BeyondTrust

U-Series Appliance 4.0
Administration Guide

TC:10/24/2022

Table of Contents

U-Series Appliance Administration Guide

This guide provides information on managing the U-Series Appliance. This guide is intended for network security administrators responsible for protecting their organization's computing assets.

IMPORTANT!

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

Access BeyondInsight

To manage your U-Series Appliance, you must first log in to BeyondInsight.

1. In a web browser, enter the URL to access BeyondInsight, such as **https://<server>/**.
2. The SSL certificate warning window displays. The SSL certificate automatically created for the U-Series Appliance ensures encrypted communications.

   We recommend that you replace the automatically generated certificate with a valid certificate issued by a certificate authority. Check the box to not display the information page again. Browser warnings are displayed until the SSL certificate is installed or a valid certificate is obtained.

3. The BeyondInsight **Login** page displays. Enter the username and the password you created in the Configuration Wizard, and then click **Login**.

For more information about using BeyondInsight, please see the BeyondInsight documentation at www.beyondtrust.com/docs/beyondinsight-password-safe/bi.

Access the U-Series Appliance Website

1. In a web browser, enter the URL to access the U-Series Appliance, such as **https://<Appliance-IP-Address>/appliance**.
2. For the initial login, enter the following information:
   - **Username:** The administrator username created using the Configuration Wizard.
   - **Password:** The administrator password created using the Configuration Wizard.
3. Click **Log In**.

***Note:** A user can be logged in to a U-Series Appliance website for fourteen minutes. After twelve minutes, a message displays, indicating that the session will expire in two minutes. The user must log back in to the website after the session expires.*

Session timeout applies to all U-Series Appliance websites: Roles Editor, Maintenance, Diagnostics, and High Availability. The session timeout value cannot be configured.

4. The U-Series Appliance **Home** page appears. The machine name, IP address, date, time, and time zone are displayed at the top of the U-Series Appliance console window, and are visible at all times.

> ***Note:*** *BeyondTrust is happy to announce that we are introducing a new U-Series Appliance application with an easier-to-use interface. We are releasing the new application in installments. Make sure to read the* ***New in Version*** *section to find out about the latest features. The features are accessed from the* ***Home*** *page tiles, or under their respective new menu items on the left.*
>
> *Items that are not yet in the new release are still found in the* ***Legacy App****, using the* ***LA*** *menu item on the left. When in the* ***Legacy App****, click* ***Go to New App*** *at the top right to return to the new environment and features.*

> ***Tip:*** *When the proper permissions are set up in BeyondInsight, you can also log in to the U-Series Appliance website via the* ***Assets*** *grid of the BeyondInsight Console. For more information, see U-Series Appliance, in the BeyondInsight User Guide, at https://www.beyondtrust.com/docs/beyondinsight-password-safe/bi/user/u-series.htm.*

> ***Note:*** *U-Series Appliance login activity appears in the BeyondInsight User Audits listing.*

Activate Windows

If the Windows environment is currently not activated, you can activate it on the **Product Licensing** page.

1. On the sidebar menu, click **Software and Licensing**, and then select **Product Licensing**.
2. Click the **Microsoft** tab.
    - If using the **Windows Server License** option, enter a **Microsoft Product Key**.
    - If using the **Key Management Service** option, enter a **Volume License Key**, an then enter the **KMS** key.
3. Click **Activate Windows**.

> ***Note:*** *If there is no internet connection (for example, in an air-gap environment), you must perform the activation by phone.*

Request Product Updates

On the **BeyondTrust Updates** page, you can view the version numbers for the BeyondTrust products that you are licensed to use.

To request updates:

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. The default page displayed is the **BeyondTrust Updates** page. If it is not displayed, on the **Maintenance** menu, click **BeyondTrust Updates**.
3. Click **Request Software Updates**. The update of the U-Series Appliance and BeyondInsight database starts.

Security Updates

BeyondTrust provides a bundle of Microsoft patches in a security update package. All updates are tested and approved by BeyondTrust to ensure that updates do not interfere with the proper operation of the U-Series Appliance. The packages are updated when new patches are available from Microsoft.

In U-Series Appliance versions 1.3 or later, a security update package installer ships with your U-Series Appliance. When a new package is copied to the update server, then those updates can be received by your U-Series Appliance.

Note: *If you are working in an air-gap environment, we recommend using BT Updater Enterprise to download update packages. Using BT Updater Enterprise gives you more flexibility in the updates you download and when. For more information, please see BT Updater Enterprise User Guide at https://www.beyondtrust.com/docs/bt-updater/enterprise/index.htm.*

For more information about the updates included in the package, contact BeyondTrust Technical Support.

Security Update Package Types

- **Security Patches for Windows Server**: Microsoft Windows Updates for the server operating system, screened by BeyondTrust.
- **Security Patches for SQL Server**: SQL Server service packs and security updates that may be released from Microsoft, screened by BeyondTrust.
- **U-Series Appliance Environment**: Packages created by BeyondTrust to change system settings, such as: file, registry or system changes, or updates not integrated in Windows Updates.
- **U-Series Appliance Supporting Software**: Packages created by BeyondTrust to deliver updates to software that may not be from BeyondTrust but are essential to the operation of the U-Series Appliance.

Apply Updates

You can create update schedules for more than one appliance at a time. You must ensure that API keys are exchanged to set up proper communication between appliances.

As best practice when setting up schedules in a multi-appliance environment, select one appliance as your console and always create schedules from that appliance.

New updates delivered to the appliance are added to the grid automatically every 15 minutes, for both the local appliance and remote appliances. A page refresh on the local appliance updates the current available packages for the local appliance only.

To apply the updates:

1. On the sidebar menu, click **Software and Licensing**, and then select **Security Updates**.
2. To see information about updates, select the menu for an appliance, and then select **Security Update Details**. A page displays all available updates ready to apply and any update applied in the last 24 hours.
3. If you are working in a multi-appliance environment, select each appliance you want to include in the schedule. Otherwise, select a single appliance.
4. Click **Schedule Security Update**.
5. Select when you want to run the update:

- **Schedule Security Update**: Includes the available packages in the scheduled time frame. If a new package is received before the scheduled run time starts, then the new package is *not* included. A new schedule must be created to include those new packages. A package that fails to update remains in the list of available updates. The update is automatically included in any new schedule created and attempts to update when that schedule runs.
- **Run Security Update Now**: Runs the update immediately.

6. Select a time zone to run the update: appliance or browser.
7. Set the date and time.

   The browser time zone is the local time of the administrator running the U-Series management console. The schedule for both time zones is displayed regardless of the time zone selected in step 6. You can then review the scheduled times in each time zone to determine if the time is suitable to run the updates.

8. Click **Create Schedule**.


For more information about API keys, please see "Manage U-Series Appliance Security Settings" on page 9.

View Update History

1. On the sidebar menu, click **Software and Licensing**, and then select **Security Updates**.
2. Select the menu for an appliance, and then select **Security Update History**. The page displays the historical records of previously applied patches. The list is organized by the types of packages (subscriptions).

Set the Update Method

Under the **BeyondTrust Updates** page, the **Update Method** section displays if update clients are configured to use an internal server or the BeyondTrust update servers. It also displays if a proxy is being used and if U-Series Appliance updates or security updates are disabled.

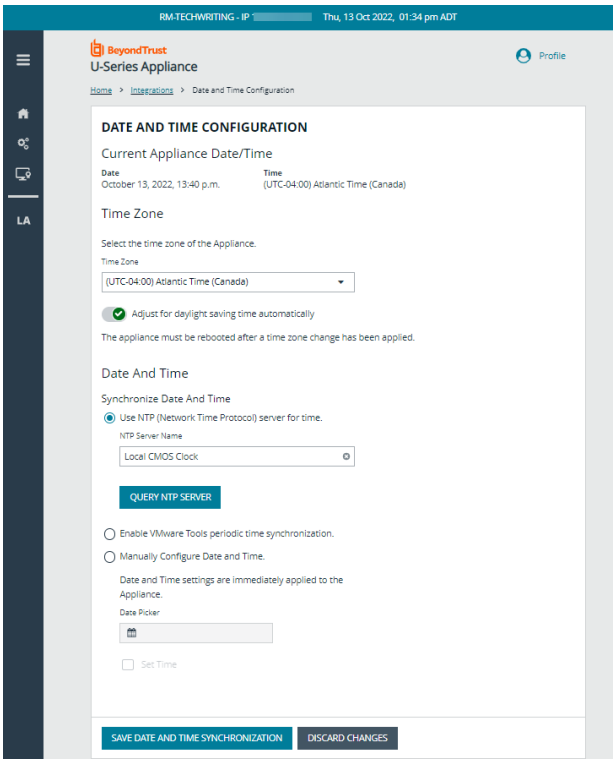
Clicking **Change the Proxy Settings** takes you to the page within **Maintenance**, where you can modify the proxy. Clicking **Change the Update Settings** takes you to the roles editor.

Configure U-Series Appliance General Settings

Adjust Date and Time Settings

You must synchronize date and time settings for your U-Series Appliance.

1. On the sidebar menu, click **Integrations**, and then select **Date and Time Configuration**.
2. Select the **Time Zone** for the appliance.
3. By default, the **Adjust for daylight savings time automatically** setting is set to **ON** . If you don't want this to happen automatically, click to set it to **OFF**.
4. In the **Date and Time** section, select one option to synchronize date and time:
    - If you select the **Network Time Protocol (NTP)** option, type the **NTP Server Name**, and then to verify the connection, click **Query NTP Server**.
    - If you select the **Manually Configure Date and Time** option, click the **Date Picker**, and then select the date.
    - To set the time, check the **Set Time** box, and then click the **Set Time** tool and set the time, in hours, minutes, and seconds.
5. Click **Save Date and Time Synchronization**.



Configure Profile Settings

You can set your U-Series Appliance profile preferences.

To configure your profile settings:

1. At the top right, click **Profile**.
2. Under **Preferences**, use the dropdown lists to:
    - Select the color scheme to use. The default is **BeyondTrust Brand Color**. If you prefer to avoid bright screens and reduce eye strain, select **Dark Mode Colors**.
    - Select the language to use (when those languages are available). The default is **English (United States)**.

Configure LCD Panel Settings

> ***Note:*** *This feature is only available/visible if working on a physical/hardware machine.*

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **General Settings**.
3. You can turn on the following settings:
    - **Allow LCD Panel to Reset Administrator Password:** Turn on to allow you to reset the admin password to a random password from the LCD panel. On the U-Series Appliance LCD panel, select **Show IP**. Hold the up and down arrows simultaneously. A random password is generated. Press the check button to accept the changed password.
    - **Buttons on LCD Panel:** Turn off to disable all the LCD panel buttons.
4. Click **Update LCD Panel Settings**.

Clear the BeyondInsight License Cache

On the **LA > Maintenance > General Settings** page, the **Clear BeyondInsight License Cache** button clears the license key in the BeyondInsight database cache. If a new license key has been recently applied, then clearing the cache ensures that the new key is saved to the BeyondInsight database.

Clearing the cache and applying the new key ensures all features are available and work properly. You can verify licensed features on the **Software and Licensing** page.

Export Settings

You can allow U-Series Appliance settings such as IP and administrator password to be set by inserting a USB drive into the U-Series Appliance.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **General Settings**.
3. Under **Export Settings**, click to turn on **Allow Appliance settings to be imported and exported on removable storage.**
4. Click **Update Export Settings**.

Configure Pre-Logon Banner Settings

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **General Settings**.
3. Under **Pre-logon Banner Settings**, enter a title and message you want to appear before the login credentials page is displayed to the user.
4. Click **Update Pre-logon Banner Settings**.

Join a U-Series Appliance to a Domain

Joining a U-Series Appliance to a domain is not recommended. However, if required for your deployment, please contact your BeyondTrust representative for assistance.

Manage U-Series Appliance Security Settings

Download a Crypto Key

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. Under **Download Crypto Key Options**, create an encryption password.
4. Click **Submit**. The crypto key zip file is created and downloaded to your system.

Upload a Crypto Key

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. Under **Upload Crypto Key Options**, enter the encryption password.
4. Drag and drop the crypto key zip file into the drop area or click the button to browse to the zip file.
5. Click **Generate the Uploaded Key**.

Check FIPS Compliance

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. Under **FIPS Compliance Checking**, click the toggle to change it to **FIPS State (Yes)**.
4. Click **Update FIPS Setting**.
5. You must reboot the U-Series Appliance for this setting to take effect.

