BeyondTrust

UVMSQL Appliance Installation Guide

TC:11/30/2020

Table of Contents

UVMSQL Appliance Installation Guide

The UVMSQL cluster appliance is specifically designed to offer SQL Server Always On Availability Group (AOAG) configuration on a BeyondTrust UVM 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 Appliance Warranty

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

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

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

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

Warranty Invalidation

This warranty is void in the event that:

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

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

IMPORTANT!

Do not log on to the Console or Remote Desktop to the virtual 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 appliance
- A private DNS A-record resolving to the static IP of your 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 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.
3. Identify the domain that the UVMSQL appliances will be joined 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.

> For more information about Group Managed Service accounts, please see https://techcommunity.microsoft.com/t5/Core-Infrastructure-and-Security/Windows-Server-2012-Group-Managed-Service-Accounts/ba-p/255910.

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 a useful tool to prepare for initial setup, please see "UVMSQL Setup Worksheet" on page 10.

Client Requirements

Supported browsers:

- Microsoft Edge
- Firefox
- Google Chrome

- Safari
- Microsoft Internet Explorer (IE) 11

Appliance Requirements

- 10/100/1000 MB 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 Appliance Specifications

UVMSQL Specifications

Specification	Description
AC Input Voltage	110 to 240 V AC, autoranging
Rated Input Frequency	50 to 60 Hz
Cooling	8 Standard Fans, 2 Standard 1U Heatsinks
Chassis	Chassis with up to 8, 3.5" Hard Drives
Dimensions	1U rack-mountable server H: 1.68 in. (4.28 cm) (10.75 in. shipping) W: 18.97 in. (48.18 cm) (24 in. shipping) D: 26.89 in. (68.30 cm) (35.75 in. shipping) Weight: approx 45 lbs. (48 lbs. shipping)
Microprocessor	2 x Intel Xeon Silver 4110, 2.1 GHz, 8-Core, 16-Thread, 11M Cache, Turbo, HT
Hard Drive	8 x 960 GB SSD SAS Mix Use 12Gbps 512n 2.5in Hot-plug
RAM	256 GB
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 BeyondTrust UVM appliances, physical and virtual, are licensed for the Microsoft Windows Server Operating System and Microsoft SQL Server based on Microsoft Core CAL licenses. Appliances ship with the Microsoft Certificate of Authenticity (COA) as proof of this licensing.*

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\eEye Digital Security\Application Bus\eeyeevnt.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)\eEye Digital Security\Retina CS\pbsmd.exe	Enabled
4489	Session Monitoring RDP	C:\Program Files(x86)\eEye 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)\eEye Digital Security\Retina CS\REMCentralPolicyService.exe	Enabled
21690	App Bus	(C:\Program Files(x86)\Common Files\eEye Digital Security\Application Bus\eeyeevnt.exe	Enabled
21690	Event Server	C:\Program Files(x86)\Common Files\eEye Digital Security\Event Server\REMEventsSvc.exe	Enabled
21691	Android Mobile Connector via BeyondInsight Web Service	C:\Program Files(x86)\eEye Digital Security\Retina CS\eEye.RetinaCS.WebService.exe	Disabled

UDP Port

Port	Purpose	Target Program/System Resource	Initial Status
4609	Appliance Discovery	C:\Program Files(x86)\Common Files\eEye Digital Security\Scheduler\eeyeschedulersvc.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 note 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 that all UVMSQL appliances will 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 will be used in 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 to 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 gMSA. This example 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 UVM 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 UVM servers in the OU

