



BeyondTrust

UVMSQL Appliance 3.5 Installation Guide

Table of Contents

UVMSQL Appliance Installation Guide	3
UVMSQL Appliance Requirements	5
Physical UVMSQL Appliance Specifications	6
View UVMSQL Appliance Firewall Settings and Port Requirements	8
UVMSQL Setup Worksheet	10
PowerShell Commands for the UVMSQL Appliance	12
Access UVMSQL Features from the UVMSQL LCD Panel	14
Set Up the UVMSQL Appliance	16
Configure the BeyondTrust UVMSQL Appliance	18

UVMSQL Appliance Installation Guide

The UVMSQL Cluster Appliance is specifically designed to offer SQL Server Always On Availability Group (AOAG) configuration on a BeyondTrust UVMSQL Appliance. This guide is intended for network security administrators responsible for protecting their organization's computing assets. The administrator should be familiar with networking and security, as well as with SQL Server.

FCC Certification

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

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

Limited Hardware UVMSQL Warranty

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

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

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

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

Warranty Invalidation

This warranty is void in the event that:

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

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

**IMPORTANT!**

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

UVMSQL Appliance Requirements

Prerequisites

The BeyondTrust UVMSQL Appliance requires the following at a minimum:

- Two available power outlets
- A high-speed network connection
- A network router or switch
- A unique, static IPv4 address for the BeyondTrust UVMSQL Appliance
- A private DNS A-record resolving to the static IP of your UVMSQL Appliance.
- An SSL web server certificate, intermediate SSL certificates, and SSL root, OR a self-signed certificate.

Preliminary Steps

You should take several steps before the BeyondTrust hardware is delivered and installed:

1. Allocate the necessary rack space for the UVMSQL Appliance. Ensure the space has the necessary power and network access. The rack space required is 1U.
2. Determine a machine name (15 characters or less) and reserve a static IP address for each UVMSQL Appliance on the network.



IMPORTANT!

Once you have named your UVMSQL Appliance, it cannot be renamed. If at any point you need to rename the appliance, you must either re-image (if it is a physical appliance) or re-deploy (if it is a virtual appliance) the image.

3. Identify the domain that you plan to join the UVMSQL Appliances to for the purpose of clustering.
4. Identify or create Domain Administrator credentials to be used during the cluster configuration process.
5. Identify the organizational unit (OU) to which the UVMSQL Appliances will belong. This OU is required to have group policy inheritance blocked.
6. Identify or create the Group Managed Service Account that will be used for the ongoing operation of the cluster.
7. Allocate a name and static IP address for the cluster that will be created with the UVMSQL Appliances.
8. Allocate a name and static IP address for the availability group listener.



For more information, please see the following:

- On Group Managed Service accounts, [Windows Server 2012: Group Managed Service Accounts at https://techcommunity.microsoft.com/t5/Core-Infrastructure-and-Security/Windows-Server-2012-Group-Managed-Service-Accounts/ba-p/255910](https://techcommunity.microsoft.com/t5/Core-Infrastructure-and-Security/Windows-Server-2012-Group-Managed-Service-Accounts/ba-p/255910)
- For a useful tool to prepare for initial setup, "UVMSQL Setup Worksheet" on page 10

Client Requirements

Supported browsers:

- Microsoft Edge
- Firefox
- Google Chrome
- Safari

UVMSQL Requirements

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

UVMSQL Package Contents

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

- UVMSQL Appliance
- Two Power Cords
- Getting Started Guide
- Rack Mount Kit
- Bezel Key
- Certificate of Authenticity with SQL Licenses

Physical UVMSQL Appliance Specifications

UVMSQL Specifications

Specification	Description
AC Input Voltage	110 to 240 V AC, autoranging
Rated Input Frequency	50 to 60Hz
Cooling	8 Standard Fans, 2 Standard 1U Heatsinks
Chassis	Chassis with up to 8, 3.5in. Hard Drives
Dimensions	1U rack-mountable server H: 1.68in. (4.28 cm) (10.75in. shipping) W: 18.97in. (48.18cm) (24in. shipping) D: 26.89in. (68.30cm) (35.75in. shipping) Weight: approx 45lbs. (48lbs. shipping)
Microprocessor	2 x Intel Xeon Silver 4110, 2.1GHz, 8-Core, 16-Thread, 11M Cache, Turbo, HT

Specification	Description
Hard Drive	8 x 960GB SSD SAS Mix Use 12Gbps 512n 2.5in. Hot-plug
RAM	256GB
RAID Configuration	RAID 10
RAID Controller	PERC H740P, 8GB NV Cache
NIC	Broadcom 57416 2 Port 10Gb Base-T + 5720 2 Port 1Gb Base-T, rNDC
Power Supply	Dual, hot-plug, Redundant Power Supply (1+1), 750W
Power Cords	2 x NEMA 5-15P to C13 Wall Plug, 125 Volt, 15 AMP, 10 Feet (3m)
Rack Rails	ReadyRails™ Sliding Rails with Cable Management Arm
PCIe Riser	Risers with up to 4, x8 PCIe slots + 2, x16 PCIe slots
Operating System	Embedded Windows Server 2016 Standard
Database	Microsoft SQL Server 2016 Enterprise



Note: All physical BeyondTrust UVMSQLs are licensed for the Microsoft Windows Server Operating System and Microsoft SQL Server based on Microsoft Core CAL licenses. UVMSQLs ship with the Microsoft Certificate of Authenticity (COA) as proof of this licensing.