Manage the U-Series Appliance API Key

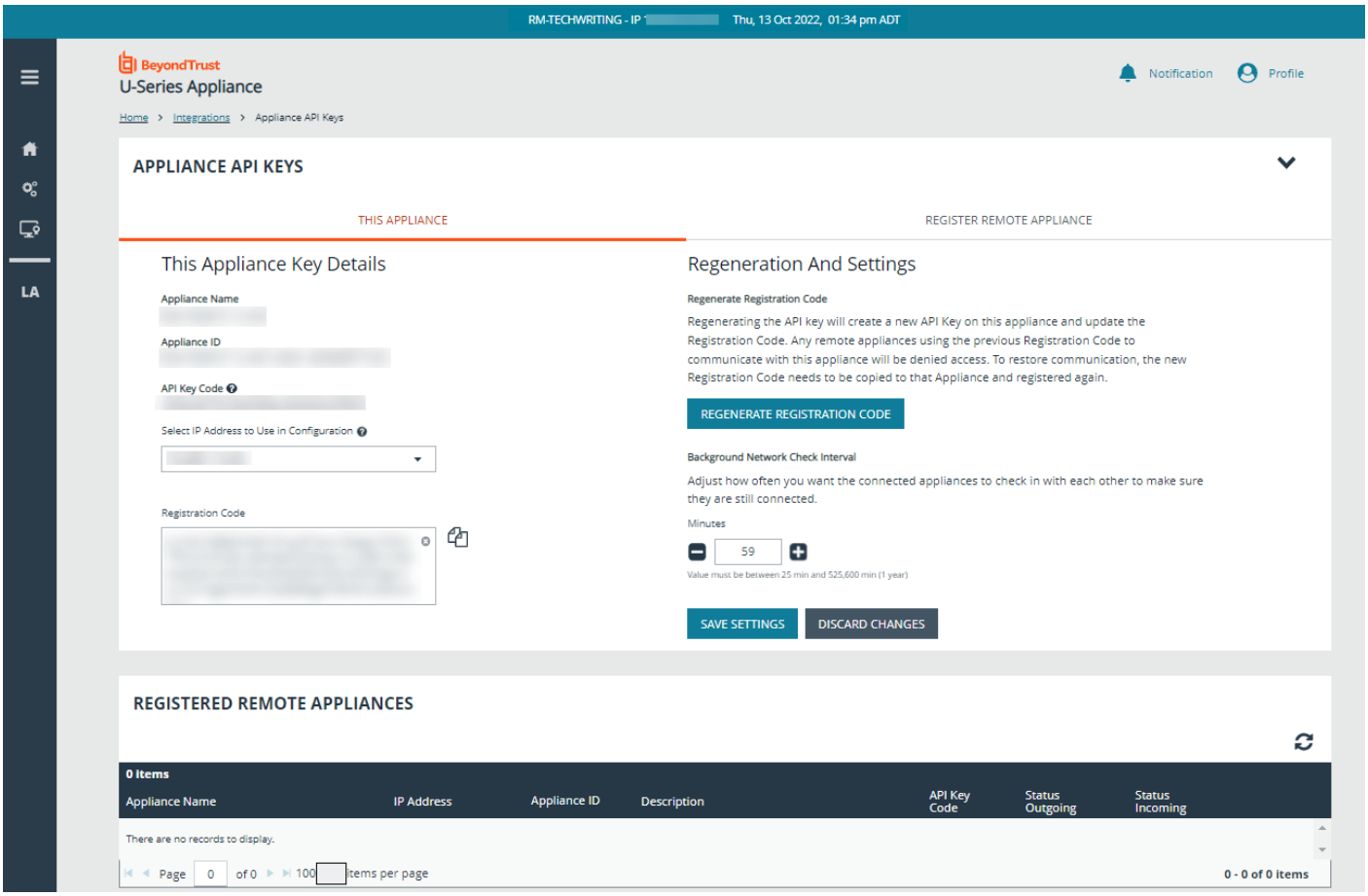
The U-Series Appliance API manages the communication between U-Series Appliances when high availability is used in your environment. The API key enables U-Series Appliances to communicate with each other.

The API key is automatically generated and is available to copy from the **Appliance API Keys** page.

Note: *For security reasons, we recommend that you regenerate the key regularly. Remote appliances using the previous Registration Code to communicate with this appliance will be denied access until the new Registration Code is copied to that appliance and registered again.*

To view this appliance's key details:

1. On the sidebar menu, click **Integrations**, and then select **Appliance API Keys**.
2. Ensure that the **This Appliance** tab is selected. The details appear in the **Appliance Key Details** section.
3. To view the **Registration Code**, from the dropdown list, select an **IP Address to Use in Configuration**.



Regeneration and Settings

To create a new API key:

1. Click **Regenerate Registration Code**. A new API key appears in the **Appliance Key Details** section on the left.
2. From the dropdown list, select an **IP Address to Use in Configuration**. The associated registration code appears.
3. At the right of the **Registration Code** field, click the **Copy** button.

You must copy the new registration code to the remote appliances that you want to communicate with this appliance.

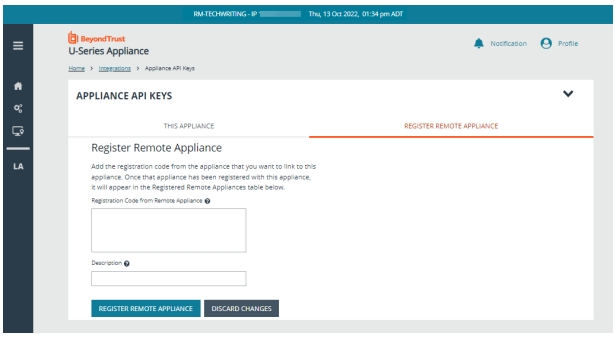
Register a Remote Appliance

Communication between appliances requires both appliances to be registered with each other.

To register a remote appliance:

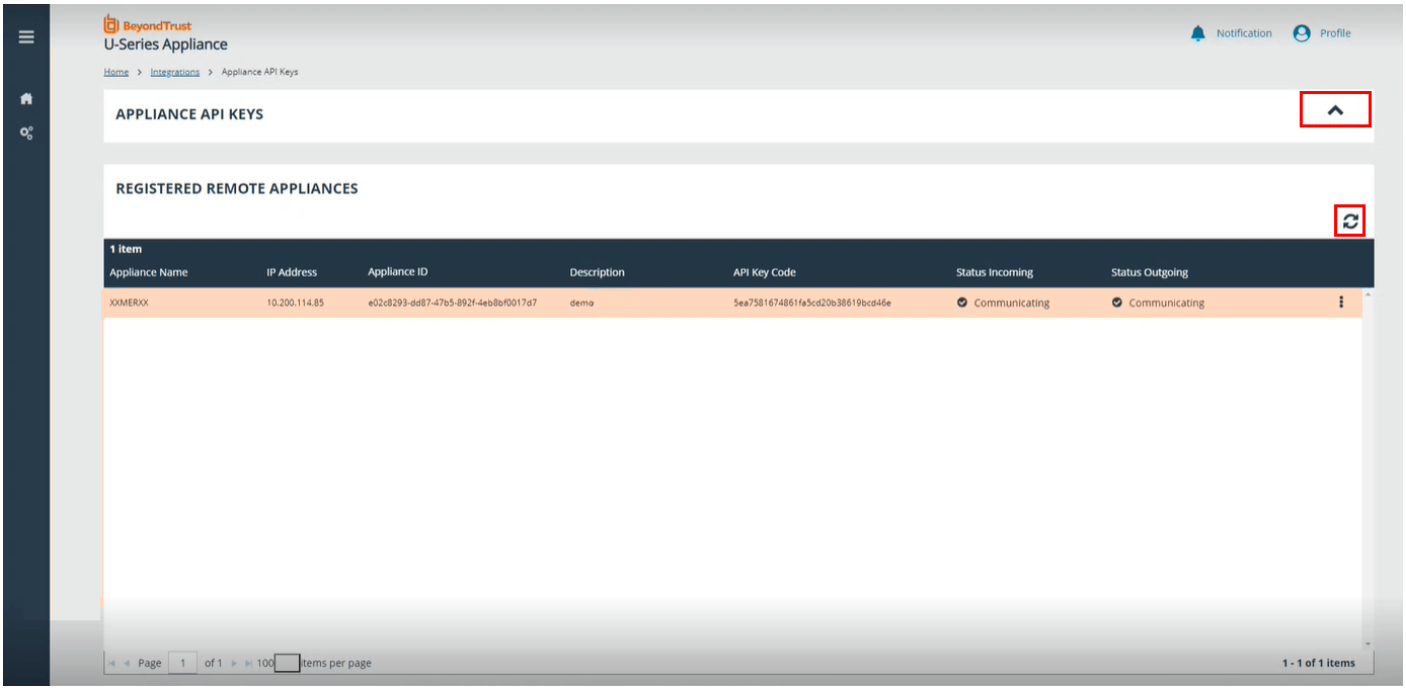
1. Open the U-Series Appliance Console on the *remote* appliance first.
2. On the sidebar menu, click **Integrations** and select **Appliance API Keys**.
3. Click the **Register Remote Appliance** tab.

4. Copy and paste in the registration code from the *first* appliance.
5. (Optional). Enter a short **Description** for the appliance being registered.
6. Click **Register Remote Appliance**.
7. Click the **This Appliance** tab.
8. To view that appliance's **Registration Code**, from the dropdown list, select an **IP Address to Use in Configuration**.
9. At the right of the **Registration Code** field, click the **Copy** button.
10. Go back to the *first* appliance's console, and go to the **Appliance API Keys** page again.
11. Click the **Register Remote Appliance** tab.
12. Paste the registration code from the *remote* appliance.
13. (Optional). Enter a short **Description** for the appliance being registered.
14. Click **Register Remote Appliance**.



The registered remote appliance now appears in the **Registered Remote Appliance** table at the bottom of the page. At any time, to refresh that list, click the **Refresh** button at the top right of the table.

To view more of the table, at the right of the **Appliance API Keys** section, click the *down* arrow to collapse that section.



Background Network Check Interval

In the **Registered Remote Appliance** table listing, you might see the word *Communicating* under the **Status Ongoing** and **Status Incoming** headings. You can adjust how often the connected appliances check with each other to make sure they are still connected.

To set the **Background Network Check Interval**:

1. Under the **This Appliance** tab, in the **Regeneration and Settings** section, enter the number of minutes for the background network check interval.
2. Click **Save Settings**.

Turn SSL Authentication Off or On

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. Under **Event Service SSL Requirement**, click the toggle to **Event Service SSL/Certificate Required (No)** to ignore SSL certificate authentication.
4. Click **Submit**.

IMPORTANT!

We do not recommend disabling SSL certificate authentication. SSL authentication should be disabled only in certain rare circumstances, such as during testing.

Analytics & Reporting Endpoints

If the BeyondInsight Analytics & Reporting website is unreachable, you can refresh the settings to establish the connection.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. Under **Analytics & Reporting Web Service Endpoints**, click**Refresh**.

Generate and Export Certificates

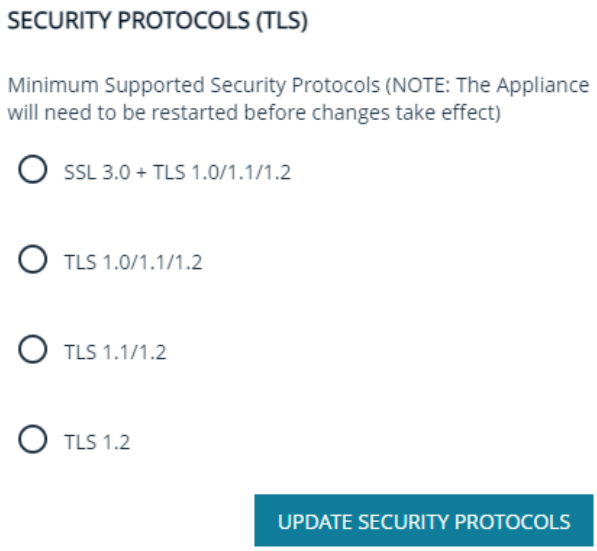
1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. To regenerate the SSL certificate to match the U-Series Appliance network name, under **Generate SSL Certificate**, click **Generate Certificate**.

Note: *This certificate will not be trusted by the client browser.*

4. To export the client certificate, under **Export Client Certificate**, enter the password for the certificate, and then click **Export Certificate**.

Set a Security Protocol

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. Under **Security Protocols (TLS)**, select the security protocol that applies to your environment.
4. Click **Update Security Protocols**.



Note: *To use TLS 1.2 on a U-Series Appliance running Windows Server 2008 R2 and SQL Server 2014, ensure the following patches have been applied to your U-Series Appliance.*

- *KB2979597: https://support.microsoft.com/en-us/topic/kb2979597-sql-server-2008-r2-service-pack-3-release-information-25af206d-68ab-4be5-ddc9-4d2e69c7d2fb*
- *KB3144517: https://support.microsoft.com/en-us/topic/kb3144517-cumulative-update-package-13-for-sql-server-2014-f69a0087-2489-316b-2d83-944438f4e30b*

Turn On HSTS

You can apply extra security to the U-Series Appliance website by using HTTP strict transport security (HSTS) technology.

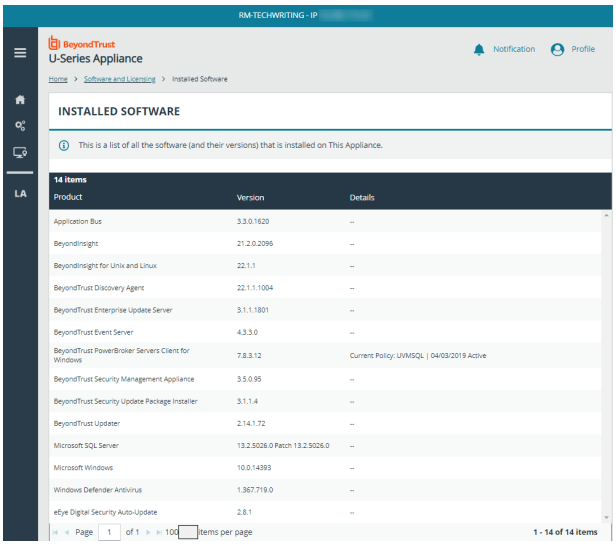
1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. Under **HTTP Strict Transport Security**, toggle the switch to *on*.
4. Click **Update HSTS Setting**.

Accounts and Licensing Settings in the U-Series Appliance

View Installed Software

You can view the list of all software installed on the U-Series Appliance, including versioning info.

To view the software list, from the sidebar menu, click **Software and Licensing**, and then select **Installed Software**.



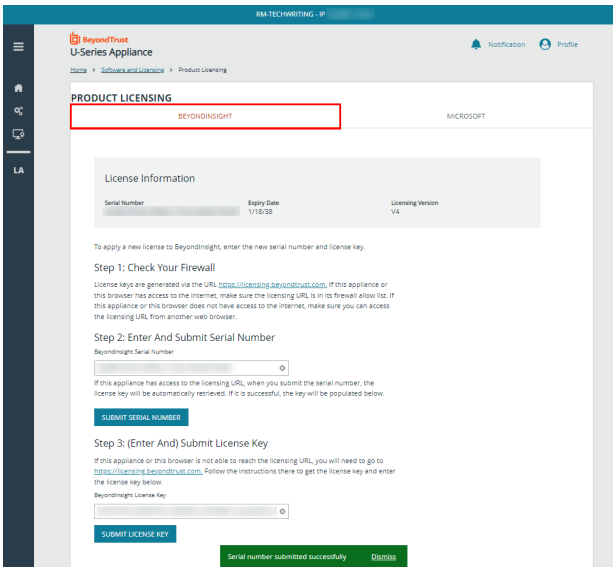
Manage Product Licensing

You can view the license information for the BeyondInsight and Microsoft products.