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

Create a Security Group for the UVM service accounts in the OU

```
New-ADGroup -Name "UVMSvcAcctGroup" -SamAccountName UVMSvcAcctGroup -GroupCategory Security -
GroupScope Global -DisplayName "UVM Service Accounts" -Path
"OU=CLUSTER,OU=UVMSQL,DC=UVMLAND,DC=LOCAL" -Description "Members of this group are UVM 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 UVM Servers security group permission to retrieve the managed password

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

Add the gMSA to the UVM service accounts security group

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

Give the UVM service accounts group full control of the UVM 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 Features from the UVM LCD Panel

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

Access Settings Menu

To access the settings:

The LCD panel displays *Please wait*. Once the appliance completes the powering procedures, UVM 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 *UVM 20 Ready* is displayed.

1. Press the check ✓ to enter **Settings / Show IP**.
2. Press check ✓. The IP address of the appliance is displayed.
3. Hold both the up ▲ and down ▼ button 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 appliance to reset the administrator password.
3. Select **Show IP** to view the IP address.
4. Hold the up ▲ and down ▼ buttons simultaneously on the UVM LCD panel. A random password is generated.
5. Press the check ✓ to accept the changed password.

Power Off

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

1. Plug the power cables for the appliance into a safe power source. The appliance's power supplies will 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 appliance. The power LED immediately to the right of the reset button will illuminate, and the HDD activity LED (immediately to the right of the power LED) will begin to flash. Initialization of the appliance will complete in about 60 seconds.

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

Perform Initial Network Configuration

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

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 UVM 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**.

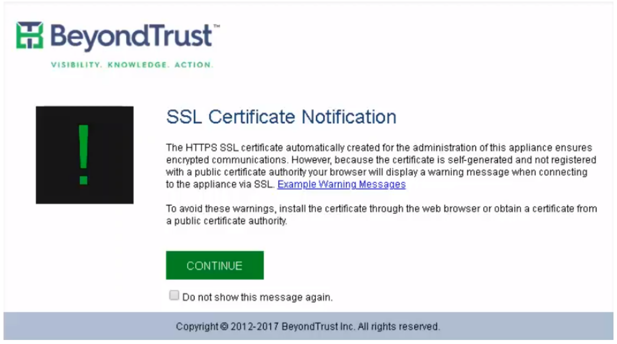
Hardware Notes

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

Configure the BeyondTrust UVMSQL Appliance

1. To access your appliance the first time, open a browser on a device on the same network subnet as the appliance. Enter the appliance's factory IP address as displayed on the LCD screen, preceded by **https://** (example, https://10.10.123.456). You can find this IP address using the LCD display of the appliance.
2. You will see an SSL certificate notification. Click **Continue**. You will replace the default certificate with a signed certificate later in the process.



SSL Certificate Notification

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

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

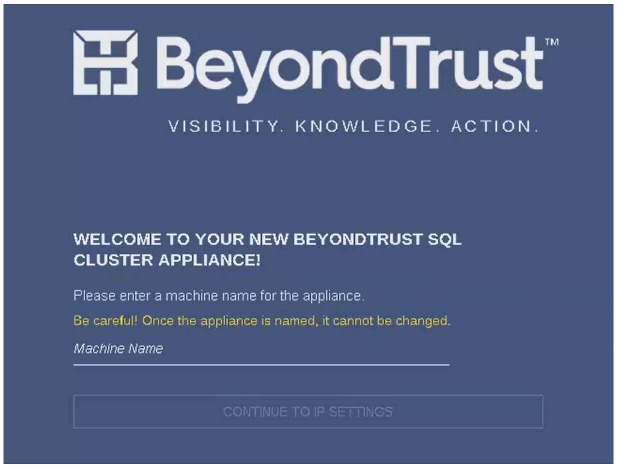
□ Do not show this message again.

Copyright © 2012-2017 BeyondTrust Inc. All rights reserved.

3. On the welcome page, create a name for your UVMSQL appliance.

