BeyondInsight

Analytics & Reporting 7.0

Table of Contents

BeyondInsight Analytics & Reporting

BeyondInsight contains a data warehouse solution with business intelligence and analytics. This module extracts data from the BeyondInsight database and then processes the data in Microsoft SQL Server Integration and Analysis Services. These cubes can be browsed in BeyondInsight, Microsoft SQL Server Management Studio, or using tools such as Microsoft Excel.

Using BeyondInsight, you can:

- Run reports on your vulnerability, attack, malware, Endpoint Privilege Management, or Password Safe data from the BeyondInsight management console.
- Subscribe to reports on a schedule for automatic delivery to a network file share or through email.
- Save report views to easily reuse a report with predefined parameters.
- Create report snapshots to save static views of report data.
- Interactively explore data and create and save custom reports with a Pivot Grid.
- Evaluate risk on assets using the Threat Analyzer.
- Find and examine audits using the Audit Viewer.

Report Categories

- Account
- Audit Groups
- Asset
- Attack
- Clarity
- Configuration
- Configuration Compliance
- Console Reports
- Endpoint Privilege Management
- Licensing
- Organizational
- Patch Management
- PowerBroker Password Safe
- PowerBroker Identity Services
- PowerBroker Sudo
- PowerBroker for Unix & Linux
- Regulatory Reporting
- Saved Report Views
- Scan
- Vulnerability Management

Note: *Some report categories are visible only if certain product licenses are present or if certain permissions have been set in the management console. Administrators can view all reports.*

Run Reports in BeyondInsight

> 💡 **Tip:** To view reports in BeyondInsight, you can use Internet Explorer or Edge, Safari, Firefox, or Chrome. Only Internet Explorer allows you to print results directly. In other browsers, you must first create a PDF before printing.
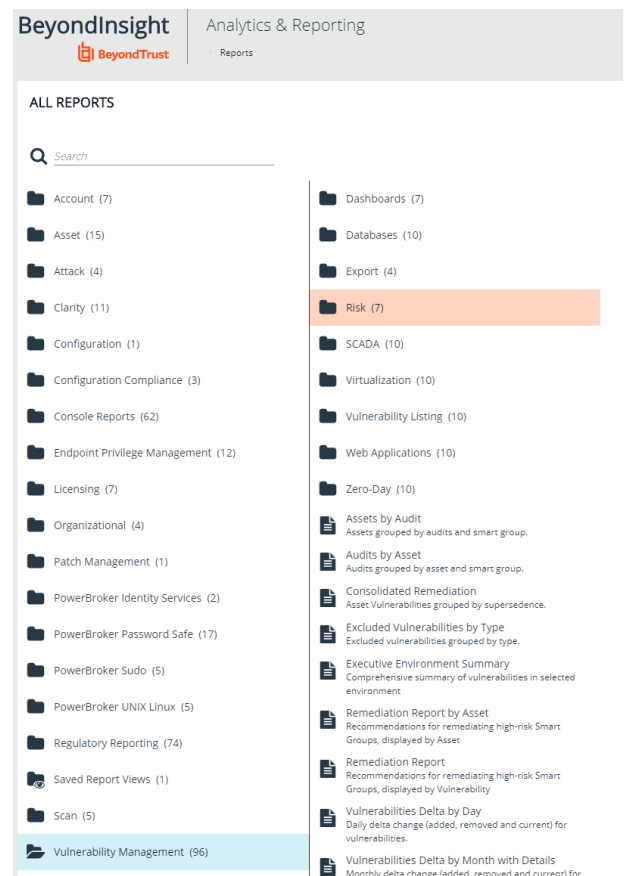
> 📌 **Note:** To make sure that all Analytics & Reporting features work properly, please set your browser's pop-up blocker to allow pop-ups from your BeyondInsight management console.

> 📌 **Note:** A drill-through action that opens a new report is limited to 10,000 rows of data by design.

1. Log into your BeyondInsight management console and click **Analytics & Reporting**.
2. Click **View All Reports**.
3. You can search to find a report based on title or description keywords.
4. Select a report from the navigation pane.

5. From the **Configure Report** pane, select the report parameters (default option).

6. Click **View Report** at the bottom of the page.

> ℹ️ After viewing the report, you can create a subscription to it by clicking the envelope button. For more information, please see "Manage Subscriptions in BeyondInsight" on page 11.

CONFIGURE REPORT ‹

| PARAMETERS | SAVED VIEWS | SUBSCRIPTIONS |

Show Cover Page (No)

Show Parameters (No)

From Date
Last 7 Days

To Date
Today

Smart Group
All

Audit Group
All

Severity
All

RELOAD REPORT

Heat Map Report Results

A heat map report groups vulnerabilities by risk. You can generate heat maps to isolate the highest-risk vulnerabilities and assets.

The following vulnerability risk reports use the heat map view:

- Risk exploitability by assets
- Risk exploitability by vulnerabilities
- Risk matrix by assets
- Risk matrix by vulnerabilities
- Risk severity by assets
- Risk severity by vulnerabilities

> 📌 *Note: Vulnerabilities associated with a configuration item (CCE) are automatically excluded from these reports.*

1. Select **Vulnerability Management > Risk**, and then select a heat map report.
2. Select the parameters.
3. Click **View Report**.
4. Click the links within the report to view more information about the vulnerabilities.

5. In this particular report example, a list of vulnerabilities is displayed. Click the **Vulnerability** link to review CVSS scores and references.
6. Click the **Asset Count** link to review a complete list of affected assets.
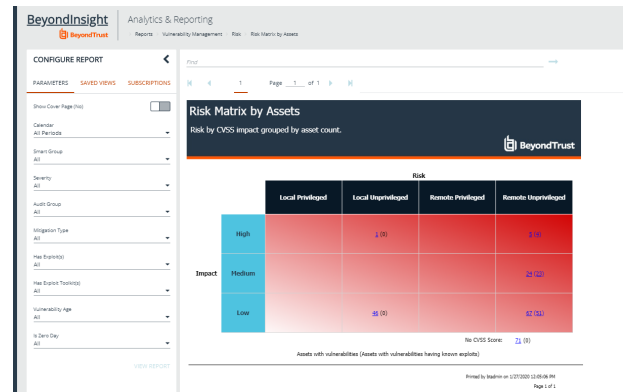
Collect Mitigation Information

BeyondInsight uses CPE data to help you determine which assets have patches available. Currently, the CPE value is derived from two sources:

- An audit of updates and patches downloaded through Auto Update.
- Asset data collected by the BeyondTrust Network Security Scanner.