To view product licensing information, from the sidebar menu, click **Software and Licensing**, and then select **Product Licensing**.

BeyondInsight Licensing

Click the **BeyondInsight** tab. If licensed, the license information is displayed.



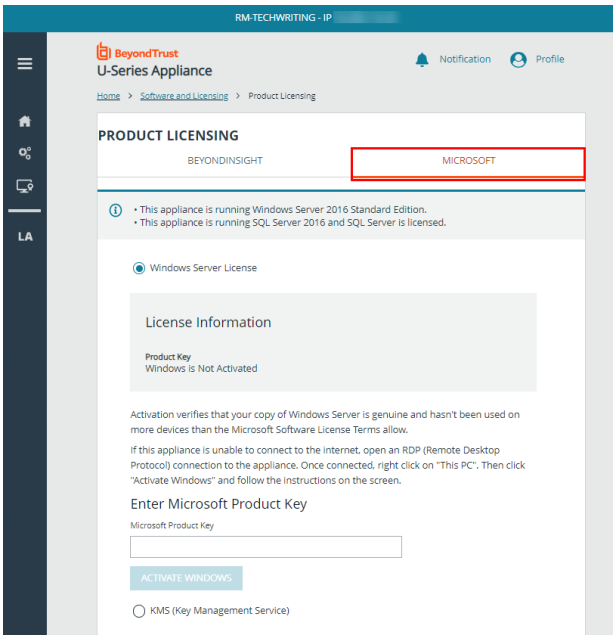
If not licensed yet or to apply a new license:

1. Check your firewall first. License keys are generated via the URL https://licensing.beyondtrust.com.
    - If this appliance or this browser has access to the internet, make sure the licensing URL is in its firewall allow list.
    - If this appliance or this browser does not have access to the internet, make sure you can access the licensing URL from another web browser.
2. Enter a **Serial Number** and click **Submit Serial Number**. If this appliance has access to the licensing URL, when you submit the serial number, the license key is automatically retrieved and added to the **BeyondInsight License Key** field below.
3. If this appliance or this browser is not able to reach the licensing URL, go to https://licensing.beyondtrust.com. Follow the instructions there to get the license key.

    Enter the **BeyondInsight License Key** and click **Submit License Key**.

Microsoft Licensing

Click the **Microsoft** tab.



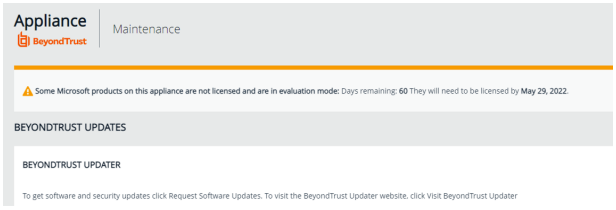
By default, **Windows Server License** is selected. If licensed, the license information is displayed.

- If Windows is not activated and this appliance is unable to connect to the internet, open an RDP connection to the appliance. Once connected, right-click **This PC**, and then click **Activate Windows** and follow the instructions on the screen.
- If not licensed, enter a **Microsoft Product Key**, and then click **Activate Windows**.

Customers who are authorized to use a Key Management Service (KMS) server can select the **KMS** option, which displays two fields to complete.

1. Enter your **Volume License Key**.
2. Enter the **KMS server address** that will validate and track the license. This is only valid on appliances created as volume images.
3. Click **Activate Windows**.

If you do not activate Windows, messaging on the **U-Series Appliance** website indicates you are using the software in evaluation mode. The number of days remaining for the evaluation period is shown.



Key Management Service Support

After installation and configuration, if your server does not automatically discover the Key Management Service (KMS) server, you may receive a *Windows activation failed* message. Specify the KMS key and IP address again.

You can replace our key with a known Volume License Key and then call into your KMS server to count against your total (number of licenses).

To activate your volume license key:

1. From the sidebar menu, click **Software and Licensing**, and then select **Product Licensing**.
2. Click the **Microsoft** tab, and select the **KMS** option, which displays two fields to complete.
3. Enter your **Volume License Key**.
4. Enter the **KMS server address** that will validate and track the license. This is only valid on appliances created as volume images.
5. Click **Activate Windows**.

For more information, please see Why did Windows activation fail on my EC2 Windows instance? at https://aws.amazon.com/premiumsupport/knowledge-center/windows-activation-fails/.

Purge U-Series Appliance Data

IMPORTANT!

Be careful! Purging the U-Series Appliance data erases the database, user configuration data, and events from the U-Series Appliance.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Maintenance** menu, select **Accounts and Licensing**.
3. Under **Purge All Configuration Data and Events**, click **Wipe Appliance**. The data is purged from the U-Series Appliance.

Change Administrator Password

IMPORTANT!

*While it is possible here to change administrator **usernames**, we recommend contacting Support and discussing the implications of this action on your systems, **before** making any changes. The username change may affect various areas of your deployment, and require restarting services or appliances.*

You can reset the U-Series Appliance administrator password, BeyondInsight administrator password, and BT Updater password. Make sure you review the password complexity requirements.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Maintenance** menu, select **Accounts and Licensing**.
3. Under **Change Admin Password**, check the box for the password that you want to change.
4. Change the password.
5. Click **Update Credentials**.

***Note:** If changing the U-Series Appliance administrator username or password, you must log back into the **Maintenance** page.*

Use Two-Factor Authentication

Using a RADIUS server, you can require users to log in to the U-Series Appliance using a configured two-factor authentication method. You must configure the RADIUS server settings in BeyondInsight.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Maintenance** menu, select **Accounts and Licensing**.
3. Under **Configure RADIUS Authentication**,click the **RADIUS Authentication Enabled** toggle to on.
4. From the **RADIUS Settings Alias** dropdown, select an available RADIUS server. This uses the settings configured in BeyondInsight to populate the hostname, port, request timeout, authentication mechanism, and initial action.
5. Enter the username. This is the user account that is used to log in to the RADIUS server.

***Note:** The RADIUS user account password must match the U-Series Appliance administrator password.*

6. Click **Update Settings**.

Network and RDP Settings in the U-Series Appliance

Configure RDP

In your U-Series Appliance, RDP access is off by default. RDP access is not required for daily use, regardless of licensing or roles. BeyondTrust Technical Support can turn on RDP access for troubleshooting. RDP and two-factor activities are tracked with audit log entries in the Security event logs.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Maintenance** menu, select **Network and RDP Settings**.
3. Toggle the **Enable Remote Desktop** switch to on.
4. Toggle the **2-Factor required** switch to enable the settings for two-factor authentication when using remote desktop.

> ***Note:*** *If you need to disable two-factor authentication, you must first contact BeyondTrust Technical Support and request them to generate a time-limited password for you. You must enter this password before the toggle will switch off.*

5. Click **Save RDP Settings**.

Set an IP Address for the U-Series Appliance

You can obtain an IP address automatically using DHCP, or you can manually configure the IPv4 address.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Maintenance** menu, select **Network and RDP Settings**.
3. In the **IP Settings** section, select a network card from the list.
4. Toggle on the switch to **Obtain IP address automatically**, or toggle it off to set the IP address information manually.
5. If setting the IP manually, enter the IP address, subnet mask, gateway, and DNS information.
6. Click **Update IP Settings**.

Enter Email SMTP Server Settings

> ***Note:*** *Enterprise Update Server has reached End of Life. SMTP Credentials will not be updated for that product.*

You can configure SMTP settings for the appliance and BeyondInsight. The BeyondInsight SMTP settings are stored in the database, which might not always be available (for example, offline for maintenance). To ensure consistent SMTP access, appliance SMTP settings can also be configured.

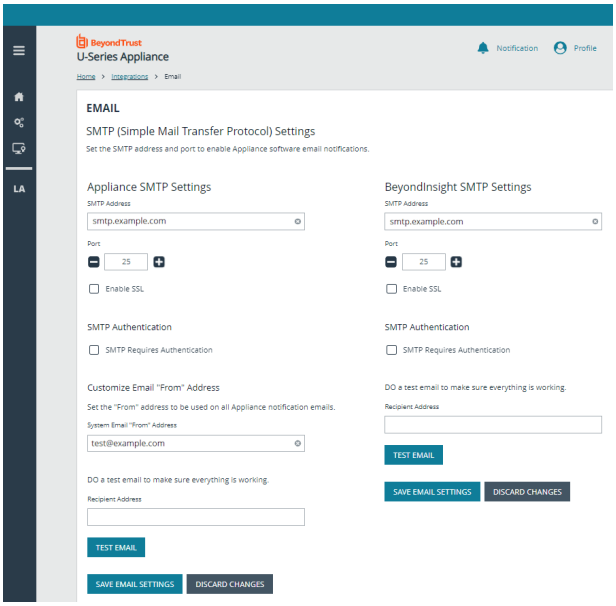
Set the U-Series Appliance and BeyondInsight SMTP addresses and ports to enable the appliance software email notifications.

To configure the email settings, from the sidebar menu, select **Integrations**, and then select **Email**.

Appliance SMTP Settings

To configure the **U-Series Appliance** SMTP settings:

1. Type in the **SMTP Address**.
2. Set the **Port Number**.
3. Check the box to **Enable SSL**.
4. In the **SMTP Authentication** section, check the box to ensure SMTP requires authentication.
5. In the **Customize Email "From" Address** section:
    - Set the **System Email "From" Address** to be used on all U-Series Appliance notification emails.
    - Type in a **Recipient Address** test email you can use to verify that the notifications are working.
    - Click **Test Email**. Verify the recipient email address you used for reception of the notification.
6. After a successful test, at the bottom of the **Appliance SMTP Settings**, click **Save Email Settings**.



BeyondInsight SMTP Settings

To configure the **BeyondInsight** SMTP settings:

1. Type in the **SMTP Address**.
2. Set the **Port Number**.
3. Check the box to **Enable SSL**.
4. In the **SMTP Authentication** section, check the box to ensure SMTP requires authentication.
5. In the **Customize Email "From" Address** section:
    - Type in a **Recipient Address** test email you can use to verify that the notifications are working.
    - Click **Test Email**. Verify the recipient email address you used for reception of the notification.
6. After a successful test, at the bottom of the **BeyondInsight SMTP Settings**, click **Save Email Settings**.

Configure Proxy Settings

> ***Note:*** *Enterprise Update Server has reached End of Life. Proxy Credentials will not be updated for that product.*

You can configure a proxy server if one is required for internet access.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Maintenance** menu, select **Network and RDP Settings**.
3. Toggle the **Use proxy server for external communication** switch to on.
4. Enter the IP address and port for the server.

5. If the proxy server requires authentication, enter the credentials.
6. Click **Update Proxy Settings**.

Manage BITS Throttle

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Maintenance** menu, select **Network and RDP Settings**.
3. Drag the slider to the appropriate level of throttling.
4. Click **Update BITS Throttling Setting**.

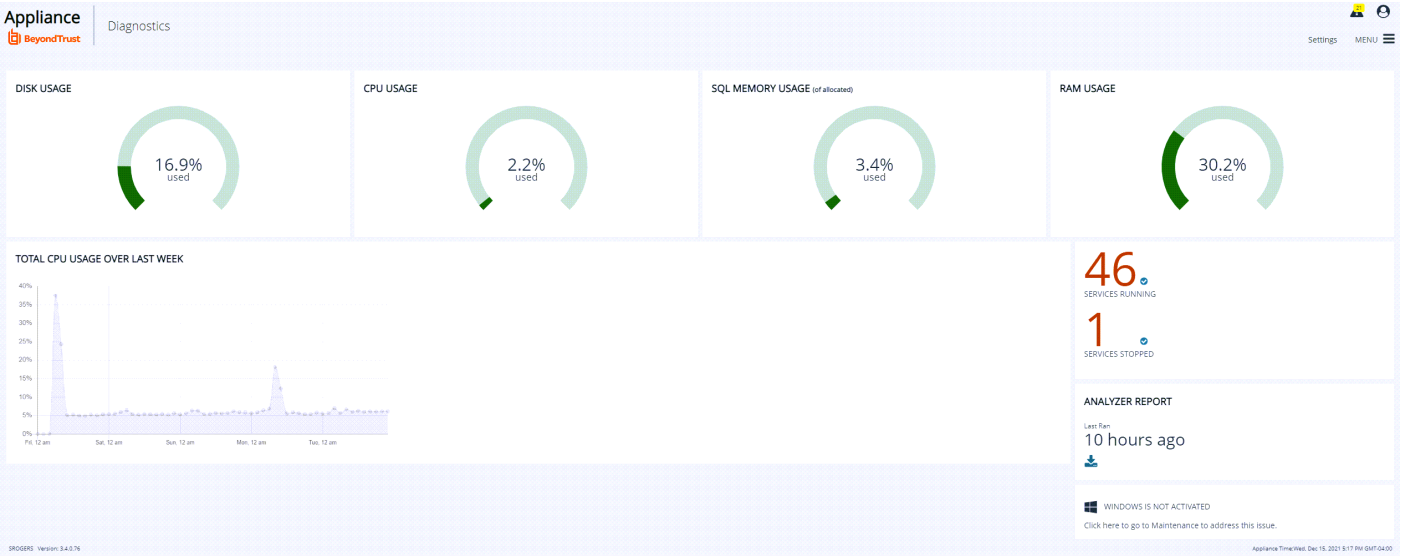
Appliance Health in the U-Series Appliance

On the **Diagnostics** pages, you can keep track of U-Series Appliance services, hardware faults, and performance metrics.