IMPORTANT!

Once you have named your appliance, it cannot be renamed.



WELCOME TO YOUR NEW BEYONDTRUST SQL CLUSTER APPLIANCE!

Please enter a machine name for the appliance.

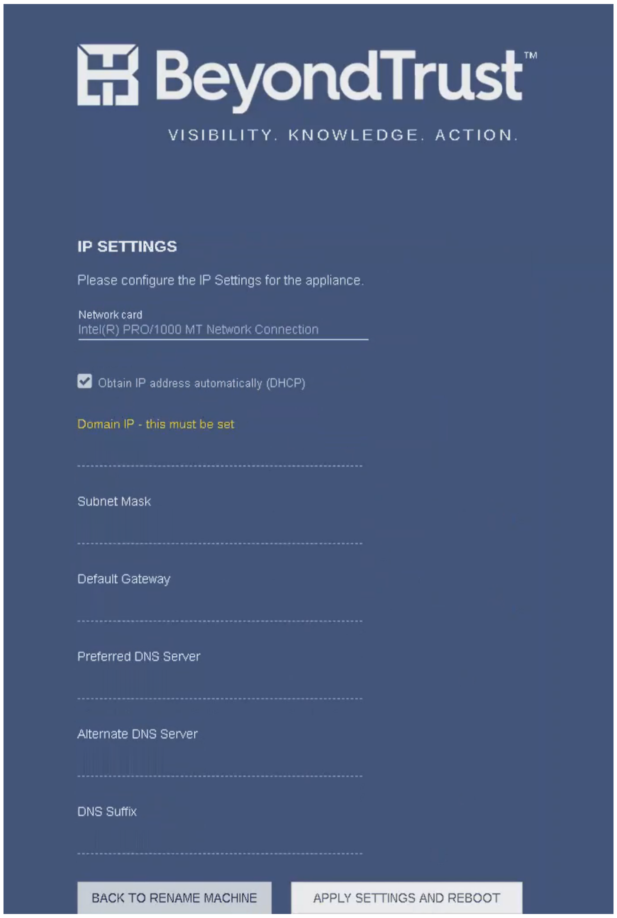
Be careful! Once the appliance is named, it cannot be changed.

Machine Name

4. On the **IP Settings** page, select the network card to use. The drop-down list shows only connected network ports. If you select **Obtain IP address automatically**, the following fields will 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 (example, 255.255.255.0).*

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



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

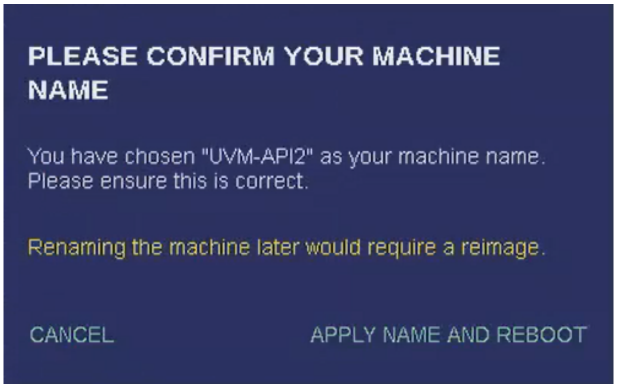
Alternate DNS Server

DNS Suffix

6. You will be prompted to confirm your appliance name. Click **Cancel** to go back, or click **Apply Name and Reboot** to continue.

IMPORTANT!

Once you pass this step, you cannot rename your appliance.

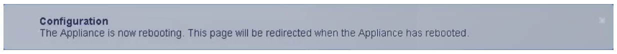


PLEASE CONFIRM YOUR MACHINE NAME

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

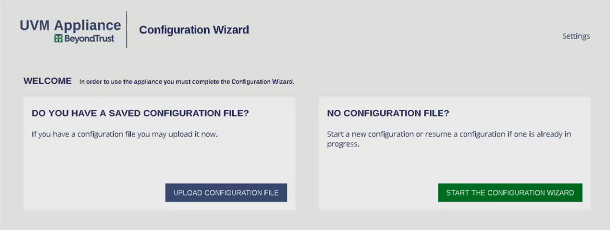
Renaming the machine later would require a reimage.

7. The appliance reboots to apply its name and IP address settings.



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

8. Once the reboot completes, you are prompted to upload a saved configuration file or to start the configuration wizard.



WELCOME In order to use the appliance you must complete the Configuration Wizard.

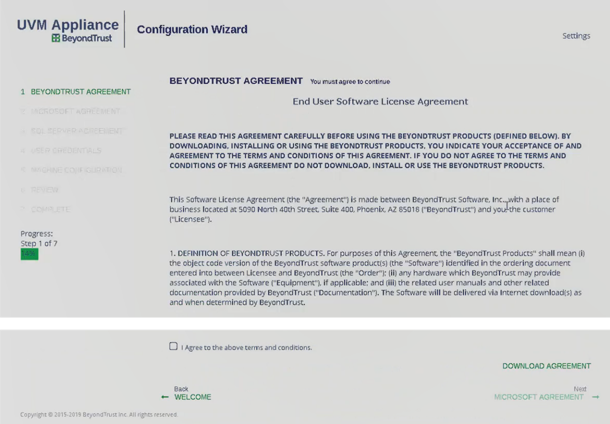
DO YOU HAVE A SAVED CONFIGURATION FILE?

If you have a configuration file you may upload it now.

NO CONFIGURATION FILE?

Start a new configuration or resume a configuration if one is already in progress.

9. 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**.



Progress:
Step 1 of 7
14%

BEYONDTRUST AGREEMENT You must agree to continue

End User Software License Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE BEYONDTRUST PRODUCTS (DEFINED BELOW). BY DOWNLOADING, INSTALLING OR USING THE BEYONDTRUST PRODUCTS, YOU INDICATE YOUR ACCEPTANCE OF AND AGREEMENT TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT DO NOT DOWNLOAD, INSTALL OR USE THE BEYONDTRUST PRODUCTS.

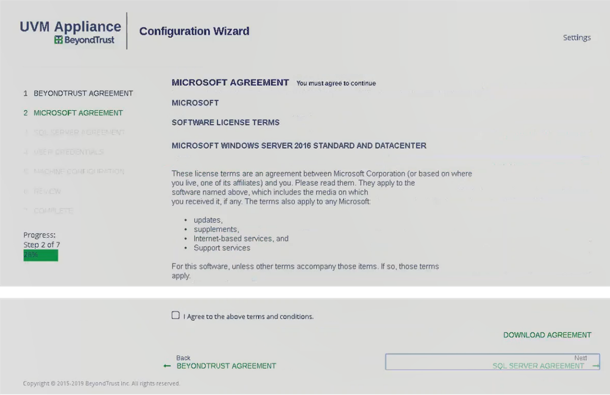
This Software License Agreement (the "Agreement") is made between BeyondTrust Software, Inc., with a place of business located at 5090 North 40th Street, Suite 400, Phoenix, AZ 85018 ("BeyondTrust") and you, the customer ("Licensee").

1. DEFINITION OF BEYONDTRUST PRODUCTS. For purposes of this Agreement, the "BeyondTrust Products" shall mean (i) the object code version of the BeyondTrust software product(s) (the "Software") identified in the ordering document entered into between Licensee and BeyondTrust (the "Order"); (ii) any hardware which BeyondTrust may provide associated with the Software ("Equipment"), if applicable; and (iii) the related user manuals and other related documentation provided by BeyondTrust ("Documentation"). The Software will be delivered via Internet download(s) as and when determined by BeyondTrust.

☐ I Agree to the above terms and conditions.

Copyright © 2015-2019 BeyondTrust Inc. All rights reserved.