However, vSphere and Hyper-V images only have a SQL Server license. The Windows OS license key is provided with information to download images.

View UVMSQL Appliance Firewall Settings and Port Requirements

Firewall Settings

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

TCP Ports

Port	Purpose	Target Program/System Resource	Initial Status
80	HTTP	System	Enabled
443	HTTPS	System	Enabled
445	SMB	System	Disabled
1433	SQL Server	C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Binn\sqlservr.exe	Enabled
2000	App Bus	C:\Program Files(x86)\Common Files\Eye Digital Security\Application Bus\leeyeevnt.exe	Disabled
2383	SQL Analysis Services	C:\Program Files\Microsoft SQL Server\MSAS13.MSSQLSERVER\OLAP\bin\msmdsrv.exe	Enabled
3389	RDP	C:\Windows\System32\svchost.exe	Enabled
4422	Session Monitoring SSH	C:\Program Files(x86)\Eye Digital Security\Retina CS\pbsmd.exe	Enabled
4489	Session Monitoring RDP	C:\Program Files(x86)\Eye Digital Security\Retina CS\pbsmd.exe	Enabled
5022	SQL Server Mirroring	C:\Program Files\Microsoft SQL Server\MSSQL13.MSSQLSERVER\MSSQL\Binn\sqlservr.exe	Enabled
5985	WinRM	System; Restricted to 10.0.0.0-16	Enabled
8530	WSUS HTTP	System	Disabled
8531	WSUS HTTPS	System	Disabled
10001	Central Policy v1	C:\Program Files(x86)\Eye Digital Security\Retina CS\REMCentralPolicyService.exe	Enabled
21690	App Bus	(C:\Program Files(x86)\Common Files\Eye Digital Security\Application Bus\leeyeevnt.exe	Enabled
21690	Event Server	C:\Program Files(x86)\Common Files\Eye Digital Security\Event Server\REMEventsSvc.exe	Enabled

UDP Port

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

ICMPv4 Protocol

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

UVMSQL Setup Worksheet

UVMSQL Machine Name

Each UVMSQL Appliance requires a unique name using Microsoft naming standard.

UVMSQL Appliance Name: _____

Domain Admin Credentials

Each UVMSQL Appliance must be joined to an Active Directory domain. Please make a note of the credentials used to make this connection.

Username: _____ Password: _____

Organizational Unit (OU) Name

The OU name is the location where the UVMSQL Appliance will exist in Active Directory as a part of the clustering process.

Organizational Unit Name: _____

Security Group for UVMSQL Appliances

The security group for all UVMSQL Appliances to be added to during AOAG configuration. This group must be created in the OU.

Server Security Group Name: _____

Security Group for Service Account

This group is used to give the Group Managed Service Account local administrator permissions on the UVMSQL Appliance. The security group must be created in the OU.

Service Account Security Group Name: _____

Group Managed Service Account (gMSA)

This account is used during the AOAG configuration process. The associated Windows services on the UVMSQL Appliance will continue to run under this account. The Server Security Group must be given permission to retrieve the password of the gMSA. The gMSA must be a member of the Service Account Security Group.

Username: _____

Name and Static IP for Windows Cluster

Every cluster has an endpoint consisting of a name and an IP address.

Cluster Name: _____ Cluster IP: _____

Listener Name and Static IP Address for Each Availability Group

Listener Name: _____ Listener IP: _____

PowerShell Commands for the UVMSQL Appliance

This section contains a sample of PowerShell commands that could be used to prepare the OU, security groups, and Group Managed Service Accounts (gMSAs). This instruction assumes the following:

Domain	UVMLAND.LOCAL
OU	UVMSQL.CLUSTER
Server security group	UVMServerGroup
Service account security group	UVMSvcAcctGroup
Group Managed Service Account	UVMSvcAccount

Create an Organizational Unit (OU) for the UVMSQL Appliances

```
New-ADOrganizationalUnit -Name "CLUSTER" -Path "OU=UVMSQL,DC=UVMLAND,DC=LOCAL"
```

Block Inheritance for the OU

```
Set-GPinheritance -Target "OU=CLUSTER,OU=UVMSQL,DC=UVMLAND,DC=LOCAL" -IsBlocked Yes
```

Create a Security Group for the UVMSQL Appliance Servers in the OU

```
New-ADGroup -Name "UVMServerGroup" -SamAccountName UVMServerGroup -GroupCategory Security -  
GroupScope Global -DisplayName "UVMSQL Appliance Servers" -Path  
"OU=CLUSTER,OU=UVMSQL,DC=UVMLAND,DC=LOCAL" -Description "Members of this group are UVMSQL  
Appliances"
```

