BeyondTrust

BeyondTrust Updater Enterprise User Guide 2.7

 TC:4/24/2019

Table of Contents

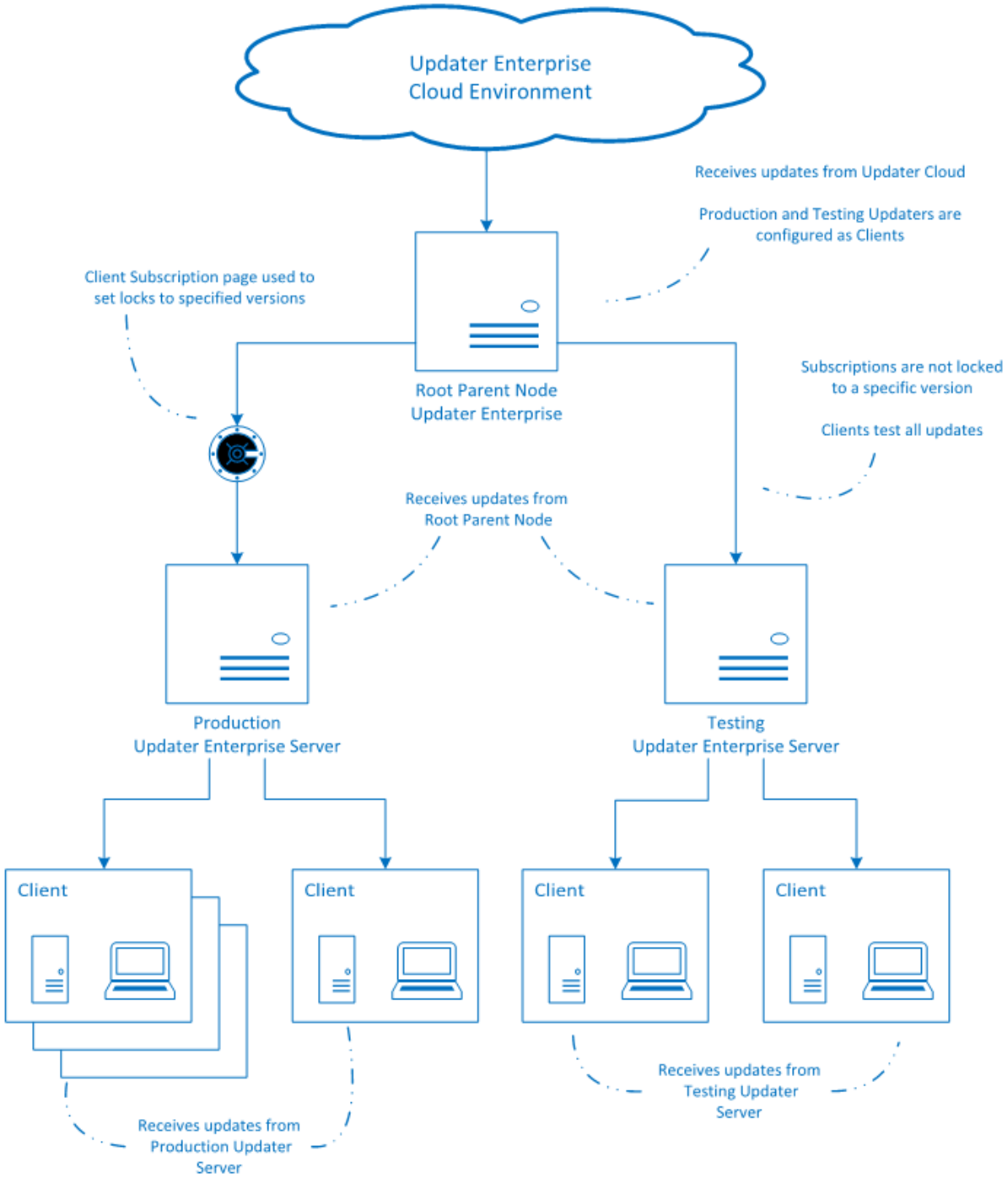
Best Practices for Deploying Updater Enterprise

BeyondTrust recommends the following configuration to deploy BeyondTrust Updater Enterprise in your environment.

We recommend you designate a server as the root parent node (top-level Updater server) with Updater Enterprise installed and configured to receive updates from the BeyondTrust cloud environment. You should then configure two Updater servers to receive updates from the root parent node. One server will be designated as the **Testing Updater Server** and the other as the **Production Updater Server**. You can then set client subscriptions for the production server and the testing server using the **Client Subscriptions** page in Updater on the root parent node.