Monitor the Health Dashboard

View dynamic, real-time U-Series Appliance metrics, including:

- Used disk space on the C: drive
- CPU usage
- SQL Server memory usage
- RAM usage
- SQL Server CPU usage
- Services running and stopped
- Analyzer reporting



> ***Note:*** *View health metrics on BeyondTrust components and services running in your environment.*

> ***Note:*** *If you use your own SQL Server deployment rather than the SQL Server version that ships with the U-Series Appliance, then the SQL Server metrics are not displayed on the health dashboard.*

Monitor Services and Hardware

The U-Series Appliance periodically checks the running state of the services to make sure that they are in the expected state, considering the current roles that are set. Additionally, alerts can be triggered when the service control manager raises errors, such as when a service fails to start or terminates unexpectedly.

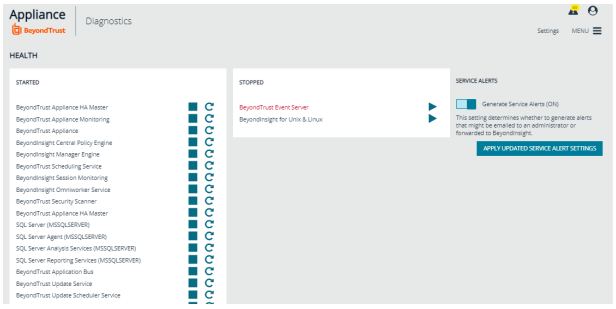
The U-Series Appliance also monitors the hardware. Alerts can be triggered when an error is raised by Dell OpenManage monitoring software.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Diagnostics** menu, select **Appliance Health**.
3. Turn on the alerts, then click **Apply Updated Settings**.

Check Services

You can manage U-Series Appliance services.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Diagnostics** menu, select **Appliance Health**.



	Restart the service.
	Start the service.
	Stop the service.

Configure Counters for Performance Metrics

You can configure the threshold values for performance metrics. When the threshold is exceeded, email alerts can be sent to the email account configured on the notifications page.

For example, you might not want CPU usage over 50% for too long. In this case, you might set the thresholds to:

- Low: 50
- Medium: 65
- High: 70
- Threshold Duration: 10 minutes

If the running average reads at 52%, then a low level alert is sent.

After a counter alerts at a certain level, it does not generate further alerts for that level (or below) until it is reset. An alert is considered in a reset state when the average is below the reset threshold for the specified time span.

If a metric in an alerted state goes below the configured reset threshold for the specified time, the alert is cleared, and a reset alert is generated. At this point, the performance counter receives alerts if it exceeds the threshold again.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Diagnostics** menu, select **Performance Counters**.
3. Select notification settings:
    - **Generate Alerts for Monitored Performance Data:** Turns on email notification for alerts.
    - **Generate Daily Summaries of Performance Data:** Collects performance metrics every two hours and emails them on a daily basis.

4. By default, four base counters are listed: **SQL Server Memory Percentage**, **CPU Overall Usage**, **SQL Server CPU Usage**, and **Disk Usage**. You may select additional counters from the list, and then click **Add to List**.
5. Adjust the performance and reset thresholds.
6. Click **Apply Updated Settings**.

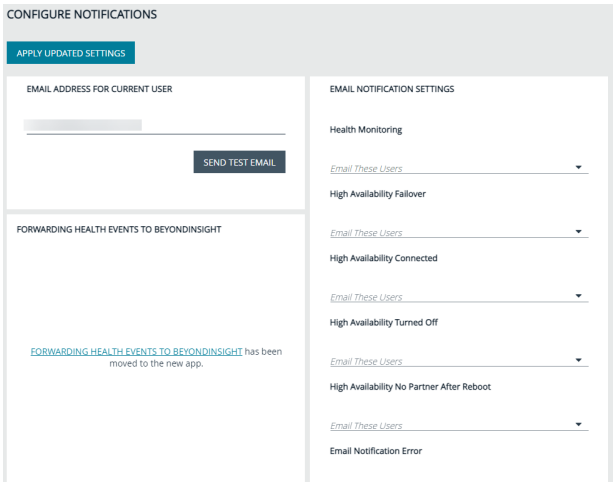
Configure Notifications

You can set notifications for the following types of events:

- **Health monitoring:** includes performance thresholds, service alerts, hardware alerts, and daily performance summaries.
- **High availability monitoring:** includes failover alerts, connection alerts, no partner alerts, and off state alerts.
- **High availability mirror change:** includes suspend and resume activities on SQL mirroring.
- **Backup monitoring:** includes backup success and failure alerts and restore success alerts.

To configure email notifications:

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. At the top right, click the **Notifications** icon, and then click the **Configure Appliance Notifications** icon.
3. Under **Email Notification Settings**, for each event type, click **Email These Users**, and select the users who you want to receive notifications.
4. Click **Apply Updated Settings**.



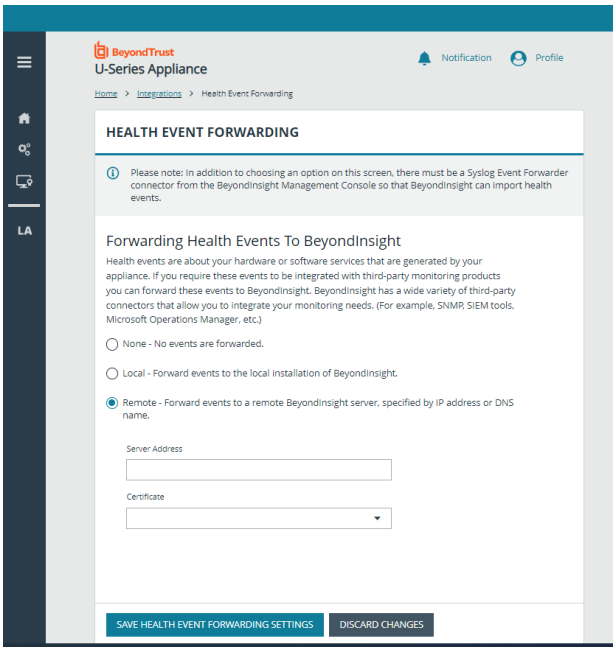
Set Up Health Event Forwarding

Note: *BeyondInsight 6.0 or higher is required to use this feature.*

You can send alerts from the U-Series Appliance to your BeyondInsight management console for further analysis.

Health events are about the hardware or software services that are generated by your appliance. If you require these events to be integrated with third-party monitoring products, you can forward these events to BeyondInsight.

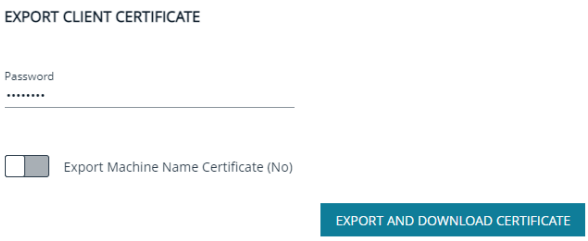
BeyondInsight has a wide variety of third-party connectors that allow you to integrate your monitoring needs (for example, SNMP, SIEM tools, Microsoft Operations Manager, etc.).



> ***Note:*** *In addition to choosing an option on this page, there must be a* ***Syslog Event Forwarder connector*** *from the BeyondInsight Management Console so that BeyondInsight can import health events.*

To set up health event forwarding:

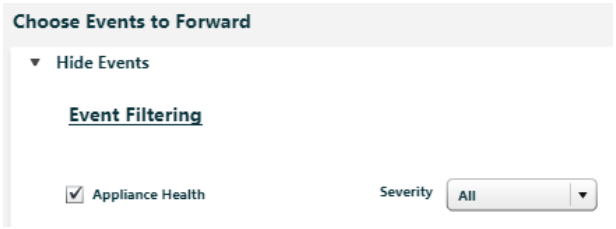
1. From the sidebar menu, click **Integrations**, and then select **Health Event Forwarding**.
2. Select an option:
   - **None**: No events are forwarded.
   - **Local**: Forward events to the local BeyondInsight installation.
   - **Remote**: Forward events to a remote BeyondInsight server, specified by **IP Address** or **DNS Name**.
3. If using the **Remote** option, two additional fields appear. You must *export* a certificate from the remote server and *import* the certificate to the local U-Series Appliance.
4. If the remote server is another U-Series Appliance, log in to that U-Series Appliance's website.
   - On the sidebar menu, click **LA** (if you are in the new environment only).
   - Under **Export Client Certificate**, enter a password and click **Export and Download Certificate**.
   - Import the certificate on the local U-Series Appliance.
   - Return to the **Health Event Forwarding** page, under the **Remote** option, enter a **Server Address**, and select a **Certificate** from the list.



5. If the remote server is a software install of BeyondInsight, use the BeyondInsight Configuration Tool to create and export the certificate.
6. Click **Save Health Event Forwarding Settings**.

You must also create a connector from the BeyondInsight management console.

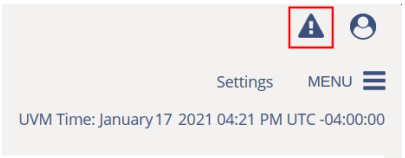
1. Log in to BeyondInsight.
2. Select **Configuration** from the menu, and then select **Connectors**.
3. Click **+** and select **Syslog Event Forwarding**.
4. Enter the details for the U-Series Appliance, including IP address, protocol, and facility.
5. Check the **Appliance Health** box.
6. By default, all severity levels are included. You may select an alternate level if needed.



> *For more information on importing a certificate to the U-Series Appliance, please see "Upload SSL Certificate" on page 32.*

View Notifications

To view notifications,click the icon at the top right of the **Legacy App** environment.

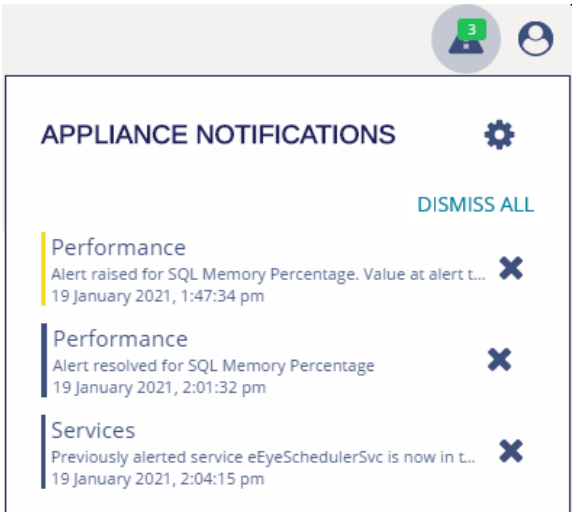


After notifications are received, a green number indicates the number of notifications. Click the icon to view more information about the notifications.

The bar next to the notification indicates severity.

Color Legend

	Info
	Low
	Medium
	High



Diagnose Network Connectivity Issues

You can view network configuration information and use **ping** to assist with diagnosing network connectivity issues.

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Diagnostics** menu, select **Tools**.
3. Under **Network Configuration**, click **Refresh** to view the results from **IPConfig /all**.
4. To ping a server, enter the fully qualified domain name, hostname, or IP address in the **Ping** section, and then press **Enter**.

Download Log Files

Downloading log files is typically done when troubleshooting a recent issue.

Download Individual Log Files

To download individual log files:

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Diagnostics** menu, select **Appliance Logs**.
3. At the right of a log entry, click the **Download** button.

Download All Log Files

> ***Note:*** *The "download all" process includes the last three months of logs.*

To download all log files:

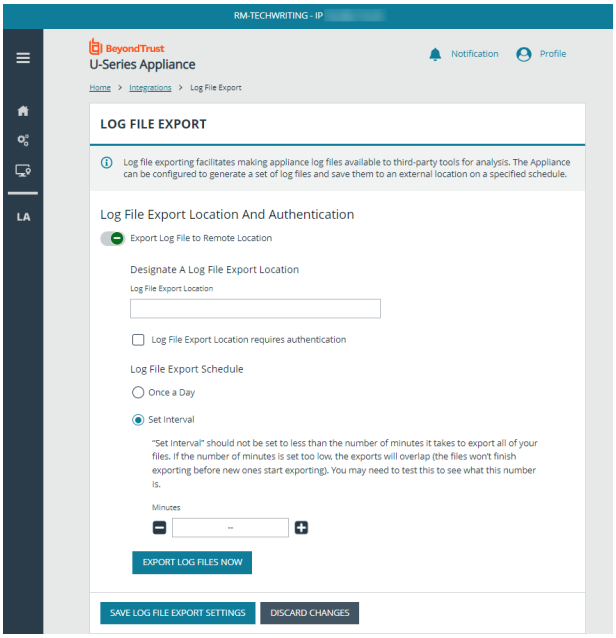
1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. From the **Diagnostics** menu, select **Appliance Logs**.
3. At the bottom right of the log entries list, click **Download All**.

Export Log Files

Log file exporting facilitates making appliance log files available to third-party tools for analysis. The U-Series Appliance can be configured to generate a set of log files and save them to an external location, on a specified schedule.

By default, the **Export Log File to Remote Location** option is on. When it is turned off, none of the setup options are visible.

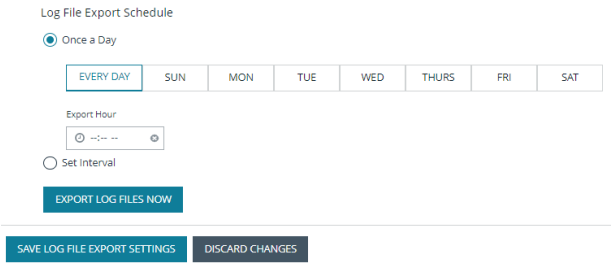
> ***Note:*** *The file cannot be saved on the U-Series Appliance.*



To set up log file export and authentication:

1. On the sidebar menu, click **Integrations**, and then select **Log File Export**.
2. Enter a **Log File Export Location**.
3. If the log file export location requires authentication, check the box.
    - Enter the **Log File Export Location Username**.
    - (Optional). Enter a **Log File Export Location Password**.
    - (Optional). Enter the **Domain**.
    - To verify the authentication, click **Test Credentials**.