> 📌 **Note:** *The management console uses only CPE values which apply to operating systems. Application CPE values are not used to evaluate vulnerabilities and related patches.*

Mitigation report filters are available for the following reports:

- Vulnerability by security patch
- Extended executive summary
- Vulnerabilities delta by month

The following mitigation parameters are available:

- **Not applicable:** No matching CPE data is available for the asset. This filter applies to vulnerabilities related to software on the asset.
- **Unknown:** No CVE information is available. A vulnerability that can be mitigated with a patch always contains CVE information. This status may also indicate that a combined patch (a patch mitigating the vulnerability for more than one platform) is available but might not apply to all platforms.

- **Incomplete:** No CPE information is available for the asset.
- **Patchable Pending Prerequisites:** Operating systems from both CPE sources match exactly, and there are prerequisites in the audits download. However, the prerequisites do not need to match exactly.
- **Patchable:** Operating systems from both CPE sources match exactly, and prerequisites for both CPE sources match exactly. This status might also occur when CPE sources match exactly but there are no prerequisites in the audits download.
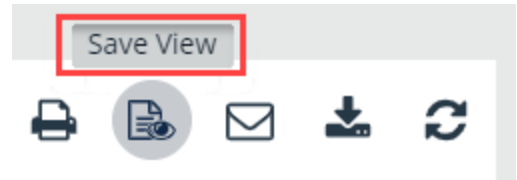
Example

In this screen shot, the **Vulnerability by Security Patch** report is shown, with the **Patchable** parameter selected. The **Patch** column in the report indicates the patch number that can be applied to the asset to remediate the vulnerability.

Save a Report View

If you generate a certain report frequently and use the same parameters, you can save those parameters in a **Saved Report View**.

1. Select the report.
2. Select the report parameters.
3. Click the **Save View** button.
4. Enter a name and description for the report view, select an **Organization** from the list, and then click **Save Report View**. The name must be unique.
5. This view is now located in the **Saved Views** panel on the **Analytics & Reporting** homepage and in the **Saved Report Views** folder on the **All Reports** page.
6. When you select the saved view, the report loads automatically with the saved parameters.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

9

Save a Report as Your Home Page
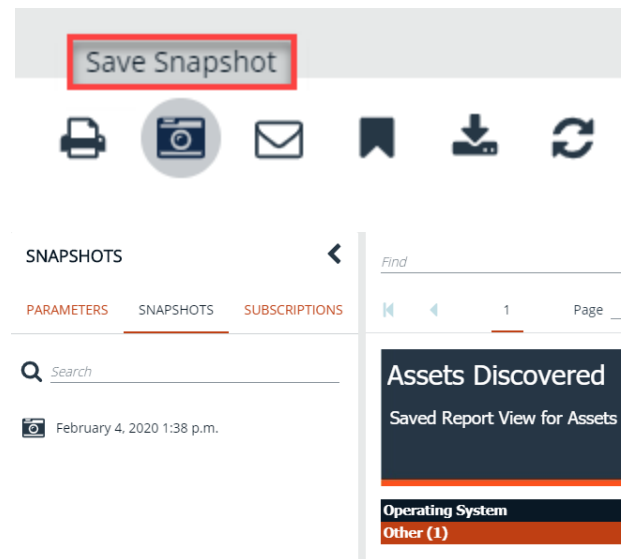
When you save a report view, you can set the report to display as your Analytics & Reporting homepage by checking the **Make this my Homepage** box.

Save a Snapshot

When you generate a report from a saved view, you can save the data in a snapshot. A snapshot is the saved report and results as they were when the snapshot was created. Time and date information is displayed with the snapshot.

1. Open a saved view either from the **Saved Views** panel of the **Analytics & Reporting** homepage or from the **Saved Report Views** folder of the **All Reports** page.
2. Once the report is displayed, click the **Save Snapshot** button.

3. From the saved report view, you can view the snapshots from the left panel.

Manage Subscriptions in BeyondInsight

In addition to running reports on demand, you can set up a subscription to the report. With a subscription, you can set a schedule to run a report and deliver the report output in an email or to a shared folder.

> 📌 *Note: SQL Server Reporting Services (SSRS) must be configured for email delivery. Use the **Reporting Services Configuration** tool to configure the SMTP server or gateway and verify that the **Report Server** Windows service account user is granted the **Send As** right.*

Create a Subscription

After generating a new report or accessing a saved report view, you can subscribe to the report.

1. Click **Menu > Analytics & Reporting > View All Reports**.
2. In the **All Reports** page select the folder that contains the report you want to subscribe to.
3. Select the report parameters and click **View Report**, or click the saved report view.
4. Once the report displays, click the **Subscribe to Report** button.
5. Select a delivery method:
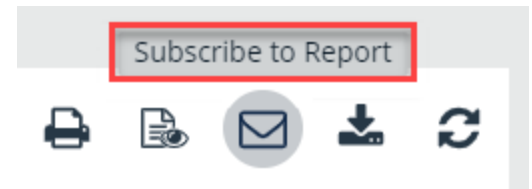
   - **Deliver the report through email:** After selecting this option, click **Next** and enter the email addresses to send the report to, along with an email subject.
   - **Deliver the report to a shared folder:** After selecting this option, click **Next** to enter the network information for the share, network credentials, report file format, and file overwrite options.

> 📌 *Note: This email option is not available if SMTP is not configured in the **Reporting Services Configuration Manager**.*