The client subscriptions for the testing server and all clients configured to receive updates from it would not be locked to specific product versions, as the clients will be used for testing updates. The client subscriptions for the production server and all clients configured to received updates from it would be locked to specific product versions that have been successfully tested on the testing clients. As updates are tested successfully, you should reset the client subscription locks for the production clients to match the versions that were tested.

Please see the following diagram for a visual representation of the recommended configuration.



Install BeyondTrust Updater Enterprise

Introduction

BeyondTrust Updater Enterprise is an application that downloads and installs updates for BeyondTrust products and includes the following features:

- View the currently installed software version
- Set up a subscription to download product updates
- Lock the software at specified versions, when necessary

This guide provides instructions to install and configure BeyondTrust Updater Enterprise.

IMPORTANT!

Enterprise Update Server is a separate product unrelated to BeyondTrust Updater Enterprise. For more information, please see the Enterprise Update Server Installation and Configuration Guide.

Security

BeyondTrust Updater enforces the following security measures:

- productupdates.beyondtrust.com is secured by an SSL certificate.
- On download, the hash of the file and file length are verified to ensure it matches the requested download.
- After extraction of the package, the certificate on the file is checked to ensure it is a BeyondTrust certificate.
- Certificate pinning is enabled to ensure the server authority.

Requirements

Operating System	Windows Server 2008 R2 (64-bit only) – latest service pack is required Windows Server 2012 and 2012 R2 (64-bit only) Windows Server 2016
Processor	Intel Dual Core 2.0 GHz or compatible (minimum)
Memory	16 GB Minimum (Requires x64 operating system)
Hard Drive	20 GB
Server Requirements	Microsoft .NET Framework 4.5 (Application Server Role, Windows Process Activation Service Support/HTTP Activation) Microsoft Internet Information Server (IIS) 7.5 or later with ASP.Net support (Web Server (IIS) role)

Installation

IMPORTANT!

Before installing, verify that you can access the product updates landing page at https://productupdates.beyondtrust.com/landing.html.

To install Updater Enterprise, follow the below steps.

1. Open a command prompt as an administrator.
2. Run the following command:
   ```
   C:\BeyondTrustUpdaterInstaller.exe ENABLE_ENTERPRISE=1
   ```

Log Into BeyondTrust Updater Enterprise

To log into the Updater Enterprise website, follow the below steps.

1. Open a browser, and then enter the following:
   https://[FQDN]/UpdaterSettings/

> ***Note:*** *We recommend providing the Fully Qualified Domain Name (FQDN) for your Updater Enterprise server in the URL when accessing the site. FQDN is the complete domain name for the server. It includes the host name and the domain name, including the top-level domain. For example,* ***myUpdaterServer.myCompany.com****.*

2. Enter credentials for an administrator account on the server where BeyondTrust Updater Enterprise is installed.

> ***Note:*** *To create a login for BeyondTrust Updater Enterprise, you must log in with a Windows user account that is a member of the local machine's* ***Administrator*** *group. This creates an account in Updater Enterprise with the same user name and password. We recommend that you change the password after you log in for the first time. The password change propagates to all Updater Enterprise clients.*

Configure Updater Enterprise Server

The Updater Enterprise server allows you to connect to an Updater server in your network to receive software updates, rather than connecting to the BeyondTrust cloud servers for updates. Using BeyondTrust Updater Enterprise allows you to configure one Updater Enterprise server as the root parent node (top-level Updater server) that connects to the cloud and all other servers connecting to Updater Enterprise servers in your network.

> For more information, please see Best Practices for Deploying Updater Enterprise.

Updater Enterprise allows you to control updates distributed across your environment and the global settings applied to all clients using policy.

To access the **Settings** page, follow the below steps.

1. Log into the BeyondTrust Updater Enterprise website.
2. Select **Settings** from the menu.

From the **Settings** page, you can configure the following:

- Subscription frequency (interval for checking for updates)
- Specify an Updater Enterprise server and a proxy server
- Set download throttling and speed
- Set a schedule for downloading and publishing updates
- Clear cached download files
- Change the password for your administrative account
- Set the session timeout value
- Set up notifications to get notified by email when new downloads are available
- Configure Air-Gapped Mode

Set an Interval to Check for Updates

To set an interval to check for updates, follow the below steps.

