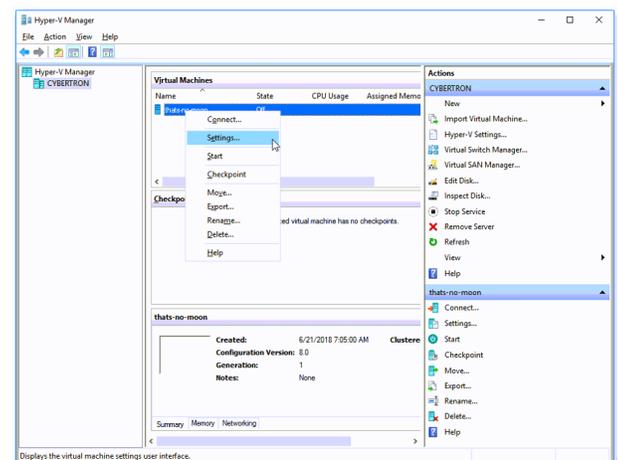


9. Select **Use an existing virtual hard disk** and select the **BeyondTrust-br.v.2.vhdx** file that was extracted earlier from the download archive. BeyondTrust recommends putting the VHD file in the same location where the VM resides. Click **Next**.

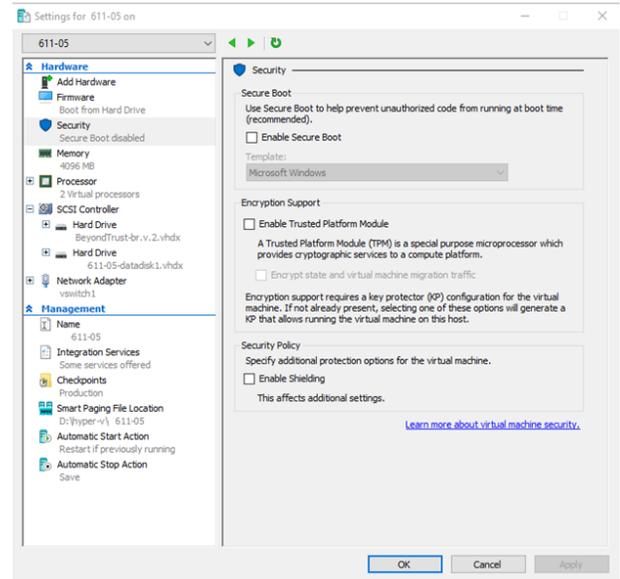


10. Review the VM details on the **Summary** page and click **Finish**.

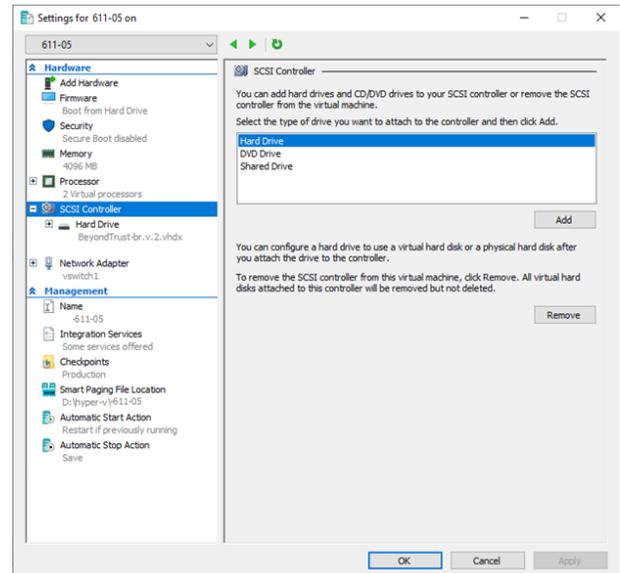
11. Once the VM has been created, right-click it and select **Settings**.



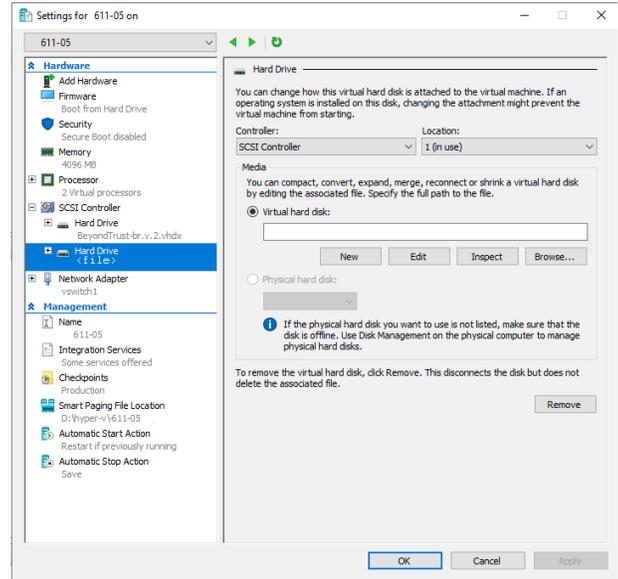
- Click **Security**, and uncheck **Enable Secure Boot**. This helps to prevent unauthorized code from running when the machine is started.



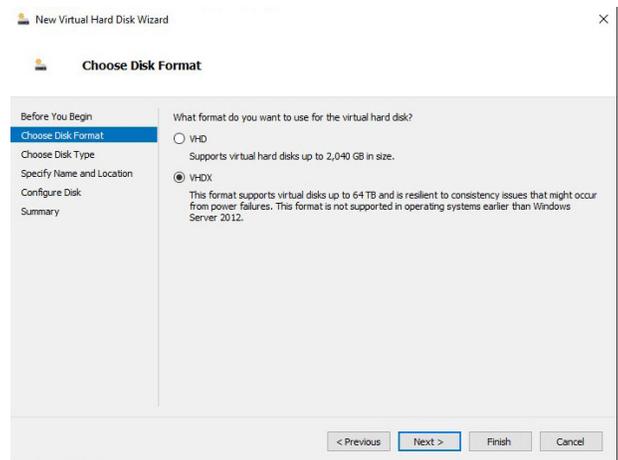
- Click **SCSI Controller** and select **Hard Drive**. Then click **Add**.



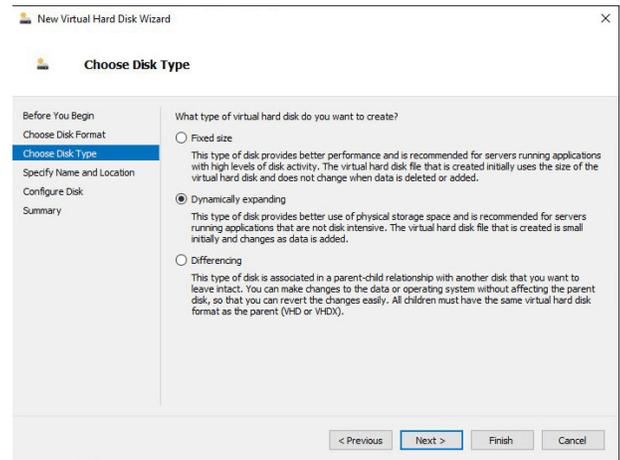
- Click the **New** button to create a new virtual hard disk. The **New Virtual Hard Disk Wizard** launches.



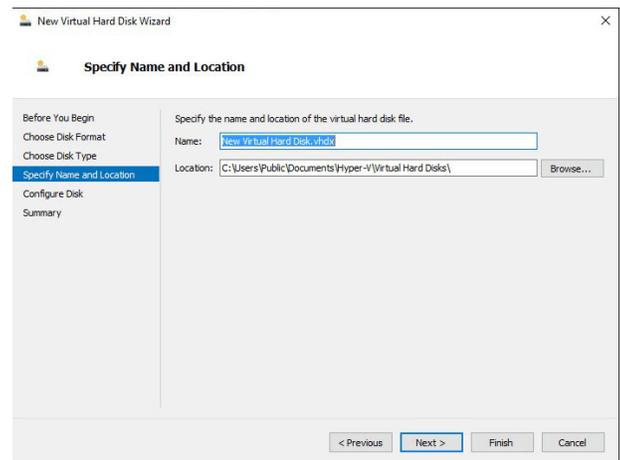
- On the **Choose Disk Format** page, select **VHDX** and click **Next**.



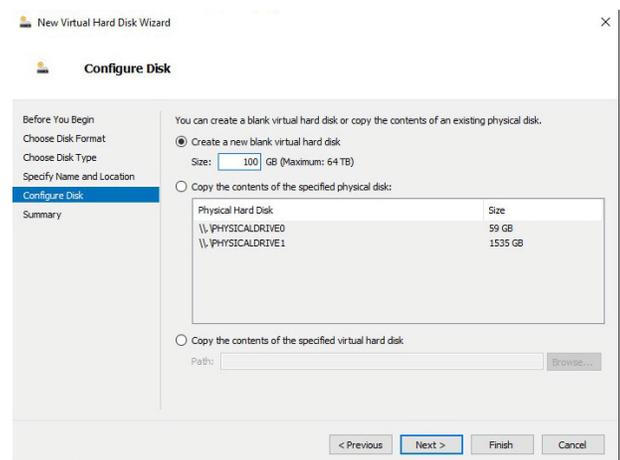
- Choose your desired disk type on the **Choose Disk Type** page, and click **Next**.



- On the **Specify Name and Location** page, provide a name and location for the virtual hard disk file. Click **Next**.



- Select **Create a new blank virtual hard disk** and specify a size of **100 GB**. Click **Next**.

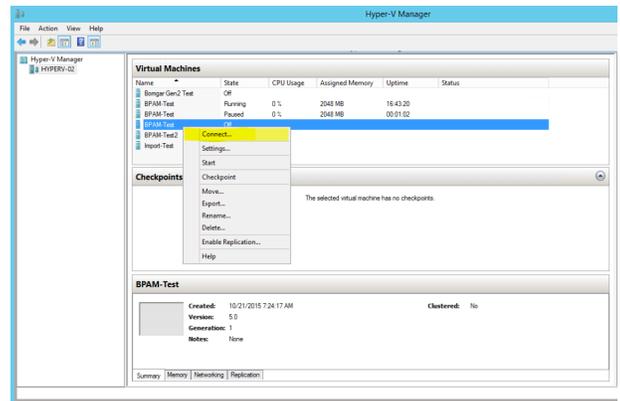


- Review the hard disk option on the **Summary** page and then click **Finish**.
- If your sizing requirements are for a medium or larger virtual machine, follow the above steps to create an additional disk, and specify a size of **500 GB**.