4. Select a **Log File Schedule** option. The default is **Set Interval**.
    - If using the default **Set Interval** option, enter the number of **Minutes**, as per the instructions onscreen. The interval should not be set to less than the number of minutes it takes to export all of your files.
    - Click **Save Log File Export Settings**.
5. If using the **Once a Day** option, the day and time options appear.
    - Select a day option, and then enter the **Export Hour**.
    - Click **Save Log File Export Settings**.



***Note:** At any time after the settings are initially configured, you can click **Export Log Files Now** to save the log file to the share.*

Configure U-Series Appliance Roles

Select U-Series Appliance roles if you are deploying more than one U-Series Appliance to scale BeyondInsight in larger networks. Roles must be selected for at least one of the U-Series Appliances.

> ***Note:*** *When you select roles, any dependencies or conflicts that exist between roles are displayed. The* ***Apply Roles*** *button is available only after dependencies and conflicts are resolved.*

Role Descriptions

Vulnerability Scanner Role

Turn on the **Vulnerability Scanner** role to activate the Discovery Scanner agent.

Event Collector Role

On the **Event Collector** page, select the BeyondTrust service that will be responsible for sending events between components. You can use BeyondInsight AppBus Service or Event Server. Event Server is preferred for enterprises and can manage a greater load of data than AppBus. The default port for Event Server is **21690**.

After selecting which service to use, click **Apply Changes**.

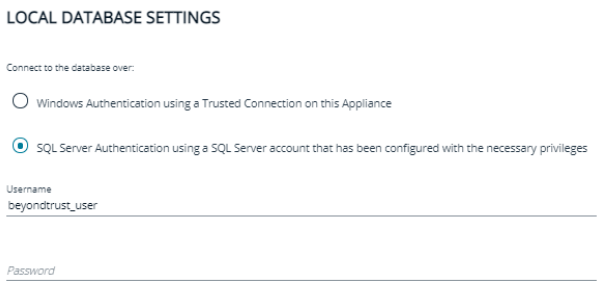
SQL Server Database Role

This role provides access to the SQL Server database. Check the box to allow database access from remote computers. If you are using your SQL Server deployment, no action is required.

BeyondInsight Database Access Role

This role provides access to the BeyondInsight database. You can set either a local SQL Server database or configure settings for a remote database.

When configuring a local database, select an authentication type. When you select SQL Server, **Username** is populated with the same user name in the Configuration wizard during your initial U-Series Appliance setup. The account is created with least privilege.



To use an existing remote database, you must import a password protected crypto key from the appliance running the BeyondInsight Management console that created the database.

The BeyondInsight configuration provides the same least privilege SQL Server account during the database configuration.

For more information, please see the following:

- *"Download a Crypto Key" on page 9*
- *For the permissions assigned to the least privilege SQL Server account, see section "Least Privilege Database User Account Setup" in the BeyondInsight Installation Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/documents/bi/bi-install.pdf*

Patch Management Role

Turn on this role to activate the LanMan service on the U-Series Appliance to host third-party patches.

BeyondInsight Omniworker Service Role

The BeyondInsight Omniworker service manages task queues. Turn on this service when your environment uses more than one U-Series Appliance.

Password Safe Web Portal Role

Turn on this role to activate services needed to run the Password Safe web portal.

Note: *This role is available only when a Password Safe license is applied.*

High Availability Role

Turn on this role to activate services needed to run Password Safe in high-availability mode.

1. Log in to the U-Series Appliance website on the primary server.
2. From the menu, select **Roles Editor**.
3. Click **High Availability**, then select a mirroring option:
    - **HA will mirror both Server and Database**
    - **HA mirroring for services only**

Note: *To save resources, you can turn off services that are not required to run on any secondary U-Series Appliances. Check the* ***Standalone Password Safe Worker Node*** *box. Check the corresponding boxes to turn off services:* ***Disable BeyondInsight UI*** *or* ***Disable Password Safe UI****.*

4. Click **Apply Changes**.
5. On the main **Roles Editor** page, click **Apply Pending Changes**.
6. Repeat these steps for the secondary server.

BeyondInsight for Unix & Linux Role

Activate the role to configure a database connection for BeyondInsight for Unix & Linux.

> ***Note:*** *The role is available only when BeyondInsight for Unix & Linux is installed and can be enabled with a local or remote database.*

For a local database, enter a username and password for SQL Server. The account is created if it doesn't already exist. A SQL Server account is required for BeyondInsight for Unix & Linux to access the database.

To set up a remote database:

1. Add the server name where the database resides.
2. Optionally, enter the name of the SQL Server instance.
3. Enter a port number to communicate to the server.
4. Add the name of the BeyondInsight for Unix & Linux database, and the username and password. The remote database must already exist on the remote host.
5. Click **Test Remote Connection Settings** to verify the connection to the remote database.

Once the role is enabled, you must configure BeyondInsight for Unix & Linux. The BeyondInsight database is added to backup and restore functions and is included with high availability database synchronization.

Analysis Services Role

Turn on this role to enable the SQL Server Analysis service. You can click the link to run BeyondInsight Analytics & Reporting.

> ***Note:*** *This role is available only if you use BeyondInsight Analytics & Reporting.*

Reporting Services Role

If you use BeyondInsight Analytics & Reporting to render reports, the service must run locally. Turn on this role to run the service locally when using a remote database.

Auto-Update Role

To automatically download product updates when available, turn on this role.

1. On the U-Series Appliance website, select **Roles Editor** from the menu.
2. Click **Auto Update**.
3. You can configure one server for all updates or configure servers based on functional area. If you have configured different update servers, click **Load Default Settings** to reset the default BeyondTrust server.
4. Click **Apply Changes**.
5. On the main **Roles Editor** page, click **Apply Pending Changes**.

Enterprise Update Server Role

Turn on this role to use the enterprise update server to update your U-Series Appliances.

IMPORTANT!

Enterprise Update Server has reached End of Life. SMTP and Proxy Credentials will not be updated for that product.

BeyondTrust Updater Role

Turn on this role to use the Azure web-based update tool.

BeyondTrust PowerBroker End Point Protection Role

If turned on, you can disable the U-Series Appliance protection policy which is applied. We recommend you leave this role on, disabling it only for troubleshooting reasons when working with BeyondTrust Technical Support.

Cold Spare Role

Turn on this role to configure options to set the automatic restore schedule and temporary machine name. When this role is enabled, the name of the U-Series Appliance is changed so that there is no conflict on the network with the main U-Series Appliance. When the cold spare U-Series Appliance is required, the role is disabled, the machine name is automatically reverted, and services are started.

Configure Password Safe on the U-Series Appliance

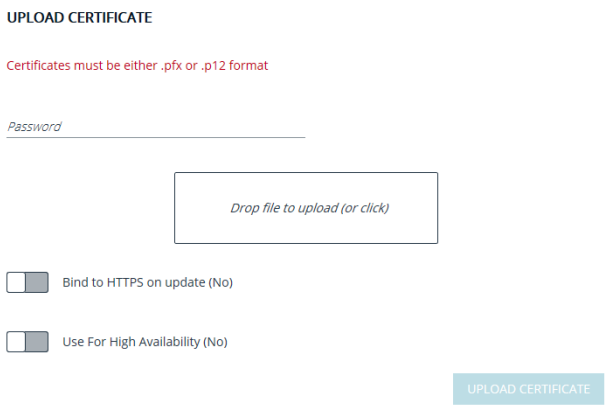
To set up Password Safe on the U-Series Appliance, you must turn on the **Password Safe** role.

> ***Note:*** *If you use Password Safe, all credentials are stored in the database using an AES-256 block cipher by RijndaelManaged.*

> *For more information, please see "Password Safe Web Portal Role" on page 29.*

Upload SSL Certificate

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. Under **Upload Certificate**, drag the certificate file into the drop area or click the button to browse.
4. Enter the password.
5. To update the bindings in IIS, click the **Bind to HTTPS on update** toggle to the on setting.
6. To enable this certificate for multiple U-Series Appliances, toggle the **Use for High Availability** switch to the on setting .
7. Click **Upload Certificate**.



To generate an SSL certificate to match the U-Series Appliance name:

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the **Maintenance** menu, click **Security Settings**.
3. To regenerate the SSL certificate to match the U-Series Appliance network name, under **Generate SSL Certificate**, click **Generate Certificate**.

> ***Note:*** *This certificate will not be trusted by the client browser.*

4. To export the client certificate, under **Export Client Certificate**, enter the password for the certificate, and then click **Export Certificate**.

Archive Password Safe Session Monitoring Events

To make more disk space available on the U-Series Appliance, you can transfer session monitoring files from the U-Series Appliance to another server for storage. You can view these archived files in Password Safe.

There are three types of remote hosts that can be used to store session archive files:

- Remote Network share. We recommend that you use a secure network share which requires authentication.
- Network File System (NFS) share.
- Run the Configure Repository Installer on a remote server which creates an IIS site and enables Background Intelligent Transfer Service (BITS). This uses BITS to transfer files.

Session monitoring files are archived in one of two ways:

- Automatically by the U-Series Appliance. Automatic archives occur in the following cases:
  - When the file reaches the configured age.
  - When free space on the U-Series Appliance hard drive is below the configured threshold.
- Manually through Password Safe. Archive files are never deleted.

For more information, please see the following:

- *Password Safe Administration Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/index.htm*
- *"Set Up the Repository Host" on page 33*

Set Up the Repository Host

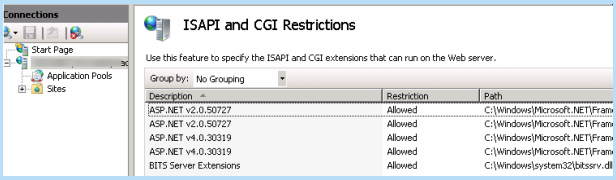
Repository Host Requirements

- Windows 2008 or later.
- Port 443 open.
- IIS 7.5 or later.
- ASP.NET 4.5
- Setup Session Monitoring Repository tool, located at **C:\Appliance\Tools\ConfigureRepository.exe**.

Note: *In Server Manager, install and enable BITS. Activating BITS ensures prerequisites are installed regardless of OS or IIS version installed.*

Note: *If you are using IIS 7.5 and the ASP.NET 4.5 role did not install automatically:*

1. *Install the ASP.NET role.*
2. *Run the command **C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -i**.*
3. *Log in to Server Manager and select the IIS instance.*
4. *Double-click **ISAPI and CGI Restrictions**.*
5. *Ensure that ASP.NET 4.0 is set to **Allowed**.*



Run the Repository Configuration Tool

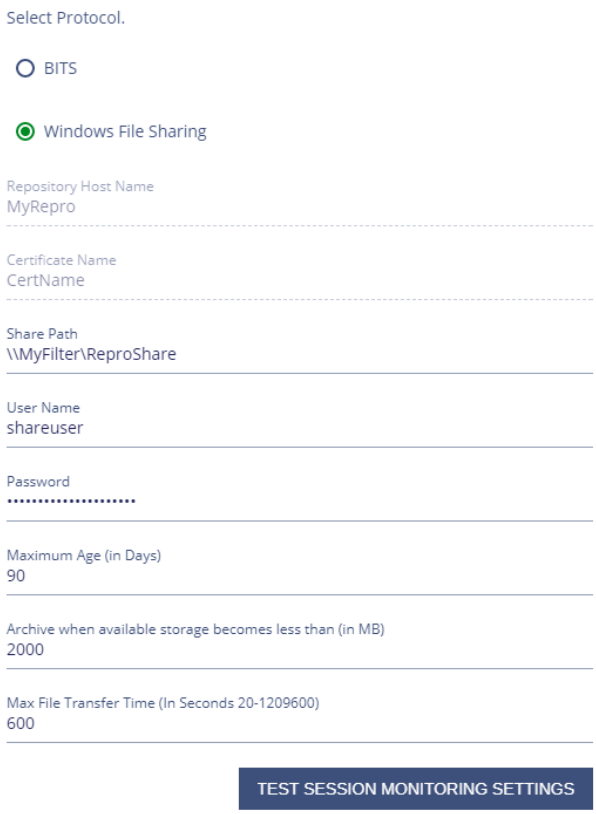
The repository configuration tool creates a certificate on the host computer.

1. Run the repository configuration tool.
2. Click the **Create Certificate** button.
3. Enter a password for the exported certificate.
4. Click **Export Certificate** and choose a location for the file with the exported certificate.
5. Copy the exported certificate to a location that can be accessed by the U-Series Appliance. You must import the certificate using the **Diagnostics** website.

Set Up the U-Series Appliance

If using the installed repository, you must register the certificate on the U-Series Appliance. Optionally, you can change the archive settings, such as the number of days that should pass before the files are archived.

1. On the **Maintenance** menu, click **Security Settings**.
2. Upload the certificate that you created on the host, and then click **Upload Certificate**.
3. On the menu, select **Roles Editor**.
4. Click **PowerBroker Password Safe Web Portal**.
5. Check the **Enable Session Monitoring Archiving** box.
6. Select the way to store the archive files:
    - **BITS:** Enter the name of the repository computer and the name of the certificate. These are the same name.
    - **Windows File Sharing:** Enter the name of the share and credentials to access the share. Windows file sharing is the preferred method.
7. Optionally, change the archive settings:
    - **Maximum Age (in Days):** Enter the number of days that pass before the files are archived. The default value is **90** days.
    - **Archive when available storage becomes less than:** This value applies to the storage available on the U-Series Appliance. Enter the amount of storage remaining on the U-Series Appliance before the file transfer occurs. The transfer of files will free up the disk space when the value is reached.
    - **Max File Transfer Time:** This value is the maximum time to wait for a file transfer to occur before the transfer times out.
8. Click **Test Session Monitoring Settings** to ensure the repository computer is set up correctly and can communicate with the U-Series Appliance computer.
9. Click **Apply Changes** to save the settings.