1. In the **Subscription Frequency** section, click the slider to enable automatic checking for updates.
2. Set your desired check interval frequency.
3. Click **Apply Changes**.

Set the Connection for Updater Enterprise Server and Proxy Server

Configure an Updater Enterprise server and a proxy server in the **Connection** section.

1. Enter the server name or IP address for **Updater Enterprise** in your network.

> ***Note:*** *If an Updater Enterprise server is not specified, or has been deleted, Updater connects to the BeyondTrust cloud server for updates.*
>
> *Once an Updater Enterprise server has been entered, the* ***Subscription Frequency*** *settings are disabled as this instance of Updater now checks for updates every 30 minutes from the Updater Enterprise provided. Air-Gapped Mode is also disabled.*

2. Click the slider to enable **Use secure connection**.
3. Enter the **Address**, **Port**, **Username**, and **Password** for your proxy server.
4. Click **Test Connection** to verify connectivity.
5. Click **Apply Changes** to save the settings.

Set Throttling and Speed for Downloads

Configure throttling and download rates to mitigate bandwidth usage concerns in the **Download Settings** section.

1. Enter the maximum number of kilobytes (KB) that can be downloaded in a day for **Throttle**.
2. Enter the number of KB per second that can downloaded for **Rate**.
3. Click **Apply Changes**.

Schedule Download and Installation Times for Updates

Specify days and time frames for update downloads and installations in the **Schedule** section.

1. Select the check boxes for the days you would like updates to be downloaded.
2. Select times in the **From** and **To** lists to specify a time frame for downloads to be updated from the server.
3. Select the check boxes for the days you would like updates to be published.
4. Select times in the **From** and **To** lists to specify a time frame for downloads to be published.
5. Click the slider to enable the **Allow machine to reboot when required** setting. If a restart is required, enabling this setting will mean the computer is restarted after an update has been installed.

> ***Note:*** *If this setting is disabled, a message is displayed after the update is installed indicating a restart is required. You must be logged in to receive the message.*

6. Click **Apply Changes**.

Clear Cached Downloads

Downloaded packages are cached and stored locally. This occupies disk space over time. Clear the data periodically to remove outdated packages from the system in the **Clear Cache** section.

1. Enter the number of days to keep stored packages.
2. Click **Clear Cache**.
3. Click **Apply Changes**.

Change Your Password

You can change the password for your login account in the **Change Password** section.

1. Enter your **Current Password**.
2. Enter your **New Password** following the specified password requirements.
3. Enter your new password again to **Confirm New Password**.
4. Click **Change Password**.

Set the Session Timeout

You can set a timeout value for each Updater Enterprise session in the **Session Timeout** section.

1. Enter the number of minutes for **Timeout**.
2. Click **Apply Changes**.

Set Up Email Notifications

Configure SMTP settings to send email notifications to specified email addresses when new packages are available for download. Configure the **Email Notifications / SMTP Settings** section.

1. Enter the **Host** name or IP address for your SMTP server.
2. Enter **Port** number, if applicable.
3. Click the slider to enable **Use secure connection**.
4. Enter **Username**, **Password**, and **From Display Name** as required. These fields are optional.
5. Enter **From Email Address**.
6. Enter **To Email Addresses**.
7. Click **Send Test Email** to verify the email configuration works as expected.
8. Click **Apply Changes** to save settings.

Use Air-Gapped Mode

To enable Air-Gapped Mode, click the **Air-Gapped Mode** slider and then click **Apply Changes**. When enabled, this feature tells Updater to not communicate to an external Updater server. Updater instead checks the local cache for available updates and install packages that were loaded using the offline tool.

Create an Offline Package

Use the following steps to create offline packages.

1. On a computer that contains the latest updates, navigate to the folder **\Program Files (x86)\BeyondTrust\Updater\Service**.
2. Double-click the **OfflineTool.exe** file.
3. Click **Create Offline Package**.
4. Click **Quick Select**.
5. Select your subscriptions from the list, and then click **OK**.

6. By default, the latest package is selected in each subscription. If needed, you can select the check box for any other installs that you want to include in the package.
7. Click **Download Selected**.
8. Confirm the packages that you want to include, and then click **Create Offline Package**.
9. Name the .opkg file and save it to a desired location. The default location is the **Desktop**.
10. Copy the .opkg file to computers that require the updates but are not connected to the internet.

