BeyondTrust

U-Series Appliance 4.2
Administration Guide

TC:6/28/2024

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 the image (if it is a virtual appliance).

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 Deployment & 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 Deployment & Configuration Wizard.
   - **Password:** The administrator password created using the Deployment & 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: **Home (Dashboard)**, **Network**, **Integrations**, **Features and Services**, **Software and Licensing**, **Business Continuity**, and **Security and Compliance**. The session timeout value cannot be configured.*

4. The U-Series Appliance **Home (Dashboard)** 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.

***Tip:** Users with sufficient permissions, have the option to log in to the U-Series Appliance directly from the **Assets** grid in BeyondInsight. For more information, please 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** grid.*

Request Product Updates

1. From the left menu, under **Software and Licensing**, click **Installed Software**.
2. From the **Installed Software** page, you can view a list of all the software and their versions that is installed on this appliance.
3. If any of your updates failed, click the **BeyondTrust Updater** link above the list of products to be taken to the BT Updater site where you can retry downloading the update.

Manage 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 Security 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. From the left menu, under **Software and Licensing**, click **Security Updates**.
2. To see information about updates, click the vertical ellipsis for an appliance, and then select **Security Update Details** from the menu. 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 either **Appliance Time Zone** or **Browser Time Zone** to run the update.
7. Set the **Date** and **TIme**.

Note: *The browser time zone is the local time of the administrator running the U-Series Appliance 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 8.

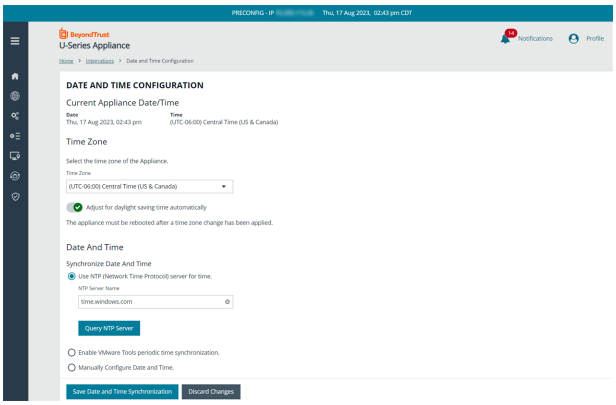
View Update History for Security Updates

1. From the left menu, under **Software and Licensing**, click **Security Updates**.
2. Click the vertical ellipsis for an appliance, and then select **Security Update History** from the menu. The page displays the historical records of previously applied patches. The list is organized by the types of packages (subscriptions).

Configure U-Series Appliance General Settings

Adjust Date and Time Settings

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



1. From the left menu, under **Integrations**, click **Date and Time Configuration**.
2. Select the **Time Zone** for the appliance.
3. By default, the **Adjust for daylight savings time automatically** setting is enabled. If you don't want the time to be adjusted automatically for daylight savings, click the toggle to disable this option.
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 settings and preferences, as follows:

1. At the top right of the console, click **Profile**.
2. Click **Change Email** to change the email account associated with the current logged in user account.
3. Under **Preferences**, use the dropdowns 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 available only if working on a physical (hardware) appliance.*

1. From the left menu, under **Security and Compliance**, click **LCD Panel**.
2. 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.

3. Click **Update LCD Panel Settings**.

Configure Pre-login Banner Settings

The pre-login banner displays a message to any user who attempts to log in to the appliance software. The pre-login message banner is useful for enforcing security or compliance policy; for example, to inform the user all activities are logged.

1. From the left menu, under **Security and Compliance**, click **Pre-login Banner**.
2. Click the toggle to enable the **Pre-login Banner** option.
3. Enter a title and message you want to appear before the login credentials page is displayed to the user.
4. Click Update **Pre-Login 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 and Upload a Crypto Key

1. From the left menu, under **Security and Compliance**, click **Data Encryption Key**.
2. To download a crypto key:
    - Under **Download Crypto Key Options**, create an encryption password and confirm it.
    - Click **Export and Download Crypto Key**. The crypto key zip file is created and downloaded to your system.
3. To upload a crypto key:
    - Under **Upload Crypto Key Options**, enter the encryption password.
    - Drag and drop the crypto key zip file into the drop area or click the button to browse to the zip file.
    - Click **Generate Uploaded Crypto Key**.

Check FIPS Compliance

Federated Information Processing Standard (FIPS) is a US and Canadian government standard that defines a minimum set of security requirements for cryptographic systems. Enabling **FIPS Mode** in your local computer policy enforces Windows to use FIPS compliant algorithms for encryption, hashing, and signing.

To enable FIPS Mode, take the following steps:

1. From the left menu, under **Security and Compliance**, click **Local Computer Policy**.
2. Expand the **FIPS Compliance** section.
3. Click the toggle to enable **FIPS Mode**.
4. Click **Update FIPS Settings**.
5. You must reboot the U-Series Appliance for this setting to take effect.

Manage the U-Series Appliance API Key

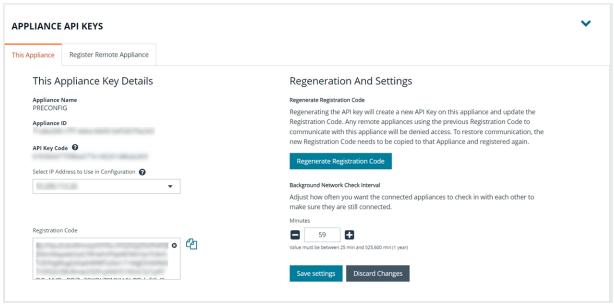
The U-Series Appliance API manages the communication between U-Series Appliances when high availability is used in your environment. The API key enables U-Series Appliances to communicate with each other.

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 are denied access until the new registration code is copied to that appliance and registered again.*

To view this appliance's key details:

1. From the left menu, under **Integrations**, click **Appliance API Keys**.
2. From **This Appliance** tab, you can view the API key details for this appliance in the **This Appliance Key Details** section.
3. To view the registration code:
    - Select the IP address the remote appliance uses to communicate with this appliance from the **Select IP Address to Use in Configuration** list.
    - The registration code displays in the **Registration Code** box. Click the **Copy** button next to the box to copy the code.



4. To create a new API key:
    - Under **Regeneration And Settings**, click **Regenerate Registration Code**.
    - Follow step 3 to view and copy the new registration code.

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. From the left menu, under **Integrations**, click **Appliance API Keys**.
3. Click the **Register Remote Appliance** tab.
4. Add the registration code from the appliance that you want to link to this appliance into the **Registration Code from Remote Appliance** box.
5. Optionally, enter a short **Description** for the appliance being registered.
6. Click **Register Remote Appliance**.
7. Click the **This Appliance** tab.
8. Select an IP from the **Select IP Address to Use in Configuration** dropdown.
9. Click the **Copy** button to the right of the **Registration Code** box.
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. Optionally, 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** grid at the bottom of the page. To refresh that list at any time, click the **Refresh** button at the top right of the table.

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

Set the Background Network Check Interval

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

1. On the **This Appliance** tab, under 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. From the left menu, under **Security and Compliance**, click **Client Connections**.
2. Under **Event Service Security**, click the toggle to enable or disable the **SSL (Secure Socket Layer) and Client Certificate Authentication Required** option.

IMPORTANT!

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

Generate and Export Certificates

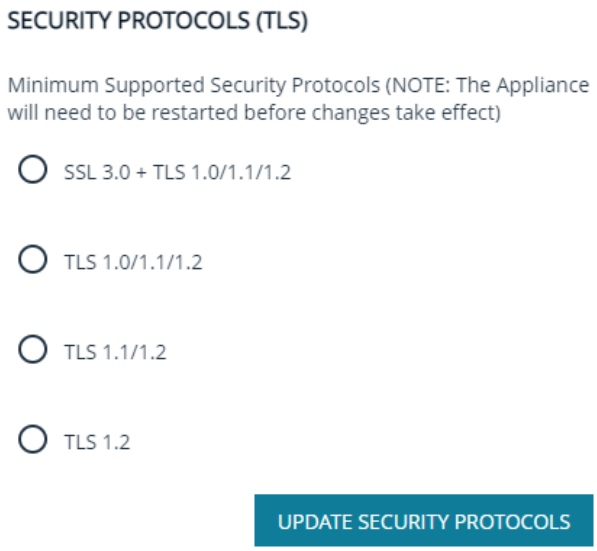
1. From the left menu, under **Security and Compliance**, click **Certificate Management**.
2. To regenerate the SSL certificate to match the U-Series Appliance network name, under **Generate SSL Certificate**, click **Generate Certificate**.