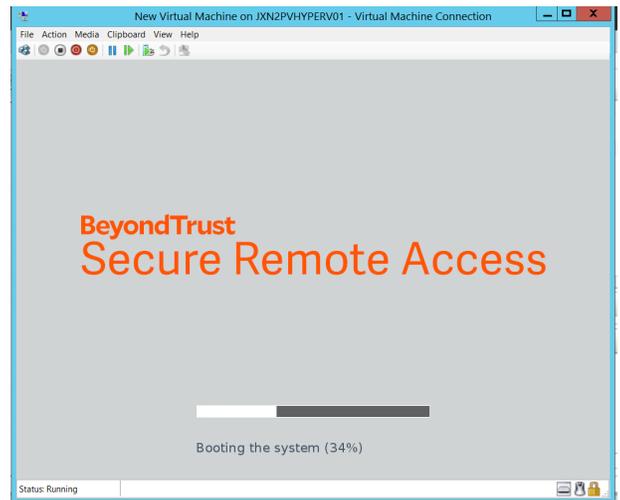


For more information about sizes, please see ["Review License and Sizing Conditions" on page 4.](#)

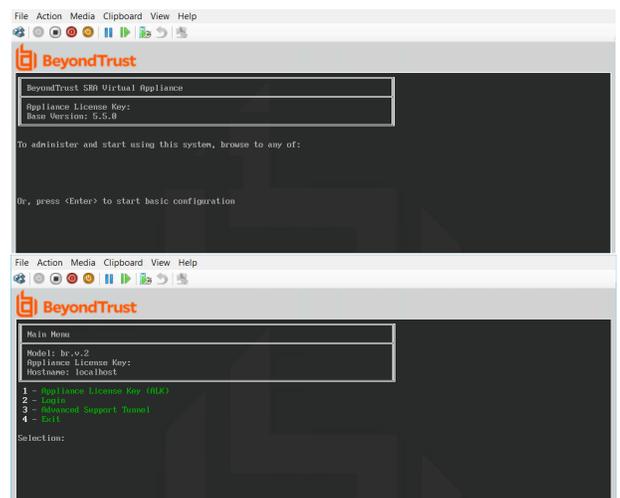
21. Finally, right click on the virtual machine and select **Connect**.



22. Click the **Start** button to start the Hyper-V virtual machine.



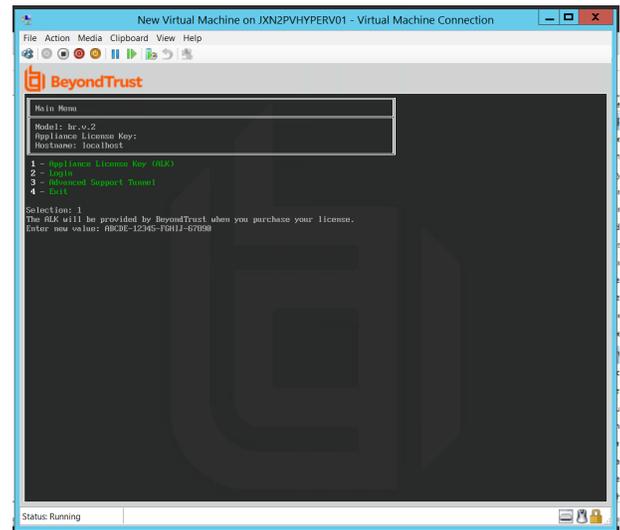
23. From the initial console configuration screen, press **Enter**, and then press **1** to enter the Appliance License Key.



- Go back to the email you received from BeyondTrust Technical Support, get the Appliance License Key, enter it here, and then press **Enter**.



Note: If you are unable to provide the Appliance License Key at this time, you can manually enter it later from the virtual machine console.



Configure via PowerShell

- Open the email you received from BeyondTrust Technical Support and click the link to download the **BeyondTrust SRA Virtual Appliance (Hyper-V and Azure)** file.
- Save the file to an appropriate location to import to your Hyper-V host, and then double-click the ZIP file to extract your SRA Virtual Appliance.

BeyondTrust Download Available

 BeyondTrust Build System <mysupport@beyondtrust.com>
To

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Greetings,

Thank you for choosing BeyondTrust for your Secure Remote Access needs!

Your BeyondTrust Virtual Appliance is registered in our systems for deploy.beyondtrust.com and is ready for download.

To install and configure this Virtual Appliance, follow all of the instructions below.

The BeyondTrust Virtual Appliance

Download your BeyondTrust Virtual Appliance

- Click here for your BeyondTrust Virtual Appliance (VMware)
- Click here for your BeyondTrust Virtual Appliance (Hyper-V and Azure)
- Click here for your BeyondTrust Virtual Appliance (Nutanix AHV)

Deploy your BeyondTrust Virtual Appliance in AWS

- Link your AWS account(s) by clicking [here](#).

BeyondTrust Virtual Appliance Setup

- Follow the appropriate installation guide for your product:
 - [BeyondTrust RS Virtual Appliance Installation guide](#)
 - [Privileged Remote Access Virtual Appliance Installation guide](#)
- When prompted for the Appliance License Key (ALK), enter
- Install any available BeyondTrust updates using "Check for Updates"

Contacting BeyondTrust

If you need additional assistance, please contact [BeyondTrust Support](mailto:mysupport@beyondtrust.com).

We look forward to serving you. If you have any questions, don't hesitate to contact us at mysupport@beyondtrust.com.

Best Regards,

BeyondTrust Support Team

- Double click **BeyondTrust Privileged Remote Access-hyperv-azure.exe** within your file browser to begin extraction.
- Choose the destination directory for the extraction and click **Extract**.



Note: Extract to a directory where you want to run the virtual machine from.

- When extraction is complete, the following files appear in the designated location:
 - Deploy-AzBeyondTrustVM.ps1:** PowerShell script to assist deployment of your appliance to Hyper-V.
 - Deploy-HyperVBeyondTrustVM.ps1:** PowerShell script to assist Azure deployment. Not used.

- **BeyondTrust-br.v.2.vhdx.**

6. **Deploy- HyperVBeyondTrustVM.ps1** uses the Hyper-V PowerShell module. Right-click on the script and click **Edit**.

7. Once the PowerShell script opens, locate the following variables and edit for your environment:

- **\$vmName:** The name for the virtual machine.
- **\$vmLocation:** The directory that the virtual machine resides in.
- **\$vmSwitch:** The virtual switch this virtual machine uses.
- **\$beyondtrustVHD:** The name of the VHDX. Leave as is.

Deploy-HyperVBeyondTrustVM.ps1* X

```

1  #####
2  ## BeyondTrust Hyper-V Deployment script
3  ##
4  ## This script will create a vm using
5  ## the BeyondTrust VHD.
6  ## Refer to BeyondTrust support documentation for custom
7  ## deployment options.
8  ##
9  ## Required variables:
10 ## vmName: What to call this vm in Hyper-V
11 ## vmLocation: the folder to create this vm in
12 ## vmSwitch: the switch to attach this vm to
13 ## BeyondTrustVHD:
14 ##     The name of the vhd provided by BeyondTrust.
15 ##     THIS VHD SHOULD ALREADY BE IN $vmLocation
16 #####
17
18 $vmName = ""
19 $vmLocation = ""
20 $vmSwitch = ""
21 $beyondtrustVHD = "BeyondTrust-br.v.2.vhd"
22

```

8. Set the value of the **\$size** variable to the desired deployment size for your virtual machine. The options are:

- **small**
- **medium**
- **large**

```

22
23 #####
24 ## Select a size based on the number of
25 ## licenses or endpoints. Only uncomment one.
26 ## (Refer to BeyondTrust support for details)
27 ##
28 ## Small (1-20 licenses or 1-3000 endpoints) (Default)
29 $size = "small"
30
31 ## Medium (20-100 licenses or 3001-15000 endpoints)
32 #$size = "medium"
33
34 ## Large (100+ licenses or 15000+ endpoints)
35 #$size = "large"

```

 For more information about sizes, please see ["Review License and Sizing Conditions" on page 4.](#)

9. Save and run the script in **Windows Powershell**.
10. Once complete, you can view the newly created virtual machine in **Hyper-V Manager** or via PowerShell Hyper-V commands.

Network Location Considerations for B Series Appliances	
Network Location	Advantages/Disadvantages
Outside your firewall	Does not require that ports 80 and 443 be open inbound for TCP traffic on your firewall. Simplifies the setup process significantly because both the representative and customer clients are built to resolve to a specific DNS; if your registered DNS resolves to a public IP address directly assigned to your B Series Appliance, no additional setup is required by you to initiate a session.
DMZ	Might require additional setup depending on your router or routers.
Inside your firewall	Requires port forwarding on your firewall and possibly additional setup of your NAT routing and internal DNS.

Deploy the BeyondTrust SRA Virtual Appliance into a Microsoft Azure Environment

Review Prerequisites for Microsoft Azure

You must have a Microsoft Azure account and environment, including Microsoft Azure Resource Manager (ARM), already configured.

For deployment via Microsoft Azure, make sure the following is in place prior to deployment:

- A resource group.
- A storage account with a VHDX container.
- A VNET and subnet has been configured.

For deployment via Powershell, make sure the following is in place prior to deployment:

- Powershell AZ module installed.
- Powershell Hyper-V module installed.



For more information about installing and configuring the Azure PowerShell Module, please see [Install and configure Azure PowerShell](https://docs.microsoft.com/en-us/powershell/azure/install-Az-ps?view=azps-4.1.0) at <https://docs.microsoft.com/en-us/powershell/azure/install-Az-ps?view=azps-4.1.0>.

Deploy the SRA Virtual Appliance

To deploy the BeyondTrust SRA Virtual Appliance into a Microsoft Azure environment, follow the steps below:

1. Open the email you received from BeyondTrust Technical Support and click the **Click Here for your BeyondTrust Virtual Appliance (Hyper-V and Azure)** link to download the file.
2. Click **BeyondTrust Privileged Remote Access-hyperv-azure.exe** within your file browser to begin installation.
3. If you receive a **Security Warning** prompt, click **Run**.
4. Choose where you wish the files to be extracted. Click **Extract**.
5. When extraction is complete, **Deploy-AzBeyondTrustVM.ps1**, **Deploy- HyperVBeyondTrustVM.ps1**, and **BeyondTrust-br.v.2.vhdx** files appear in the location you designated during the extraction process. A PowerShell script is provided to assist in the deployment of your B Series Appliance to Azure: **Deploy-AzBeyondTrustVM.ps1**. A second script, **Deploy-HyperVBeyondTrustVM.ps1**, is provided to assist with Hyper-V deployments, and should not be used to deploy to Azure. **Deploy-AzBeyondTrustVM.ps1** uses the Az module. Right-click **Deploy-AzBeyondTrustVM.ps1** and click **Edit**.

BeyondTrust Download Available

 BeyondTrust Build System <mysupport@beyondtrust.com>
To

 Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Greetings,

Thank you for choosing BeyondTrust for your Secure Remote Access needs!

Your BeyondTrust Virtual Appliance is registered in our systems for `deploy.beyondtrust.com` and is ready for download.

To install and configure this Virtual Appliance, follow all of the instructions below:

The BeyondTrust Virtual Appliance

Download your BeyondTrust Virtual Appliance

- [Click here for your BeyondTrust Virtual Appliance \(Vmware\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Hyper-V and Azure\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Nutanix AHV\)](#)

Deploy your BeyondTrust Virtual Appliance in AWS

- Link your AWS account(s) by clicking [here](#).

BeyondTrust Virtual Appliance Setup

1. Follow the appropriate installation guide for your product:
 - o [BeyondTrust RS Virtual Appliance Installation guide](#)
 - o [Privileged Remote Access Virtual Appliance Installation guide](#)
2. When prompted for the Appliance License Key (ALK), enter
3. Install any available BeyondTrust updates using 'Check for Updates'

Contacting BeyondTrust

If you need additional assistance, please contact [BeyondTrust Support](#).