Load an Offline Package

Updater Enterprise must be installed on computers that are not connected to the internet. The packages can be uploaded using the **OfflineTool.exe** tool.

1. Navigate to the folder **\Program Files (x86)\BeyondTrust\Updater\Service** and double-click the **OfflineTool.exe** file.
2. Click **Load Offline Package**.
3. Locate and select your offline package (.opkg) file, and then click **Open**.
4. Click **OK** on the **Completed Successfully** message box.
5. On the Updater Enterprise **Subscriptions** page, click **Update Now**.

Note: *You can confirm packages were successfully updated on the* ***Activity Feed*** *page.*

IMPORTANT!

If you selected an older package version in the ***Create Offline Package*** *dialog box, then this package might not be applied. Most subscriptions look for the latest package.*

An outdated package is skipped. Some subscriptions are sequential and all the missing packages are required to apply the updates in order.

Manage Updater Enterprise Subscriptions

To access the **Subscriptions** page, follow the below steps.

1. Log into the BeyondTrust Updater Enterprise website.
2. Select **Subscriptions** from the menu.

The following features are available on the **Subscriptions** page:

- View your current and available subscriptions
- Lock your subscriptions to specific product versions
- Unlock your subscriptions
- Subscribe to new subscriptions
- View the status of downloads and installs
- Find out when BeyondTrust Updater Enterprise last checked for updates and when the next check will occur
- See if auto-update is enabled or disabled
- Manually check for updates now

You are automatically subscribed to products that are installed on the same system where BeyondTrust Updater Enterprise is installed. BeyondTrust Updater Enterprise is licensed as part of your products.

You are automatically subscribed to the BeyondTrust Updater subscription. By default, Updater Enterprise checks for updates every 12 hours, and if a schedule isn't defined for downloads, updates can be pushed at any time.

***Note:** The update process will close the application. If desired, you can disable automatic checking for updates on the **Settings** page and manually update at any time by clicking **Update Now** on the **Subscriptions** page.*

To enable or disable automatic checking for updates, follow the below steps.

1. Select **Settings** from the menu.
2. In the **Subscription Frequency** section, click the slider to enable or disable **Automatically check for updates**.
3. If you are enabling automatic checking, set your desired **Check Internal** time and **Interval** setting.
4. Click **Apply Changes**.

***Note:** The subscriptions managed on the **Subscriptions** page only apply to the system where BeyondTrust Updater Enterprise is installed. Each installation of BeyondTrust Updater Enterprise has its own database.*

For more information, please see Manage Updater Enterprise Client Subscriptions to manage subscriptions for clients connected to and receiving updates from BeyondTrust Updater Enterprise.

Use the Current Subscriptions List

Subscriptions are versioned packages that can be delivered to systems connected through BeyondTrust Updater. The **Current Subscriptions** list shows all subscriptions that you are currently subscribed to, the version that has been delivered, and the version

that is available for download. You can also search for current subscriptions using keywords in the **Search current subscriptions** box.

The **Delivered** column shows the version that has been downloaded or installed. Applicable icons are displayed for the subscription to indicate whether the package has been downloaded successfully, installed successfully, or if the upload has failed.

The **Available** column shows the version that is available for download in the Updater cloud environment . An icon may be displayed to indicate that a newer version is available for download.

If an update fails, a red exclamation mark icon is displayed next to the subscription. You can retry the update as follows:

1. Click the **More Options** icon (vertical ellipsis) for the subscription.
2. In the **Details** window, click **Retry** where it indicates there was an error with the update.

The following table lists various icons found in the **Current Subscriptions** list.

	**Manual Install:** Indicates the product was installed or updated externally from Updater. The manually installed version is displayed.
	**Installed Successfully:** Indicates a subscription update has been successfully installed.
	**Update Failed:** Indicates a subscription update has failed installation. You can retry the update by clicking **More Options** (vertical ellipsis) for the subscription, and clicking **Retry** where it indicates there was an error with the update.
	**Downloaded Successfully:** Indicates an update has been downloaded successfully. Some subscription updates are download only and must be manually installed externally from Updater. When the subscription is selected, instructions for installation are provided in the **Details** pane.
	**Newer Version Available:** Indicates a newer version is available for the subscription, but not currently installed. This will be updated at scheduled settings or manually installed by clicking **Update Now**.