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

3. To export the client certificate, under **Export Certificate**, enter and confirm the password for the certificate, and then click **Export and Download Certificate**.

Set a Security Protocol

1. From the left menu, under **Security and Compliance**, click **Security Protocols**.
2. Under **Security Protocols**, select the security protocol that applies to your environment.
3. Click **Update Security Protocols**.



Turn On HSTS

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

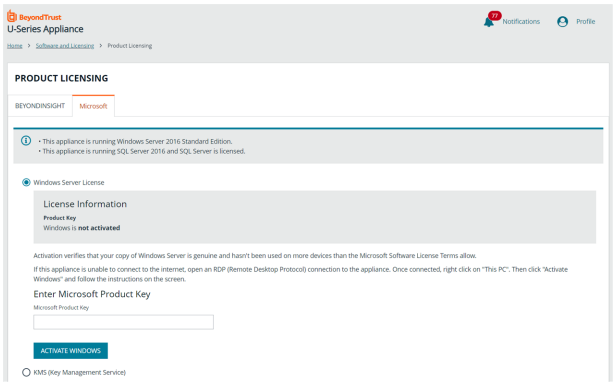
1. From the left menu, under **Security and Compliance**, click **Client Connections**.
2. Under **HSTS ()**, toggle the option to enable it.

Manage Licensing and Admin Accounts in the U-Series Appliance

Activate Windows

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

1. From the left menu, under **Software and Licensing**, click **Product Licensing**.
2. Click the **Microsoft** tab.
3. By default, **Windows Server License** is selected.
    - If licensed, the license information is displayed.
    - If not licensed, enter a **Microsoft Product Key**, and then click **Activate Windows**.
    - If this appliance is unable to connect to the internet (for example, in an air-gap environment), you must perform the activation by phone, as follows:
        - Open an RDP connection to the appliance
        - Once connected, right-click **This PC**, and then click **Activate Windows**.
        - Follow the instructions on the screen.



> ***Note:*** *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).

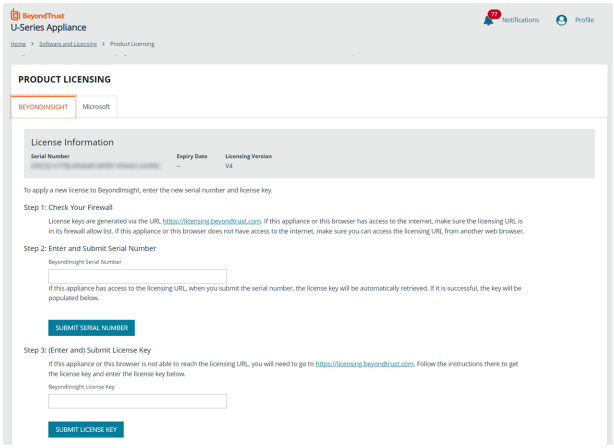
To activate your volume license key:

1. From the left menu, under **Software and Licensing**, click **Product Licensing**.
2. Click the **Microsoft** tab, and select the **KMS (Key Management Service)** option, which displays two fields to complete.
3. Enter your **Volume License Key**.
4. Enter the **KMS (Key Management Service)** 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/.*

Manage BeyondInsight Licensing

You can view the license information for the BeyondInsight products from the **Product Licensing** page, as follows:



1. From the left menu, under **Software and Licensing**, click **Product Licensing**.
2. Click the **BeyondInsight** tab.
3. If licensed, the license information is displayed. If not licensed yet or to apply a new license, continue with the following steps.
4. 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.
5. 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.
    - 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 and enter the **BeyondInsight License Key**.
6. Click **Submit License Key**.

View Installed Software

You can view the list of all software and their versions installed on the U-Series Appliance on the **Installed Software** page.

To view installed software:

From the left menu, under **Software and Licensing**, click **Installed Software**.

Change Administrator Password

IMPORTANT!

*While it is possible to change the administrator username, 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 update the passwords for the following administrator credentials:

- U-Series Appliance administrator
- BeyondInsight administrator
- BeyondTrust Updater administrator.

Make sure you review the password complexity requirements for each credential type.

1. From the left sidebar, click **Security and Compliance**.
2. Click the **Account Management** card.
3. Click the down arrow to expand the section for the credential you wish to update.
4. Change the password.
5. Click **Update Credentials**.

Note: *If changing the U-Series Appliance administrator username or password, you must log out and log back in to the appliance.*

Note: *Support for login via RADIUS has been deprecated as of the U-Series Appliance 4.1 release.*

Configure Network and RDP Settings

The below sections detail how to configure the following network settings for your U-Series Appliance:

- Enable remote desktop protocol (RDP) and multi-factor authentication to gain access to your appliance.
- Configure IP settings for your appliance's network adapter.
- Configure proxy server settings for your appliance.
- Set Background Intelligent Transfer Service (BITS) throttle speed

Enable RDP and Console Access

RDP and console access is disabled by default as a security measure. RDP access is not required for daily use, regardless of licensing or feautures. BeyondTrust Technical Support can enable RDP access for troubleshooting. RDP and multi-factor activities are tracked with audit log entries in the Security event logs.

> ***Note:*** *When multi-factor authentication is enabled, an activation code from BeyondTrust Technical Support is required to enable RDP and appliance console access. RDP and console access reverts back to being disabled after a 4 hours.*

1. From the left sidebar, click **Network**.
2. Click the **RDP and Console Access** card.
3. Click the toggle for the **Enable RDP and Appliance Console Access** option to turn it on.
4. Click the **Advanced Options** tab.
5. Click the toggle for the **Multi-factor Authentication** option to enable the settings for two-factor authentication when using remote desktop.
6. Click **Activate Multi-factor Authentication**.

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

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. From the left sidebar, click **Network**.
2. Click the **IP Settings** card.
3. Select a network card from the list.
4. Click the toggle for the **Obtain IP address automatically (DHCP)** option to enable it, 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**.

Set Email SMTP Server Settings

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, when offline for maintenance). To ensure consistent SMTP access, appliance SMTP settings can also be configured.

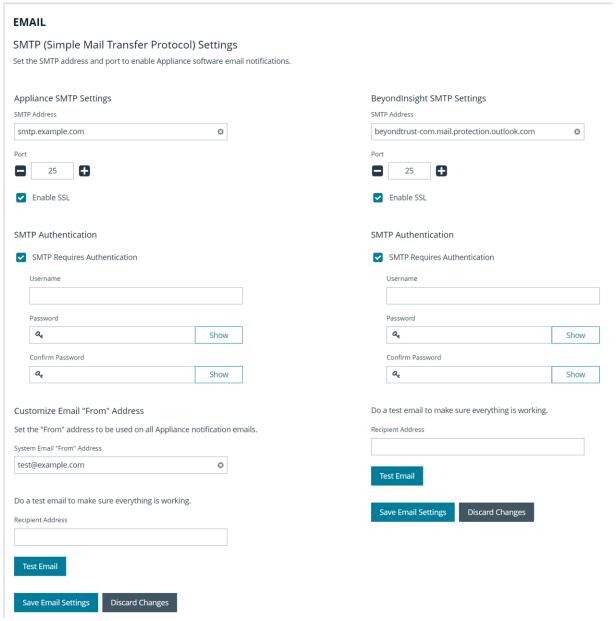
Set the U-Series Appliance and BeyondInsight SMTP addresses and ports to enable the appliance software email notifications.

To configure the email settings, from the left menu, under **Integrations**, click **Email** and then follow the below steps.

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, and enter credentials.
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, and enter credentials.
5. Type in a **Recipient Address** test email you can use to verify that the notifications are working.
6. Click **Test Email**. Verify the recipient email address you used for reception of the notification.
7. After a successful test, at the bottom of the **BeyondInsight SMTP Settings**, click **Save Email Settings**.

Configure Proxy Settings

You can configure a proxy server for the appliance if one is required for internet access following the below steps. Appliance proxy server settings are synchronized with **Configuration > System > Proxy Settings** in BeyondInsight. Changing this value on the appliance or within BeyondInsight applies to all proxy-enabled features on the appliance, including BeyondTrust Updater.

1. From the left sidebar, click **Network**.
2. Click the **Proxy Server** card.
3. Click the toggle for the **Use proxy server for external communication** option to enable it.
4. Enter the FQDN or IP address for the proxy server.
5. Enter the port number for the proxy server.
6. If the proxy server requires authentication, enter the credentials.
7. Click **Test the Proxy Settings** to ensure a successful connection.
8. Check the **Local proxy override** option to bypass a configured proxy for all addresses that do not contain a period.
9. Click **Save Proxy Settings**.