We look forward to serving you. If you have any questions, don't hesitate to contact us at mysupport@beyondtrust.com.

Best Regards,

BeyondTrust Support Team

6. Once the PowerShell script opens, locate **STEP 1** and modify the following variables based on the specifics of your Microsoft Azure environment:

- **resourceGroupName**
- **storageAccountName**
- **location** (westus, for example)
- **vnetName**
- **subnetName**

```

12 #####
13 # Instructions
14 #
15 # This script deploys a BeyondTrust Appliance to the Microsoft Azure
16 #
17 # STEP 1 (REQUIRED): Fill out these variables
18 # resourceGroupName:
19 #   The name of the Resource Group to create the VM in
20 # storageAccountName: The name of the Storage Account to
21 #   upload and create VHDs in
22 # NOTES: This must already exist with a container
23 #   named the same as 'vhdFolder' (default: vhds)
24 # vnetName: The name of the virtual network to add the NIC to
25 # subnetName: The name of the subnet to add the NIC to
26 # location: The Location that the vm should be created in
27 #   (must match the location of previous settings)
28 # vmName: what name to set the vm to in Azure
29 #   (Name must only contain alphanumeric (A-z 0-9)
30 #   dash (-), underscore (_), or period (.))
31 #####
32
33 $resourceGroupName = ""
34 $storageAccountName = ""
35 $vnetName = ""
36 $subnetName = ""
37 $location = ""
38 $vmName = "BeyondTrust-br.v.2"

```

 **Note:** The *vmName* does not need to be changed.

 **Note:** The storage account used for storing the Azure Virtual Appliance must be General purpose v2.

7. In the **Deploy-AzBeyondTrustVM.ps1** script, set the value of **\$size** to the desired deployment size of your SRA Virtual Appliance. The options are:

- **small**
- **medium**
- **large**

```

40 #####
41 # REQUIRED
42 # Sizes:
43 #   small: 1-20 licenses
44 #   medium: 21-100 licenses
45 #   large: 100+ licenses
46 #####
47
48 $size = "small"
49
50 #####
51 # REQUIRED
52 # Subscription and Tenant are required for Az module
53 #####
54
55 $subscription = ""
56 $tenant = ""
57
58 #####
59 # STEP 2 (OPTIONAL): Change these variables as needed
60 # vhdFolder: the blob storage container in the storageAccount
61 #   where VHDs will be created (default: vhds)
62 # createPublicIP: Whether to create this vm with or without a
63 #   public IP [$true or $false] (default: $true)
64 # networkSecurityGroup: the nsg to use or create
65 #   (if it does not exist, will create one
66 #   with ports 80 and 443 open)
67 #   (default: BeyondTrust-NSG)
68 #####
69
70 $vhdFolder = "vhds"
71 $createPublicIP = $true
72 $networkSecurityGroup = "BeyondTrust-NSG"
73
74 # Azure US Government Account
75 # Set this to $true if your account is in Azure US Government
76 $azureUSGovernment = $false
77
78 #####
79 # STEP 4: Save this file and run
80 #####

```

 For more information about sizes, please see ["Review License and Sizing Conditions" on page 4.](#)

8. The **Az module** requires a subscription and tenant ID from Azure to deploy. Enter this information.
9. Change optional variables as required for your Microsoft Azure environment.
10. For US government accounts, set the value of **\$azureUSGovernment** to **\$true**.

11. Save, then run the script in **Windows PowerShell**.

```

Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\Users\> cd .\Downloads\BeyondTrust-br-v.2\
PS C:\Users\Downloads\BeyondTrust-br-v.2> ls

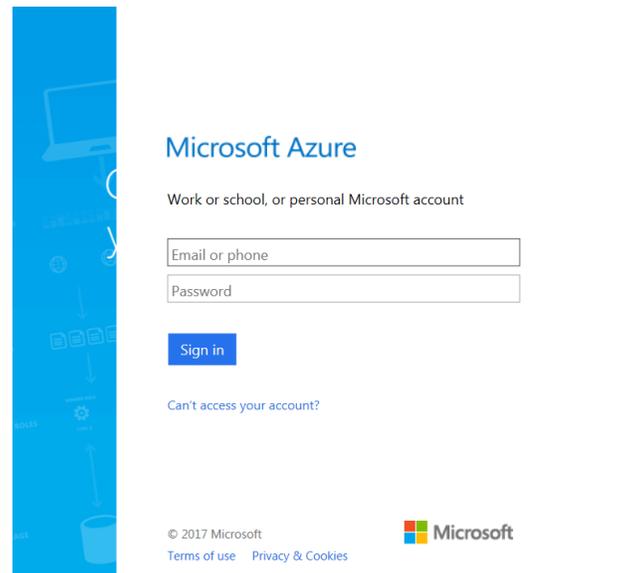
Directory: C:\Users\Downloads\BeyondTrust-br-v.2

Mode                LastWriteTime         Length Name
----                -
a-----          7/30/2021  1:36 PM           3560964098 BeyondTrust-br-v.2.vhdx
a-----          8/12/2021  10:26 AM           11183 Deploy-AzBeyondTrustVM.ps1
a-----          8/12/2021  10:28 AM            2224 Deploy-HyperVBeyondTrustVM.ps1

PS C:\Users\Downloads\BeyondTrust-br-v.2> .\Deploy-AzBeyondTrustVM.ps1
  
```

12. When prompted, enter your credentials and sign into your **Microsoft Azure** account.

13. Next, the system configures an MD5 hash, uploads the SRA Virtual Appliance into your Azure environment, and configures a public IP address for your BeyondTrust SRA Virtual Appliance.



```

Uploading
2.7% complete; Remaining Time: 00:05:59; Throughput: 37.1Mbps
[OO]
00:05:59 remaining.
  
```

14. You are prompted to go to the IP address configured for your SRA Virtual Appliance. The message reads *For Appliance administration, go to <https://xx.xx.xx.xxx/appliance>*.

```

Administrator: C:\Windows\system32\cmd.exe
PS C:\Users\Downloads\BeyondTrust-br-v.2> .\Deploy-AzBeyondTrustVM.ps1

Checking for "BeyondTrust-br-v.2.vhd" in gastorageeast\vhd
BeyondTrust-br-v.2.vhd not found. Uploading to gastorageeast\vhd
MD5 hash is being calculated for the file C:\Users\Downloads\BeyondTrust-br-v.2\BeyondTrust-br-v.2.vhd.
MD5 hash calculation is completed.
Elapsed time for the operation: 00:01:04
Creating new page blob of size 34359738880...
Elapsed time for upload: 00:08:27
-----
Account      SubscriptionName  TenantId  Environment
-----
@beyondtrust.com  dev              82072f05  AzureCloud

LocalFilePath : C:\Users\Downloads\BeyondTrust-br-v.2\BeyondTrust-br-v.2.vhd
DestinationUri : https://storageeast.blob.core.windows.net/vhds/BeyondTrust-br-v.2.vhd

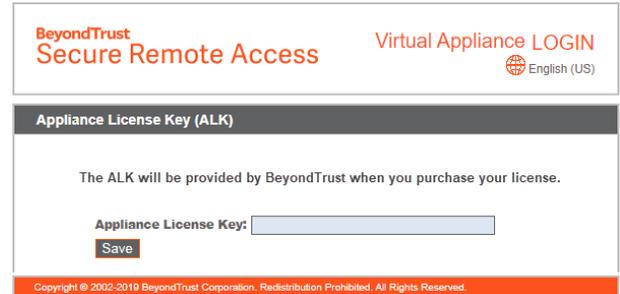
BeyondTrust-NSG found
Patching VNet and Subnet information
Creating a new Dynamic Public IP
Creating a new NIC
Attaching OS disk BeyondTrust-br-v.2_os_disk
Attaching BeyondTrust-br-v.2_data_disk
Creating the BeyondTrust Virtual Machine
WARNING: Since the VM is created using premium storage or managed disk, existing standard storage account,
gastorageeast, is used for boot diagnostics.

RequestID      :
IsSuccessStatusCode : True
StatusCode     : OK
ReasonPhrase   : OK

You can access this appliance at https://20.185.153.167/appliance

PS C:\Users\Downloads\BeyondTrust-br-v.2>
  
```

15. On the /appliance page, enter your **Appliance License Key** provided in the email from BeyondTrust Technical Support. Click **Save**.
16. To setup a persistent URL for your SRA Virtual Appliance, you can perform one of two options:
 - In the Azure console, set the SRA Virtual Appliance's external IP to static. Then assign your DNS entry to that external IP.
 - Apply a DNS name within Azure. Set a CNAME record pointed to that address.



For information about using BeyondTrust Vault with an Microsoft Azure Active Directory Domain Services Account, please see the [Beyond Trust Vault Guide](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/index.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/vault/index.htm>.

Deploy the BeyondTrust SRA Virtual Appliance into an Amazon AWS Environment



Note: You must have an Amazon AWS account and support plan already configured. You are also responsible for registering the DNS hostname for your site.

Administrators can deploy the BeyondTrust SRA Virtual Appliance into their Amazon Web Services (AWS) environment by following the steps below.

1. Open the email you received from BeyondTrust Technical Support and select the **Link your AWS account(s)** link to be redirected to the BeyondTrust site.

BeyondTrust Download Available

 BeyondTrust Build System <mysupport@beyondtrust.com>
To

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Greetings,

Thank you for choosing BeyondTrust for your Secure Remote Access needs!

Your BeyondTrust Virtual Appliance is registered in our systems for [deploy.beyondtrust.com](#) and is ready for download.

To install and configure this Virtual Appliance, follow all of the instructions below.

The BeyondTrust Virtual Appliance

Download your BeyondTrust Virtual Appliance

- [Click here for your BeyondTrust Virtual Appliance \(VMware\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Hyper-V and Azure\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Nutanix AHV\)](#)

Deploy your BeyondTrust Virtual Appliance in AWS

- Link your AWS account(s) by clicking [here](#).

BeyondTrust Virtual Appliance Setup

1. Follow the appropriate installation guide for your product:
 - o [BeyondTrust RS Virtual Appliance Installation guide](#)
 - o [Privileged Remote Access Virtual Appliance Installation guide](#)
2. When prompted for the Appliance License Key (ALK), enter
3. Install any available BeyondTrust updates using 'Check for Updates'

Contacting BeyondTrust

If you need additional assistance, please contact [BeyondTrust Support](#).

We look forward to serving you. If you have any questions, don't hesitate to contact us at mysupport@beyondtrust.com.

Best Regards,

BeyondTrust Support Team

BeyondTrust Secure Remote Access

Please enter your AWS GovCloud (US) or Commercial AWS Account ID to obtain access to the BeyondTrust Virtual Appliance. It will be shared with this account as a Private AMI within an hour. For more information on how to locate your AWS Account ID, see [this guide](#). For more information and further steps to deploy your BeyondTrust Virtual Appliance, please review our Virtual Appliance Installation Guide and other documentation at: [beyondtrust.com/docs](#).

Enter AWS Account ID:

[Add Account ID](#)

Registered AWS Account IDs

No Accounts exist

2. Enter your **Commercial AWS Account ID** or **Government AWS Account ID** in the text box and click **Add Account ID**. Your SRA Virtual Appliance is shared with your Amazon AWS account as a Private Amazon Machine Image (AMI) within an hour. The AMI is shared to each of your AWS regions.