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



Progress:
Step 2 of 7
28%

MICROSOFT AGREEMENT You must agree to continue

MICROSOFT

SOFTWARE LICENSE TERMS

MICROSOFT WINDOWS SERVER 2016 STANDARD AND DATACENTER

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft:

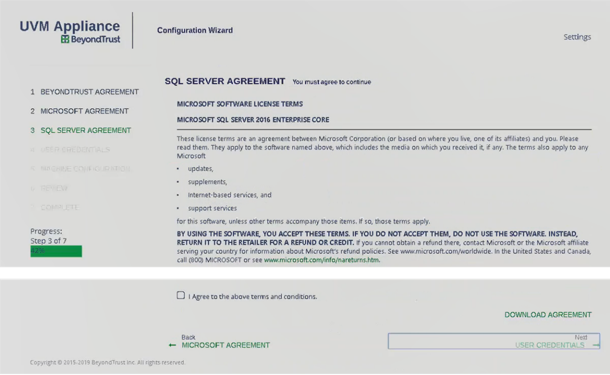
- updates,
- supplements,
- Internet-based services, and
- Support services

For this software, unless other terms accompany those items. If so, those terms apply.

☐ I Agree to the above terms and conditions.

Copyright © 2015-2019 BeyondTrust Inc. All rights reserved.

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



Progress:
Step 3 of 7
42%

SQL SERVER AGREEMENT You must agree to continue

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT SQL SERVER 2016 ENTERPRISE CORE

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

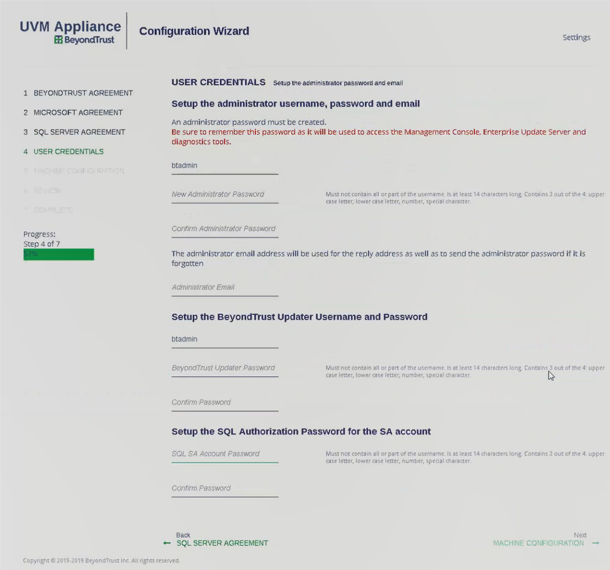
BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE. INSTEAD, RETURN IT TO THE RETAILER FOR A REFUND OR CREDIT. If you cannot obtain a refund there, contact Microsoft or the Microsoft affiliate serving your country for information about Microsoft's refund policies. See www.microsoft.com/worldwide. In the United States and Canada, call (800) MICROSOFT or see www.microsoft.com/info/nareturns.htm.

☐ I Agree to the above terms and conditions.

Copyright © 2015-2019 BeyondTrust Inc. All rights reserved.

12. On the **User Credentials** page, set up an administrator username, password, and email address for the BeyondTrust software. You will 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.*



UVM Appliance BeyondTrust | Configuration Wizard

Settings

1 BEYONDTRUST AGREEMENT
2 MICROSOFT AGREEMENT
3 SQL SERVER AGREEMENT
4 USER CREDENTIALS
5 MACHINE CONFIGURATION
6 REVIEW
7 COMPLETE

Progress:
Step 4 of 7
57%

USER CREDENTIALS Setup the administrator password and email

Setup the administrator username, password and email

An administrator password must be created.
Be sure to remember this password as it will be used to access the Management Console, Enterprise Update Server and diagnostics tools.

btadmin

New Administrator Password — Must not contain all or part of the username. Is at least 14 characters long. Contains 3 out of the 4: upper case letter, lower case letter, number, special character.

Confirm Administrator Password

The administrator email address will be used for the reply address as well as to send the administrator password if it is forgotten

Administrator Email

Setup the BeyondTrust Updater Username and Password

btadmin

BeyondTrust Updater Password — Must not contain all or part of the username. Is at least 14 characters long. Contains 3 out of the 4: upper case letter, lower case letter, number, special character.

Confirm Password

Setup the SQL Authorization Password for the SA account

SQL SA Account Password — Must not contain all or part of the username. Is at least 14 characters long. Contains 3 out of the 4: upper case letter, lower case letter, number, special character.

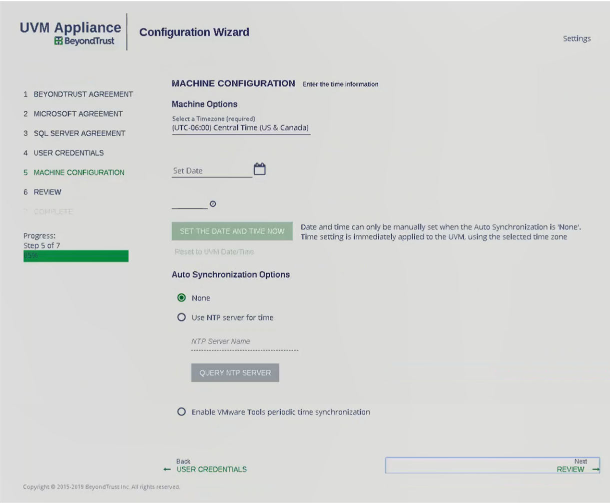
Confirm Password

Back ← SQL SERVER AGREEMENT

Next MACHINE CONFIGURATION →

Copyright © 2015-2019 BeyondTrust Inc. All rights reserved.