Create a Security Group for the UVMSQL Appliance Service Accounts in the OU

```
New-ADGroup -Name "UVMSvcAcctGroup" -SamAccountName UVMSvcAcctGroup -GroupCategory Security -  
GroupScope Global -DisplayName "UVMSQL Appliance Service Accounts" -Path  
"OU=CLUSTER,OU=UVMSQL,DC=UVMLAND,DC=LOCAL" -Description "Members of this group are UVMSQL  
Appliance Service Accounts"
```

Create the KDS Root Key if One Is Not Already Created for the Forest



Note: This is required for creating gMSAs. The **EffectiveImmediately** argument takes about ten hours to create and propagate the key.

```
Import-Module ActiveDirectory
Add-KdsRootKey -EffectiveImmediately
```

or

```
Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10)) //to use immediately
```

Create the Group Managed Service Account (gMSA) giving the UVMSQL Appliance Servers security group permission to retrieve the managed password

```
New-ADServiceAccount -Name UVMSvcAccount -DnsHostName UVMSvcAccount.UVMLAND.LOCAL -
PrincipalsAllowedToRetrieveManagedPassword "UVMServerGroup"
```

Add the gMSA to the UVMSQL Appliance Service Accounts Security Group

```
Add-ADGroupMember -Identity UVMSvcAcctGroup -Members "CN=UVMSvcAccount,CN=Managed Service
Accounts,DC=UVMLAND,DC=LOCAL"
```

Give the UVMSQL Appliance Service Accounts Group Full Control of the UVMSQL Appliance OU

```
$ou = "AD:\OU=CLUSTER,OU=UVMSQL,DC=UVMLAND,DC=LOCAL"
$group = Get-ADGroup UVMSvcAcctGroup
$group_sid = New-Object System.Security.Principal.SecurityIdentifier $group.SID
$ou_acl = Get-Acl $ou
$ace = New-Object System.DirectoryServices.ActiveDirectoryAccessRule $group_sid, "GenericAll",
"Allow"
$ou_acl.AddAccessRule($ace)
Set-Acl -AclObject $ou_acl $ou
```

Access UVMSQL Features from the UVMSQL LCD Panel

You can access the following features from the UVMSQL LCD panel.

Access Settings Menu

To access the settings:

The LCD panel displays *Please wait*. Once the UVMSQL completes the powering procedures, the UVMSQL displays the following actions.

LCD Panel Functionality

LCD Panel	Description
	Press the check to enter or accept the setting.
	Press the up or down arrow to navigate through the menus.
	Press the right or left arrow to access settings in the menu.
	Press the X to cancel the setting.

Enable RDP

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

1. Press the check  to enter **Settings / Show IP**.
2. Press check . The IP address of the UVMSQL is displayed.
3. Hold both the up  and down  buttons for four seconds. Do not do anything else between the previous step and this one.

Reset Administrator Password

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

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

Power Off

You can power off the UVMSQL using the LCD panel. To power off, on the LCD panel, select **Power Off**. The UVMSQL powers off.

Set Up the UVMSQL Appliance

Your UVMSQL Appliance is designed to be configured and used with a web browser.



IMPORTANT!

If you purchased Professional Services, schedule your engagement with your Professional Services representative before starting the Configuration Wizard.

Power on the UVMSQL

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



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

Perform Initial Network Configuration

The UVMSQL is configured to use DHCP and receives an assigned IP address. To access your UVMSQL the first time, open a browser on a device on the same network subnet as the UVMSQL. Enter the UVMSQL's factory IP address as displayed on the LCD screen, preceded by **https://**, for example, **https://10.10.123.456**. You can find this IP address using the LCD display of the UVMSQL. You will need the IP address later in the process when you configure the UVMSQL.

Display IP Address

To display the IP address, select **Show IP** on the LCD panel. The IP address automatically displays.

Automatically Enter IP Address

On the LCD panel, select **Config IP**, then select **Auto DHCP**. The UVMSQL automatically updates the IP address to the DHCP protocol.

Manually Enter IP Address

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

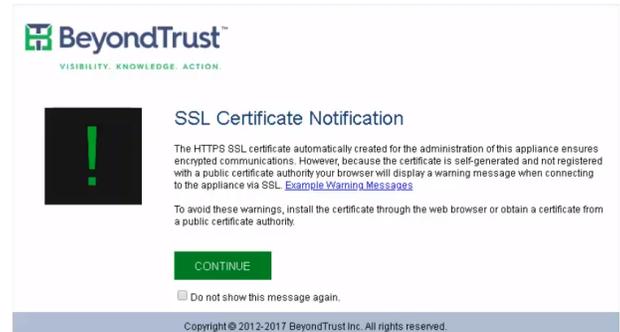
Hardware Notes

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

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

Configure the BeyondTrust UVMSQL Appliance

1. To access your UVMSQL the first time, open a browser on a device on the same network subnet as the UVMSQL. Enter the UVMSQL's factory IP address as displayed on the LCD screen, preceded by **https://**, for example, **https://10.10.123.456**. You can find this IP address using the LCD display of the UVMSQL.
2. An SSL certificate notification displays. Click **Continue**. You will replace the default certificate with a signed certificate later during the configuration process.
3. On the welcome page, create a name for the UVMSQL Appliance.