Note: If you are uncertain what your AWS Account ID is, the email contains a link to an Amazon help page that details how to find it.

3. In the AWS EC2 Dashboard, in the **AWS services section**, click the **EC2** link to start the wizard.
4. Browse to **Images > AMI**.
5. Select **Private Images** from the dropdown.
6. Select the SRA Virtual Appliance (for example, **BeyondTrust SRA Appliance - 6.x.x**) in the AMI list. This is the base software image, which must next be updated and configured.
7. Click the **Launch** button.
8. Choose an instance type. BeyondTrust supports all T3 and M5 instance types.



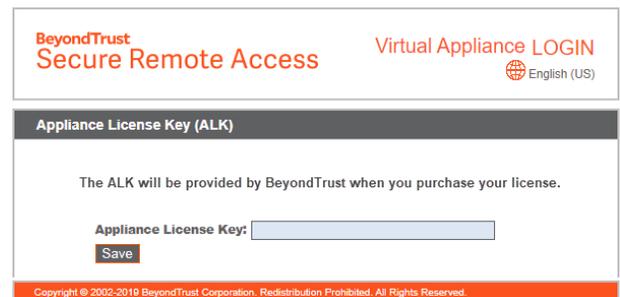
For more information about sizes, please see "[Review License and Sizing Conditions](#)" on page 4.

9. Click **Next: Configure Instance Details**.
10. After configuring the instance launch details, click **Next: Add Storage**.
11. On the **Add Storage** page, configure the sizes and volume types of the drives you wish to include on the AMI. A second EBS volume is set to device **/dev/sdb** with a size of 10GB. We recommend you increase this second disk to 100GB. If you need a large volume for recordings, and this is a cost-sensitive deployment, then you can provision a third drive and configure it as **Magnetic (standard)**. The third drive must be added as **/dev/sdg**. You may enable the **Encrypted** option if desired.
12. Click **Next: Add Tags**.
13. Click **Next: Configure Security Group**.
14. The Launch Wizard creates a security group which you must edit, or you can create a new security group after you deploy the image, so that the site is accessible on ports 443 and 80. This can be accomplished from **Network & Security > Security Groups** in the **EC2 Dashboard**.
15. Click **Review and Launch**. Review your instance details and click **Launch**.
16. Skip the option to select or create a key pair, as the instance does not allow SSH access. Instead, select **Proceed without a key pair**, check the acknowledgment box, and click **Launch Instances**.
17. After the site launches, browse to **Instances > Instances** in the EC2 Dashboard and locate the assigned **Public IP** address in the **Description** tab. This is the IP address used to configure your B Series Appliance and your DNS A record.



Note: If you stop or terminate your Instance, you are not guaranteed to retrieve the same IP address after it reboots. To facilitate managing your DNS, we recommend purchasing an Elastic IP address.

18. Navigate in a web browser to [https://\[Public IP address\]/appliance](https://[Public IP address]/appliance).
19. Enter your **Appliance License Key** provided in the email from BeyondTrust Technical Support. Click **Save**.



Deploy the BeyondTrust SRA Virtual Appliance into a Nutanix AHV Environment

Review Prerequisites for Nutanix

You must have a Nutanix account and environment already configured.

Before beginning the BeyondTrust SRA Virtual Appliance setup, please review the following prerequisites:

- Nutanix AHV 20190916.410+.
- At least 4GB of memory available.
- At least 140GB of storage available.
- One 32GB partition for the BeyondTrust OS, and at least 100GB available for logs and recordings.
- External IP SANs require a 1Gbit or 10Gbit reserved network with a 10K RPM disk or better.



For more information about sizes, please see ["Review License and Sizing Conditions" on page 4.](#)

- A static IP for your SRA Virtual Appliance.
- A private DNS A-record resolving to the static IP of your SRA Virtual Appliance. A public A-record and a public IP are also required if public clients access the B Series Appliance. The DNS A-record is the fully qualified domain name (FQDN) of your site (access.example.com, for example).



Note: "Public clients" include any client software (browsers, BeyondTrust access consoles, endpoint clients, etc.) which connect from external networks and VPN(s) local to the B Series Appliance's network.

- A valid NTP server that is reachable by the B Series Appliance.
- Ensure that the system time between the host ESXi server and the guest BeyondTrust OS are in sync. Variations by only a few seconds can potentially result in performance or connectivity issues.

Deploy the SRA Virtual Appliance

Administrators can deploy and configure the BeyondTrust SRA Virtual Appliance into their Nutanix AHV environment by following the steps below.

1. Open the email you received from BeyondTrust Technical Support, and click the **Click Here for your BeyondTrust Virtual Appliance (Nutanix AHV)** link to download the file. Save the file to an appropriate location to be uploaded to your Nutanix environment.
2. Log in to Nutanix AHV.

BeyondTrust Download Available

 BeyondTrust Build System <mysupport@beyondtrust.com>
To

 Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Greetings,

Thank you for choosing BeyondTrust for your Secure Remote Access needs!

Your BeyondTrust Virtual Appliance is registered in our systems for `deploy.beyondtrust.com` and is ready for download.

To install and configure this Virtual Appliance, follow all of the instructions below:

The BeyondTrust Virtual Appliance
Download your BeyondTrust Virtual Appliance

- [Click here for your BeyondTrust Virtual Appliance \(VMware\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Hyper-V and Azure\)](#)
- [Click here for your BeyondTrust Virtual Appliance \(Nutanix AHV\)](#)

Deploy your BeyondTrust Virtual Appliance in AWS

- Link your AWS account(s) by clicking [here](#).

BeyondTrust Virtual Appliance Setup

1. Follow the appropriate installation guide for your product:
 - o [BeyondTrust RS Virtual Appliance Installation guide](#)
 - o [Privileged Remote Access Virtual Appliance Installation guide](#)
2. When prompted for the Appliance License Key (ALK), enter
3. Install any available BeyondTrust updates using 'Check for Updates'

Contacting BeyondTrust

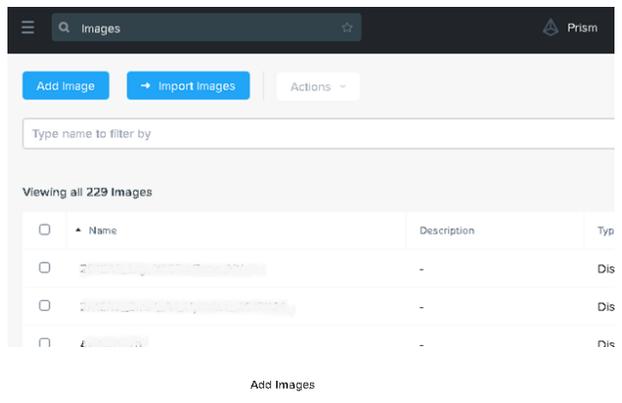
If you need additional assistance, please contact [BeyondTrust Support](#)

We look forward to serving you. If you have any questions, don't hesitate to contact us at mysupport@beyondtrust.com.

Best Regards,

BeyondTrust Support Team

3. Go to **Menu > Virtual Infrastructure > Images** and click **Add Image** to upload the **BeyondTrust.qcow2** file to the image repository.



4. Click **Next**.

1 Select Image 2 Select Location

Image Source

Image File URL VM Disk

+ Add File

Source: [LOCAL]BeyondTrust.qcow2 Remove

Name: Type:

Description:

Checksum: SHA-1

Cancel **Next**

5. Select the location for the image in your Nutanix cluster.
6. Click **Save**.
7. Go to **Home > VM** and select **+ Create VM**.

Add Images

1 Select Image
 2 Select Location

Placement Method

Place image directly on clusters
 This option is good for smaller environments. The image will be placed on all selected clusters below.

Place image using Image Placement policies
 This option is good for larger environments. It requires you to first set up Image Placement policies between categories assigned to clusters and categories assigned to images. From there on, you only need to associate a relevant category to an image while uploading it here.

Select Clusters

Select the set of clusters to use for placement.

All clusters

Name
 NTXCLUSTER01

Back
Save

8. In the **Create VM** dialog, select the desired CPU and Memory configuration for this Appliance.
9. Click **Next**.

Create VM

1 Configuration
 2 Resources
 3 Management
 4 Review

Name

Description

Cluster
 NTXCLUSTER01

Number of VMs

VM Properties

CPU	Cores Per CPU	Memory
2 vCPU	1 Cores	4 GB

Next

10. Click **Attach Disk**.

Create VM

Disks Attach Disk

#	Type	Image	Size	Bus Type	Actions
1	Disk	BeyondTrust Appliance	32 GiB	SCSI	
2	Disk	-	100 GiB	SCSI	

Networks Attach to Subnet

Subnet	VLAN ID / VPC	Private IP	Public IP	Actions
it-lab106	106	Auto-Assign	None	

Boot Configuration

Legacy BIOS Mode
 UEFI Mode
 Secure Boot
 Windows® Defender Credential Guard

Back Next

11. Change **Operation** to **Clone from Image Source** and select the previously uploaded BeyondTrust image.
12. Click **Add**.
13. Click **Attach Disk**.

Add Disk ? x

Type

Operation

Bus Type

Image

Size (GiB)

Please note that changing the size of an image is not allowed.

Index

Cancel Add

14. Create a disk of at least 100GB.

i For more information about sizes, please see ["Review License and Sizing Conditions" on page 4.](#)

15. Click **Add**.

16. Click the **X** next to the CD-ROM disk.

17. Select **UEFI** under **Boot Configuration**.

18. Click the **Attach to Subnet** text button.

19. Select the desired network in the dropdown.

20. Click **Add**.

? ✕

Add Disk

Type

Operation

Bus Type

Storage Container

Size (GiB) ?

Index

Create VM

Disks Attach Disk

#	Type	Image	Size	Bus Type	Actions
1	Disk	BeyondTrust Appliance	32 GiB	SCSI	
2	Disk	-	100 GiB	SCSI	

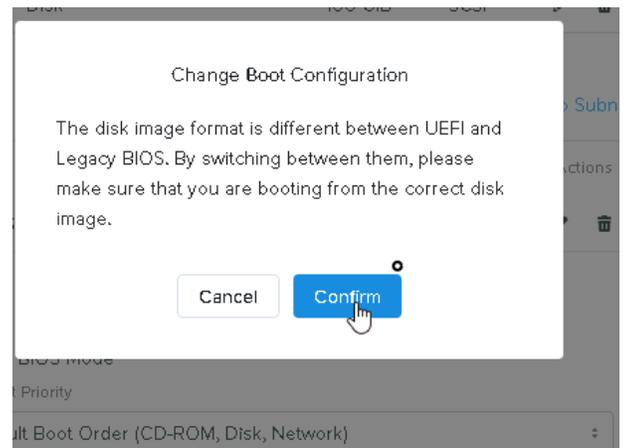
Networks Attach to Subnet

Subnet	VLAN ID / VPC	Private IP	Public IP	Actions
it-lab106	106	Auto-Assign	None	

Boot Configuration

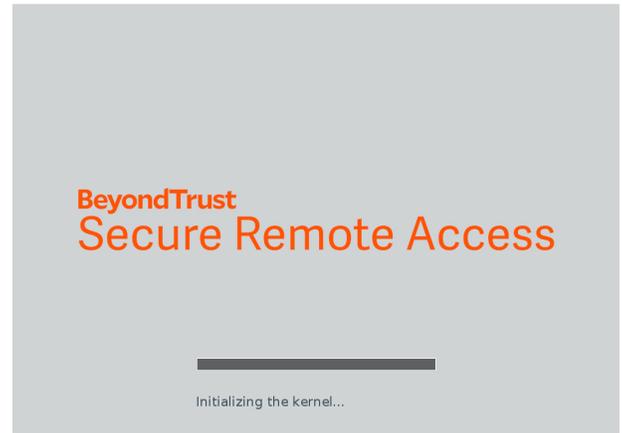
Legacy BIOS Mode
 UEFI Mode ?
 Secure Boot
 Windows® Defender Credential Guard ?