13. 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**.



UVM Appliance BeyondTrust | Configuration Wizard

Settings

1 BEYONDTRUST AGREEMENT
2 MICROSOFT AGREEMENT
3 SQL SERVER AGREEMENT
4 USER CREDENTIALS
5 MACHINE CONFIGURATION
6 REVIEW
7 COMPLETE

Progress:
Step 5 of 7
85%

MACHINE CONFIGURATION Enter the time information

Machine Options

Select a Timezone (required)
(UTC-06:00) Central Time (US & Canada)

Set Date

SET THE DATE AND TIME NOW — Date and time can only be manually set when the Auto Synchronization is 'None'. Time setting is immediately applied to the UVM, using the selected time zone

Reset to UVM Date/Time

Auto Synchronization Options

● None
○ Use NTP server for time

NTP Server Name

QUERY NTP SERVER

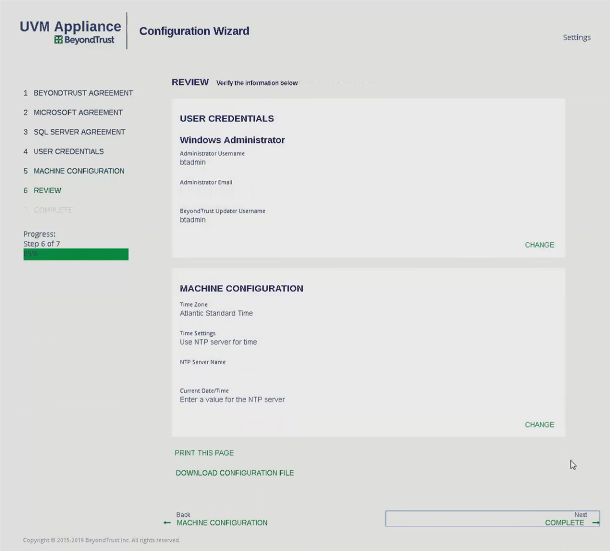
○ Enable VMware Tools periodic time synchronization

Back ← USER CREDENTIALS

Next REVIEW →

Copyright © 2015-2019 BeyondTrust Inc. All rights reserved.

14. On the **Review** page, confirm that your 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**.



UVM Appliance BeyondTrust | Configuration Wizard Settings

1 BEYONDTRUST AGREEMENT
2 MICROSOFT AGREEMENT
3 SQL SERVER AGREEMENT
4 USER CREDENTIALS
5 MACHINE CONFIGURATION
6 REVIEW
7 COMPLETE

Progress:
Step 6 of 7

REVIEW Verify the information below

USER CREDENTIALS

Windows Administrator

Administrator Username
btadmin

Administrator Email

BeyondTrust Updater Username
btadmin

CHANGE

MACHINE CONFIGURATION

Time Zone
Atlantic Standard Time

Time Settings
Use NTP server for time

NTP Server Name

Current Date/Time
Enter a value for the NTP server

CHANGE

PRINT THIS PAGE

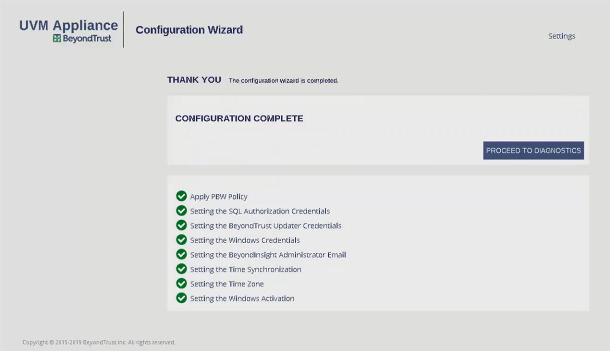
DOWNLOAD CONFIGURATION FILE

Back ← MACHINE CONFIGURATION

Next COMPLETE →

Copyright © 2015-2019 BeyondTrust Inc. All rights reserved.

15. The configuration wizard applies the settings to the UVMSQL appliance. Once the configuration is complete, click **Proceed to Diagnostics**.



UVM Appliance BeyondTrust | Configuration Wizard Settings

THANK YOU The configuration wizard is completed.

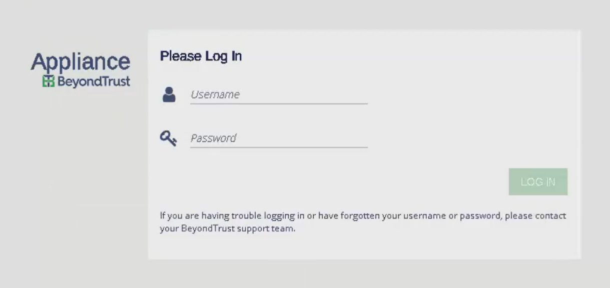
CONFIGURATION COMPLETE

PROCEED TO DIAGNOSTICS

- ✓ Apply PBW Policy
- ✓ Setting the SQL Authorization Credentials
- ✓ Setting the BeyondTrust Updater Credentials
- ✓ Setting the Windows Credentials
- ✓ Setting the BeyondInsight Administrator Email
- ✓ Setting the Time Synchronization
- ✓ Setting the Time Zone
- ✓ Setting the Windows Activation

Copyright © 2015-2019 BeyondTrust Inc. All rights reserved.

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



Appliance BeyondTrust

Please Log In

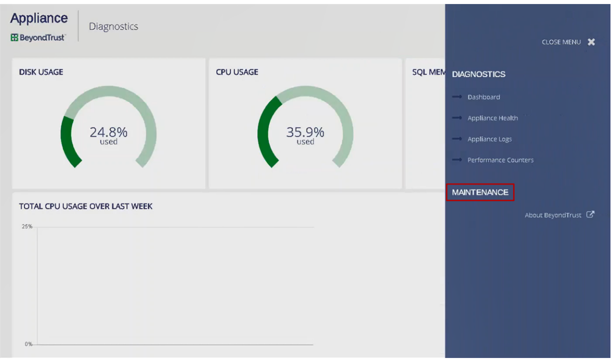
Username

Password

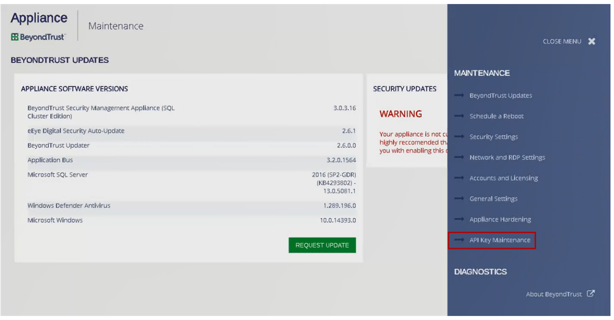
LOG IN

If you are having trouble logging in or have forgotten your username or password, please contact your BeyondTrust support team.

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



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



BEYONDTRUST UPDATES

APPLIANCE SOFTWARE VERSIONS

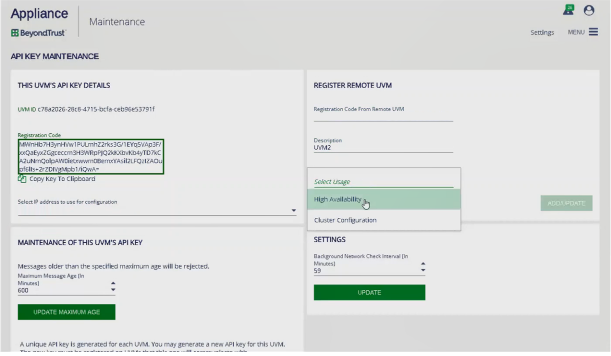
BeyondTrust Security Management Appliance (SQL Cluster Edition)	3.0.3.16
eEye Digital Security Auto-Update	2.6.1
BeyondTrust Updater	2.6.0.0
Application Bus	3.2.0.1564