Note: *You can also review the log files to assist with troubleshooting any update failures. The log files are located in* ***C:\ProgramData\BeyondTrust\Updater\Logs****.*

Lock and Unlock a Subscription Version

You can lock your subscription at a particular version of the product so packages for the subscription are not downloaded. You might consider locking subscriptions for your production environment until you test the packages in your test environment. Locking a subscription also prevents the update from being downloaded. Once you have chosen a version to lock, that version will be installed according to scheduled settings or by clicking **Update Now** to install the downloaded version immediately.

IMPORTANT!

Once a version has been locked for BeyondInsight and Password Safe subscriptions, you commit to install the update at scheduled settings. ***You are required to manually update to the same lock version on all instances of Updater Enterprise or it could result in a loss of service****. Best practice is to click* ***Update Now*** *once an update has been downloaded and then manually update all instances of BeyondInsight and Password Safe immediately.*

To lock a subscription version, follow the below steps.

1. Under **Current Subscriptions**, click the **More Options** icon (vertical ellipsis) for the subscription, and then select **Lock**. This will lock the subscription to the current delivered version.
2. To lock a different version, select the version from the drop down list in the **Details** pane, and then click **Lock**.
3. When you are ready to download and install new updates for the subscription, click the **More Options** icon (vertical ellipsis) for the subscription, and then select **Unlock**.

Unsubscribe from a Subscription

1. In the **Current Subscriptions** list, click the **More Options** icon (vertical ellipsis) for the subscription.
2. Select **Unsubscribe** from the menu.

View Release Notes

Release notes for the current subscriptions are downloaded and available on the **Subscriptions** page. To view release notes for a subscription, follow the below steps.

1. In the **Current Subscriptions** list, click the **More Options** icon (vertical ellipsis) for the subscription.
2. Select **View release notes...** from the menu.
3. Select a version from the drop down list to view the release notes for that version.

Subscribe to a Subscription

On the **Subscriptions > Other Available Subscriptions** list, click **Subscribe**. You can also search for an available subscription by using a keyword search in the **Search available subscriptions** box.

Manage Updater Enterprise Client Subscriptions

The following features are available on the **Client Subscriptions** page:

- View client machines that are configured to receive updates from the Updater Enterprise server
- Lock subscriptions to specific versions of products
- Unlock your subscriptions
- Set throttling rates that apply when updates are uploaded to client machines
- Copy policy settings to the Updater Enterprise client machine (enabled by default)

Any changes that you apply on the **Client Subscriptions** page are reflected on the **Activity Feed** page. Client subscriptions apply to individual clients as configured on the **Client Subscriptions** page. They are unrelated to the subscriptions listed on the **Subscriptions** page, which are specific to the Updater Enterprise server itself.

Lock and Unlock Client Subscription Versions

To lock and unlock client subscription versions, follow the below steps.

1. Log into the Updater Enterprise website.
2. Select **Client Subscriptions** from the menu.
3. Select a client from the **Client** list. The subscriptions for this client are then listed under the **Subscription** list.
4. Select a subscription from the list, and then click the **More Options** (vertical ellipsis) icon.
5. Select **Lock** from the menu to lock the current delivered version.
6. To lock a different version, select the version from the drop down list in the **Details** pane, and then click **Lock**.

   Note: *Once you have locked a version, you are committing to update to that version at scheduled settings.*

7. When you are ready to download and install new updates for the subscription, click the **More Options** (vertical ellipsis) icon, and then select **Unlock** from the menu.

Client Settings

The following client setting configuration options are available:

- To set a throttling rate for uploading updates to client machines, enter the maximum KB/day in the **Upload Settings** box.
- To copy settings from the Updater Enterprise server to its clients, click the slider in the **Policy** box.

Once the **Policy** option has been enabled, the following settings are sent to Enterprise clients:

- Subscription frequency (update check interval)
- Download and publish schedule settings, including the configuration option **Allow machine to reboot when required**.
- Password changes. Changes will only be sent to the Updater Enterprise clients if the client is pointing to the root parent Updater Enterprise server.

Manage the BeyondTrust Updater Network

You can use the Updater Enterprise website to centrally manage your clients receiving subscription details from the Updater Enterprise server. The clients are set up to receive policy and subscription information from the Updater Enterprise website.

View the Network Map

The network map is a visual representation of your clients. You can see if client machines are offline and view general health statistics for a client.

1. Log into the Updater Enterprise website.
2. Select **Network** from the menu.
3. View the network map for the clients where the Updater tool is deployed.
4. Click a client node to view detailed health information.