21. Select **UEFI Mode** and click **Confirm** on pop-up.
22. Click **Save**.
23. Nutanix AHV begins deploying the BeyondTrust Appliance.
24. Wait for the appliance to deploy, then select the BeyondTrust Appliance and click **Power On**.



SRA Virtual Appliance First Boot

1. In the virtual infrastructure client, browse to the VM folder you configured, and locate the new entry for the SRA Virtual Appliance. Right-click on this entry and then select **Open Console**.
2. Click the play button to start booting your BeyondTrust SRA Virtual Appliance.

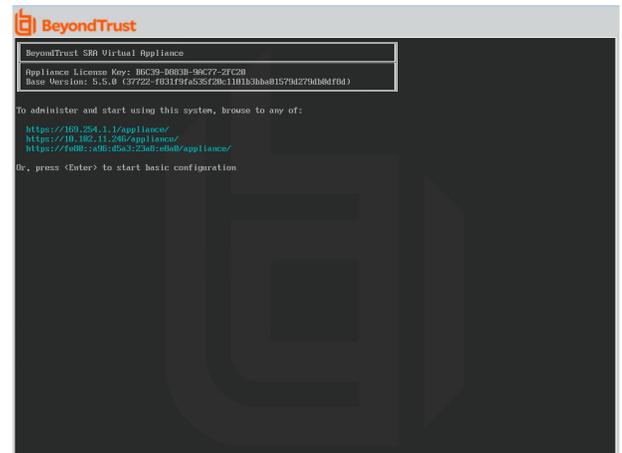


3. After your BeyondTrust SRA Virtual Appliance has finished booting, one or more IP addresses display.



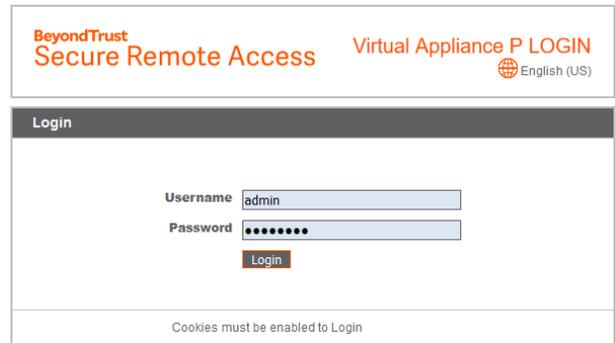
Note: If you were unable to provide the Appliance License Key during deployment, press **Enter** to start basic configuration. **Selection 1** on the next menu screen allows you to manually enter the Appliance License Key. Then exit back to the main screen.

4. From a computer on the same network, open a web browser and browse to any of the IP addresses listed, followed by **/appliance**. If none of the IPs listed are accessible, see "[SRA Virtual Machine Console Administration](#)" on [page 38](#) to assign a usable IP address using the console interface. Otherwise, you are done with the VMware portion of the setup and can close the VMware console.

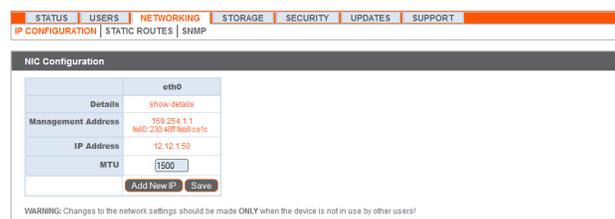


Configure the SRA Virtual Appliance

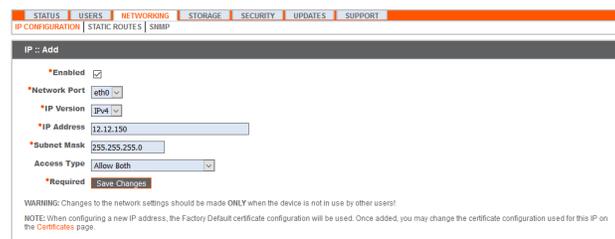
1. From the `/appliance` interface of your BeyondTrust SRA Virtual Appliance, log in using **admin** as the username and **password** as the default password. You are prompted to change your password the first time you log in.



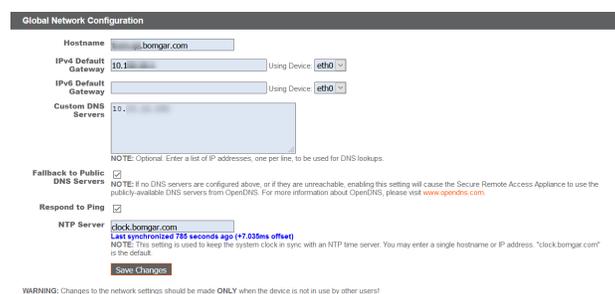
2. Next, go to **Networking > IP Configuration**.
3. Under the **NIC Configuration** section, click **Add New IP**.



4. Enter the static IP address and subnet mask for your BeyondTrust Appliance B Series. You can decide if this IP addresses session traffic, web traffic, or both. Then click **Save Changes**.

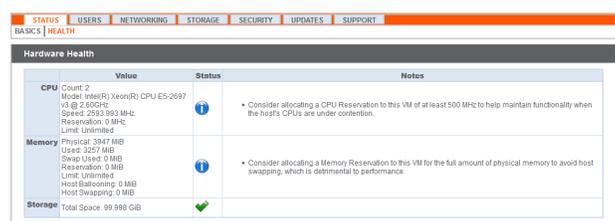


5. Under the **Global Network Configuration** section, set your default gateway. Configuring DNS servers is not required but we highly recommend it. After entering the required information, click **Save Changes**.

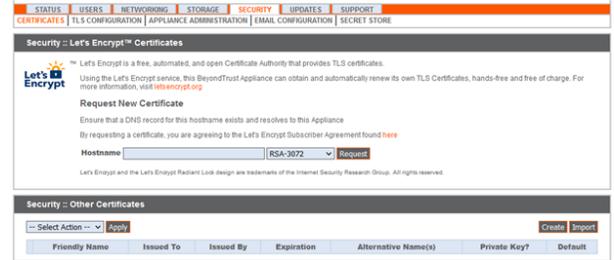


 **Note:** Valid DNS settings are required for failover and automatic updates to function properly. To help determine the appropriate IP and DNS configuration for your network, see [The BeyondTrust Appliance B Series in the Network at https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz/index.htm](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/dmz/index.htm).

6. Wait for the format to complete, and then go to **Status > Health** to verify that the needs of the SRA Virtual Appliance are being met.



7. Go to **Security**.
8. Configure an SSL certificate, using one of the following four options. Follow the link for instructions for each option.
 - [Request a Let's Encrypt certificate](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-ca-signed.htm#LetsEncrypt), at <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-ca-signed.htm#LetsEncrypt>.
 - [Import a CA signed certificate, key, and chain](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-ca-signed.htm#Import), at <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-ca-signed.htm#Import>.
 - [Create a CSR for a CA signed certificate and import the certificate and chain](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-ca-signed.htm#Create_CSR_Import), at https://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-ca-signed.htm#Create_CSR_Import.
 - [Create a self-signed certificate](https://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-self-signed.htm), at <https://www.beyondtrust.com/docs/privileged-remote-access/how-to/sslcertificates/create-self-signed.htm>. This option is not recommended, but may be used temporarily for testing.



For more information, please see "[View SRA Virtual Appliance Health](#)" on page 39.

URL reference

<https://access.example.com/login> - User Administration

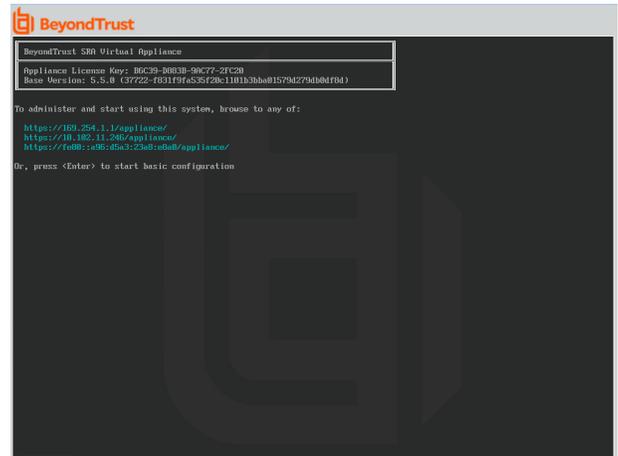
<https://access.example.com/appliance> - Appliance Administration

SRA Virtual Machine Console Administration

After you have finished deploying your SRA Virtual Appliance, you can launch the virtual machine console to access some administrative functions.

The first screen of the virtual machine console lists the hostnames and IP addresses for this SRA Virtual Appliance.

Press **Enter** to view the configuration menu. From here, you can log in to make configuration changes, or use the support tunnel to enable BeyondTrust Technical Support to resolve complex issues with your B Series Appliance.

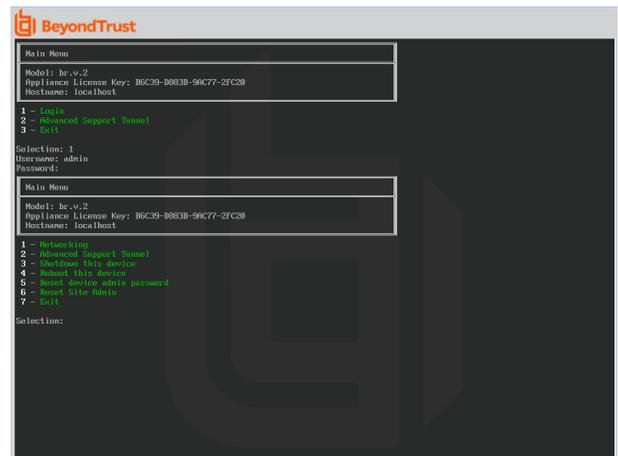


Configuration Options

Logging in provides additional configuration options. You can update your network settings, allow an advanced support tunnel, shut down or reboot the SRA Virtual Appliance, or reset the B Series Appliance password or a site's administrative password.

The **Networking** option allows you to manage the hostname, IP addresses, the default gateway, static routes, and DNS servers.

Select a network interface to manage its speed or duplex communication. From here, you also can add or edit IP addresses.



View SRA Virtual Appliance Health

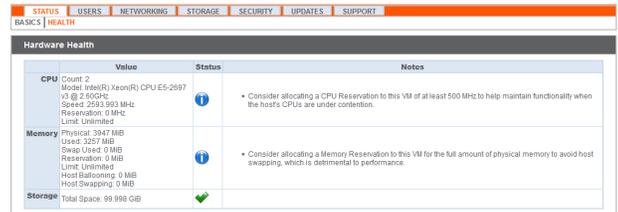
The **Status > Health** page in the /appliance administrative interface offers information to help you ensure efficiency from your BeyondTrust SRA Virtual Appliance installation. The information presented can help you solve problems you may encounter with your SRA Virtual Appliance.