6. Click **Next**.
7. Select scheduling information.
8. Click **Complete**.

> **Note:**
> *If you have chosen to deliver the report output to a network share and the SSRS host server resides outside the domain, you must install a reporting services delivery extension file.*
>
> 1. *Install the following MSI file on the server hosting the SSRS server:*
>
>   ***C:\Program Files (x86)\eEye Digital Security\Retina CS\Support\BeyondInsight-ReportingServicesExtensionsSetup.msi***
>
> 2. *Configure* **Analytics & Reporting** *with the SSRS server that is hosted on a server that is not a member of the domain.*
>
> 3. *Create a subscription that writes to a domain network share using domain credentials. The subscription will be saved to the network share.*
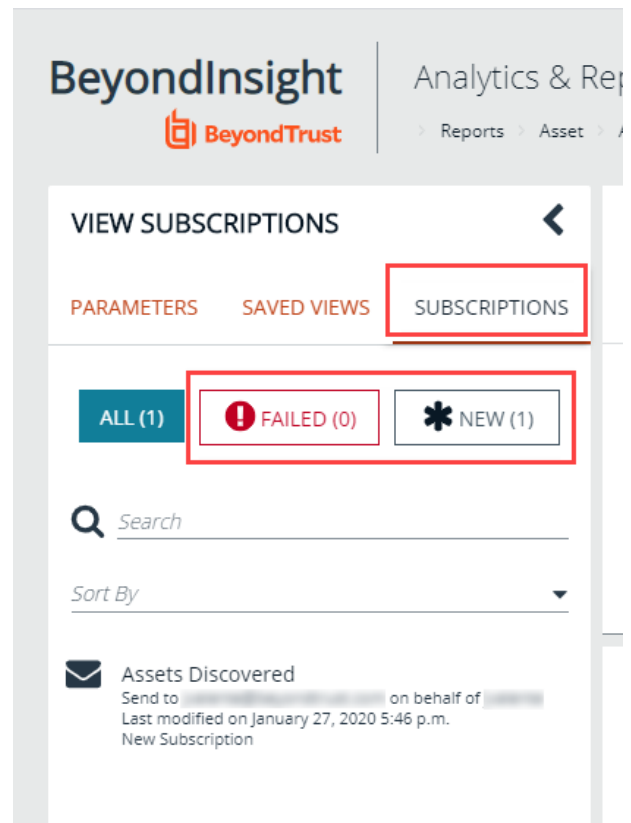
View, Edit, and Delete Subscriptions

You can view, edit, and delete subscriptions from the **Analytics & Reporting** page, from the **Configuration** page, or from the report where the subscription was created. Only subscription owners and administrators can edit or delete a subscription.

From the Analytics & Reporting Page

1. On the left side menu, click **Home**.
2. Select **Analytics & Reporting**.
3. Click **Subscriptions**.
4. By default, all subscriptions are listed. Click **Failed** or **New** to filter the subscriptions.

5. To edit a subscription:

   - Select the subscription, then click **Edit Options**. The same wizard is displayed as when you create a subscription.

   - Change the settings as needed, and then click **Save Changes**.

6. To delete a subscription, select the subscription, then click the **Delete** button.
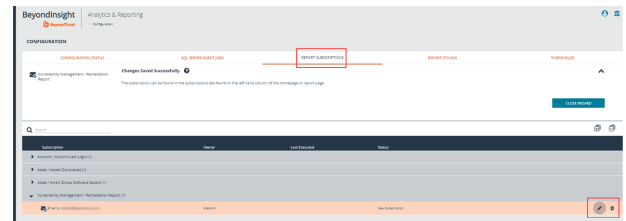
From the Configuration Page

1. On the **Configuration** page, under **Analytics & Reporting**, click **Configuration**.

2. Enter the administrative username and password to log into the **Configuration** pages.

3. Click **Report Subscriptions**.

4. To edit a subscription:

   - Click the report name or saved report view to expand its subscriptions.

   - On the subscription, click the **Edit** button. The same wizard is displayed as when you create a subscription.

   - Change the settings as needed, and then click **Save Changes**.
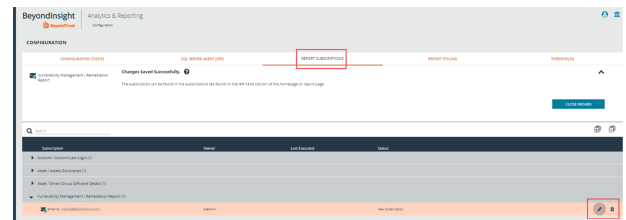
5. To delete a subscription, click the **Delete** button for the subscription.

From a Report or Saved Report View

1. Open **Analytics & Reporting** and click **View All Reports**.

2. Select the folder where the report is located, or select the **Saved Report Views** folder.

3. Select the report or saved report view.

4. Click **Subscriptions** in the left pane.

5. By default, all subscriptions are listed. Click **Failed** or **New** to filter the subscriptions.

6. To edit a subscription:

   - Select the subscription, then click **Edit Options**. The same wizard is displayed as when you create a subscription.

   - Change the settings as needed, and then click **Save Changes**.

7. To delete a subscription, select the subscription, then click the **Delete** button.

Override the Owner of a Subscription

You might need to override a subscription owner if the creator no longer has a BeyondInsight account (subscriptions tied to non-existent users will fail). You can change the owner of a subscription only if you are a BeyondInsight administrator.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

13

1. Edit the subscription you wish to take ownership of.
2. An **Override** check box displays on the first page of the subscription wizard if the administrator is not currently the owner. Check this box to set your user account as the owner of the subscription.

Edit Subscription ❓

You can subscribe to a report to allow it to be scheduled for automatic delivery. Reports can be delivered through email or posted to a shared folder on the network. You can choose from a range of rendering and scheduling options.

Report Name
Asset Item State

Owner
0nonAdmin ☐ Override

Please Choose A Report Delivery Option

🔘 Deliver the report through email
You can choose to deliver the report through email. You can specify multiple recipients, the subject line, and add an optional comment if so desired.

⚪ Deliver the report to a shared folder
This will deliver the report to a file share on the network, you can specify overwrite actions, the file name and the share path, and enter credentials for access to the share.

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

14

Work with Pivot Grids in BeyondInsight

Using pivot grids, you can interact with multidimensional data from the BeyondInsight cube and can create custom views of the data. Pivot grids use standard analytical cube features:

- **Measures:** Provide the calculated data values that you want to view.
- **Dimensions:** Provide the filters, groups, and labels for the view.

Create a Pivot Grid

Using the measures and dimensions provided, you can build comprehensive pivot grid views to analyze your data.