Manage BITS Throttle Speed

Background Intelligent Transfer Service (BITS) facilitates the transfer of files between computers using idle network bandwidth. On the appliance, BITS is used to transfer the database when pairing high availability partners and may also be used to transfer session recording files to an archive location. This setting limits the network bandwidth that BITS uses for background transfers. If you do not configure this setting, BITS uses all available unused bandwidth for background transfers.

1. From the left menu, under **Network**, click **BITS**.
2. Enter the throttle speed in Kbps.
3. Click **Save Throttle Speed**.

Manage U-Series Appliance Health

From the **Home** page, you can view a dashboard to help you understand performance metrics, and keep track of services and hardware faults, for your U-Series Appliance. You can also view and export historical data and access links to navigate to other configuration areas in your appliance.

Monitor the Health Dashboard

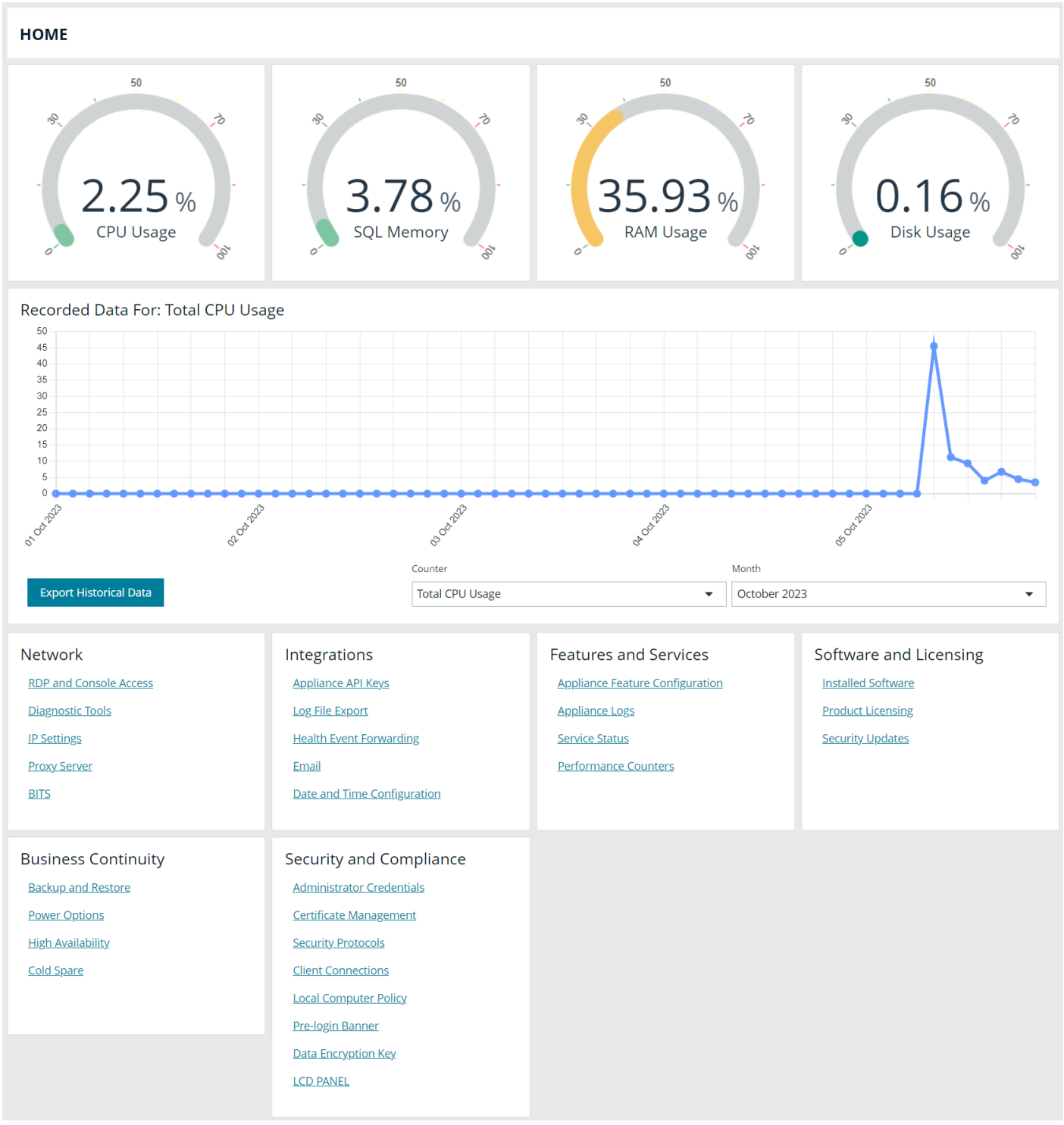
View dynamic, real-time U-Series Appliance metrics, including:

- CPU usage
- SQL Server memory usage
- RAM usage
- SQL Server CPU usage
- Used disk space on the C: drive

You can also view recorded data by month by using the **Counter** and **Month** dropdown lists. You can view data for:

- Total CPU Usage
- SQL Memory Usage
- SQL CPU Usage Percentage
- Disk Free Percentage (C Drive)
- RAM Usage

To download the above information, click the **Export Historical Data** button.



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 features 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.

Enable Service Alerts

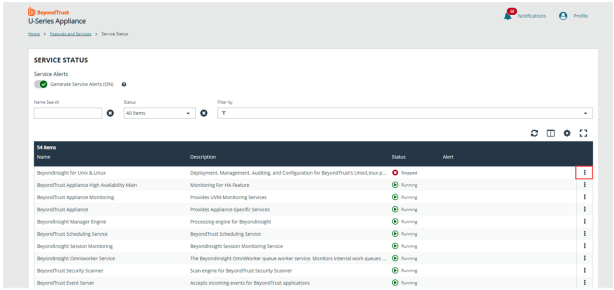
Turning service alerts on determines whether or not to generate alerts that might be emailed to an administrator or forwarded to BeyondInsight. Enable service alerts as follows:

1. From the left menu, under **Features and Services**, click **Service Status**.
2. Toggle the **Generate Service Alerts** switch to **ON**.

Check Services

You can manage U-Series Appliance services, as follows:

1. From the left menu, under **Features and Services**, click **Service Status**.
2. Click the vertical ellipsis to the right of the service:
    - Select **Start** to start a stopped service
    - Select **Stop** or **Restart** to restart a running service.



Configure Counters for Performance Metrics

You can configure the threshold values for performance metrics. When the threshold is exceeded, email alerts are sent to the email accounts configured on the **Configure 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. From the left menu, under **Features and Services**, click **Performance Counters**.
2. Select notification settings:
    - **Generate Alerts When The Average Value Of A Counter Exceeds Its Configured Threshold:** Turns on email notification for alerts.
    - **Generate Daily Summaries of Performance Data For Base Counters:** Collects performance metrics every two hours and emails them on a daily basis.
3. By default, the following five base counters are enabled. You may enable additional counters by checking the box next to the counter:
    - **CPU Overall Usage**
    - **RAM Usage**
    - **SQL Server CPU Usage**
    - **SQL Server Memory %**
    - **Disk % Used**
4. Adjust the performance and reset thresholds.
5. Click **Apply Settings**.

Configure Notifications

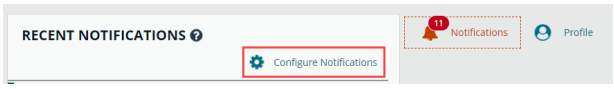
You can set notifications for the following types of events:

- **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.
- **General:** Includes Windows Defender alerts, RDP change of state notifications, license evaluation expiry reminders, SUPI successful and failed installs, scheduled reboot reminders and errors, and successful and failed user logon attempts.

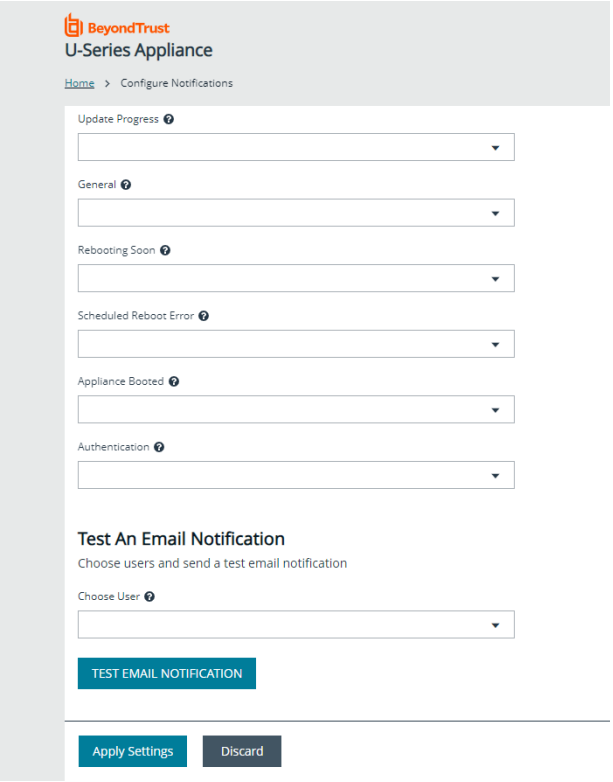
> ***Note:*** *In the event of a large number of successful or failed logon events, not all events send notifications. However, all System Security events can be found from the* ***Appliance Logs*** *page, listed as* ***Windows System Security Event Log*** *items in the grid.*

To configure email notifications:

1. At the top right of the console, click **Notifications**, and then click **Configure Notifications**.



2. For each event type, click the dropdown list to select the users who you want to receive notifications.
3. Click **Apply Settings**.
4. To **Test an Email Notification**, select one or more users from the dropdown list, and then click **Test Email Notification**.