Real-time information displays in three categories: **CPU**, **Memory**, and **Storage**. For each category, the item's **Value**, **Status**, and any associated **Notes** are listed.

Value displays the specific CPU, Memory, and Storage parameters associated with your SRA Virtual Appliance installation.

Status displays green check, blue exclamation mark, or red X icons to help you quickly assess your installation's performance.

Notes are displayed when changes are recommended, or installation errors have occurred.



Category	Value	Status	Notes
CPU	Count: 2 Model: Intel(R) Xeon(R) CPU E5-2697 V3 @ 2.50GHz Speed: 2593.993 MHz Reservation: 0 MHz Limit: Unlimited		• Consider allocating a CPU Reservation to this VM of at least 500 MHz to help maintain functionality when the host's CPUs are under contention.
Memory	Physical: 3247 MB Used: 3267 MB Swap Used: 0 MB Reservation: 0 MB Limit: Unlimited Host Ballooning: 0 MB Host Swapping: 0 MB		• Consider allocating a Memory Reservation to this VM for the full amount of physical memory to avoid host swapping, which is detrimental to performance.
Storage	Total Space: 99.998 GiB		

Status Icons



A green check icon shows you at a glance that a certain category is sufficiently configured for optimal SRA Virtual Appliance performance.



A blue exclamation mark indicates that you may need to make changes to improve performance. Suggested changes are listed in the adjacent **Notes** column.



A red X icon alerts you to a memory error situation that could cause disruptions for your SRA Virtual Appliance. The suggested changes to correct the issue associated with a red X are listed in the adjacent **Notes** column and may require you to contact BeyondTrust Technical Support.

Migrate Sites and Licenses to a New BeyondTrust SRA Virtual Appliance

Existing sites and licenses can be migrated to a new BeyondTrust SRA Virtual Appliance using the built-in site migration tool. A manual process is also available.

BeyondTrust offers a variety of implementation service packages that provide customized migration planning and upgrade assistance. For more details, please contact your account manager.

Your existing SRA Virtual Appliance must be running a recent software version. Older versions must be upgraded before migrating.



Note: If you are migrating to Atlas Cloud, please contact www.beyondtrust.com/support for assistance.



For more information about installation, please see [SRA Virtual Appliance Installation](https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/virtual-sra/index.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/getting-started/deployment/virtual-sra/index.htm>.

For more information about upgrading, please see [Upgrade the BeyondTrust Privileged Remote Access Software](https://www.beyondtrust.com/docs/privileged-remote-access/updates/upgrade/index.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/updates/upgrade/index.htm>.

Use the Site Migration Tool

1. Log in to the /login interface of your current SRA Virtual Appliance.
2. Click on **Management** in the left menu.
3. Click on the **Software** tab.
4. Scroll down to **Site Migration**.
5. Read and review the conditions and instructions there, including steps to follow after the migration is complete. Post-migration steps can be reviewed again after the migration.
 - The site address and API account provided are used to download a backup from the source site and restore it onto this site automatically. The provided API account must have read-only or higher access to the command API, as well as permission to use the backup and vault encryption key APIs.
 - Recordings are not included as part of this migration. If you need to retain access to existing recordings you can either keep the source appliance online with a different hostname or use the integration client to back up the recordings before doing the migration.
 - The site must be a BeyondTrust Privileged Remote Access site.

SITE MIGRATION

Migrate all configuration and data from another site to this one. The site address and API account provided will be used to download a backup from the source site and restore it onto this site automatically. The provided API account must have read-only or higher access to the command API, as well as permission to use the backup and vault encryption key APIs.

Recordings are not included as part of this migration. If you need to retain access to existing recordings you can either keep the source appliance online with a different hostname or use the integration client to backup the recordings before doing the migration.

The site must be a BeyondTrust Privileged Remote Access site.

Once the migration is complete, you will need to update the DNS of your primary hostname to point to this appliance to complete the migration process and allow clients to connect to this instance and upgrade.

1. Create a new DNS entry for the hostname that you would like to use to access the old site. You may not use the original BeyondTrust Privileged Remote Access hostname shown in the Status page of /login.
2. In the old site's Management > Site Configuration, add the new hostname address under HTTP. This step ensures that the old site will respond appropriately to the new hostname.
3. After the DNS entries are propagated, confirm that you can access the old site under the new hostname.
4. Swing the DNS entries to point to this site instead of the old site.
5. Wait for all DNS entries to finish propagating across the networks from which your clients resolve those addresses.
6. From the old site's Status page, click the "Restart Software" button to trigger all clients to reconnect to your new site and begin upgrading themselves.

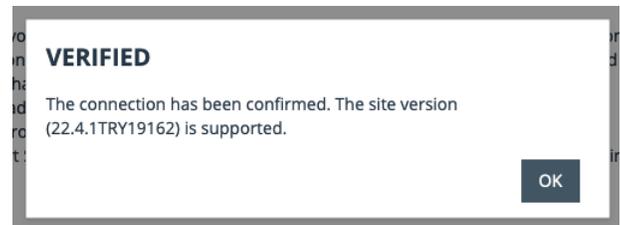
• Required field

Hostname •

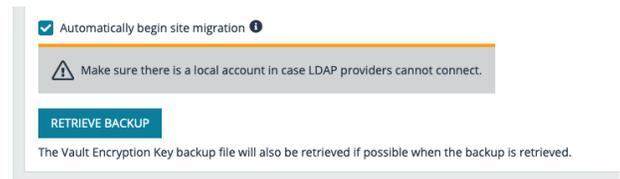
OAuth Client ID •

OAuth Client Secret •

6. Enter the **Hostname**, **OAuth Client ID**, and **OAuth Client Secret**.
7. Click **Verify Connection**.
8. Once the connection is verified, click **OK**. If the connection does not verify, review the connection information that was entered.

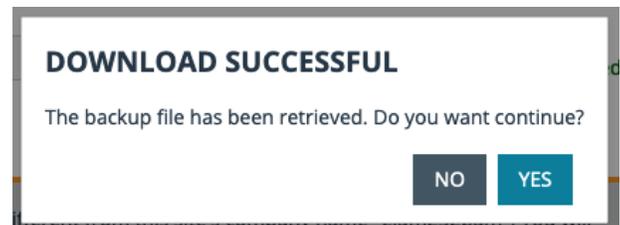


9. Check **Automatically begin site migration** to start the migration after downloading the backup files. Uncheck to manually confirm each backup file.

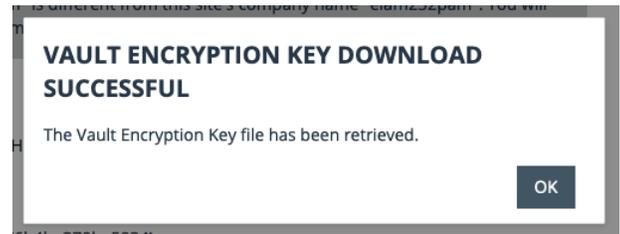


 **Note:** Make sure there is a local account in case LDAP providers cannot connect.

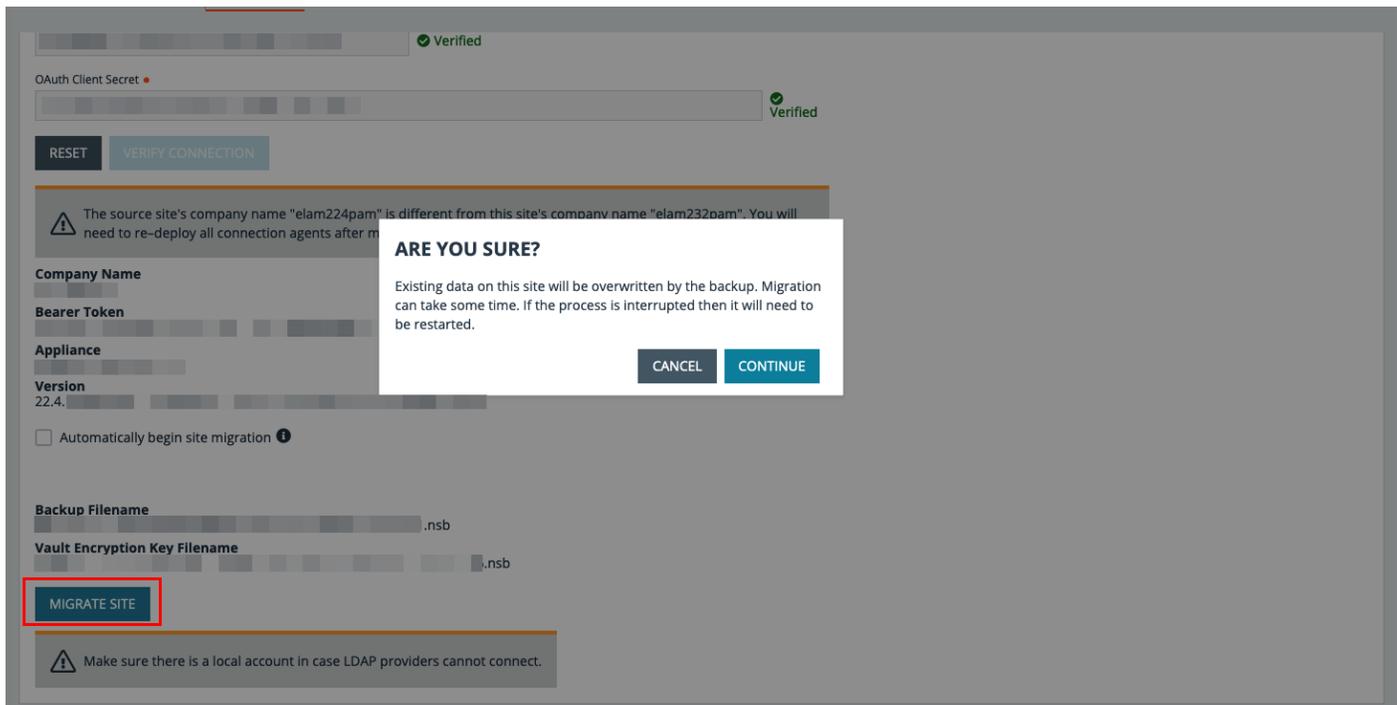
10. Click **Retrieve Backup**.
11. If the migration is not automatic, a series of pop-up notifications require confirmation for each download.