Microsoft SQL Server	2016 (SP2-GDR) (KB4293802) - 13.0.5081.1
Windows Defender Antivirus	1.289.196.0
Microsoft Windows	10.0.14393.0

SECURITY UPDATES

WARNING

Your appliance is not cu
highly reccomended th
you with enabling this c

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



API KEY MAINTENANCE

THIS UVM'S API KEY DETAILS

UVM ID c78a2026-28c8-4715-bcfa-ceb96e53791f

Registration Code
MWnHb7H3ynHVw1PULmhZ2rks3G/1EYq5VAp3F/xxQaEyxZGgceccm3H3WRpPJQ2kKXbvKb4yTD7kCA2uNmQolpAW0ietxwwm0BemxYAsil2LFQzIZAOupf6lls+2rZDIVgMpb1/iQwA=

Select IP address to use for configuration

REGISTER REMOTE UVM

Registration Code From Remote UVM

Description
UVM2

MAINTENANCE OF THIS UVM'S API KEY

Messages older than the specified maximum age will be rejected.

Maximum Message Age (In Minutes)
600

SETTINGS

Background Network Check Interval (In Minutes)
59

A unique API key is generated for each UVM. You may generate a new API key for this UVM.

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

20. To pair two UVMSQL appliances, switch to the configuration page for the second appliance.
    a. Open the menu and select **API Key Maintenance**.
    b. From **Select IP address to use for configuration**, select the appropriate IP address.
    c. Under **Register Remote UVM**, paste the copied code into **Registration Code from Remote UVM**.
    d. Enter a **Description** to identify this appliance.
    e. From **Select Usage**, choose **Cluster Configuration**.
    f. Click **Add/Update**.
    g. You will see a prompt that the key has been registered. Click **OK**.
    h. Copy the registration key from this appliance's details.

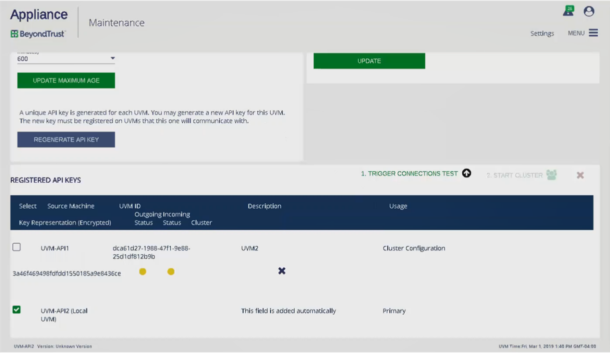
> ***Note:*** *Registering a key from another appliance allows this appliance to accept calls from the other appliance.*

21. Switch to the first appliance's configuration page.
    a. From **Select IP address to use for configuration**, select the appropriate IP address.
    b. Under **Register Remote UVM**, paste the copied code into **Registration Code from Remote UVM**.
    c. Enter a **Description** to identify this appliance.
    d. From **Select Usage**, choose **Cluster Configuration**.
    e. Click **Add/Update**.
    f. You will see a prompt 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 any link between this appliance and another. You must copy the new registration code and paste it to the paired appliance to reestablish the connection.

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



600

A unique API key is generated for each UVM. You may generate a new API key for this UVM. The new key must be registered on UVMs that this one will communicate with.

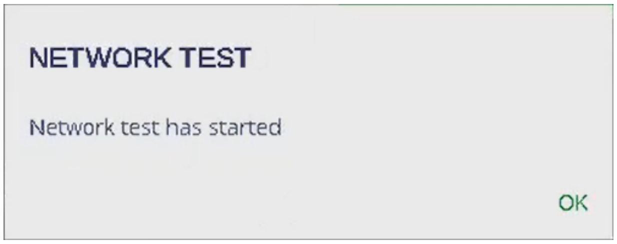
REGISTERED API KEYS

Select	Source Machine	UVM ID	Description	Usage
Key Representation (Encrypted)		Outgoing Status / Incoming Status / Cluster		
☐	UVM-API1	dca61d27-1988-47f1-9e88-25d1df812b9b	UVM2	Cluster Configuration
3a46f469498fdfdd1550185a9e8436ce		● ● ✖		
☑	UVM-API2 (Local UVM)		This field is added automatically	Primary

UVM-API2 Version: Unknown Version

UVM Time:Fri, Mar 1, 2019 1:40 PM GMT-04:00

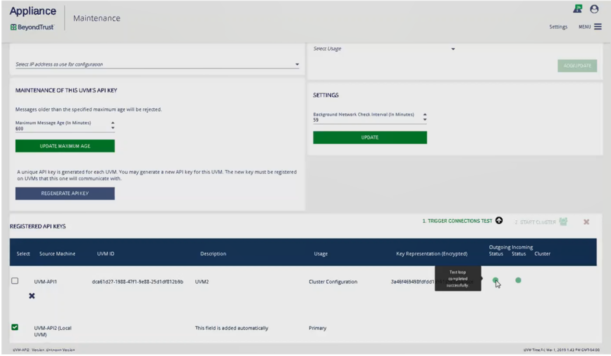
24. You are notified that the test has started. Click **OK**.