Set Up Health Event Forwarding

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.

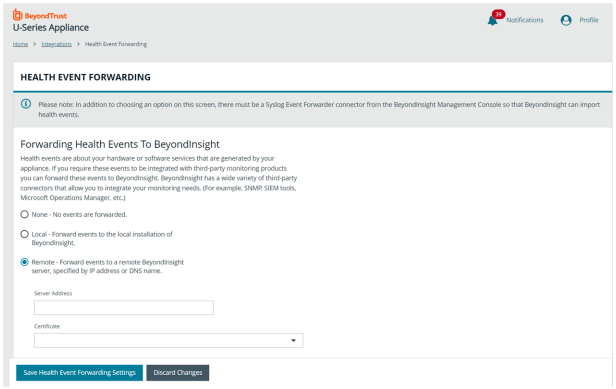
BeyondInsight has a wide variety of third-party connectors that allow you to integrate your monitoring needs (for example, SNMP, SIEM tools, Microsoft Operations Manager, etc.).

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

To set up health event forwarding:

1. From the left menu, under **Integrations**, click **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.

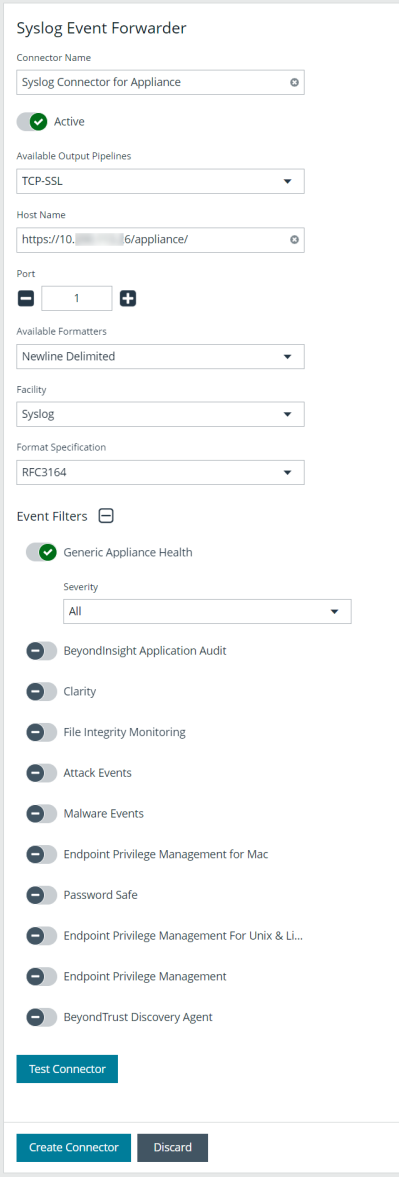


    - From the left menu, under **Security and Compliance**, click **Certificate Management**.
    - Under **Export Certificate**, enter a password and confirm it, and then click **Export and Download Certificate**.
    - Import the certificate on the local U-Series Appliance, as follows:
        - From the left menu, under **Security and Compliance**, click **Certificate Management**.
        - Upload the certificate by dragging the file into the drag and drop box, and entering the password created in the previous step.
    - 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, as follows:

1. Log in to BeyondInsight.
2. Navigate to **Configuration > General > Connectors**.
3. Click **Create New Connector +**.
4. Enter a **Connector Name**.
5. Select **Syslog Event Forwarder** from the **Connector Type** dropdown.
6. Click **Create Connector**.

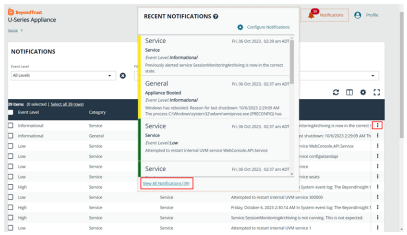
7. Enter the details for the U-Series Appliance, including IP address, protocol, and facility.
8. Expand the **Event Filters** section.
9. Toggle the **General Appliance Health** filter to enable it.
10. By default, all severity levels are included. You may select an alternate level if needed.
11. Click **Create Connector**.



For more information on importing a certificate to the U-Series Appliance, please see "Upload SSL Certificate" on page 33.

View Notifications

After notifications are received, a red number indicates the number of notifications. Click **Notifications** to view the 10 most recent notifications.



> ***Note:*** *The red notification number indicates the number of notifications in total, and not the number of unread notifications.*

The bar next to the notification indicates severity.

Color Legend

	Info
	Low
	Medium
	High

Click the **View All Notifications** link at the bottom of the **Recent Notifications** window to be taken to the **Notifications** grid where all notifications are listed.

To view more details about a notification, click the vertical ellipsis for the notification and then select **Notification Details**.

To delete an individual notification, by click the vertical ellipsis to the right of the notification and then select **Delete Notification**.

To delete multiple notifications or all notifications, select them in the grid or click **Select all x rows** at the top of the grid, and then click **Delete Notification** above the grid.

Diagnose Network Connectivity Issues

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

1. From the left menu, under **Network**, click **Diagnostic Tools**.
2. To ping a server:
    - Select **Ping Command**.
    - Enter the fully qualified domain name, hostname, or IP address in the **Server Address** field.
    - Click **Get Results**.
3. Select **Network Configuration** to view the results from **IPConfig /all**.

Download Log Files

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

Download Individual Log Files

To download individual log files:

1. From the left menu, under **Features and Services**, click **Appliance Logs**.
2. At the right of a log entry, click the **Download Log** button.

Download All Log Files

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

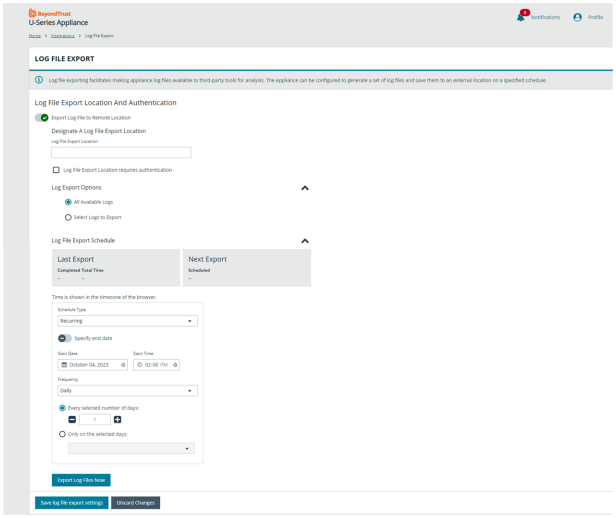
To download all log files:

1. On the sidebar menu, under **Features and Services**, select **Appliance Logs**.
2. At the top right of the log entries list, click the **Download All** icon.

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. From the left menu, under **Integrations**, click **Log File Export**.
2. Toggle the **Export Log File to Remote Location** switch to enable it.
3. Enter a **Log File Export Location**.
4. 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**.
5. Expand the **Log Export Options** section.
    - Click **All Available Logs** to export everything.
    - Click **Select Logs to Export** to export individually checked logs.

6. Expand the **Log File Export Schedule** section.
    - If using the default **Recurring** option:
        - Enter the **Start Date** and **Start Time**, and then select the **Frequency** from the dropdown list.
        - If required, toggle the **Specify end date** option to set an end date and time.
        - Select additional options based on the frequency of the export.
    - Select **Immediate** for an immediate export. Click the **Export Log Files Now** button.
    - Select **One Time** for a single export. Set the **Start Date** and **Start Time**.
    - Click **Save Log File Export Settings**.

Configure U-Series Appliance Features

From the **Features and Services > Appliance Feature Configuration** page, you can select U-Series Appliance features if you are deploying more than one U-Series Appliance to scale BeyondInsight in larger networks. Features must be selected for at least one of the U-Series Appliances.