12. Click **OK** on the last download.

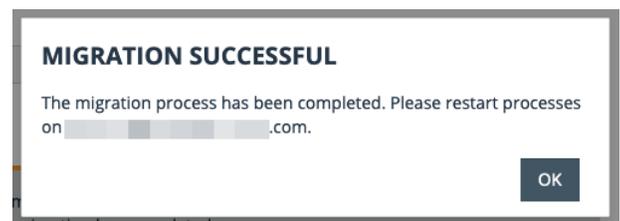


13. Click **Migrate Site**. Review the notification and click **Continue**.



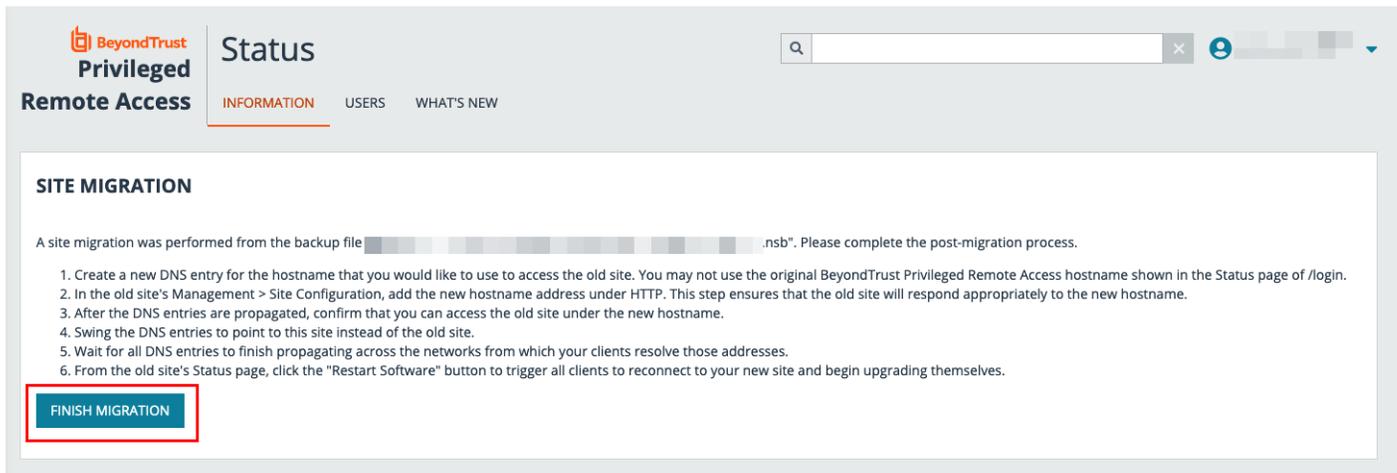
14. Pop-up notifications advise that the migration is in progress, and when it is complete.

15. Click **OK** on the **Migration Successful** notification.



16. Once the migration is complete, you must update the DNS of your primary hostname to point to this appliance. This will complete the migration process, and allow clients to connect to this instance and upgrade. The required steps display on the screen.

- a. Create a new DNS entry for the hostname that you would like to use to access the old site. You may not use the original BeyondTrust Privileged Remote Access hostname shown in the Status page of /login.
- b. In the old site's **Management > Site Configuration**, add the new hostname address under HTTP. This step ensures that the old site responds appropriately to the new hostname.
- c. After the DNS entries are propagated, confirm that you can access the old site under the new hostname.
- d. Swing the DNS entries to point to this site instead of the old site.
- e. Wait for all DNS entries to finish propagating across the networks from which your clients resolve those addresses.
- f. From the old site's **Status** page, click **Restart Software** to trigger all clients to reconnect to your new site and begin upgrading themselves.



BeyondTrust Privileged Remote Access **Status**

INFORMATION USERS WHAT'S NEW

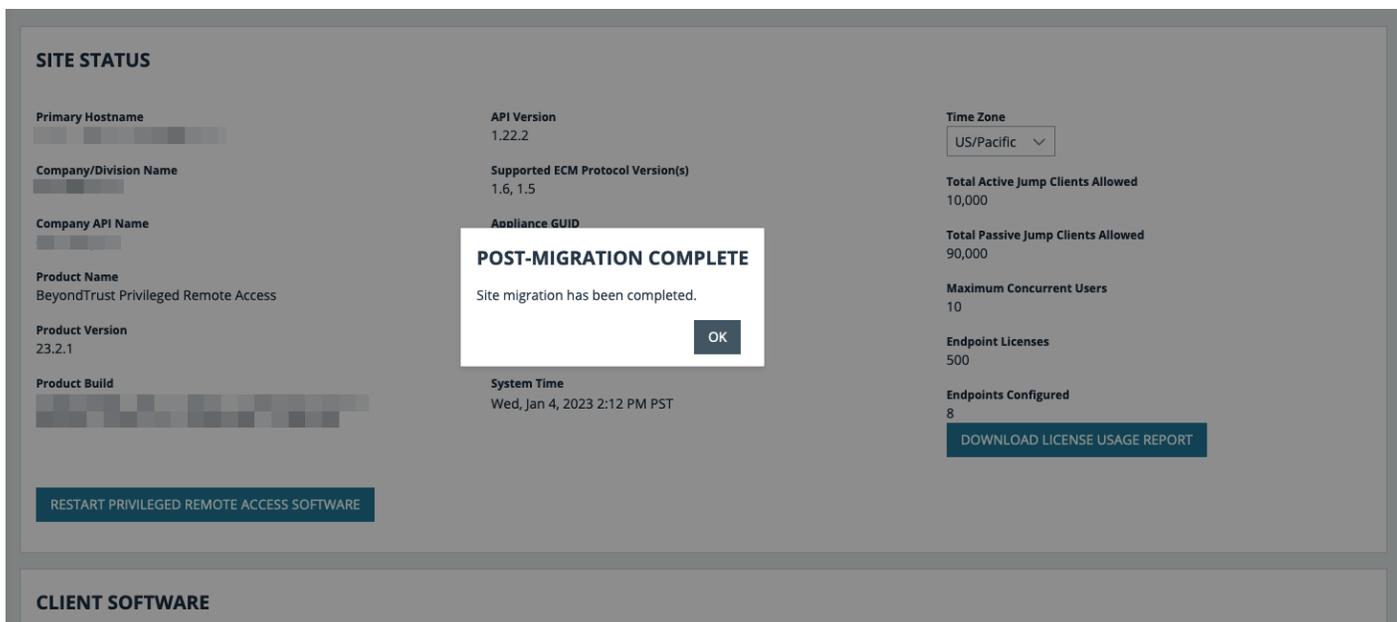
SITE MIGRATION

A site migration was performed from the backup file [redacted].nsb". Please complete the post-migration process.

1. Create a new DNS entry for the hostname that you would like to use to access the old site. You may not use the original BeyondTrust Privileged Remote Access hostname shown in the Status page of /login.
2. In the old site's Management > Site Configuration, add the new hostname address under HTTP. This step ensures that the old site will respond appropriately to the new hostname.
3. After the DNS entries are propagated, confirm that you can access the old site under the new hostname.
4. Swing the DNS entries to point to this site instead of the old site.
5. Wait for all DNS entries to finish propagating across the networks from which your clients resolve those addresses.
6. From the old site's Status page, click the "Restart Software" button to trigger all clients to reconnect to your new site and begin upgrading themselves.

FINISH MIGRATION

17. Click **Finish Migration**.
18. A pop-up notification confirms the migration is complete.



SITE STATUS

Primary Hostname [redacted]	API Version 1.22.2	Time Zone US/Pacific
Company/Division Name [redacted]	Supported ECM Protocol Version(s) 1.6, 1.5	Total Active Jump Clients Allowed 10,000
Company API Name [redacted]	Appliance GUID [redacted]	Total Passive Jump Clients Allowed 90,000
Product Name BeyondTrust Privileged Remote Access		Maximum Concurrent Users 10
Product Version 23.2.1		Endpoint Licenses 500
Product Build [redacted]	System Time Wed, Jan 4, 2023 2:12 PM PST	Endpoints Configured 8

POST-MIGRATION COMPLETE
Site migration has been completed. **OK**

RESTART PRIVILEGED REMOTE ACCESS SOFTWARE

DOWNLOAD LICENSE USAGE REPORT

CLIENT SOFTWARE

Manual Site Migration

Manually migrating your sites and licenses to a new BeyondTrust SRA Virtual Appliance can vary by environment, individual case preferences, and setup conditions. The steps below represent the most common requirements.

Back Up the Current SRA Virtual Appliance Configuration

Follow the steps below to make a backup of your current SRA Virtual Appliance configuration:

1. Log in to the `/login` interface of your current SRA Virtual Appliance.
2. Click on **Management** in the left menu.
3. Click on the **Software** tab.
4. Enter and confirm a **Backup Password**, if desired.
5. Leave **Include logged session reporting data** checked.
6. Click **Download Backup**. If you did not enter a backup password, you are prompted to confirm you want to proceed without one.
7. Save the backup file to a secure location.

Export the Existing SSL Certificate Chain from Your Current SRA Virtual Appliance

Next, export your existing SSL certificate chain from your current SRA Virtual Appliance:

1. Log in to the `/appliance` interface of your current SRA Virtual Appliance.
2. Browse to the **Security** tab, the **Certificates** sub-tab, and then the **Certificates** section.
3. Check the box next to your correct BeyondTrust site certificate.
4. Select **Export** from the **Select Action** dropdown box, and click **Apply**.
5. On the next screen, choose **ALL** options: **Include Certificate**, **Include Private Key**, and **Include Certificate Chain** (if available).
6. Click the **Export** button.
7. Save this file to a secure location.

Install the New Software Version

Use the directions in the BeyondTrust SRA Virtual Appliance Installation Kit to install the software in your virtual environment. These include instructions on how to access the `/appliance` web interface via an IP address.



Note: You must allocate storage space before booting your BeyondTrust SRA Virtual Appliance.

You must install Base software update(s) on the new SRA Virtual Appliance. There is a separate email containing instructions on how to install and update the Base software for the new SRA Virtual Appliance. The Base software is tied to the new SRA Virtual Appliance serial number.

Locate the SSL chain exported earlier, and import it into the SRA Virtual Appliance.

1. To do this, log in to the `/appliance` interface of your new SRA Virtual Appliance.
2. Click the **Security** tab, then the **Certificates** sub-tab.
3. Select **Import**.

4. Browse to the certificate file that you previously exported, and click **Upload**.
5. Mark this as the default certificate by clicking the radio button in the right hand column of the **Certificate** description.

Install a License Package

Once the previous steps are completed, install the Privileged Remote Access software following the steps in the Privileged Remote Access [Upgrade Guide](https://www.beyondtrust.com/docs/privileged-remote-access/updates/upgrade/index.htm) at <https://www.beyondtrust.com/docs/privileged-remote-access/updates/upgrade/index.htm>.

- If the SRA Virtual Appliance has internet access, follow the steps for automatic updates.
- If the SRA Virtual Appliance does not have internet access, follow the steps for manual updates.

You now should have a functioning support portal and be able to access the /login interface to create user accounts and manage other settings.

1. For your first login, use the credentials emailed with the license information.



Note: If you are trying to reach /login by using the IP address and not the hostname, you need to mark the new site as the default site. This setting is located at **/appliance > Status > Basics > Default Site**.

2. Once logged in, click **Management**, then **Software Management**.
3. Click **Choose File** and locate the backup file you created at the beginning of the process. A warning appears to remind you that you also need to provide a Vault key backup if you are restoring a configuration containing Vault credentials onto a new SRA Virtual Appliance.
4. Click **Yes**, and then click **Upload Backup**.
5. Next, update the DNS record and confirm login.
 - Update the DNS A-record to route BeyondTrust site traffic to the IP address of the new SRA Virtual Appliance.
 - Log in to your access console and allow it to update (if applicable for your situation).
 - Test by starting a access session.