IMPORTANT!

Once you have named your UVMSQL Appliance, it cannot be renamed. If at any point you need to rename the appliance, you must either re-image (if it is a physical appliance) or re-deploy (if it is a virtual appliance) the image.

- On the **IP Settings** page, select the network card to use. The dropdown list shows only connected network ports. If you select **Obtain IP address automatically**, the remaining fields fill automatically. Otherwise, enter the IP and DNS information.



Note: The domain IP must be a static IPv4 address. Use quad-dotted notation for the subnet mask. For example, 255.255.255.0.

- If you are satisfied with the settings, click **Apply Settings and Reboot**. If you need to rename your UVMSQL Appliance, click **Back to Rename Machine**.

- You are prompted to confirm your UVMSQL Appliance name.

- Click **Cancel** to go back, or click **Apply Name and Reboot** to continue.
- The UVMSQL Appliance reboots to apply its name and IP address settings.



BeyondTrust™
VISIBILITY. KNOWLEDGE. ACTION.

IP SETTINGS

Please configure the IP Settings for the appliance.

Network card
Intel(R) PRO/1000 MT Network Connection

Obtain IP address automatically (DHCP)

Domain IP - this must be set

Subnet Mask

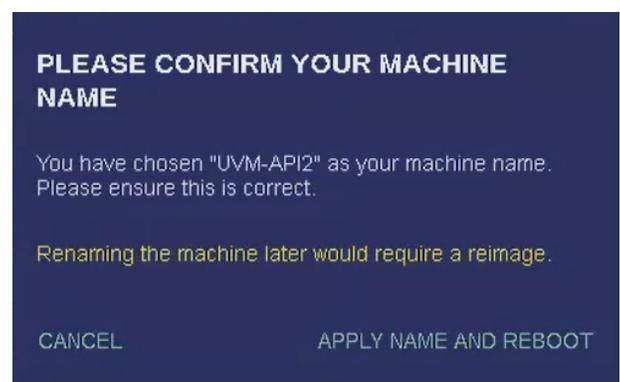
Default Gateway

Preferred DNS Server

Alternate DNS Server

DNS Suffix

BACK TO RENAME MACHINE APPLY SETTINGS AND REBOOT



PLEASE CONFIRM YOUR MACHINE NAME

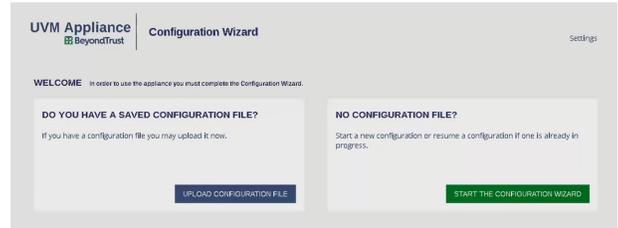
You have chosen "UVM-API2" as your machine name. Please ensure this is correct.

Renaming the machine later would require a reimage.

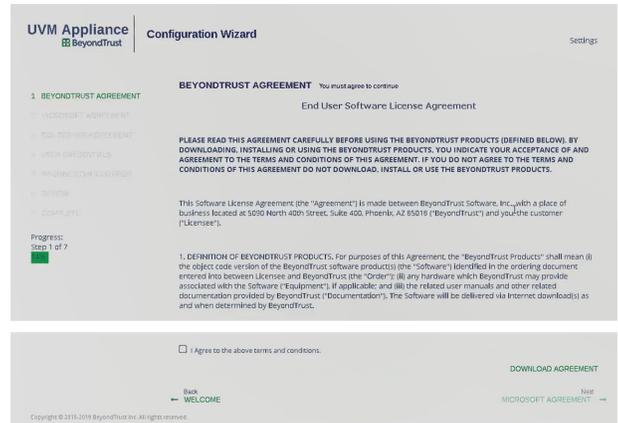
CANCEL APPLY NAME AND REBOOT

Configuration
The Appliance is now rebooting. This page will be redirected when the Appliance has rebooted.

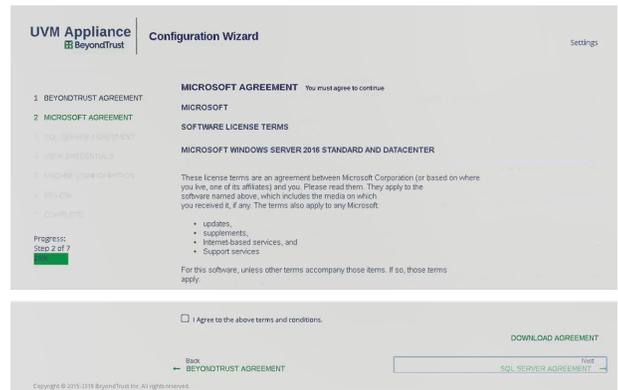
9. Once the reboot completes, you are prompted to upload a saved configuration file or to start the Configuration Wizard.