1. In the console, click **Menu**.
2. Under **Analytics & Reporting**, click **Pivot Grid**.
3. In the **Configure** panel under **Filters**, select a **View**, a **Cube**, and a **Measure Group**. You can perform a keyword search to find measures and attributes that contain specific words.
4. Drag and drop measures and dimensions on indicated drop zones: **Measure Fields**, **Column Fields**, and **Row Fields**.
5. Drag and drop multiple dimensions to enable more options that you can drill down through.
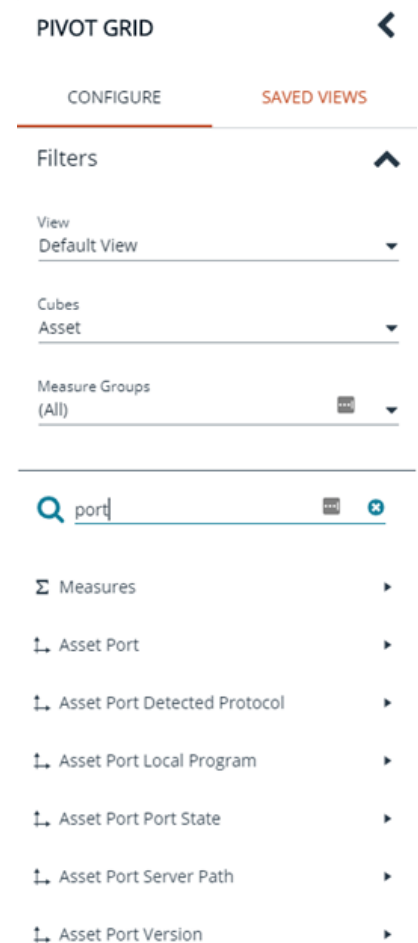
6. The available information populates the grid once the fields are selected. Use the **Expand Visible** and **Collapse All** buttons in the toolbar to show or hide all available data.
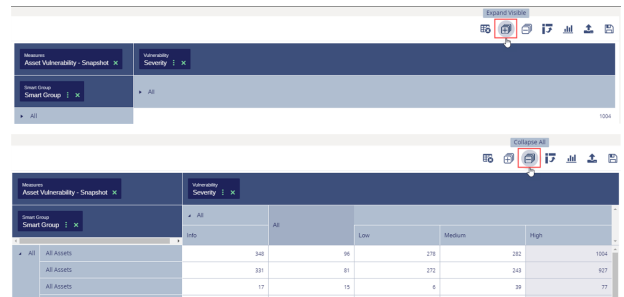
7. To completely clear the pivot grid and start over, click **Clear Pivot Grid** in the toolbar.

8. To pivot your data in the grid, click **Pivot** in the toolbar. This flips the rows to columns and the columns to rows.
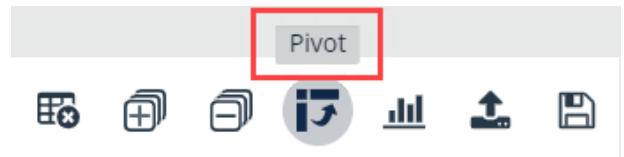
Save Pivot Grid Views

Once you have created a pivot grid, you can save your selected filters, measures, and dimensions as a view for later use.

1. In the pivot grid toolbar, click **Save > Save as View**.
2. Enter a **Name** and **Description**.
3. Select the appropriate group for **Allowed Access**.
4. Choose if other BeyondInsight users can see the saved pivot grid.
5. Click **Save As View**.

6. Your saved view is now listed under **Saved Views** in the left panel. You can also search to find views that contain the keyword.

7. Select the saved view, and then click **Display Saved View** to see the most current information for that pivot grid. The data is retrieved from the cube each time you select the saved view.

8. To delete the saved view, click the **Delete** button.
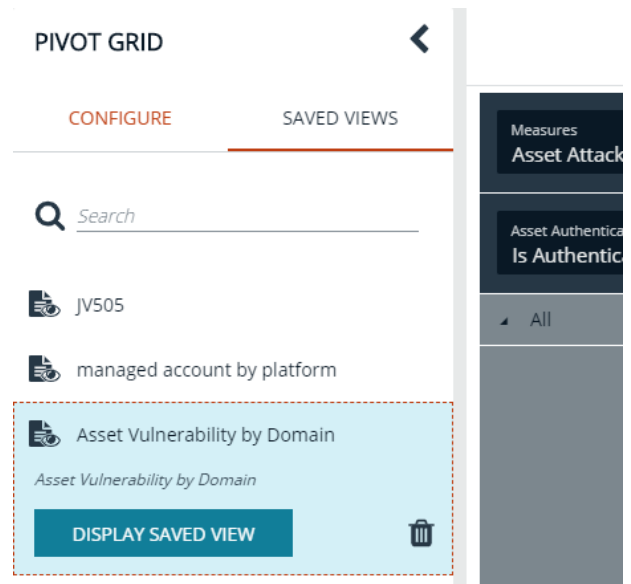
> 📌 **Note:** *You can collapse and expand the **Filters** section of the **Configure** panel using the arrow. Each time you open a saved view, the **Filters** section is either closed or open, depending on its state when it was saved.*
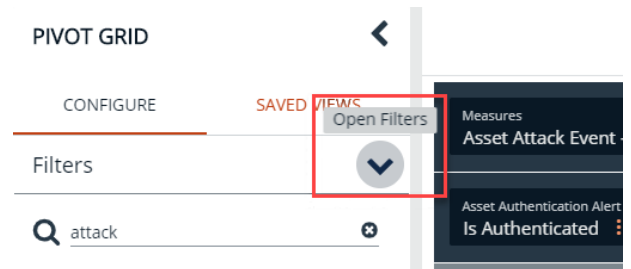
Save Data to a File

You can save the pivot grid data in JSON format and reload the data at a later time.

1. In the toolbar, click **Save > Save as JSON**.
2. The file automatically saves to your default download location.
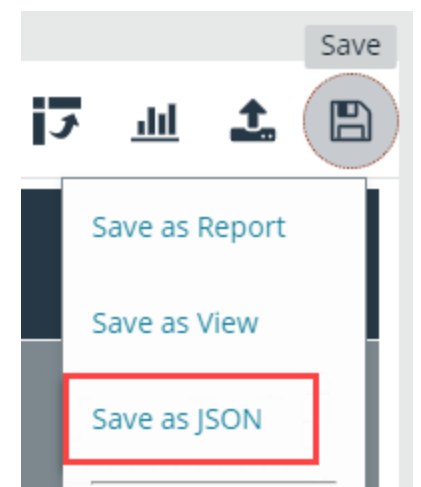
Import the JSON File

1. In the toolbar, click **Import**.

2. Locate the JSON file from the download location and drag and drop the file into the drop box. Alternatively, click in the drop box to open a file browser to navigate to the JSON file to upload it.
3. Click **Apply to Pivot Grid**.
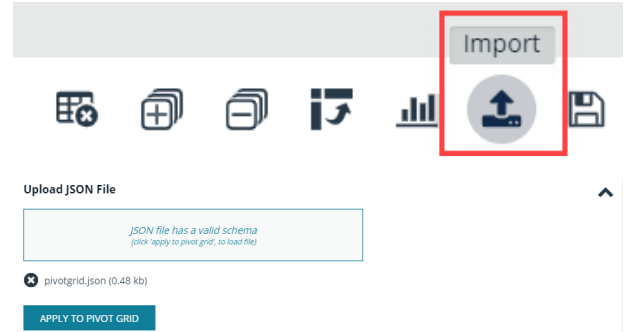
Display Data as a Chart

Once you have created a pivot grid, you can display the data as a chart.