Note: DNS changes can take up to 72 hours to propagate.

To migrate currently deployed Jump Clients over to the new SRA Virtual Appliance, you must power down the old SRA Virtual Appliance.

If you need technical assistance, please visit www.beyondtrust.com/support to request a live support session.

SRA Virtual Appliance Frequently Asked Questions

The following are some of the questions frequently asked about administering the SRA Virtual Appliance and answers to these questions from BeyondTrust Technical Support.

VMware

Can I Install VMware Tools Onto My BeyondTrust SRA Virtual Appliance?

The BeyondTrust SRA Virtual Appliance ships with the VMware guest tools pre-installed.

Can a Time Skew Between My ESXi Host and My BeyondTrust SRA Virtual Appliance Cause Connectivity Issues?

Yes, any time difference between the BeyondTrust SRA Virtual Appliance and the host ESXi server can cause connectivity issues. To prevent this, specify a valid NTP source in the SRA Virtual Appliance /appliance interface as well as ensuring that your ESXi host is using a valid NTP source. VMware also has an option to sync the guest OS time with the host ESXi server time. If you use this option, then the NTP source within the BeyondTrust SRA Virtual Appliance does NOT need to be set. It is recommended to use one method or the other but NOT both together.

What Version of VMware is Supported to Host the BeyondTrust SRA Virtual Appliance?

BeyondTrust certifies support for VMware vCenter 6.5+, Virtual Hardware Version 13+.

Does the BeyondTrust SRA Virtual Appliance Require Reserved Resources in VMware?

For troubleshooting purposes, a BeyondTrust Technical Support representative may require the BeyondTrust SRA Virtual Appliance to have reserved resources to effectively diagnose a support issue.

Does BeyondTrust Support Using the VMware Snapshot Functionality?

BeyondTrust supports the use of the snapshot technology only in upgrade situations. A snapshot of a powered-off BeyondTrust SRA Virtual Appliance can be taken prior to an upgrade and can be utilized as a fallback in the case of a failed upgrade.



Note: BeyondTrust does not recommend or support taking snapshots of actively running SRA Virtual Appliances.

Can I Run the BeyondTrust SRA Virtual Appliance in My Clustered VMware Environment?

Yes, when installed in a vSphere cluster, the BeyondTrust SRA Virtual Appliance can benefit from many of VMware's value-added technologies, such as VMotion, DRS, and HA, to maximize performance and uptime.

Can I Specify an Alternate Disk for Recordings?

Yes, in some cases you may want to separate the disks for recordings if your VMware environment has tiered storage. Add a third disk to your BeyondTrust SRA Virtual Appliance and reboot. Once the BeyondTrust SRA Virtual Appliance is rebooted, the third disk is provisioned and used for recordings.

The Virtual Hardware of My BeyondTrust SRA Virtual Appliance is Currently on an Old Version and Needs to be Upgraded. What Are BeyondTrust's Recommendations for Virtual Hardware Version Upgrades?

BeyondTrust certifies support for VMware vCenter 6.5+, Virtual Hardware Version 13+.

If your configuration does not match one of the above configurations, BeyondTrust does recommend updating the virtual hardware version of your BeyondTrust SRA Virtual Appliance.

What is the Error: "The OVF certificate file is invalid"?

When importing a new BeyondTrust SRA Virtual Appliance to VMware using the OVA installation package, it is possible for VMware to return an error stating "The OVF certificate file is invalid". This happens when attempting to import the OVF file which is packaged inside the B Series Appliance's .ova file. This would require extracting the contents of the OVA package, and this would invalidate the package as a whole. To resolve this, re-download the OVA file and re-import it without extracting the OVA. If using Internet Explorer, it may be necessary to replace .tar with .ova in the download's file extension.

Should the Second Virtual Disk Use Thick or Thin Provisioning?

In current versions, the OVF template automatically chooses thick provisioning for the second and (if present) third virtual disk(s).

According to ESXi and vCenter Server 5 Documentation, thin provision initially allocates only the space actually needed by the virtual machine and grows dynamically as needed. In contrast, both forms of thick provisioning allocate all the assigned disk space to the virtual machine upon creation, locking it from use by other machine (see "About Virtual Disk Provisioning Policies" in the ESXi and vCenter Server 5 Documentation under **vSphere Virtual Machine Administration > Configuring Virtual Machines > Virtual Disk Configuration** in the vSphere Documentation Center at vmware.com/support/pubs/). Although the B Series Appliance is expected to operate correctly with thin provisioning, this is not the preferred choice.

Why Does the Virtual Appliance Download Come as a TAR File?

When using Internet Explorer, BeyondTrust's OVA installer may download as a *BeyondTrust-br.v.2.tar* file instead of *BeyondTrust-br.v.2.ova*. To install the file per the SRA Virtual Appliance Setup Guide, replace the .tar extension with .ova and follow the guide as normal.

Can the Virtual Hard Disks be Stored in Multiple Datastores?

Some customers with BeyondTrust SRA Virtual Appliances may be interested in distributing the various SRA Virtual Appliance disks across multiple VMware datastores. BeyondTrust does support this configuration, so we expect our B Series Appliances to work satisfactorily when their virtual drives are located in different datastores from one another.

Hyper-V

What Version of Hyper-V is Supported to Host the BeyondTrust SRA Virtual Appliance?

BeyondTrust certifies support of Hyper-V on Windows Server 2012 R2, Windows Server 2016, and Windows Server 2019. We support both a stand alone Hyper-V server and Windows Server with the Hyper-V Role installed.

Does BeyondTrust Support Using the Hyper-V Snapshot Functionality?

BeyondTrust supports the use of the snapshot technology only in upgrade situations. A snapshot of a powered-off BeyondTrust SRA Virtual Appliance can be taken prior to an upgrade and can be utilized as a fallback in the case of a failed upgrade.

Can I Specify an Alternate Disk for Recordings?

Yes, in some cases you may want to separate the disks for recordings if your Hyper-V environment has tiered storage. Add a third disk to your BeyondTrust SRA Virtual Appliance and reboot. Once the BeyondTrust SRA Virtual Appliance is rebooted, the third disk is provisioned and used for recordings.

The Virtual Hardware of My BeyondTrust SRA Virtual Appliance is Currently on an Old Version and Needs to be Upgraded. What Are BeyondTrust's Recommendations for Virtual Hardware Version Upgrades?

For Hyper-V, BeyondTrust supports only Generation 2 virtual machines at this time. The VA image is delivered as a Generation 2 VM.

If your configuration does not match the above configuration, BeyondTrust does recommend updating the virtual hardware version of your BeyondTrust SRA Virtual Appliance.

Microsoft Azure

Is the Azure Classic Deployment Model Supported?

No. The only supported model is Azure Resource Manager (ARM).

Do I Need to Configure the Windows PowerShell Script Differently if I Have a Premium Storage Account?

Yes. If you have a premium storage account, you need to modify the **vmSize** information in **STEP 2** of the script to indicate **Premium** along with the applicable size.

Can I Use Any Additional Azure Features Provided by Using Azure Linux Agent with My BeyondTrustSRA Virtual Appliance?

BeyondTrust does not support any of these features at this time.

Do I Need to Enter My Public IP Anywhere in the BeyondTrust /appliance Interface?

No. The Azure network layer maps the public IP to the private IP. The BeyondTrustSRA Virtual Appliance assigns the private IP using DHCP.

Is Failover Needed? Is Failover Supported for Microsoft Azure?

Although the risk for downtime is much lower within Azure, it is still possible to need a failover B Series Appliance. Failover is supported in Azure; however, IP sharing does not work with Azure networking. A DNS swing is needed to failover to a backup B Series Appliance.

Do I Need a Static IP for My BeyondTrust SRA Virtual Appliance?

Assigning a static IP is the easiest way to ensure there are not any DNS issues across reboots and also to make sure any integration points that require an IP address work properly. However, assigning a CNAME record for your B Series Appliance's DNS entry should suffice for most deployments.

General Issues

Can an Evaluation SRA Virtual Appliance be Converted to Production?

Yes, the existing SRA Virtual Appliance can be converted to production.

Once the SRA Virtual Appliance licenses are purchased, confirm your intent to convert to production with your Account Manager.

Can Available Resources be Modified?

It is possible to add additional resources to a BeyondTrust SRA Virtual Appliance, and it is possible to decrease available memory and CPU cycles; however, it is not possible to decrease available storage safely, and none of the above should be done when the B Series Appliance is powered on. After shutting down the B Series Appliance and making your changes, the B Series Appliance should recognize the changes upon next boot.

SRA Virtual Appliances have either two or three virtual hard disks, depending on which configuration was selected during deployment: Small, Medium, or Large. Small and Medium deployments have two disks, while Large deployments have three. The first disk is used for the root of the operating system in all three cases while the second disk is used for /login site data and recordings in Small and Medium deployments.

In Large deployments, recordings are moved from the second disk to the third. If your SRA Virtual Appliance was originally deployed with two virtual hard disks, you can add a third later, and the B Series Appliance automatically stores session recordings on the third disk. The B Series Appliance cannot use more than three disks.

1. Shut down the BeyondTrust SRA Virtual Appliance.
2. Adjust the RAM and/or CPU allocation and/or increase the disk space using VMware.
3. Power on the BeyondTrust SRA Virtual Appliance.

Can the SRA Virtual Appliance Fail Over to a Slower Storage Tier?

Organizations may choose to present storage to SRA Virtual Appliances by means of tiered storage in a SAN. "Fast-tier 1" storage typically refers to arrays which employ SSD technology for frequently accessed data, and "slow" storage typically refers to data placed on technologies such as SAS, NL-SAS, or SATA. Either of these work with BeyondTrust, but certain storage configurations are not supported when using two B Series Appliances in failover.

In cases where the primary SRA Virtual Appliance has storage in SSD / tier-1 storage, these rules apply to the backup B Series Appliance:

- Large SRA Virtual Appliances must be provisioned with storage of the same tier.
- Small and Medium SRA Virtual Appliances may have lower tier storage if it is backed by 10K or 15K disks.
- No backup SRA Virtual Appliance may have less than 10K / 15K disk storage speed.

The exact specs for Small, Medium and Large are described in the product specific deployment sections of this document. It is important to note that BeyondTrust does not require any particular tier for a SRA Virtual Appliance to boot and function in isolation. Tiered storage becomes a concern only when two B Series Appliances are used in failover.

Is Cloning SRA Virtual Appliances Supported?

After a BeyondTrust SRA Virtual Appliance is installed in an ESX or ESXi environment, the administrator may wish to clone the B Series Appliance. Cloning a virtual machine creates a duplicate of the virtual machine with the same configuration and installed software as the original. This feature of ESX and ESXi is not supported by the BeyondTrust SRA Virtual Appliance at this time.

Does the SRA Virtual Appliance Support vCenter Site Recovery Manager (SRM)?

vCenter's Site Recovery Manager (SRM) builds off of vSphere Replication to provide disaster recovery. Administrators running BeyondTrust in a vCenter system may be interested in leveraging this with BeyondTrust SRA Virtual Appliances. While BeyondTrust is expected to work with vCenter SRM, restoring from a replication like this would appear to the B Series Appliance like pulling the power cable, so there would be a risk for file system corruption, which may result in potential data loss.