The features are listed as read-only initially. Click **Change Configuration** to enable to ability to turn features on and off and configure feature settings where applicable.

> ***Note:*** *When you turn features on and off, any dependencies or conflicts that exist between features are displayed. The* ***Save Configuration*** *button is available only after dependencies and conflicts are resolved.*

Feature Descriptions

BeyondInsight Management Web Console

The BeyondInsight Management Web Console is a web application where administrative users can log in, view dashboards, manage assets, create and configure Smart Rules, and make most configuration changes.

BeyondInsight Manager Engine

This is the processor for BeyondInsight. Enabling this, enables BeyondInsight Management Web Console, BeyondInsight Omniworker Service, BeyondInsight Database Access, and SQL Server Database, if they are not already enabled.

BeyondInsight Omniworker Service

The BeyondInsight Omniworker is a worker node that manages task queues. It processes background tasks involved in the operation of BeyondInsight and Password Safe, including the regularly scheduled rotation of passwords. Turn on this service when your environment uses more than one U-Series Appliance. Adding worker nodes allows your solution to scale up to meet the demands of your organization.

BeyondInsight Database Access

BeyondInsight Database Access is a foundation on which many other features rely. Turning off BeyondInsight Database Access also turns off BeyondInsight Event Collector, BeyondInsight Omniworker Service, BeyondInsight Management Web Console, and Password Safe Web Portal, when they are on.

This feature provides the settings for the locally installed software products to connect to the BeyondInsight database. Depending on your solution architecture, you may be using a local database, a remote database on another appliance, a SQL Server Always-On Availability Group, or an Azure SQL Cloud Database.

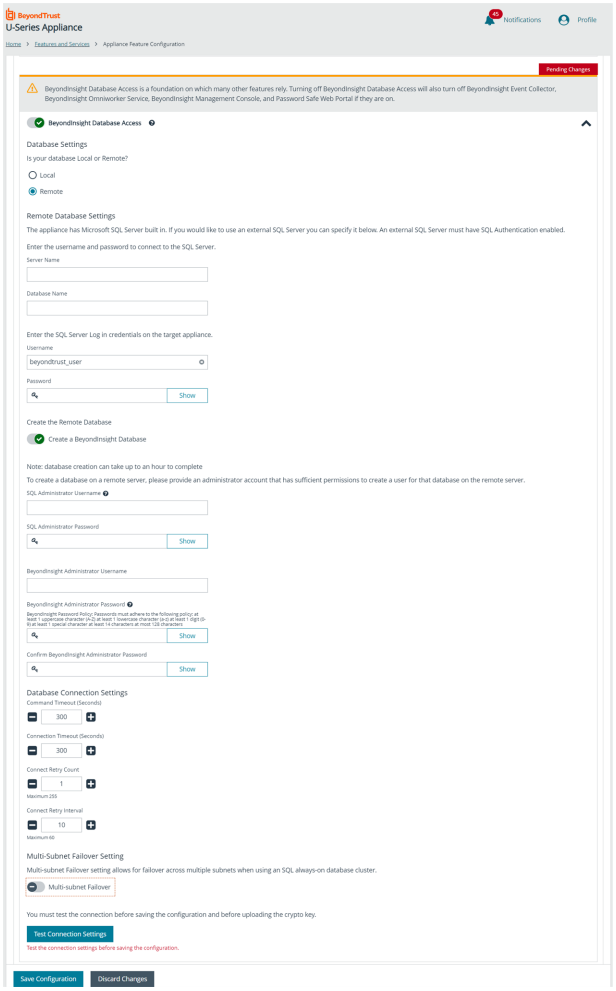
When configuring a local database, select an authentication method. When you select SQL Server Authentication, **SQL Server Username** is populated with the same user name used in the U-Series Appliance Deployment & Configuration wizard during your initial appliance setup. The account is created with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

To create a new remote BeyondInsight database:

1. Click the **Remote** option for **Database Settings**.
2. If using an external SQL Server:
    - Enter the IP address for **Server Name** and provide the **Database Name**.
    - Enter the username and password to connect to the SQL Server. An external SQL Server must have SQL Authentication enabled.
3. Click the toggle to enable the **Create a BeyondInsight Database** option in the **Create the Remote Database** section.
4. Enter SQL Administrator username and password. This credential must have sufficient permissions to create a database and to create a user for that database.
5. Enter the BeyondInsight Administrator username and password.
6. Leave the default **Database Connection Settings**, or update these if required.
7. Click the toggle to enable the **Multi-subnet Failover** setting. Multi-subnet failover allows for failover across multiple subnets when using an SQL always-on database cluster.
8. To ensure a connection to the database server can be established, click **Test Connection**.
9. Click **Save Configuration**.



***Note:** Database creation can take up to an hour to complete.*

For more information, please see the following:

- *"Download and Upload a Crypto Key" on page 8*
- *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*

BeyondInsight Event Collector

The BeyondInsight Event Collector is responsible for forwarding information gathered from scanners and endpoint protection agents, and forwarding policy for BeyondTrust integrations.

To enable the BeyondInsight Event Collector feature, 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**.

> ***Note:*** *An event server can be deployed on its own to scale up your solution or to facilitate communication with specific network segments.*

BeyondInsight Unix & Linux

BeyondInsight for Unix & Linux (BIUL) is a web-based tool that you can use to manage software for AD Bridge, Privilege Management for Unix & Linux, Privilege Management for Unix & Linux Basic, and Solr.

Turn on the BeyondInsight Unix & Linux feature to configure a database connection for BeyondInsight for Unix & Linux.

BeyondInsight for Unix & Linux conditionally requires the SQL Server Database feature. Turning on BeyondInsight for Unix & Linux may turn on SQL Server Database if it is not already on. Some configuration may be required.

> ***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 feature 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.

Password Safe Web Portal

The Password Safe web portal is where end users log in to perform tasks, such as making and approving password requests, accessing remote systems and applications, and managing recorded sessions. Additional Password Safe portals can help you reach geographically diverse users, or scale up to serve higher volumes. Turn on this role to activate services needed to run the Password Safe web portal.

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

> ***Note:*** *Turning off **Password Safe Web Portal** also turns off the **Session Monitoring Archive** feature, if it is on.*

Session Monitoring Archive

Session Monitoring Archive allows you to configure the transfer of session monitoring files from this appliance to an external data repository. This prevents filling the local storage.

> ***Note:*** *Session Monitoring Archive requires the Password Safe Web Portal feature. Turning on Session Monitoring Archive turns on Password Safe Web Portal, if it is not already on.*

BeyondTrust Updater

The BeyondTrust Updater Service provides updates for all BeyondTrust managed products. This feature can be disabled for troubleshooting purposes, but otherwise should always be enabled. Specific product updates can be managed by configuring the settings in the BeyondTrust web application. You can click the link to access BeyondTrust Updater Settings.

Privilege Management for Desktops

Configure a connection to Privilege Management for Desktops.

SQL Server Database

This feature controls the local database service, and allows you to enable external access if you are using this appliance as a database server. This feature cannot be enabled on SQL-Free appliances. Check the **TCP/IP Database Connections** option to allow database access from remote computers. If you are using your SQL Server deployment, no action is required.

SQL Server Analysis Services

SQL Server Analysis Services is the analytical data engine behind BeyondInsight Analytics & Reporting. It hosts the data cube (evolution of data over time) and provides data for reports generated by SQL Server Reporting Services.You can click the link to run BeyondInsight Analytics & Reporting.

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

SQL Server Reporting Services

SQL Server Reporting Services is the reporting engine behind BeyondInsight Analytics & Reporting. It generates reports from data in the BeyondInsight database and data processed by SQL Server Analysis Services .If you use BeyondInsightAnalytics & Reporting to render reports, the service must run locally. Turn on this feature to run the service locally when using a remote database.

Endpoint Privilege Management (EPM) Event Collector

The EPM Event Collector processes information gathered from EPM agents. It is dependent on the BeyondInsight Event Collector, which first receives the incoming events and forwards them to the EPM Event Collector for processing. The EPM Event Collector requires the EPM Database Access and BeyondInsight Event Collector features to be enabled, which requires BeyondInsight Database Access.

Endpoint Privilege Management Database Access

Select one of the following options for database settings for EPM:

- **Single Appliance using the Local Database**:
    - Select this option if this is the only appliance in your environment. This option applies the configuration for EPM using the SQL Server configured on this local appliance.