NETWORK TEST

Network test has started

25. When the test completes, the page displays the results.



Select IP address to use for configuration

Select Usage

MAINTENANCE OF THIS UVM'S API KEY

Messages older than the specified maximum age will be rejected.

Maximum Message Age (In Minutes): 600

A unique API key is generated for each UVM. You may generate a new API key for this UVM. The new key must be registered on UVMs that this one will communicate with.

SETTINGS

Background Network Check Interval (In Minutes): 59

REGISTERED API KEYS

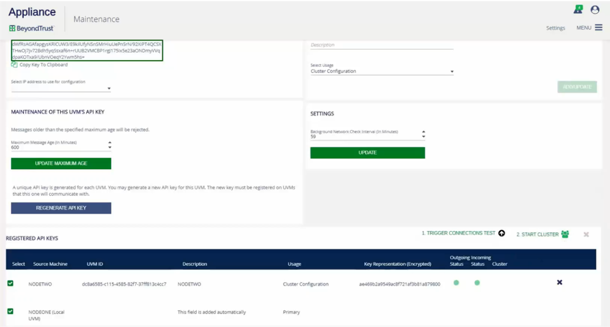
Select	Source Machine	UVM ID	Description	Usage	Key Representation (Encrypted)	Outgoing Status	Incoming Status	Cluster
☐ ✖	UVM-API1	dca61d27-1988-47f1-9e88-25d1df812b9b	UVM2	Cluster Configuration	3a46f469498fdfdd1	●	●	
☑	UVM-API2 (Local UVM)		This field is added automatically	Primary				

Test loop completed successfully.

UVM-API2 Version: Unknown Version

UVM Time:Fri, Mar 1, 2019 1:43 PM GMT-04:00

26. To group UVMSQL appliances into a cluster, select the appliances, and then click **Start Cluster**.



dWfRsAGAfapgysKRICUW3/E9kilUfyNSnSMrHiuUePnSrN/92XIPT4QCSXTHwOj7jv72Bdh5yqSsxaf6n+rUUB2VMCBP1rgJ175Ix5e23aONDmyVVqdpaKOTxa9/UbnVOeqY2Ywm5hs=

Description

Select Usage: Cluster Configuration

Select IP address to use for configuration

MAINTENANCE OF THIS UVM'S API KEY

Messages older than the specified maximum age will be rejected.

Maximum Message Age (In Minutes): 600

A unique API key is generated for each UVM. You may generate a new API key for this UVM. The new key must be registered on UVMs that this one will communicate with.

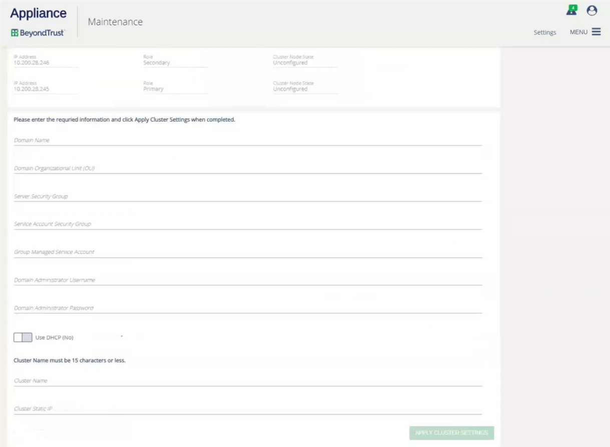
SETTINGS

Background Network Check Interval (In Minutes): 59

REGISTERED API KEYS

Select	Source Machine	UVM ID	Description	Usage	Key Representation (Encrypted)	Outgoing Status	Incoming Status	Cluster
☑	NODETWO	dc8a6585-c115-4585-82f7-37ff813c4cc7	NODETWO	Cluster Configuration	ae469b2a9549ac8f721af3b81a879800	●	●	✖
☑	NODEONE (Local UVM)		This field is added automatically	Primary				

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



IP Address	Role	Cluster Node State
10.200.28.246	Secondary	Unconfigured
10.200.28.245	Primary	Unconfigured

Please enter the requried information and click Apply Cluster Settings when completed.

Domain Name

Domain Organizational Unit (OU)

Server Security Group

Service Account Security Group

Group Managed Service Account

Domain Administrator Username

Domain Administrator Password

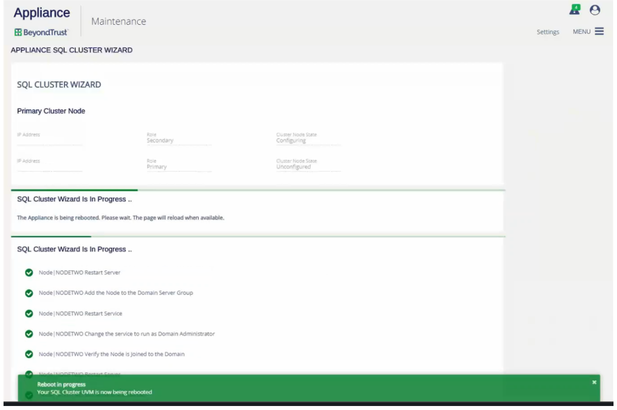
Use DHCP (No)

Cluster Name must be 15 characters or less.

Cluster Name

Cluster Static IP

33. The SQL cluster wizard runs, showing status messages of its progress.



APPLIANCE SQL CLUSTER WIZARD

SQL CLUSTER WIZARD

Primary Cluster Node

IP Address	Role	Cluster Node State
	Secondary	Configuring
	Primary	Unconfigured

SQL Cluster Wizard Is In Progress ..

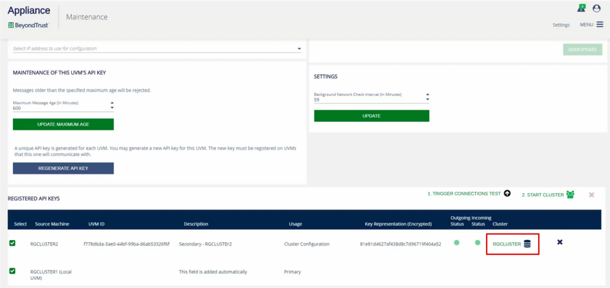
The Appliance is being rebooted. Please wait. The page will reload when available.

SQL Cluster Wizard Is In Progress ..

- ✓ Node | NODETWO Restart Server
- ✓ Node | NODETWO Add the Node to the Domain Server Group
- ✓ Node | NODETWO Restart Service