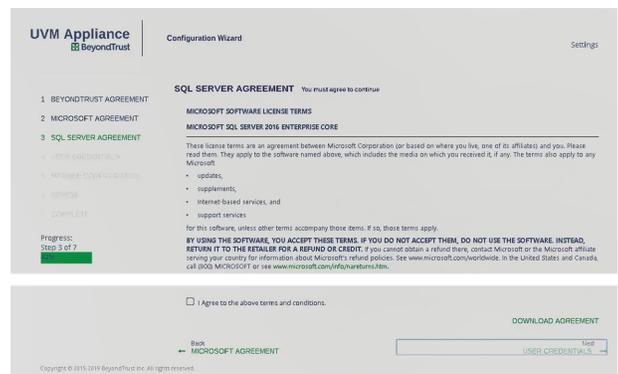
10. The Configuration Wizard starts with the BeyondTrust license agreement. After reading the terms, click **I Agree to the above terms and conditions**. Then click **Next: Microsoft Agreement**.



11. After reading the Microsoft agreement, click **I Agree to the above terms and conditions**. Then click **Next: SQL Server Agreement**.



12. After reading the SQL Server agreement, click **I Agree to the above terms and conditions**. Then click **Next: User Credentials**.





IMPORTANT!

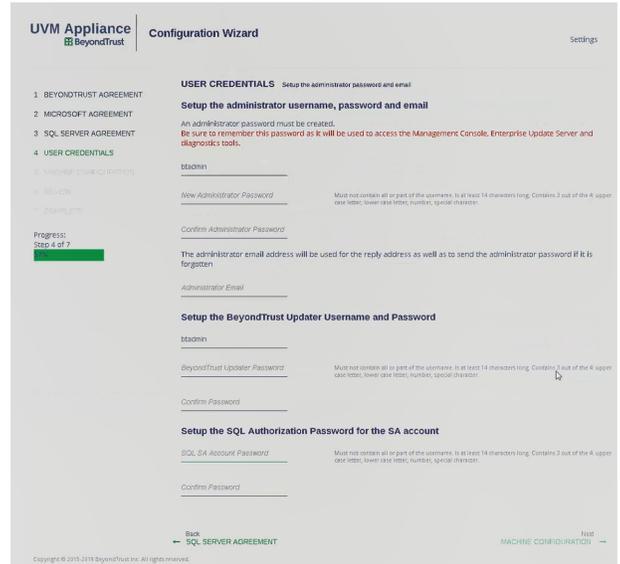
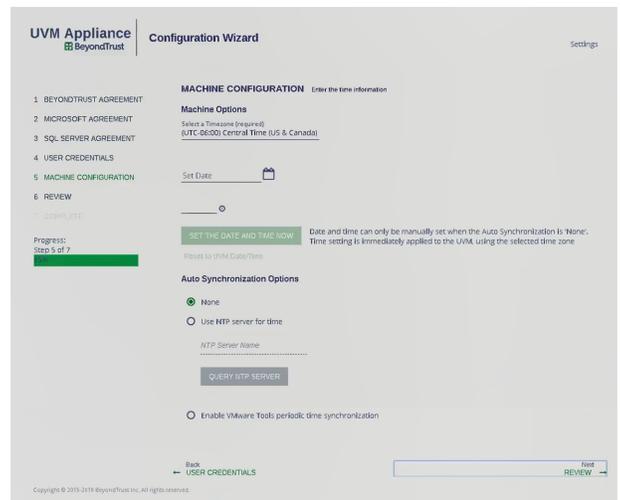
While it is possible to **rename** the Administrator accounts later, we recommended choosing account names carefully during installation (next step), to **avoid** renaming them later.

- On the **User Credentials** page, set up an administrator username, password, and email address for the BeyondTrust software. On this page, also set up a username and password for the BeyondTrust Updater tool, as well as a password for the SQL Server Administration account. Then click **Next: Machine Configuration**.

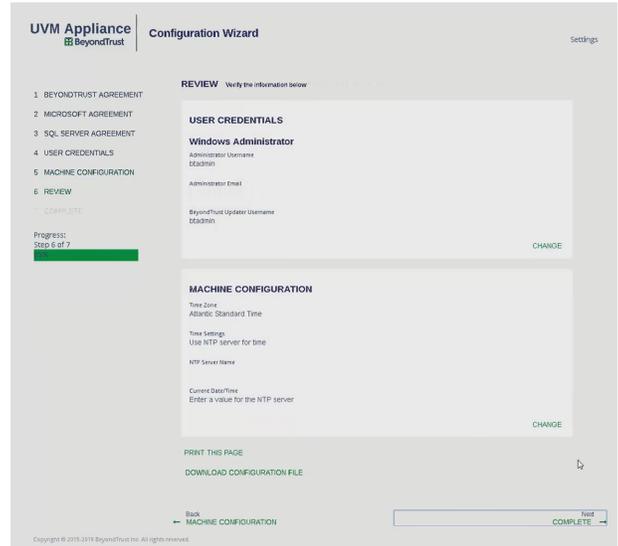


Note: The email address is used as a reply address, as well as if the administrator password is forgotten.