    - Enter SQL credentials for the EPM Event Collector and PMR Report Reader.
- **Multi-node deployment using the Local Database**:
    - Select this option if you have more than one appliance deployed in your environment and SQL Server is configured on this local appliance.
    - Select this local appliance from the **Server Name** dropdown. It must be the FQDN or IP address of this appliance (not localhost).
    - Enter SQL credentials for the EPM Event Collector and PMR Report Reader.
- **Remote Privilege Reporting Database**:
    - Select this option if you have more than one appliance deployed in your environment and the BeyondInsight and EPM databases are on remote SQL Servers. This option saves the connection details to the remote BeyondInsight database.
    - Enter the FQDN or IP address of the remote server where the EPM database exists.
    - The EPM database must already exist on the destination server.
    - Enter the SQL credentials provided by your database administrator to connect to the EPM Event Collector and PMR Report Reader.
    - Test the connection settings.

Privilege Management Reporting

Endpoint Privilege Management Reporting includes a rich set of dashboards and reports designed to simplify the centralized management and auditing of EPM activity throughout the desktop and server estate. This feature is separate from and unrelated to BeyondInsight Analytics & Reporting. This feature requires the EPM Database Access feature.

Endpoint Privilege Management Web Policy Editor

The EPM Web Policy Editor allows you to view, unlock, edit, and lock existing EPM policies, as well as create new policies directly from the BeyondInsight console, eliminating the need to use a standalone policy editor. This feature requires the BeyondInsight Database Access feature.

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 Web Portal** feature.

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 " on page 30.

Upload SSL Certificate

1. From the left menu, under **Security and Compliance**, click **Certificate Management**.
2. Under **Upload Certificate**, drag the certificate file into the drop box or click the box to browse and select a file to upload.
3. Enter the password.
4. To update the bindings in IIS, toggle the **Bind to HTTPS on update** toggle to the on setting.
5. To enable this certificate for multiple U-Series Appliances, toggle the **Use for High Availability** switch to the on setting .
6. Click **Upload Certificate**.

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

1. From the left menu, under **Security and Compliance**, click **Certificate Management**.
2. 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.*

3. To export the client certificate, under **Export Certificate**, enter and confirm the password for the certificate, and then click **Export and Download 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:

- *View Recorded Sessions in the Password Safe Admin Guide at https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/view-recorded-sessions.htm*
- *"Set Up the Repository Host" on page 34*

Set Up the Repository Host

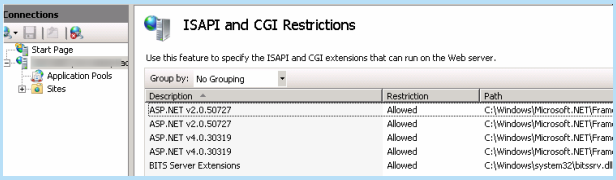
Repository Host Requirements

- Windows 2016 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.

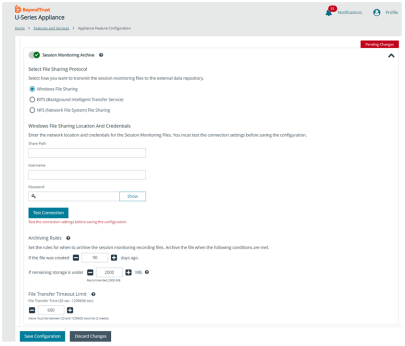
1. Run the repository configuration tool.
2. Click the **Create Certificate** button.
3. Enter a password for the exported certificate.

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. From the left menu, under **Security and Compliance**, click **Certificate Management**.
2. Upload the certificate that you created on the host, and then click **Upload Certificate**.
3. From the left menu, under **Features and Services**, click **Appliance Feature Configuration**.
4. Click the **Change Configuration** button at the bottom of the page.
5. Click the toggle to turn on the **Session Monitoring Archive** feature.
6. Select how you want to transmit the session monitoring files to the external data repository:
    - **Windows File Sharing:** Enter the full path to the share and credentials to access it. Windows file sharing is the preferred method.
    - **BITS (Background Intelligent Transfer Service):** Enter the name of the repository computer and the name of the certificate. These are the same name.
    - **NFS (Network File System) File Sharing:** Enter the full path to the share.
7. Set the rules for when to archive the session monitoring recording files and the time limit for transferring files.
8. Click **Save Configuration** to save the settings.



Use High Availability with U-Series Appliances

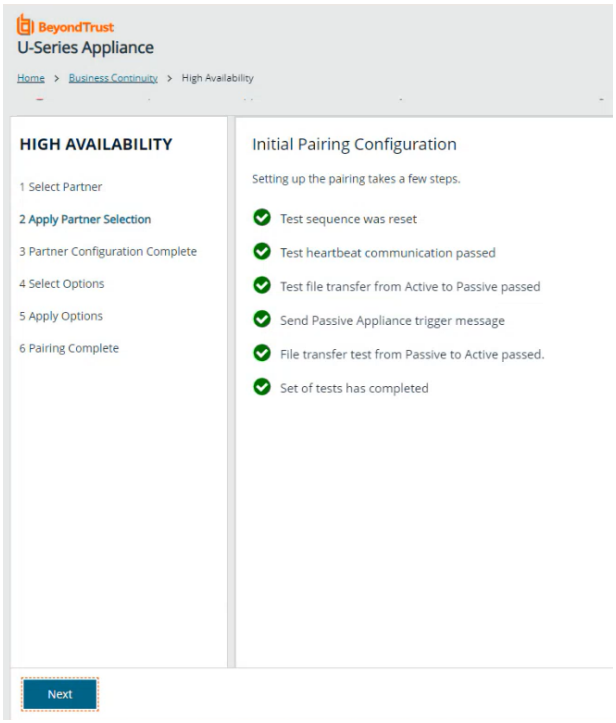
High availability (HA) is designed to work in an active / passive configuration. At any time, one of your two servers has the role of the *active* node, while the other is the *passive* node. When the passive server detects that the active server has failed, then the passive is promoted to active, and the active is demoted. Setting up high availability for your appliances involves the following steps using the High Availability wizard:

- Configuring pairing between your primary appliance and a secondary remote partner appliance.
- Enabling pairing between partner appliances, which overwrites the database on the secondary partner with the primary partner's database.
- Managing the high availability partnership settings and operations once configured and enabled.

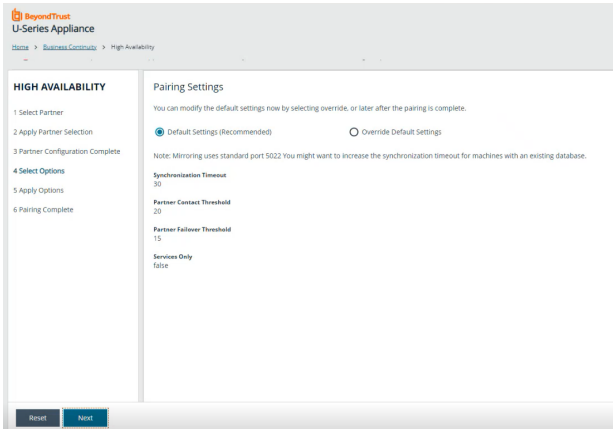
Configure High Availability Using the Wizard

To configure high availability for your appliances using the wizard, follow the below steps:

1. Log in to the U-Series Appliance website on the primary server.
2. From the left menu, under **Business Continuity**, click **High Availability**.
3. Select the remote appliance you want to pair your primary appliance with from the grid. If you need to register a new appliance:
    - Click the **go to Appliance API Keys** link above the grid.
    - Select the **Register Remote Appliance** tab.
    - Paste in the full encrypted registration code value obtained from the remote appliance and provide a description.
    - Click **Register Remote Appliance**.
    - The appliance is now listed in the grid for you to select as a pairing partner.+
4. The pairing process begins and the status of each step involved in the process displays on the screen. Click **Next** once all steps are successful, as indicated by green check marks.

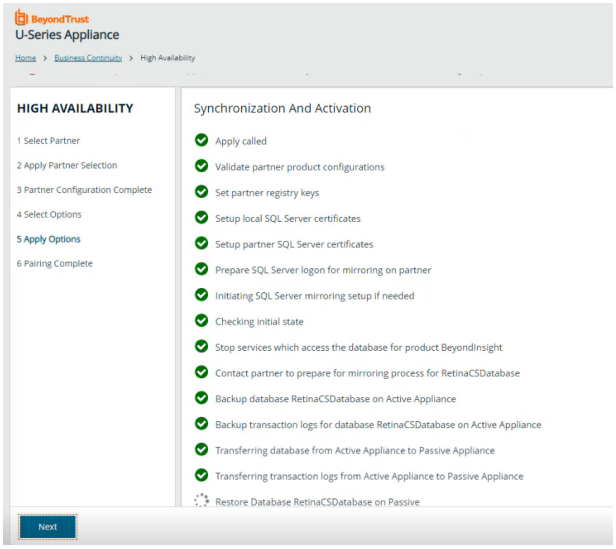


5. On the **Partner Configuration Complete** screen, click **Next** to continue with configuring the settings for the pairing. Alternatively, click **Reset** if you must reverse the pairing and start over.
6. On the **Pairing Settings** screen, we recommend keeping the default settings. Click **Next**.