Use High Availability with U-Series Appliances

High availability (HA) is designed to work in an active / passive configuration. At any time, one of your two servers has the role of the *active* node, while the other is the *passive* node. When the passive server detects that the active server has failed, then the passive is promoted to active, and the active is demoted.

> ***Note:*** *Starting with U-Series v3.4, the* ***Team Password Service*** *has been added to the services managed by high availability. This ensures that if a failover occurs, the service is started on the passive node when it becomes the active node.*

Turn on High Availability Pairing

> ***Note:*** *Before setting up high availability, you must turn on the* ***High Availability*** *role in the* ***Roles Editor*** *for both the active and passive U-Series Appliances. For more information, please see* *"High Availability Role" on page 29**.*

1. Log in to the U-Series Appliance website on the primary server.
2. From the menu, select **Roles Editor**.
3. Click **High Availability**, then select a mirroring option:
    - **HA will mirror both Server and Database**
    - **HA mirroring for services only**

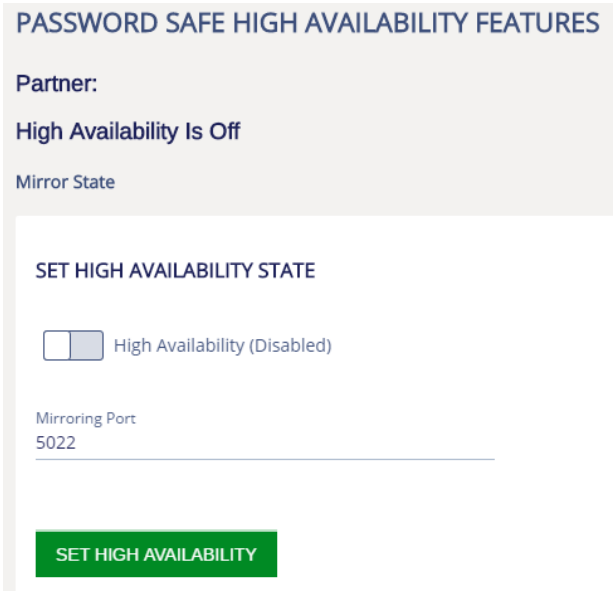
> ***Note:*** *To save resources, you can turn off services that are not required to run on any secondary U-Series Appliances. Check the* ***Standalone Password Safe Worker Node*** *box. Check the corresponding boxes to turn off services:* ***Disable BeyondInsight UI*** *or* ***Disable Password Safe UI****.*

4. Click **Apply Changes**.
5. On the main **Roles Editor** page, click **Apply Pending Changes**.
6. Repeat these steps for the secondary server.

Configure High Availability

1. Log in to the U-Series Appliance, and then select **High Availability**. For a first-time configuration, the **Initial Setup** page displays. Certificates must be set up between the U-Series Appliances for secure communication.
2. Click **Go to the API Key Maintenance Page**.
3. Copy the API registration keys between the partner U-Series Appliances. Registering the API key with the partner U-Series Appliance permits secure communication between the U-Series Appliances.
4. Enter the host name of the passive U-Series Appliance, then click **Apply**.
5. A message displays that the exchange is in progress. If an error occurs during the certificate exchange, a **Show/Hide Results** button displays. Exchanging certificates can take up to approximately five minutes. After the certificates are exchanged with no errors, the configuration settings display.

6. Toggle the **High Availability** switch on to turn on the feature.
7. Enter the mirroring port number. The default port is **5022**.
8. Click **Set High Availability**.



9. For **Partner Contact Timeout**, enter the number of minutes that pass with no contact between the active server and passive server. When the active server receives no response from the passive server, then the active continues to start. If the passive server has no contact with the active, the passive server starts up as the active one. The default setting is 25.
10. For **Partner Failover Timeout**, enter the number of minutes that pass with no ping received from the primary server. After this time, the passive server switches to the active one. The default setting is 14.
11. For **Reboot Blackout Window**, enter the number of minutes that should pass before the passive server takes control. On graceful shutdown, the passive server switches to the active one after no response for this length of time. The default setting is 14.

    This is useful when you want to shut down the active U-Series Appliance but do not want the passive U-Series Appliance to take control. For example, you might want to move the active U-Series Appliance and know this will take about thirty minutes. To be sure the passive U-Series Appliance does not take control while the active U-Series Appliance is offline, set this value to sixty minutes.

> ***Note:*** *You must shut down the primary U-Series Appliance from the* ***Maintenance > Schedule a Reboot*** *page.*

12. We recommend that you enable **Attempt Auto-Resync** only for testing scenarios.
13. **Synchronize Session Archving Files** synchronizes local session recording files from Password Safe with the partner U-Series Appliance. This allows you to replay the session recordings from within Password Safe if a failover occurs and the passive U-Series Appliance is made active.
14. You can select **Send Alerts on Failover** to send either an email or events to BeyondInsight.
15. If you select **Medium Failover Mode**, then when communication between the pairs is lost, the passive U-Series Appliance is in a failover-pending state only. Action is required on your part to start a failover process.

16. In **Background Settings Update Rate**, enter the number of minutes that pass before a file synchronization occurs. Files copied to the passive server are configuration files, certificates, and registry files.
17. Set the **Failed Notification Rate** to provide notification after your active U-Series Appliance has failed over. If you are using medium failover mode, the email indicates that action is required on your part. The default value is fifteen minutes.
18. You can click **Queue File Synchronization** to start a file synchronization.
19. Click **Update Settings**.

For more information, please see the following:

- *"Test High-Availability Failover" on page 38*
- *"Configure Notifications" on page 23*
- *"Use Medium Failover Mode" on page 38*

Use a Load Balancer in an Active / Passive Configuration

When setting up an active / passive pair, you might want to configure a load balancer that acts as a DNS redirector. Configure the load balancer between two U-Series Appliances so that it can determine which U-Series Appliance is active and which is passive. The load balancer then sends the traffic to the active U-Series Appliance.

You can use the following endpoint API to configure the load balancer. Refer to your load balancer documentation to ensure that it is configured to use the endpoints.

```
GET https://<ApplianceAddress>/UVMInterface/api/HighAvailability
```

The code above returns an object with one member:

```
{
string Role;
}
```

You can set the formatting of the requested return value in the **Content-Type** request header.

Example: *To return a value in JSON format, you can specify:*

```
Content-Type: application/json;charset=UTF-8
```

The available values for **Role** are:

- **Off:** High Availability is not turned on.
- **Active:** The U-Series Appliance is in active mode.
- **Passive:** The U-Series Appliance is in passive mode.

Test High-Availability Failover

> ***Note:*** *You can use **Attempt Auto-Resync** as a quick way to restore high availability in a scenario where databases on the active and passive servers are synchronized. We do not recommend a production failover scenario. Data loss can occur if databases are not synchronized.*

1. Select **Attempt Auto Resync of database when connecting after failover**.
2. Unplug or power off the active server.
3. Wait for failover. Ensure that the passive is now the active.
4. Restore the active server (turn on or plug in).
5. The auto re-sync restores the high-availability configuration.
6. The passive server is now acting as the active server. Click **Switch Roles** to restore the server partners to their original roles.

Use Medium Failover Mode

Use medium failover mode when you do not want the services on the passive U-Series Appliance to start automatically when the communication between pairs is lost.

The passive U-Series Appliance waits in a pending state until you manually start the failover process. When the active U-Series Appliance fails, you must log in to the U-Series Appliance software to start the failover process to the passive U-Series Appliance.

1. Log in to the U-Series Appliance, and then select **High Availability**.
2. In the **High Availability Maintenance** section, click **Failover to this U-Series Appliance** to start the services and database.

> ***Note:*** *This button is active only when the primary U-Series Appliance is down.*

Resume and Suspend SQL Mirroring

You might want to pause mirroring if you want to take care of maintenance tasks on the database server. A failover cannot occur when the database is in a suspended state.

1. Log in to the U-Series Appliance, and then select **High Availability**.
2. Click **Suspend** to pause mirroring.
3. Click **Resume** to start mirroring again.

> ***Note:*** *If the U-Series Appliance is in a failover state and mirroring is suspended, you can click **Resume** to start mirroring.*

Discard High-Availability Configuration Settings

To reset the U-Series Appliances to the initial setup state, you can remove all high-availability configuration settings established between U-Series Appliances. You might want to do this if you want to set up new high-availability pairs.

1. Log in to the U-Series Appliance, and then select **High Availability**.
2. Click **Abandon Configuration**.

Recognize a Failover

Review the following to help you determine if a failover has occurred.

- If you are using a U-Series Appliance version 1.5.4 or later, an email is sent to the address set in the Configuration Wizard. If you are using a U-Series Appliance version earlier than 1.5.4, you can contact BeyondTrust Technical Support to activate the email feature.
- If you are not using a load balancer, you might notice that BeyondInsight is no longer responsive on the active server.
- On the **Diagnostics** website (for the primary), only two tabs are displayed. This indicates that the server is in passive mode.
- Confirm that the passive server is in active mode.

Prepare for Disaster Recovery

If you are using high availability as a disaster recovery solution, review the following points as a guide to restoring roles.

- Determine if the active server has failed. Confirm the role of the live server (the primary).
- If a failure has occurred on the primary, investigate and resolve issues on the primary.
- After a failover to the disaster recovery server (the secondary), you can restore roles on the active server's website.

Verify Connectivity between Servers

On the **High Availability Configuration** page, verify that the communication between U-Series Appliances is active. The **Last Heartbeat** indicates the last ping to the passive server and the return response to the active server.

Check the Database Status after a Failover

IMPORTANT!

In all scenarios, we strongly recommend investigating the cause of the failure. We do not recommend resuming database mirroring until issues are resolved.

The following database status indicators might display after a failover:

- **DISCONNECTED:** Failover was catastrophic, and the server is completely unavailable or unreachable. Turn off high availability and investigate the issues with the failed server. After the failed server is cleared for use, turn on high availability and synchronize the databases.
- **EXPOSED:** The other server is still available and possibly still healthy, but the failover was serious or lengthy enough to disable high availability. After the failed server is cleared for use, turn on high availability and synchronize the databases.
- **SUSPENDED:** The interruption was of a minor or transient nature. While it may be possible to restore connectivity without disabling high availability, we recommend that you turn off high availability and investigate the issues with the server. After the failed server is cleared for use, turn on high availability and synchronize the databases. Optionally, contact BeyondTrust Technical Support to see if mirroring can be restored.

Restore Roles After a Failover

After a failure has been identified and resolved on a U-Series Appliance, you can restore the roles to the initial state. Log in to the U-Series Appliance, and then select **High Availability**. Then click **Switch Roles**.

Review Database Metrics

On the **High Availability Settings** page, review information about earlier database synchronizations and the size of the current database.

You can then determine from these values how long a synchronization between servers might take.

Check the status of the BeyondInsight mirror state on the **High Availability** tab to ensure that synchronizations are occurring between the active and passive servers.

Database Mirror States

State	Description
EXPOSED	Databases are not mirrored.
SYNC PENDING: INITIAL DB SYNC STARTED	The process of backing up and transferring the database to the passive server has begun.
SYNC PENDING: SET MIRROR CALLED	The database has been transferred and restored to the passive server. Mirroring is being turned on.
SYNCHRONIZING	The server is actively transmitting transaction logs to the other database to apply changes.
EXPOSED: MAX SYNC ATTEMPTS REACHED	Five consecutive attempts were made and failed to establish mirroring. Mirroring was not established and is no longer trying. To troubleshoot, check for connectivity issues and ensure the database mirror port is set to **5022**.
SYNCHRONIZED	Databases are actively mirrored. High availability is considered to be working.

Configure a Remote Database for the U-Series Appliance

Use the Database Utilities tool to connect to a remote SQL Server and create a BeyondInsight database.

> ***Note:*** *The tool is not available on SQL Free or UVMSQL Appliances.*

1. From the **Maintenance** menu, select **Database Utilities**.
2. Enter the IP address and database name.
3. Enter a SQL Server username and password. The credential needs sufficient access to create a database.
4. The default database connection timeout is 360 seconds. Enter another timeout value, if required.
5. The **Remote MultiSubnet Enabled** setting is turned on by default. Click the button to turn the setting off.
6. To ensure a connection to the database server can be established, click **Test Connection**.
7. Click **Create Database**.

Configure Backup and Restore on the U-Series Appliance

Save the U-Series Appliance configuration in case of disaster recovery or if you need to revert settings to a previous configuration. You can back up the U-Series Appliance immediately or schedule a backup to occur at regular intervals.

A backup contains full packages of all data for all roles set up on the U-Series Appliance.

You can select the backup location or use the default. When configuring the backup location, you can set the number of backups that are saved. The default number is 5 (0 is unlimited). When the retention number is reached, then the oldest backups are deleted and removed from the database permanently.

There is no time limit for how long backups are retained. Backups are only deleted when the retention limit is reached or when they are manually deleted.

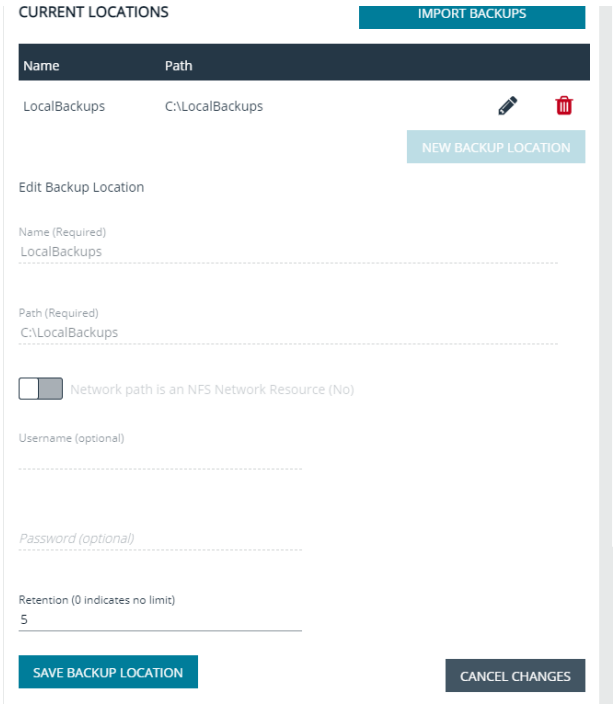
Backup Location

By default, there is one backup location already for saving backups to a local path. New backup locations can be added which are either local or remote network shares.