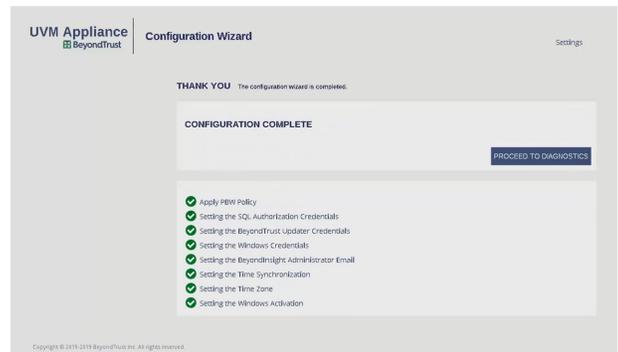
- Under **Machine Options**, select a time zone. You can configure the date and time manually, or you can synchronize the time using an NTP server or VMware Tools. Click **Next: Review**.

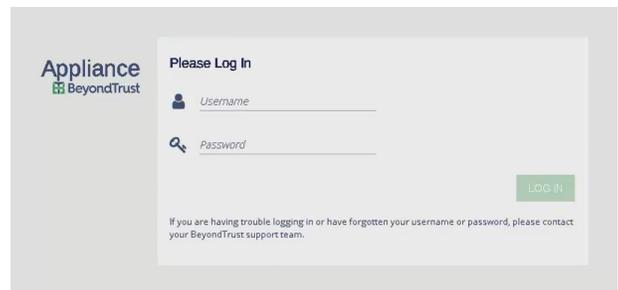
- On the **Review** page, confirm that the settings are correct. You can go back and make changes as needed. You can also download the configuration file for backup or to use on another system. Click **Next: Complete**.



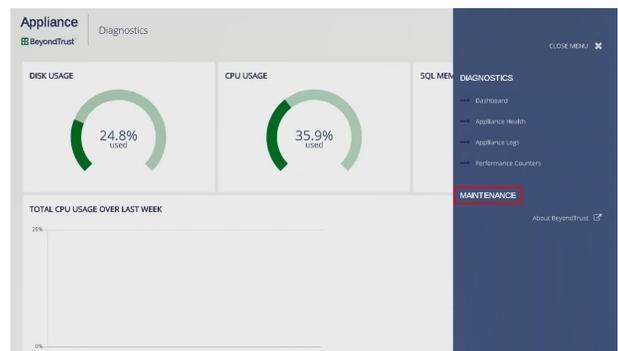
- The Configuration Wizard applies the settings to the UVMSQL Appliance. Once the configuration is complete, click **Proceed to Diagnostics**.



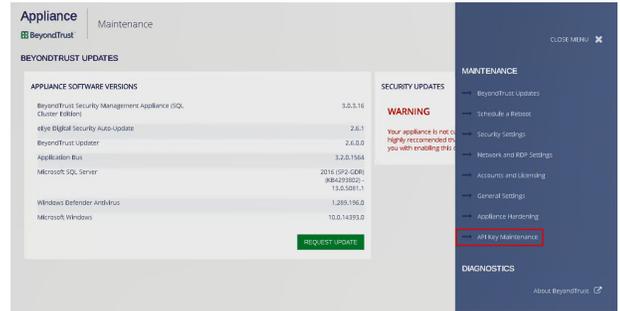
- Enter your BeyondTrust administrator username and password to log in.



- From the home page, open the menu and select **Maintenance**.

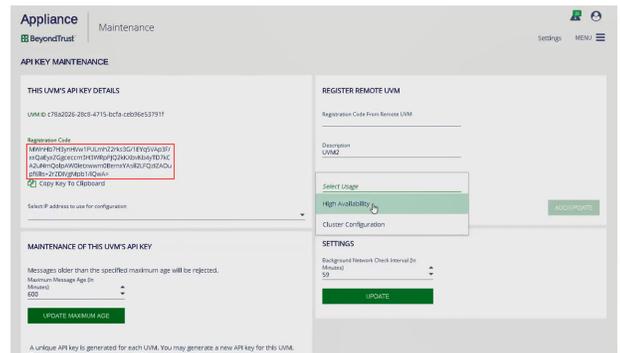


- The maintenance page loads your UVMSQL Appliance software versions. Once this information has loaded, open the menu and select **API Key Maintenance**.



- Under **This UVM's API Key Details**, copy the registration code to your clipboard.

 **Note:** Each API key is generated for a specific UVMSQL Appliance. The key itself cannot be viewed. The registration code encrypts the key along with additional metadata, such as the UVMSQL Appliance ID and the IP address.



- To pair two UVMSQL Appliances, switch to the configuration page for the second UVMSQL Appliance.