1. To display the data as a chart, click **Display Charts** in the toolbar, and then select a chart type from the menu. The following chart types are available:

   - Area
   - Category
   - Line
   - Spline
   - Spline Area
   - Step Area
   - Step Line
   - Waterfall

2. The chart displays above the grid, showing data that is currently expanded in the pivot grid.
3. Chart series data can be enabled or disabled by clicking the corresponding data in the legend.
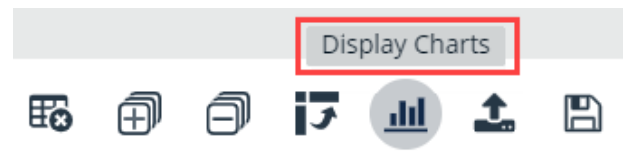
> 📌 **Note:** *If you save a pivot grid as a view while a chart is displayed, the chart will be displayed each time the saved view is loaded.*

Save a Chart as a File

You may want to save a chart without saving all of the other data in the pivot grid. Once you have displayed your pivot grid as a chart, you can save the chart as in .pdf, .png, or .svg format.

1. In the toolbar, click **Save**, and then select either **Save Chart as PDF**, **Save Chart as PNG**, or **Save Chart as SVG**.
2. The file automatically saves to your default download location.

Create a Custom Report

Once you have created a pivot grid, you can create a report based on the fields selected in the grid.

1. In the pivot grid toolbar, click **Save > Save as Report**.
2. Enter a **Name** and **Description**.
3. Select the appropriate group for **Allowed Access**.
4. Optionally, select a **Category**.
5. Click **Publish as Report**.
6. Your report is saved in the **Custom** folder on the **All Reports** page.

Publish Pivot Grid To Report ⌃

Specify a name, a category, and a description to save the pivot grid layout to a custom report.

Name
My Report

Description
My Report

No Chart will be saved with this pivot grid report.

Allowed Access
Everyone

Category
<Blank>

PUBLISH AS REPORT

Example Measures in the Vulnerabilities Cube

You can use the following table as a guide for commonly used measures in the **Vulnerabilities** cube.

To filter on…	Select this measure…
Average count of recorded attack events on assets by date range	Measures > Asset Attack Event - Average
Count over time of recorded attack events on assets	Measures > Asset Attack Event - Growth
Count of recorded attack events on assets	Measures > Asset Attack Event Count
Count of audit event instances for assets in the system	Measures > Asset Audit Event Count
Inventory (rolling count) of discovered assets	Measures > Asset Discovery - Snapshot
Inventory (rolling count) of open ports on assets. Can be used to find which ports are open on which machines	Measures > Asset Port - Snapshot
Inventory (rolling count) of services on assets	Measures > Asset Service - Snapshot
Inventory (rolling count) or shares on assets	Measures > Asset Share - Snapshot
Inventory (rolling count) of software on assets	Measures > Asset Software - Snapshot
Inventory (rolling count) of local user accounts on assets	Measures > Asset User Account - Snapshot
Count of new vulnerabilities added to assets	Measures > Asset Vulnerability - Added
The average age (in days) that a vulnerability has been open	Measures > Asset Vulnerability - Average Age
Count of unique assets that have open vulnerabilities	Measures > Asset Vulnerability - Distinct Vulnerability Count
Count of removed (fixed or not found in the defined age threshold) vulnerabilities on assets	Measures > Asset Vulnerability - Removed

To filter on…	Select this measure…
Inventory (rolling count) of open per-asset vulnerabilities	Measures > Asset Vulnerability - Snapshot

Usage Scenarios

To see the count of vulnerabilities by severity:

- In **Measure Fields**, place **Measures > Asset Vulnerability - Snapshot**.
- In **Row Fields**, place **Dimensions > Vulnerability > Severity**.

To see the count of vulnerabilities by severity, and if there is an exploit toolkit:

- In **Measure Fields**, place **Measures > Asset Vulnerability - Snapshot**.
- In **Row Fields**, place **Dimensions > Vulnerability > Severity**.
- In **Column Fields**, place **Dimensions > Vulnerability > Has Exploit Toolkit**.
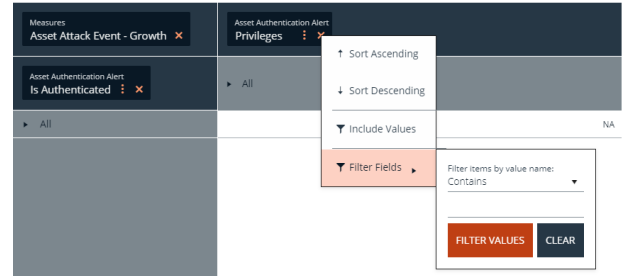
To see the count of high vulnerabilities by smart group:

- In **Measure Fields**, place **Measures > Asset Vulnerability - Snapshot**.
- In **Row Fields**, place **Dimensions > Smart Group > Smart Group**.
- In **Column Fields**, place **Dimensions > Vulnerability > Severity**.
  - Click the **More Options** button to display the menu.
  - Select **Filter Fields**.
  - Select **is equal to**.
  - Enter **high** as the value, and then click **Filter Values**.

Work with the Threat Analyzer in BeyondInsight

With the Threat Analyzer, you can perform high-level analysis on large groups of assets. This can help you decide which vulnerabilities to address first to achieve the highest risk reduction. Threat Analyzer allows you to assess risk based on assets, view audit details for assets, and learn how to mitigate the risk on assets.

Assess Risk by Smart Group

1. In the console, click **Menu**.

2. Under **Analytics & Reporting**, click **Threat Analyzer**.

3. By default, the **Smart Group Asset Score** page shows data for the **Assets and Devices Smart Group** category with **All** selected for the other parameters.

    - Each box represents data for a specific smart group based on the selected parameters.

    - The size of the box represents its relative value for those parameters, with the largest box representing assets that are at the greatest risk.