1. From the **Maintenance** menu, select **Backup and Restore**.
2. Click **New Backup Location**.
3. Enter a name and the local or remote path. If remote share requires credentials enter them here, or if the remote share is an NFS share, click that option.

> ***Note:*** *We do not recommend storing backup files on an unsecured network share.*

4. Enter a value in the **Retention** box. Retention is the number of backups saved. When the limit is reached, then older backups are deleted and removed from the database permanently.
5. Click **Create Backup Location**. This process attempts to write and delete a file. If that fails, you cannot create the backup location. Upon failure, we recommend that you verify access permissions.



Import Backups

After a backup location is added, it automatically adds any backups to the list on the page which are applicable for the U-Series Appliance.

If a backup file is added to a folder after it has already been created as an available backup location, click **Import backups** to force a rescan of the available folders.

Schedule a Backup

1. From the **Maintenance** menu, select **Backup and Restore**.
2. Click **Backup Scheduler** to turn on scheduling.
3. Select the backup location from the menu. If a new location is required, add it from the **Backup Locations** section.

4. Select the day of the week and the time to run the backup.
5. Create a password for the zip file.
6. Check the **Include Session Files in the Backup** box. This has the potential to create a large backup file, depending on the number of local session files and how often they might be archived.
7. Click **Schedule Backup**.

Back Up the U-Series Appliance Now

1. From the **Maintenance** menu, select **Backup and Restore**.
2. Select the backup location from the menu. If a new location is required, add it from the **Backup Locations** section.
3. Create a password for the zip file.
4. Check the **Include Session Files in the Backup** box. This has the potential to create a large backup file, depending on the number of local session files and how often they might be archived.
5. Click **Create Backup**.

Restore the U-Series Appliance

1. From the **Maintenance** menu, select **Backup and Restore**.
2. Search through the list of available backups and click **Restore**.
    - If the backup was taken on this U-Series Appliance, you are not prompted for a password.
    - If the backup was taken on a different U-Series Appliance, you are prompted for a password.
3. If the browser session remains open when a restore is complete, it returns a message displaying that the restore process is complete.

Download Backup

Note: *Downloads greater than 4GB cannot be downloaded from a web browser. Copy downloads greater than 4GB to a network share, or use another way to download.*

1. From the **Maintenance** menu, select **Backup and Restore**.
2. Search through the list of available backups and click the download icon.

Delete Backups

1. From the **Maintenance** menu, select **Backup and Restore**.
2. Search through the list of available backups and click the delete / trash bin icon. This removes the backup from the list displayed and also removes it from the current folder location.

IMPORTANT!

Warning: Once a backup is deleted it cannot be undone.

Contents of a Backup File

What is contained in a backup file:

BeyondInsight Analytics & Reporting

- ReportServer Database
- BeyondInsight Reporting Database
- ReportServerTempDB Database
- Cube database
- Encryption key

BeyondInsight

- BeyondInsight Database
- BeyondInsight Registry information
- Database Connection String
- Encryption Key
- System files

Event Collector

- Product registry settings

Enterprise Update Server (EUS)

- EUS Database
- EUS webconfig

U-Series Appliance

- Certificates (Client & Server)
- Roles settings
- U-Series Appliance Monitored data
- U-Series Appliance Notification data
- Performance Counters
- Log Export Database

BeyondInsight for Unix & Linux (BIUL)

- BIUL Database
- Product Configuration
- Log File
- Related product settings

BeyondTrust Auto Update:

- Proxy details
- Registration details
- Parent update server endpoint

BeyondTrust Updater

- BeyondTrust Analyzer data
- Client database
- Health check report
- Licenses
- User database
- Product related registry settings

Network Vulnerability Scanner

- Product Registry settings
- Certificates
- Database audits
- Application settings

Session Archiving

- Session Monitoring files

Set Up a Cold Spare U-Series Appliance

You can set up a U-Series Appliance that can be used as the main U-Series Appliance if the first one needs to be taken offline.

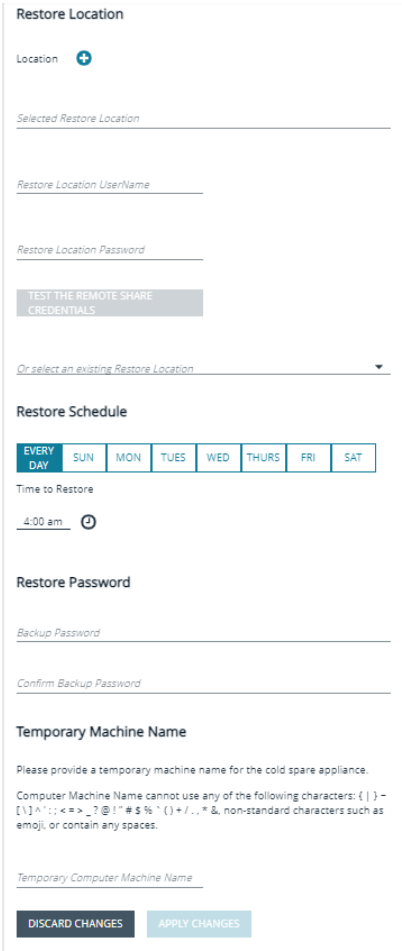
Requirements

- The BeyondInsight version on the cold spare must be the same or later than the version on the source U-Series Appliance.
- It is recommended that both U-Series Appliances have the **Auto Updates** role turned on.
- The cold spare must receive updates so that it matches the source U-Series Appliance.
- For Analytics & Reporting, ensure SQL Server versions match on both U-Series Appliances.
- The source and spare U-Series Appliances must have the same name.

> ***Note:*** *If the SQL Server database is remote, the data will not be copied to the cold spare.*

To set up the cold spare appliance:

1. On the sidebar menu, click **LA** (if you are in the new environment only).
2. On the menu, select **Roles Editor**.
3. Click the **Set Up Appliance as Cold Spare** role.
4. Turn the role *on*.
5. To set a location, click **Locations +** (or select an existing one from the dropdown list).
    - Enter the path for the **Restore Location** where you want the backup files to be saved. Optionally, select an existing location.
    - If applicable, enter the **Username** and **Password** to access the location.
    - To test the connection, click **Test the Remote Share Credentials**.
6. Select the **Day** of the week and the **Time** when you want the cold spare to retrieve the information from the backup file. When the cold spare starts, the data from the last backup file retrieved is used.
7. Enter a restore **Password**, and confirm it.
8. Provide a **Temporary Computer Machine Name**.
9. Click **Apply Changes**.
10. On the **Roles Editor** main page, click **Apply Pending Changes**.
11. Once the settings have been saved, a dialog box displays and prompts you to restart the U-Series Appliance.



Perform U-Series Appliance Recovery

Use the recovery procedure to rebuild your U-Series 20 or U-Series 50.

IMPORTANT!

All information saved or configured on the U-Series Appliance will be lost. There is no way to recover this data.

1. Start the process by retrieving the BitLocker keys. You can do this in either of two ways:
   - Open **File Explorer** and look for an external drive with a label of **U-Series Appliance-BITLOCK**. There is a text file on this drive for each drive letter on the U-Series Appliance (one drive on most images and four drives on older U-Series 50 models).
   - If the internal USB has been removed and cannot be located, type the following command into a command window to display and save the BitLocker passwords:

     ```
     Manage-bde -protectors -get c:
     ```

     To pipe to a file type:

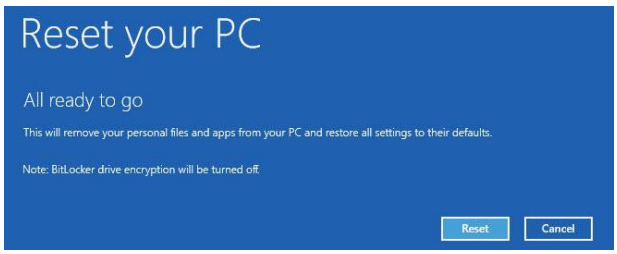
     ```
     manage-bde -protectors -get c: > "bitlocker C.txt"
     ```

2. Restart the U-Series Appliance. At the BIOS screen, press **F8** to access the Windows boot options.

***Tip:** Try pressing the F8 key every few seconds to make sure you do not miss the chance to access the boot options.*

3. Press **Enter** to go to the BitLocker key prompt.
4. Enter the BitLocker password for the C: drive (matching the ID), and press **Enter**.
5. On the **Advanced Boot Options** screen, press **Enter** to choose **Repair Your Computer**.
6. Click **Troubleshoot**.

7. Click **Reset Your PC**.
8. Enter the drive password for the displayed ID and click **Continue**.
9. Click **Next**.
10. For the U-Series 50 only, select **All drives**.
11. Click **Just remove my files**.
12. Click **Reset**.



> ***Note:*** *After you click* ***Reset****, BitLocker drive encryption will be turned off. It will be enabled again later in the process.*

13. The U-Series Appliance is imaged with the original manufacturing image.
14. Insert the USB which contains the BitLocker keys. The BitLocker keys will be regenerated and saved to the USB.
    - On the first reboot, scripts run that are required to set up the U-Series Appliance. This part of recovery is automatic and forces a system reboot when it is complete.
    - After the second reboot, a command window displays. BitLocker starts the drive encryption. Updates are displayed on the drive encryption progress.
15. After BitLocker is complete, run **Update Appliance.bat** on the desktop.
16. Click **Next** on the auto-update window.
17. All products will update to the most recent version on the public update server. When auto-update finishes, click **Next**. All updates are now complete.
18. Enter the license key for Windows and the license key for SQL Server.
19. For the final stage of preparation, run **Prepare For Shipping.bat**. All temporary and setup files are removed; Windows and SQL Server are licensed. You are now ready to configure your U-Series Appliance.

Optional U-Series Appliance Configuration

Perform Dell PowerEdge System Updates

Update the BIOS on a Dell PowerEdge Server

1. Start the process by retrieving the BitLocker keys. You can do this in either of two ways:
    - Open **File Explorer** and look for an external drive with a label of **U-Series Appliance-BITLOCK**. There is a text file on this drive for each drive letter on the U-Series Appliance (one drive on most images and four drives on older U-Series 50 models).
    - If the internal USB has been removed and cannot be located, type the following command into a command window to display and save the BitLocker passwords:

      ```
      Manage-bde -protectors -get c:
      ```

      To pipe to a file type:

      ```
      manage-bde -protectors -get c: > "bitlocker C.txt"
      ```

2. Get the service tag from the server in either of two ways:
    - Find the **EST** label on the front of the server and pull out the card.
    - When logged in to Windows, type **racadm getsysinfo** in a command line. The information returned contains the service tag number. This option is available only on newer iDRAC versions.
3. Open a browser and go to https://www.dell.com/support/home/en-us/.
4. Enter the service tag number.
5. Click **Drivers & Downloads**.
6. Change the **Category** to **BIOS**.
7. Download the BIOS package and copy it to the U-Series Appliance.
8. Double-click the downloaded .exe file and click **Install**.
9. Follow the instructions and reboot the U-Series Appliance when prompted.
10. If prompted, enter the BitLocker password on reboot.

Update the Chipset Drivers on a Dell PowerEdge Server

1. Get the service tag from the server in either of two ways:
    - Find the **EST** label on the front of the server and pull out the card.
    - When logged in to Windows, type **racadm getsysinfo** in a command line. The information returned contains the service tag number. This option is available only on newer iDRAC versions.
2. Open a browser and go to https://www.dell.com/support/home/en-us/.
3. Enter the service tag number.
4. Click **Drivers & Downloads**.

5. Change the **Operating System** to **Windows 2012 R2**, **Windows 2008 R2**, or **Windows 2016** depending on the U-Series Appliance image.
6. Change the **Category** to **Chipset**.
7. Download the chipset drivers and copy them to the U-Series Appliance.
8. Run the downloaded installer and extract to a folder.
9. In **Windows Device Manager**, right-click any unidentified hardware devices and click **Update Driver**.
10. Select the browse location where the drivers were extracted earlier. The driver files are located in a subfolder here. Search for a folder with .inf files.
11. Click **Next** and allow the driver to update.
12. Continue as needed with any other unidentified devices.

Update the iDRAC Software on a Dell PowerEdge Server

1. Start the process by retrieving the BitLocker keys. You can do this in either of two ways:
    - Open **File Explorer** and look for an external drive with a label of **U-Series Appliance-BITLOCK**. There is a text file on this drive for each drive letter on the U-Series Appliance (one drive on most images and four drives on older U-Series 50 models).
    - If the internal USB has been removed and cannot be located, type the following command into a command window to display and save the BitLocker passwords:

      ```
      Manage-bde -protectors -get c:
      ```

      To pipe to a file type:

      ```
      manage-bde -protectors -get c: > "bitlocker C.txt"
      ```

2. Get the service tag from the server in either of two ways:
    - Find the **EST** label on the front of the server and pull out the card.
    - When logged in to Windows, type **racadm getsysinfo** in a command line. The information returned contains the service tag number. This option is available only on newer iDRAC versions.
3. Open a browser and go to https://www.dell.com/support/home/en-us/.
4. Enter the service tag number.
5. Click **Drivers & Downloads**.
6. Change the **Category** to **iDRAC with Lifecycle controller**.
7. Download the latest version available and copy it to the U-Series Appliance (not the iDRAC Controller Integration).
8. Run the downloaded file.
9. Follow the instructions and reboot the U-Series Appliance when prompted.
10. If prompted, enter the BitLocker password on reboot.

Configure iDRAC

You can use Integrated Dell Remote Access Controllers (iDRAC) to remotely manage your U-Series 20 or U-Series 50.