- Open the menu and click **API Key Maintenance**.
- From **Select IP address to use for configuration**, select the appropriate IP address.
- Under **Register Remote UVM**, paste the copied code into **Registration Code from Remote UVM**.
- Enter a **Description** to identify this UVMSQL.
- From **Select Usage**, choose **Cluster Configuration**.
- Click **Add/Update**.
- A prompt displays that the key has been registered. Click **OK**.
- Copy the registration key from this UVMSQL Appliance's details.

 **Note:** Registering a key from another UVMSQL Appliance allows this UVMSQL Appliance to accept calls from the other UVMSQL Appliance.

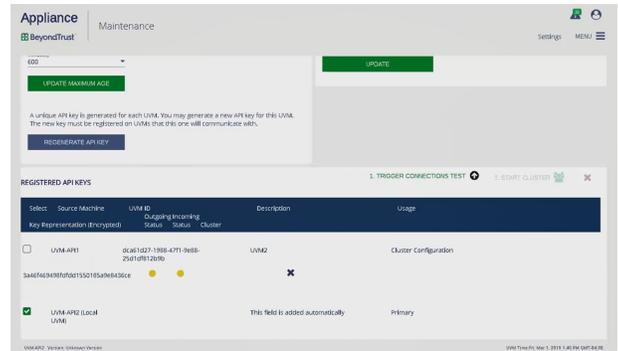
- Switch to the first UVMSQL Appliance's configuration page.

- From **Select IP address to use for configuration**, select the appropriate IP address.
- Under **Register Remote UVM**, paste the copied code into **Registration Code from Remote UVM**.
- Enter a **Description** to identify this UVMSQL.
- From **Select Usage**, choose **Cluster Configuration**.
- Click **Add/Update**.
- A prompt displays that the key has been registered. Click **OK**.

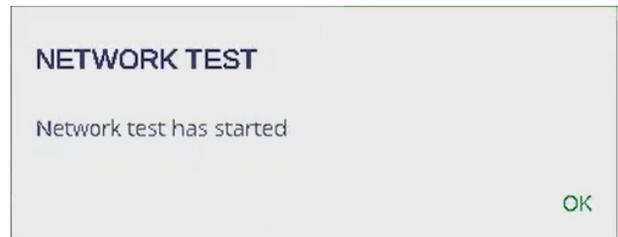
! IMPORTANT!

You can regenerate an API key if needed. However, doing so also regenerates the registration code, breaking the link between this UVMSQL Appliance and another. You must copy the new registration code and re-enter it on the other UVMSQL Appliance to re-establish the connection.

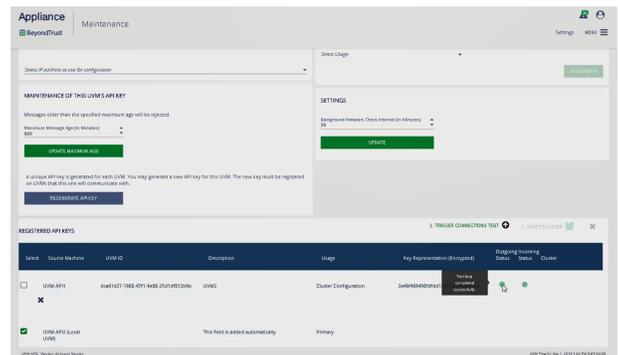
- 23. Scroll down to view the registered API keys.
- 24. Click **Trigger Connections Test**.



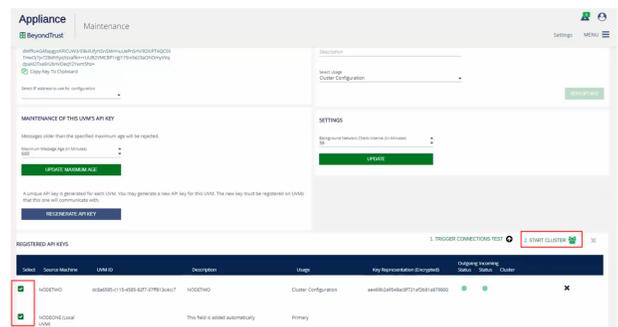
- 25. You are notified that the test has started. Click **OK**.



- 26. When the test completes, the page displays the results.