    - Scores indicate the potential for assets to be attacked. They are calculated using factors such as vulnerability, number of attacks, exposure (for example, open ports, number of users, or shares), and overall threat level.

    - You can use scores to determine which assets need the most urgent attention.

    - Hover over a box to quickly view additional information such as the number of assets in the group, the total risk on the group, and vulnerability information.

4. Select **Smart Group Vulnerability Score** and **Vulnerability Count** to view data based on those criteria. The size, color, and arrangement of the boxes change according to which page is selected.

5. Under **Configure** in the left panel, you can select new parameters, then click **Update**.
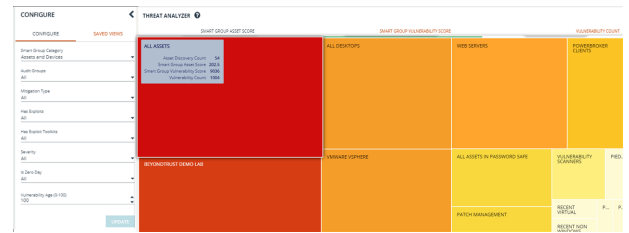
Risk Reduction Metrics and Worksheet

When you apply a recommendation for risk mitigation, the **Asset Risk** and **Vulnerability Count** metrics update in real time. Use **Risk Reduction Metrics** to view the recommended mitigation plan, and use the worksheet to mitigate threats to the assets in the selected smart group.

1. Click a box to display **Risk Reduction Metrics**.

2. To change the number of recommendations, use the up and down arrows. This affects the values for the asset risk and vulnerability count.

3. Click **Risk Reduction Worksheet**.

    - Click the **Column Chooser** button to select which columns you want to include in the worksheet.

    - To group by a column, drag and drop that column into the gray area above the columns.

    - Search within the columns using the **Search** field.

4. Click the vulnerability in the worksheet to display the **Vulnerability Details** panel.

5. Click **View Audit Details** to view an audit report.

6. Click **Save > Save Report View** to create a remediation report.
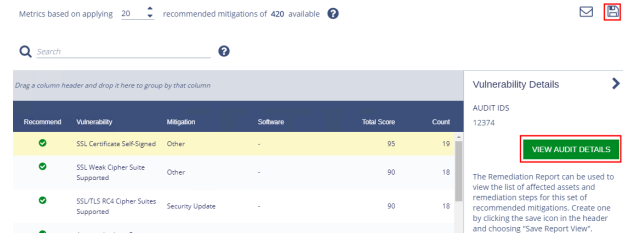
Create a Subscription

You can create a subscription based on the metrics in a risk reduction worksheet.

1. To create a subscription for a selected threat analyzer view, click the **Subscribe to Report** button.

2. A **Recommended Remediation Report** is created in SSRS, and a new node becomes available in the **Reports** navigation pane. You can view the report in the **Saved Views** folder.
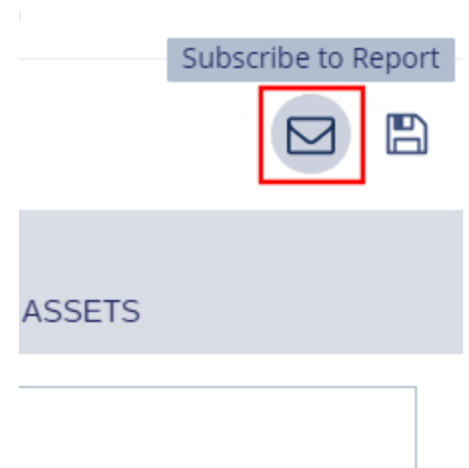
ℹ️ For more information about subscriptions, please see .

Use Audit Viewer in BeyondInsight

Set Up Permissions in BeyondInsight

To allow users to see the Audit Viewer in the BeyondInsight menu, you must set the **Audit Viewer** permission in the BeyondInsight management console.

1. In the console, click **Menu**.
2. Select **Configuration > Role Based Access > User Management**.
3. Under **Groups**, select the group you want.
4. Click **More Options** (vertical ellipse button on the right).
5. Select **View Group Details**.
6. Under **Group Details**, select **Features**.
7. Use the **Features > Show** drop down menu and select **All Features**.
8. Select the **Audit Viewer** feature.
9. Click the options button (vertical ellipse button on the right).
10. Select **Assign Permissions Full Control**.
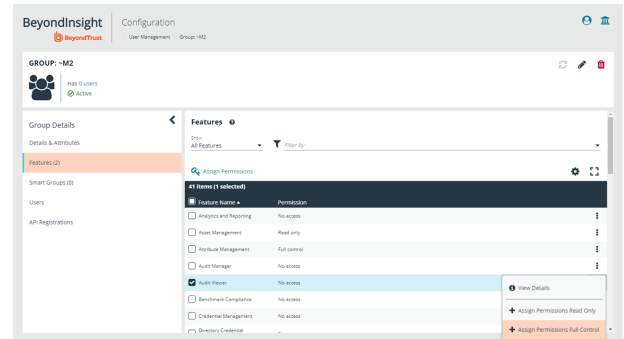
> *Tip: If you want your BeyondInsight users to see only the Audit Viewer and no other reports or tools, be sure to set only the* ***Audit Viewer*** *permission. Otherwise, you must also set the* ***Analytics & Reporting*** *permission.*

Use the Audit Viewer

You can use the Audit Viewer to track the audits downloaded from the BeyondTrust Updater Enterprise.

1. In the console, click **Menu**.
2. Under **Analytics & Reporting**, click **Audit Viewer**.
3. Select the parameters from the **Configure Report** section.
4. Click **View Report**.
5. You can sort reports by clicking the arrows in any of the report headers.
6. Click on the audit name link to drill down to more details about the vulnerability.
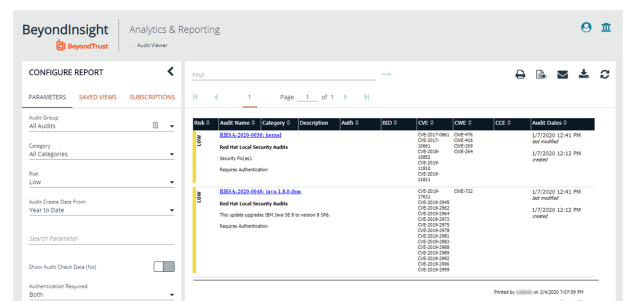
Configure BeyondInsight Analytics & Reporting

Configure Report Styles

You can customize the colors of the report, including chart colors, header and description components, and horizontal bar components. You can change the default image to your corporate logo, with a file type of .png, jpg, or .bmp. The default size is 975 x 146 pixels.