1. At startup, press **F2** to enter the setup menu.
2. Select **iDRAC Settings**.
3. Select **Network**.
4. Set **Enable NIC** to **Enabled**.
5. Configure IP address settings as specified by your network administrator (DHCP or static). Setting the NIC selection to **Dedicated** allows the physical iDRAC port on the back to be used only for iDRAC communication. Setting it to another port will allow it to share the same physical connection.
6. Save your settings.
7. If you use DHCP IP configuration, watch for the iDRAC IP address to be displayed at startup and record this for future use.
8. Open a browser and enter the IP address associated with the iDRAC port. Use the default login credentials:
    - User: root
    - Password: calvin

For more information about configuring iDRAC, please refer to Dell product documentation.

iDRAC Commands

You can use the commands below to configure iDRAC settings from a Windows command prompt.

Setting	Command
Enable	**Racadm setniccfg -o**
Set user account	**racadm config -g cfgUserAdmin -o cfgUserAdminPassword -i 2 <password>**
Set static IP	**racadm setniccfg -s <IPv4Address> <netmask> <IPv4 gateway>**
Set DHCP on	**racadm setniccfg -d**
Get info	**Racadm getniccfg**

Configure NIC Teaming or Link Aggregation

Note: *You must have the Broadcom management utility installed before continuing with these steps. On Microsoft Windows Server 2012 R2 U-Series Appliances, the* ***Broadcom Advanced Control Suite 4*** *application is already installed. For Windows 2008 R2 U-Series Appliances, please contact BeyondTrust Technical Support to get the installer file. For Windows Server 2016, use the native Windows configurable options for NIC teaming, link aggregation, and VLAN configuration.*

The U-Series Appliance has a Broadcom NetXreme II four-port network interface card. Work with your network administrator before you configure NIC teaming or aggregation. Your administrator must provide IP address information for the environment where the U-Series Appliance is being deployed.

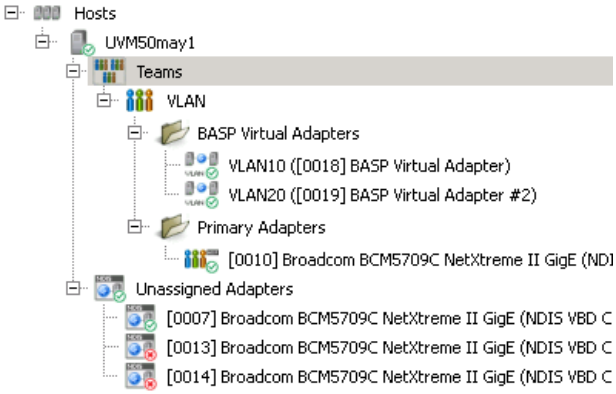
Configure VLAN

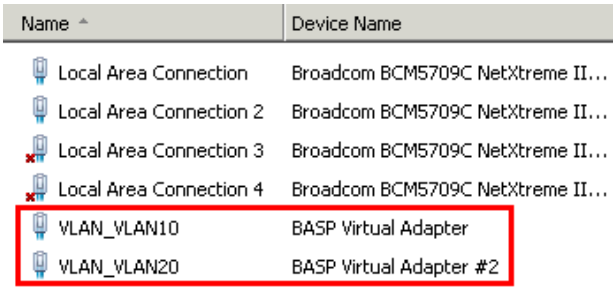
Tagged VLAN Configuration on a Physical U-Series 20 or U-Series 50

Broadcom BCM5709C NetXtreme II GigE

> ***Note:*** *You must have the Broadcom management utility installed before continuing with these steps. On Microsoft Windows Server 2012 R2 U-Series Appliances, the* ***Broadcom Advanced Control Suite 4*** *application is already installed. For Windows 2008 R2 U-Series Appliances, please contact BeyondTrust Technical Support to get the installer file. For Windows Server 2016, use the native Windows configurable options for NIC teaming, link aggregation, and VLAN configuration.*

1. Run **Broadcom Advanced Control Suite 4** from the **Start** menu.
2. Filter by **Team View** from the top menu.
3. Under **Unassigned Adapters**, select the adapter being used. If connected, it will have a green check mark.
4. Right-click and select **Create a VLAN**, then click **Next**.
    a. Enter a **Team Name** (such as **VLAN**) and a **VLAN Name** (such as **VLAN10**), then click **Next**.
    b. Select **Tagged**, then click **Next**.
    c. Enter a **VLAN Tag** (such as **10**), then click **Next**.
5. Click **Finish**.
6. Click **Yes** to acknowledge that there may be a temporary network interruption.
7. Right-click on the team that was created from the previous step and click **Add VLAN**.
    a. Enter a **VLAN Name** (such as **VLAN20**), then click **Next**.
    b. Select **Tagged**, then click **Next**.
    c. Enter a **VLAN Tag** (such as **20**), then click **Next**.
8. Click **Yes** to add more VLANs and repeat, or click **No** if finished.
9. Click **Finish**.
10. Network configuration can be static or dynamic depending on your needs or on the environment. Both are configured just as a normal adapter is configured.

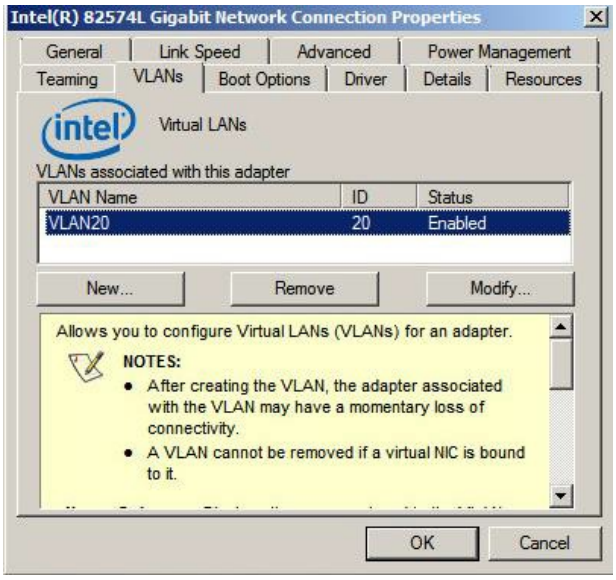




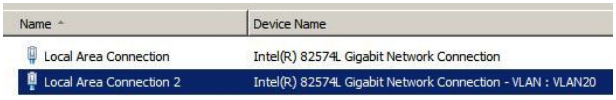
Virtual Guest Tagging (VGT) VLAN Configuration on a U-Series v20

Intel 82574L Gigabit Network Connection (Intel E1000)

1. You must install the required driver within a Windows 2012 R2 guest operating system.
    a. Download **ProWinx64** from Intel at https://www.intel.com/content/www/us/en/download/17480/23073/intel-network-adapter-driver-for-windows-server-2012-r2.html, then extract the contents to a temporary folder.
    b. Right-click the network adapter and click **Update Driver Software**.
    c. Click **Browse my computer for driver software**.
    d. Click **Let me pick from a list of device drivers on my computer**.
    e. Click **Have Disk**.
    f. Click **Browse**, then browse to the temporary location where you extracted the driver files.
    g. Click **Next** to install the driver.
2. Repeat the above steps for each network adapter you have for the virtual machine.
3. After all the adapters are updated, run the **ProWinx64.exe** file, rather than extracting it. You should now be able to install the Advanced Network Services VLANs.
4. To configure VLAN tagging on a virtual machine:
    a. Open **Device Manager**.
    b. Right-click **Network Adapter** and select **Properties**. A **VLANs** tab is now available. This is not displayed before the **ProWinx64.exe** file is installed.
    c. Click **New**.
    d. Enter a **VLAN ID** (such as **10**).
    e. Enter a **VLAN Name** (such as **VLAN10**).
    f. Click **OK**.
5. Repeat these steps for as many VLANs as are required.



6. There will now be a new network adapter displayed under **Network Connections** for each VLAN created.
7. Network configuration can be static or dynamic depending on your needs or on the environment. Both are configured just as a normal adapter is configured.



Upgrade the U-Series Appliance Software

There are two upgrade options available, depending on your environment:

- Active / passive upgrade
- Active / active upgrade

High Availability with Database and Services Synchronization - Active / Passive Upgrade

Keep the following in mind when running an upgrade:

- Do not turn high availability OFF while doing upgrades.
- Any time an installer or login page for the U-Series Appliance recommends to reboot after installation, reboot before continuing.

Package Dependencies

- U-Series Appliance software 3.2.6 and later require .NET Core 3.1.
- The .NET Core installer is included in both 2012 Supporting software and 2016 Supporting software version 210201.
- 2016 and 2012 Environment or Supporting Software packages often depend on a version of Security Update Package Installer (SUPI). It is best to upgrade SUPI to the latest version prior to upgrading the U-Series Appliance software.
- To determine the BeyondInsight upgrade path, visit the BeyondInsight release notes website: https://www.beyondtrust.com/docs/release-notes/beyondinsight-password-safe/index.htm

Start the Upgrade

1. Log on to the active U-Series Appliance.
2. Go to the **Backup** page in the Maintenance application and run a backup. This backs up settings and the database.
3. Go to the **High Availability** page and click **Suspend** to prevent failover while upgrades are running.
4. Download **Software and Security** updates using BeyondTrust Updater. Open a case with BeyondTrust Technical Support if you need links to any software not available through BeyondTrust Updater or the Customer Portal.
5. Unlock **Security Update** packages and installer subscriptions in BeyondTrust Updater:
    - Security Patches for Windows Server 2012/2016
    - Security Patches for SQL 2014/2016
    - U-Series 2012/2016 Environment
    - U-Series 2012/2016 Supporting Software
    - Security Update Package Installer
6. Click **Update Now** to download all security packages.
7. If one download stops and another does not start, click **Update Now** again until all are complete.
8. Apply security updates downloaded in step 4.
    - Log in to the **Maintenance** page; the **BeyondTrust Updates** page loads first.
    - Click **View Updates**.
    - Schedule updates. This provides two options, either to schedule now or at a later date and time.

    - If any new packages are downloaded after the schedule is made they are NOT included.
    - Updates are almost always required and the process resumes without intervention until all packages are installed.
    - Service may become unresponsive during the installation of updates.
    - Progress can also be viewed from this page.
9. Download and install the remaining products from BeyondTrust Updater.
    - Settings in BeyondTrust Updater allow you to configure specific hours to download and install packages.
10. Log in to the passive U-Series Appliance and repeat steps 2 through 7.
    - There is no need to perform a backup, because all the settings are still on the active U-Series Appliance.
    - The database is not accessible on the secondary U-Series Appliance. This is expected, due to SQL mirroring.
11. If needed, set the lock status on the **Subscriptions** page again.
12. Verify applications were upgraded.
13. Log in to the **High Availability** page, click **Resume**, and verify database state returns to synchronized.

High Availability with Services Only Synchronization - Active / Active Upgrade

Keep the following in mind when running an upgrade:

- Do not turn high availability OFF while performing upgrades.
- Any time an installer or login page for the U-Series Appliance recommends to reboot after installation, reboot before continuing.

Package Dependencies

- U-Series Appliance software 3.2.6 and later versions require .NET Core 3.1.
- The .NET Core installer is included in both 2012 Supporting Software and 2016 Supporting software version 210201.
- 2016 and 2012 Environment or Supporting Software packages often depend on a version of SUPI, so it is best to upgrade SUPI to the latest version prior to upgrading the U-Series Appliance software
- To determine the BeyondInsight upgrade path, visit the BeyondInsight release notes website: https://www.beyondtrust.com/docs/release-notes/beyondinsight-password-safe/index.htm

Start the Upgrade

1. Go to the **Backup** page in the Maintenance application and run a backup. This backs up settings but NOT any remote databases.
2. Download **Software and Security** updates using BeyondTrust Updater. Open a case with BeyondTrust Technical Support if you need links to any software not available through BeyondTrust Updater or the Customer Portal.
3. Unlock **Security Update** packages and installer subscriptions in BeyondTrust Updater:
    - Security Patches for Windows Server 2012/2016
    - Security Patches for SQL 2014/2016 (may not be subscribed if SQL Server is not installed)
    - U-Series 2012/2016 Environment
    - U-Series 2012/2016 Supporting Software
    - Security Update Package Installer
4. Click **Update Now** to download all security packages.
5. If one download stops and another does not start, then click **Update Now** again until all are complete.

6. Apply security updates downloaded in step 4:
    - Log in to the **Maintenance** page. The **BeyondTrust Updates** page loads first.
    - Click **View Updates**.
    - Schedule Updates. This provides two options, either to schedule now or at a later date and time.
        - New packages downloaded after the schedule is set are NOT included.
        - Updates are almost always required and the process resumes without intervention until all packages are installed.
        - Service may become unresponsive during the installation of updates.
        - Progress can also be viewed from this page.
7. Download and install the remaining products from BeyondTrust Updater.
    - Settings in BeyondTrust Updater allow you to configure specific hours to download and install packages.
8. Log in to the passive U-Series Appliance and repeat steps 2 through 7.
    - There is no need to perform a backup, because all the settings are still on the active U-Series Appliance.
    - The database is not accessible on the secondary U-Series Appliance. This is expected, due to SQL mirroring.
9. If needed, set the lock status on the **Subscriptions** page again.
10. Verify applications were upgraded.
11. Log in to the **High Availability** page for both active or passive U-Series Appliance and confirm the state is correct (for example, active or passive).
12. If there are other Password Safe worker nodes pointing at the remote database, then those BeyondInsight installations also need to be upgraded.

Troubleshoot Issues with U-Series Appliance

Break Glass for the Local Administrator Account

This is the local administrator account you use as the appliance logon account. By default, the account name is **btadmin**, but you might have changed the account name during the appliance configuration.

Issue: There is a database issue where you cannot access the user account through BeyondInsight or Password Safe.

Solution: Open a ticket with BeyondTrust Technical Support for the emergency access procedure which allows a password change, so that you can connect to the appliance via RDP.

Issue: The local administrator account is locked out due to too many logon attempts.

Solution: Wait 20 minutes for the policy to unlock the locked account.