- ✓ Node | NODETWO Change the service to run as Domain Administrator
- ✓ Node | NODETWO Verify the Node is Joined to the Domain

Reboot in progress
Your SQL Cluster UVM is now being rebooted

34. When the wizard completes, the appliance appears as part of the cluster. Click on the cluster database icon.



MAINTENANCE OF THIS UVM'S API KEY

Messages older than the specified maximum age will be rejected.

Maximum Message Age (In Minutes)
600

A unique API key is generated for each UVM. You may generate a new API key for this UVM. The new key must be registered on UVMs that this one will communicate with.

SETTINGS

Background Network Check Interval (In Minutes)
59

REGISTERED API KEYS

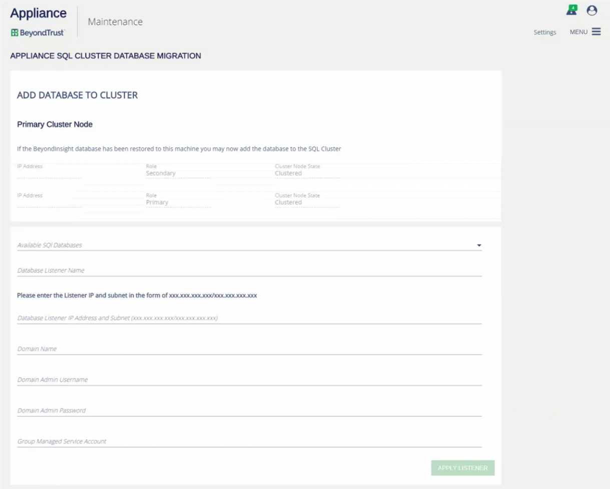
Select	Source Machine	UVM ID	Description	Usage	Key Representation (Encrypted)	Outgoing Status	Incoming Status	Cluster	
☑	RGCLUSTER2	f778d6da-3ae0-44bf-99ba-d6ab53326f6f	Secondary - RGCLUSTEr2	Cluster Configuration	81e81d4627af438d8c7d96719f404a52	●	●	RGCLUSTER	✖
☑	RGCLUSTER1 (Local UVM)		This field is added automatically	Primary					

IMPORTANT!

Before the availability group can be created, the database must exist on the UVMSQL appliance that will be 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 UVM, at the SQL **Server Agreement** step, create a database on the primary replica using the option to create a remote database.*
- *From a configured UVM or SQL Free UVM, 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.*

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



APPLIANCE SQL CLUSTER DATABASE MIGRATION

ADD DATABASE TO CLUSTER

Primary Cluster Node

If the BeyondInsight database has been restored to this machine you may now add the database to the SQL Cluster

IP Address	Role	Cluster Node State
	Secondary	Clustered
	Primary	Clustered

Available SQl Databases

Database Listener Name

Please enter the Listener IP and subnet in the form of xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx

Database Listener IP Address and Subnet (xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx)

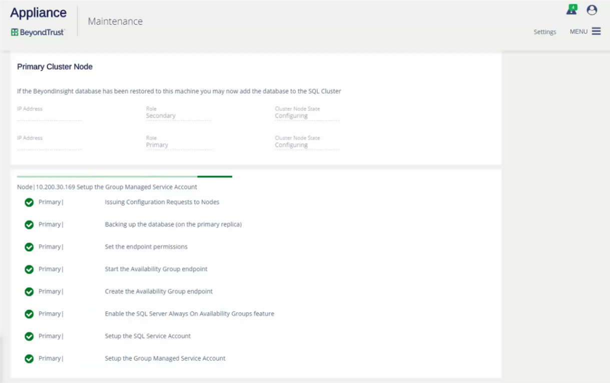
Domain Name

Domain Admin Username

Domain Admin Password

Group Managed Service Account

40. The SQL database wizard runs, showing status messages of its progress.



Primary Cluster Node

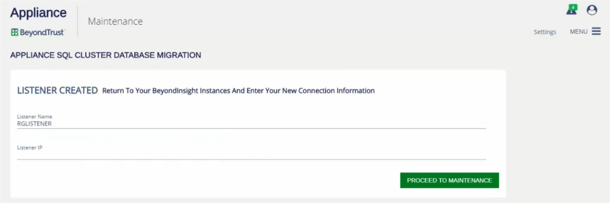
If the BeyondInsight database has been restored to this machine you may now add the database to the SQL Cluster

IP Address	Role	Cluster Node State
	Secondary	Configuring
	Primary	Configuring

Node | 10.200.30.169 Setup the Group Managed Service Account

- ✓ Primary | Issuing Configuration Requests to Nodes
- ✓ Primary | Backing up the database (on the primary replica)
- ✓ Primary | Set the endpoint permissions
- ✓ Primary | Start the Availability Group endpoint
- ✓ Primary | Create the Availability Group endpoint
- ✓ Primary | Enable the SQL Server Always On Availability Groups feature
- ✓ Primary | Setup the SQL Service Account
- ✓ Primary | Setup the Group Managed Service Account

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



APPLIANCE SQL CLUSTER DATABASE MIGRATION

LISTENER CREATED Return To Your BeyondInsight Instances And Enter Your New Connection Information

Listener Name
RGLISTENER

Listener IP