1. In the console, click **Configuration**.

2. Under **Analytics & Reporting**, click **Configuration**.

3. Enter administrative credentials.

4. Click **Report Styling**.

5. To change the report banner logo, drop an image on the box in the **Report Logo** section. You can also click inside the box to browse to your image.

6. To change **Report Colors** or **Chart Colors**, click the square you want to change, select the new color, and then click the square again.

7. You can click **Discard Changes** to reverse the most recent change.

8. Once satisfied with your color and logo changes, click **Save All Styling**.

9. To reset all changes to the default, click **Restore to Default**, then click **Reset**.
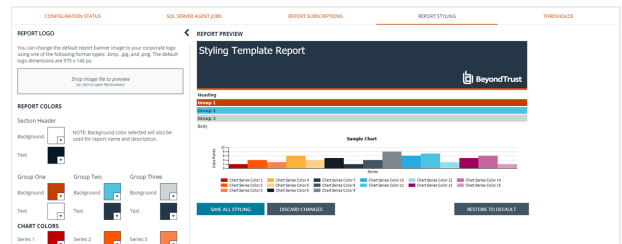
Configure Thresholds

You can configure thresholds for scorecard reports. Thresholds define the columns displayed in the report. You can configure age thresholds and vulnerability count thresholds.
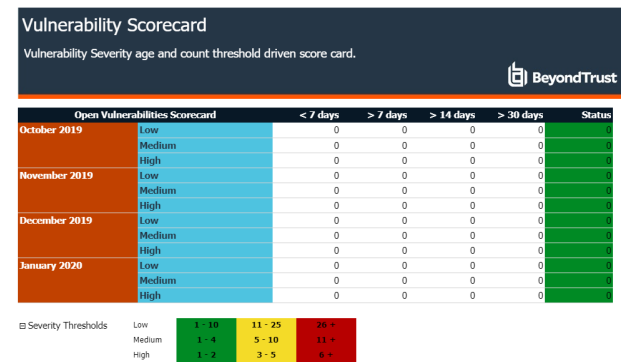
1. In the console, click **Configuration**.

2. Under **Analytics & Reporting**, click **Configuration**.

3. Enter administrative credentials.

4. Click **Thresholds**.

5. Under **Age Thresholds**, use the slides to change the age range thresholds.

6. Under **Vulnerability Count Thresholds**, select the vulnerability type from the left navigation, and then use the sliders to change the applicable thresholds for the vulnerability counts.
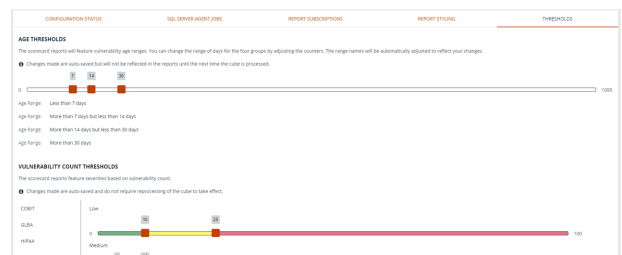
> 📌 **Note:** *Changes are automatically saved but are not reflected in the reports until the next time the cube is processed.*

SQL Server Agent Jobs

BeyondInsight uses a SQL Server agent job to retrieve data from sources and process the data into the analysis cube.

1. In the console, click **Configuration**.
2. Under **Analytics & Reporting**, click **Configuration**.
3. Enter administrative credentials.
4. Click **SQL Server Agent Jobs**.
5. Select a job type from the left navigation: **Process Daily**, **Process Full**, or **Process Full (OLAP only)**.

> 📌 **Note:** *During normal operation, you do not need to manually start the **Process Daily** job. The job is designed to run automatically each day during off-peak hours. However, the job can be started from **SQL Agent Jobs > Analytics & Reporting**.*

> ⓘ **IMPORTANT!**
>
> *Running a **Process Full** job erases all historical data and refreshes the Analytics & Reporting database with only active data from the management console. This job should not be run under normal circumstances.*

6. Review the status showing the result of the last run. Expand a job to show the job history and diagnose issues that may prevent the job from running.
7. Click **Download logs** to save diagnostic information and job history details in a .zip file.
8. Click **Refresh** to update the view.

Configure Clarity Analytics

To work with BeyondInsight Clarity, you must configure settings in the BeyondInsight management console.

Configure the Analytics Calculation

1. In the console, click **Configuration**.
2. Under **Analytics & Reporting**, click **Clarity Analytics**.
3. Enter administrative credentials.
4. From the **Analytics Calculation** section, you can:
   - Check **Enable Analytics** to turn on the feature.
   - Select the hours and minutes for **Time to run at**.
   - Select the frequency for running analysis.
   - Set the **Alert Threshold** for flagging explicit alerts. The higher the value, the higher the sensitivity and the fewer flagged alerts. The range is from 0-1. The default value is **0.65**.
   - Set the **Som Probablity Threshold** for flagging pattern alerts. The lower the value, the higher the sensitivity and the fewer flagged alerts. The range is from 0-1. The default value is **0.05**.
   - Enter an email address to send notifications to.
   - Select an **Alert malware confidence** level. Use this setting to filter on the higher potential malware risks presented in the analytics data. The default value is **Medium**.
   - Set the notification subject.
5. Click **Update Analytics Calculation Options**.
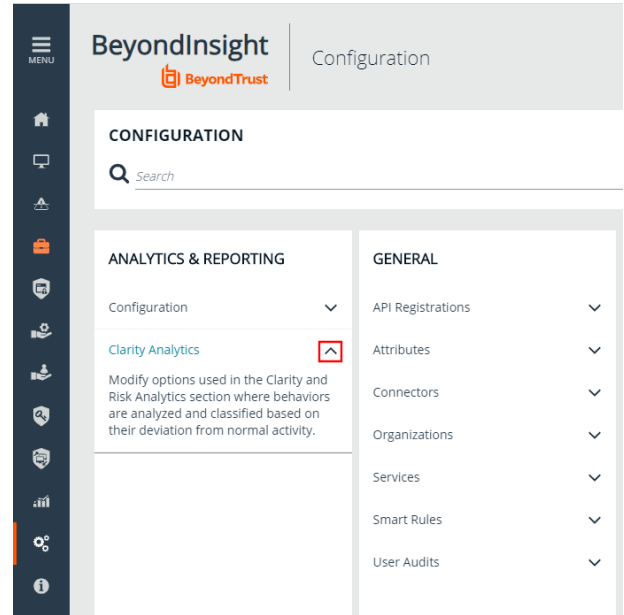
Set Alert Trigger Weighing

From the **Alert Trigger Weighing** section, you can configure Clarity to prioritize or weigh specific alerts. If an alert with a higher weight is triggered, the alert appears more pronminently in the Clarity analysis. This allows you to quickly see and react to critical alerts.