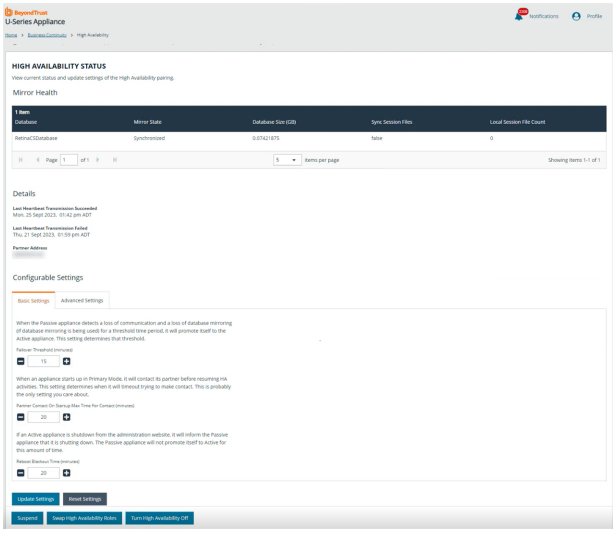
> ***Tip:*** *If the primary and secondary appliances both have SQL, click the* ***Override Default Settings*** *option to select pairing the databases and services, or to pair only services. If either appliance is SQL free, you can only pair services.*

7. Click **Set** on the pop-up message to enable the pairing between partners. This overwrites the database on the secondary appliance with the primary appliance's database.
8. The **Synchronization and Activation** screen displays indicating the status of each step involved in this process. Click **Next** once all steps are successful, as indicated by green check marks.



9. On the **Pairing Complete** screen, click **Next**.

10. You are taken to the **High Availability Status** page where you can:



- View the status of the mirroring between the appliance pairs and heartbeat details. Warning banners display at the top of the page for any of the following conditions:
    - SQL mirroring is configured and one database is not in a synchronized state.
    - The last heartbeat that failed is more recent than the last heartbeat that succeeded.
    - A heartbeat on secondary appliance is more than 4 minutes old.
- Manage basic and advanced settings for the pairing, such as:
    - Changing the failover threshold.
    - Setting max time for contacting a partner on start up.
    - Setting how often the passive appliance emails the administrator when a failover has occurred.
    - Setting how often background settings are synced from the active to the passive partner.
- Manage the operation of the high availability:
    - **Suspend:** You might want to pause mirroring if you want to perform maintenance tasks on the database server. Click **Suspend** to pause mirroring. A failover cannot occur when the database is in a suspended state. Click **Resume** to start mirroring again.
    - **Swap High Availability Roles:** Click this button to change the passive server to the active server. This is useful for testing high availability. Click the button again to restore the server partners to their original roles. Note that data loss can occur if databases are not synchronized.
    - **Turn off High Availability:** Click this button to reset the U-Series Appliances to the initial setup state and 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.

For more information, please see the following:

- *"Manage the U-Series Appliance API Key" on page 8*
- *"Configure Notifications" on page 21*

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.

IMPORTANT!

Medium Availability Mode for High Availability can no longer be configured as of release 4.1. If this was setup, it will continue to work after upgrading to release 4.1, but new deployments do not have this option.

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

From the **High Availability Status** page, verify that the communication between U-Series Appliances is active. The **Mirror State** should show as **Synchronized**. The **Last Heartbeat Transmission Succeeded** and the **Last Heartbeat Transmission Failed** are indicated under **Details**.

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 might 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 from the left menu, under **Business Continuity**, click **High Availability**. Then click **Swap High Availability Roles**.

Review Database Metrics

On the **High Availability Status** 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.

Also, check the status of the BeyondInsight mirror state 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.

Set Up a Cold Spare U-Series Appliance

You can set up a spare U-Series Appliance that can be used as the primary U-Series Appliance if the primary needs to be taken offline. The cold spare appliance is not actively used by users in your environment. It's an appliance that runs in the background restoring backups from the primary appliance on a schedule.

Requirements

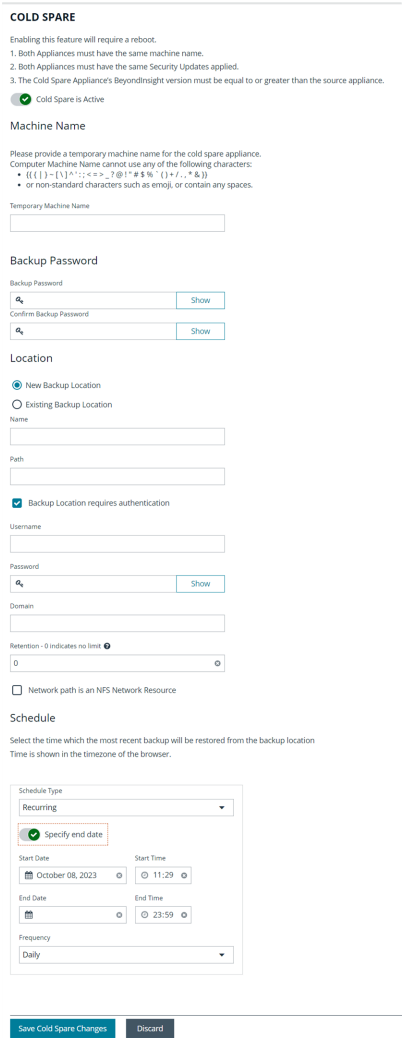
- The BeyondInsight version on the cold spare must be the same or later than the version on the source U-Series Appliance.
- We recommend that both U-Series Appliances are receiving automatic updates from BT Updater.
- The cold spare must receive updates so that it matches the source U-Series Appliance.
- 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.
- If any backup schedules are active for the appliance chosen to be the cold spare, those must be deleted before you can enable the appliance as a cold spare.

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

Configure a Cold Spare Appliance

To set up the cold spare appliance:

1. From the left menu, under **Business Continuity**, click **Cold Spare**.
2. Toggle the **Cold Spare is Active** option to enable it.
3. Enter a temporary machine name for the cold spare appliance.
4. Enter a backup password and confirm it.
5. Select the **New Backup Location** option and enter the path for the restore location where you want the backup files to be saved, and optionally provide authentication credentials. Or, select the **Existing Backup Location** option and select an existing location from the list.
6. Specify the date, time, and frequency to configure the backup schedule.
7. Click **Save Cold Spare Changes**.



Configure Backup and Restore on the U-Series Appliance

Save the U-Series Appliance configuration in case of disaster recovery or if you must 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 features set up on the U-Series Appliance.

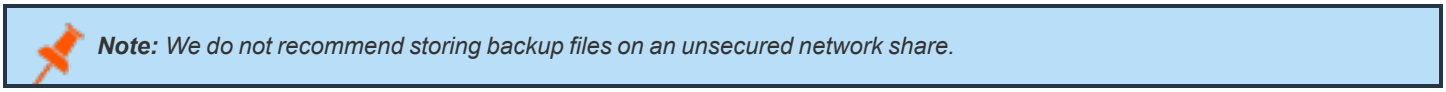
You can add multiple remote or local backup locations to use for your backups, or you can use the default local backup location already created for you in the appliance. When configuring the backup location, you can set the maximum number of backups that can be saved at that location, **0** being unlimited. The default local backup location is set to **5**. When the retention number is reached, 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.

Add a Backup Location

By default, there is one backup location already created and available for saving backups to a local path, named **LocalBackups**. You can add new backup locations, which are either local or remote network shares, as follows:

1. From the left menu, under **Business and Continuity**, click **Backup and Restore**.
2. Select the **Backup Locations** tab.
3. Click **Create New Location +**.
4. Enter a name and the local or remote path.
5. If the remote share requires credentials, check the box for that option, and enter the credentials.
6. If the remote share is an NFS share, check the box for that option.



7. 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.
8. Click **Save 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.

Schedule a Backup

1. From the left menu, under **Business Continuity**, click **Backup and Restore**.
2. Select the **Schedule a Backup** tab.
3. Click the **+** button next to **Create Backup**.
4. Select **Schedule Backup**.
5. Enter a backup password and confirm it.
6. Select an existing backup location from the dropdown or leave the default **LocalBackups** location selected.
    - Alternatively, click the **New Backup Location** option to add a new location. New backup locations are automatically added to the list on the **Backup Locations** tab.