> ***Note:*** *The link will not be enabled if no health information is available.*

5. Click **Send Analysis to Support** to send health data to a cloud server for review by BeyondTrust Technical Support. Identifiable information such as IP addresses and computer names are removed before the data is sent.

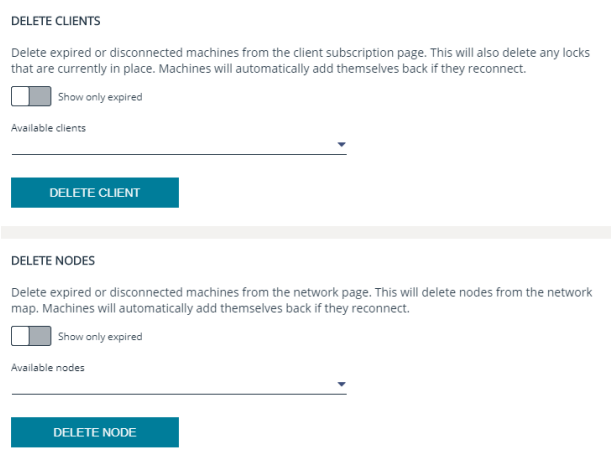
Delete Clients

Updater does not assume a client is no longer valid if it has not been online and checking for updates. If you have a client machine that no longer exists or is no longer configured to receive updates from your Updater Enterprise server, the client machine can be removed so that it no longer appears on the network map or the **Client Subscriptions** page. If the client comes back online and checks with the Updater Enterprise server for updates, it will show again as a client on the network map and **Client Subscriptions** page.

To remove a client, follow the below steps.

1. Log into the Updater Enterprise website.
2. Select **Maintenance** from the menu.
3. Toggle **Show only expired** on or off as desired to filter **Available clients**, **Available nodes**, or both.
4. To delete the client from the **Client Subscriptions** page, select the client from the list, and then click **Delete Client**.

5. To delete the client from the **Network** page, select the node from the list, and then click **Delete Node**.



Audit Activity and Log Information in Updater Enterprise

Updater Enterprise uses Windows verbose logging. Log files for Updater are located in **C:\ProgramData\BeyondTrust\Updater\Logs**.

Update activity can be audited by viewing the **Activity Feed** page. All actions performed in Updater Enterprise, including client machine actions, are logged on the **Activity Feed** page.

To access the **Activity Feed** page, follow the below steps.

1. Log into the BeyondTrust Updater Enterprise website.
2. Select **Activity Feed** from the menu.
3. Select the **Search by Term** or **Search by date** option from the **Search** filter drop down.
    - If searching by term, you can search by the subscription name or the user name. The list will automatically display filtered search results.
    - If searching by date, select your desired date range, and then click **Apply Search** to filter the list by specific dates.

You can also export the entire list of activity to a CSV file by clicking **EXPORT AS CSV** in the top right corner of the page.

Appendix A: Connection Troubleshooting

Firewall Issues

If your Updater Enterprise server is unable to connect to the Updater cloud environment, verify that your firewall isn't blocking connectivity. To verify this, you can access the product updates landing page by visiting https://productupdates.beyondtrust.com/landing.html.

Upon successful connection, you will receive a message stating you have successfully reached the service landing page. If you are unable to connect to the landing page, it is likely being blocked by your firewall.

Disable Certificate Pinning

Updater uses certificate pinning with a Windows Application Firewall (WAF) hosted in the cloud for enhanced security. In some instances, a proxy will not be able to relay the certificate correctly and may appear as a man-in-the-middle by the WAF.

To disable this feature you must set pinning to **0** in the registry.

1. Open the registry editor, and navigate to **HKLM\SOFTWARE\Wow6432Node\BeyondTrust\Updater**.
2. Add a DWORD value called **Pinned**, and set its value to **0** to turn off pinning.

Appendix B: Whitelist Incapsula IP Addresses

If you have Incapsula deployed in your network, you must whitelist Incapsula IP addresses on your web server firewall and on the firewall deployed in front of your web server. You will also need to ensure that server modules that enforce IP rate limiting are not set to Incapsula IPs.

For more information, please see Whitelist Incapsula IP addresses & Setting IP restriction rules for a list of IP address ranges that are used by Incapsula. Note that these may change from time to time. Ensure you are subscribed to Incapsula notifications regarding updates.