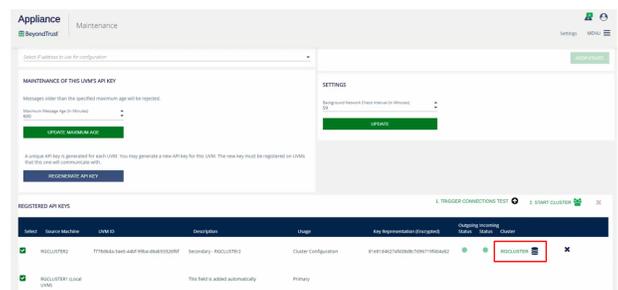
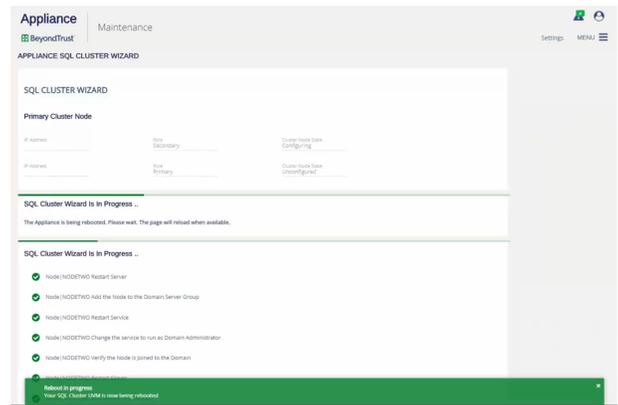
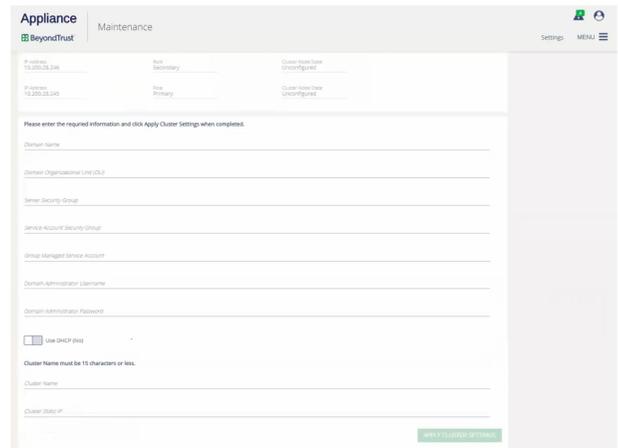
- 27. To group UVMSQL Appliances into a cluster, select the UVMSQL Appliances, and then click **Start Cluster**.



28. In the top section, you can view the IP addresses, cluster roles, and cluster node status of the selected UVMSQL Appliances.
29. Enter the domain name, organizational unit, security groups, service account, and domain administrator account.
30. Choose if the cluster should use DHCP.
31. Create a name for the cluster.
32. If the cluster is not using DHCP, enter a dedicated static IP address for the cluster.
33. Click **Apply Cluster Settings**.

34. The SQL Cluster Wizard runs, showing status messages of its progress.

35. When the wizard completes, the UVMSQL Appliance appears as part of the cluster. Click on the cluster database icon.

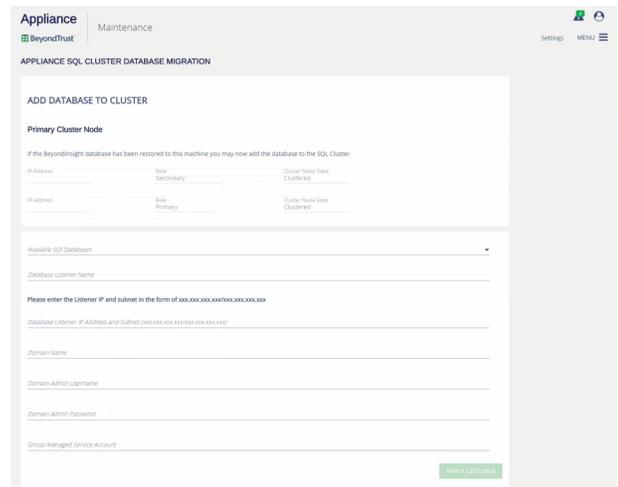



IMPORTANT!

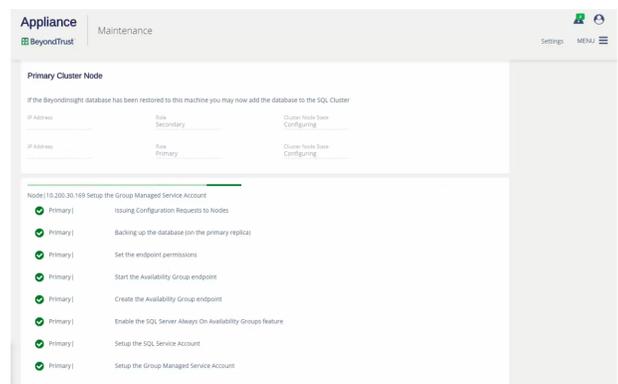
Before the availability group can be created, the database must exist on the UVMSQL Appliance you plan to make the primary replica. There are a few ways to do this; choose the method most appropriate for your situation.

- During the Configuration Wizard on a SQL Free UVMSQL Appliance, at the **SQL Server Agreement** step, create a database on the primary replica using the option to create a remote database.
- From a configured UVMSQL Appliance or SQL Free UVMSQL Appliance, go to the **Database Utilities** page of the **Maintenance** application and use the **Create a Remote BeyondInsight Database** feature to create a database on the primary replica.
- Restore a BeyondInsight database backup on the primary replica on the SQL cluster using SQL Server Management Studio.

36. In the top section, you can view the IP addresses, cluster roles, and cluster node status of the clustered UVMSQL Appliances.
37. Select a SQL database.
38. Enter a database listener name, IP address, and subnet mask.
39. Provide a domain name, domain administrator account, and service account.
40. Click **Apply Listener**.



41. The SQL Database Wizard runs, showing status messages of its progress.



42. When the wizard completes, the listener name and IP address are displayed.