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

7. Select a **Schedule Type** from the dropdown and set the date, time, and frequency for the schedule.
8. Select the features to include in the backup or select **All Enabled Features** to include them all.

> ***Note:*** *Features that are not enabled are not included in the backup.*

9. Click **Save Schedule**.
10. The scheduled backup is now listed in the grid on the **Schedule a Backup** tab, where you can click the vertical ellipsis for it, and select to edit it, deactivate it, or delete it.

Create a Manual Backup to Run Now

1. From the left menu, under **Business Continuity**, click **Backup and Restore**.
2. Select the **Schedule a Backup** tab.
3. Click the **+** button next to **Create Backup**.
4. Select **+ Create Backup Now**.
5. Enter a backup password and confirm it.
6. Select an existing backup location from the dropdown or leave the default **LocalBackups** location selected.
    - Alternatively, click the **New Backup Location** option to add a new location. New backup locations are automatically added to the list on the **Backup Locations** tab.

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

7. Leave the **Schedule Type** as **Immediate**.
8. Select the features to include in the backup or select **All Enabled Features** to include them all.

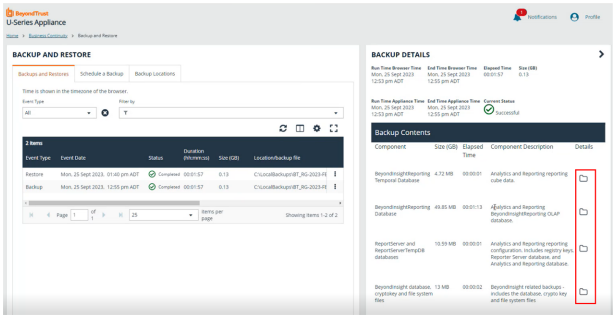
> ***Note:*** *Features that are not enabled are not included in the backup.*

9. Click **Create Backup**.

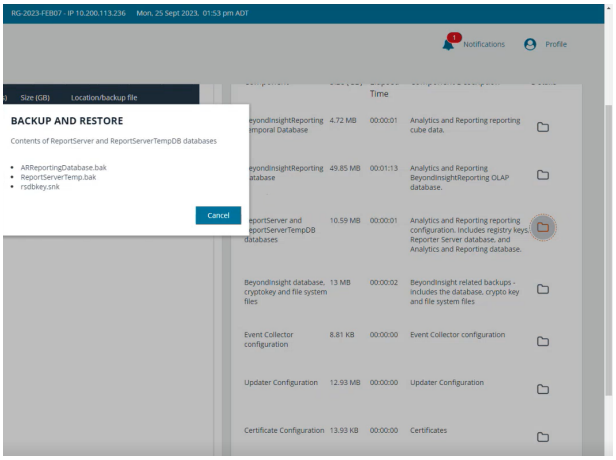
View the Details of a Backup

1. From the left menu, under **Business Continuity**, click **Backup and Restore**.
2. Select the **Backups and Restores** tab.
3. Locate the backup from the list of available backups and click the vertical ellipsis for the backup. Select **View Details**.

4. The **Backup Details** panel displays, listing all of the contents in the backup.



5. Click the folder icon in the **Details** column for an item in the list, to display a list of the specific contents for that item.



Contents of a Backup File

What is contained in a backup file:

BeyondInsightAnalytics & 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 Discovery Scanner

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

Session Archiving

- Session Monitoring files

Download a 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 left menu, under **Business Continuity**, click **Backup and Restore**.
2. Select the **Backups and Restores** tab.
3. Locate the backup from the list of available backups and click the vertical ellipsis for the backup. Select **Download**.

Delete a Backup

1. From the left menu, under **Business Continuity**, click **Backup and Restore**.
2. Select the **Backups and Restores** tab.
3. Locate the backup from the list of available backups and click the vertical ellipsis for the backup. Select **Delete**.This removes the backup from the list and also removes it from the current folder location.

IMPORTANT!

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

Restore the U-Series Appliance from a Backup

1. From the left menu, under **Business Continuity**, click **Backup and Restore**.
2. Select the **Backups and Restores** tab.
3. Search through the list of available backups and click the vertical ellipsis for the backup you wish to restore. Select **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.
4. If the browser session remains open when a restore is complete, a notification displays indicating the restore process is complete.

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.

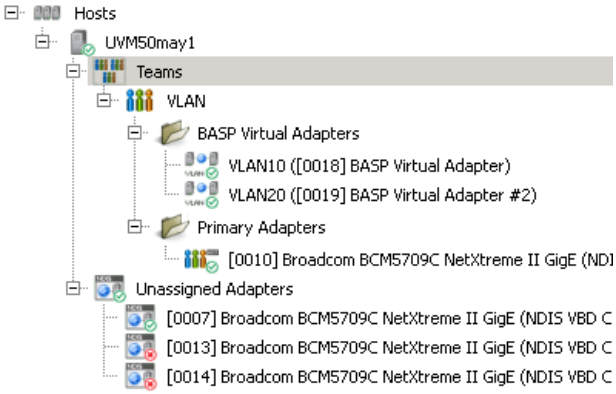
Configure VLAN

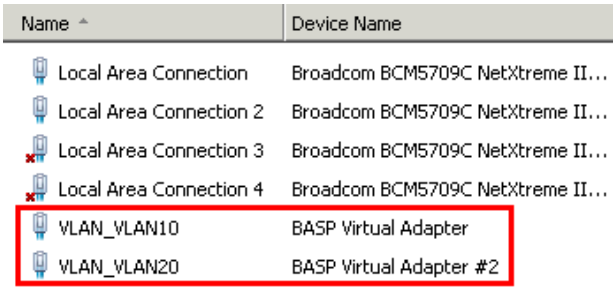
Tagged VLAN Configuration on a Physical U-Series 20 or U-Series 50

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.

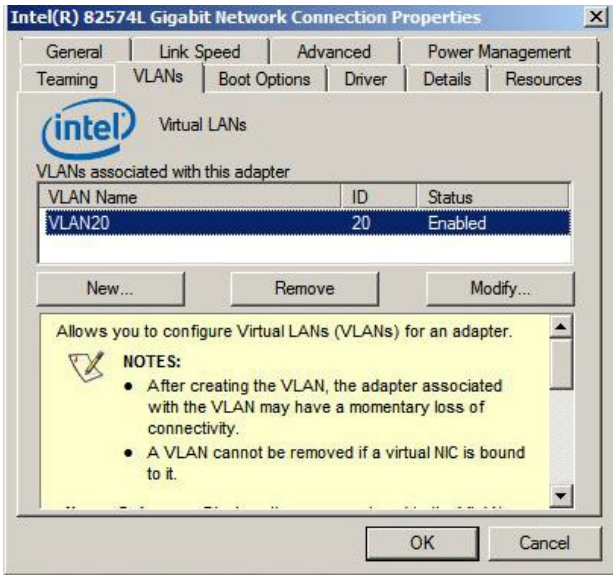




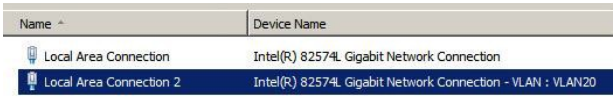
Virtual Guest Tagging (VGT) VLAN Configuration on a U-Series v20

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 While Using High Availability

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

> ***Note:*** *Each new version of U-Series Appliance Management Software might require newer versions of dependent software included in the Supporting Software packages. This typically relates to newer versions of .NET and these should be updated whenever available, but before running any appliance management software updates.*

- 2016 and 2022 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 and Restore** page 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 2016/2022
    - Security Patches for SQL 2016/2022
    - U-Series 2016/2022 Environment
    - U-Series 2016/2022 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.
    - Go to **Software and Licensing > Security Updates**.
    - Click the vertical ellipsis for the update, and then select **+ Schedule Security Udate**.
    - 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. Go 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

Note: *Each new version of U-Series Appliance Management Software might require newer versions of dependent software included in the Supporting Software packages. This typically relates to newer versions of .NET and these should be updated whenever available, but before running any appliance management software updates.*

- 2016 and 2022 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 and Restore** page 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 2016/2022
    - Security Patches for SQL 2016/2022 (may not be subscribed if SQL Server is not installed)
    - U-Series 2016/2022 Environment
    - U-Series 2016/2022 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:
    - Go to **Software and Licensing > Security Updates**.
    - Click the vertical ellipsis for the update, and then select **+ Schedule Security Udate**.
    - 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. Go 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.