To configure a weight for an alert, click on the up and down arrows to modify its numeric value, ranging from 0 to 10. When you are satified with your selections, click **Update Alert Triggering Weighing Options** to finalize.

Configure Risk Analytics

From the **Risk Analytics** section, you can configure risk analytic options for your system assets.

1. Select the **Calculation type** from the dropdown.
2. If you wish, enable the **Nomalize** setting.
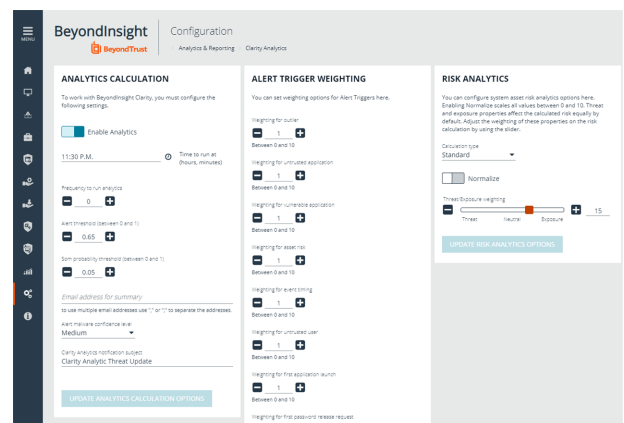
> *Note: Enabling the **Normalize** setting scales all values from 0 to 10.*

3. Slide the scale to indicate how much **Threat** and **Exposure** are weighed in the risk calculation.

> **Note:** *By default, threat and exposure are configured to be **Neutral**, which means both properties equally affect the risk calculation.*

Connect Excel to the SQL Analysis Cube in BeyondInsight

You can connect Microsoft Excel to your BeyondInsight SQL Analysis Services cube to create custom data views, build custom reports, use Excel filtering and graphing features, and use formulas to calculate custom metrics.

On the server hosting the SQL Analysis Services cube:

1. Create a local user account with the same username and password as their domain account.
2. Start SQL Management Studio, and connect to **Analysis Services**.
3. Right-click the server name in the tree and select **Properties**.
4. Click the **Security** tab.
5. Add the new local user created in the first step.

On the computer where Excel is installed:

1. Start Excel.
2. Select the **Data** tab.
3. Select **Get Data > From Other Sources > From Analysis Services**.
4. Enter the server name or IP address, making sure **Use Windows Authentication** is selected.
5. Select the **Vulnerabilities** cube.
6. Keep the default values for the remaining pages of the wizard, and then click **Finish**.
7. On the **Import Data** dialog, select to create a pivot table or a pivot chart and pivot table.
8. Click **OK**.
9. From the **Show fields related to** list, select **Asset Vulnerability**.

You can now build reports in Excel based on asset and vulnerability data.

Integrate BeyondInsight and Microsoft SharePoint

Using BeyondInsight subscriptions, you can directly integrate into SharePoint either by emailing reports to a SharePoint SMTP mail daemon or by publishing the reports to a Universal Naming Convention (UNC) share for directory-based and file-based publishing.

Begin by creating a new subscription or editing an existing subscription. Continue by choosing an email integration or a UNC share integration.
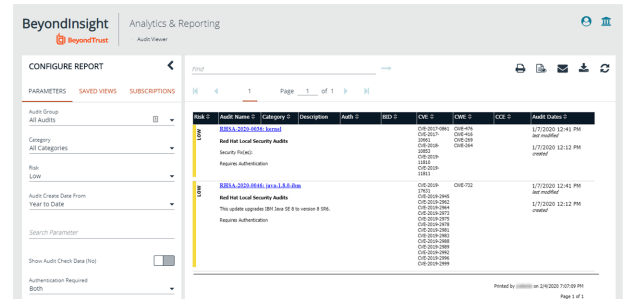
> ℹ️ For more information, please see "Manage Subscriptions in BeyondInsight" on page 11.

Email Integration to SharePoint

You can enable the receipt of SMTP email through SharePoint and set the appropriate permissions to receive .eml content. To avoid internal spam and misuse, use only security settings that permit postings from BeyondInsight or other security tools.

1. For the subscription delivery method, select **Deliver the report through email**.
2. Click **Next**.
3. In the delivery options, enter information including the SharePoint email address.
4. Click **Next**.
5. Select the recurring schedule for the report, and complete the setup.
6. The subscription generates a new report and emails it to SharePoint for publication.

UNC Share Integration to SharePoint

By default, you can access SharePoint document libraries through a UNC share, assuming the system is properly set up. An important consideration for shares is their visibility. For an additional layer of security, you may want to create shares to be hidden by suffixing the share name with a **$**.

> ℹ️ For more information, please see Connecting Web Sites to UNC Network Shares at https://docs.microsoft.com/en-us/previous-versions/tn-archive/cc768023(v=technet.10).

1. For the subscription delivery method, select **Deliver the report to a shared folder**.

2. Click **Next**.

3. In the delivery options, enter information including the report title, UNC address, file format for the report, credentials, and overwrite options.

4. Click **Test Access** to verify that files can be copied to the UNC share with the given settings.

5. Click **Next**.

6. Select the recurring schedule for the report, and complete the setup.

7. The subscription automatically writes the report to SharePoint for publication.

Report Delivery Options (Shared Folder) ❓ (1 subscription found for this report)

Specify the report delivery options, such as the file share and exporting format.

Subscription file name
Audit Viewer

☑ Add a file extension when the file is created

Network share path
\\sharepointserver01\security$\executivereports
Please enter a valid UNC path to use for delivering the report.

File format
PDF ▼

Overwrite options
Increment file names as newer versions are added ▼

Credentials Used To Access The File Share

👤 mycompany\serviceaccount

🔑 .... 🔲   TEST ACCESS

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

30